UNIVERZITET U NIŠU
ELEKTRONSKI FAKULTET

Radomir I. Prodanović

UNAPREĐENJE PROCESA DEFINISANJA ZAHTEVA ZA INFRASTRUKTURU JAVNIH KLJUČEVA

DOKTORSKA DISERTACIJA

Niš, 2022.

UNIVERZITET U NIŠU
ELEKTRONSKI FAKULTET

Radomir I. Prodanović

IMPROVING THE PROCESS OF DEFINING PUBLIC KEY INFRASTRUCTURE REQUIREMENTS

DOCTORAL DISSERTATION

Niš, 2022.

Podaci o doktorskoj disertaciji

Mentor:	Prof. dr Dejan D. Rančić, redovni profesor Univerzitet u Nišu Elektronski fakultet
Naslov:	Unapređenje procesa definisanja zahteva za infrastrukturu javnih ključeva
Rezime:	Infrastruktura javnih ključeva (Public Key Infrastructure, PKI) je složeni sistem koji zahteva posebnu pažnju u procesu identifikovanja i definisanja zahteva za sve delove sistema. Kvalitet zahteva za PKI utiče na razvoj ovog sistema kroz sve životne faze razvoja. Loše identifikovani i definisani zahtevi dovode do produženja rokova, većih finansijskih troškova, a neretko i do odustajanja od projekta. Efikasno identifikovani i definisani zahtevi su osnova za uspešan razvoj i implementaciju PKI sistema. U doktorskoj disertaciji je predložen unapređeni model za definisanje zahteva za PKI kroz sinergiju dva modela: modela za identifikovanje i definisanje zahteva zasnovanog na klasifikacionoj šemi i modela za procenu kvaliteta koji je zasnovan na rešavanju generalizovanih problema zadovoljenja fazi ograničenja. Predloženi model se može primeniti i u drugim oblastima uz odgovarajuća prilagođavanja klasifikacione šeme, izbor odgovarajućih indikatora i izbor ili izradu funkcija članica ograničenja, shodno oblasti u kojoj se model primenjuje. Primena unapređenog modela je verifikovana kroz uvođenje i dogradnje Sertifikacionog tela Ministarstva odbrane i Vojske Srbije.
Naučna oblast:	Elektrotehničko i računarsko inženjerstvo (Računarstvo i informatika)
Naučna disciplina:	Računarska tehnika
Ključne reči:	Infrastruktura javnih ključeva, PKI, inžinjering zahteva, kvalitet zahteva, klasifikaciona šema, generalizovani problem zadovoljenja fazi ograničenja, procena kvaliteta zahteva, model, indikatori zahteva, karakteristike dobrih zahteva
UDK:	004.056.55:004.41(043.3)
CERIF klasifikacija:	T-120 Sistemski inženjering, računarska tehnologija
Tip licence Kreativne zajednice:	**CC BY-NC-ND**

Data on Doctoral Dissertation

Doctoral Supervisor:	PhD Dejan D. Rančić, full professor University of Niš, Faculty of Electronic Engineering
Title:	Improving the Process of Defining Public Key Infrastructure Requirements
Abstract:	Public Key Infrastructure (PKI) is a complex system that requires special attention in the process of identifying and defining requirements for all parts of the system. The quality of PKI requirements affects the development of this system through all life stages of development. Poorly identified and defined requirements lead to extended deadlines, higher financial costs, and often to abandoning the project. Effectively identified and defined requirements are the basis for successful development and implementation of PKI systems. In this dissertation is developed an advanced model for defining requirements for PKI through the synergy of two models: a model for identifying and defining requirements based on a classification scheme and a quality assessment model based on solving Generalized Prioritized Fuzzy Constraint Satisfaction Problem. The proposed model can be applied in other areas with appropriate adjustments to the classification scheme, selection of appropriate indicators and selection or development of membership functions according to the area in which the model is applied. The application of the improved model has been verified through the introduction and upgrading of the Certification Authotity of the Ministry of Defense and the Serbian Army.
Scientific Field:	Electrical and Computer Engineering (Computer Science and Informatics)
Scientific Discipline:	Computer technology
Key Words:	Public key infrastructure, PKI, requirement engineering, quality of requirement, classification scheme, Generalized Prioritized Fuzzy Constraint Satisfaction Problem, requirement quality assessment, model, requirement indicators, characteristics of good requirement
UDC:	004.056.55:004.41(043.3)
CERIF Classification:	T-120 Systems engineering, computer technology
Creative Commons License Type:	**CC BY-NC-ND**

SADRŽAJ

1. Uvod

1.1. Predmet naučnog istraživanja

Razumevanje potreba korisnika sastavni je deo projektovanja informacionih sistema i predstavlja kritičnu tačku uspešne realizacije informacionog sistema. Životni vek informacionog sistema počinje razumevanjem zahteva korisnika. Mnoge studije su dokazale da greške napravljene u definisanju zahteva vode do projekata koji koštaju više i mogu dovesti do toga da se, u krajnjem slučaju, odbace kao neutemeljeni.

Prema proceni IAG Consulting, kompanije sa lošom praksom definisanja zahteva korisnika troše 100% više resursa po projektu nego što je predviđeno, dok kompanije koje imaju dobru praksu u definisanju zahteva potroše 21% više resursa nego što je planirano. Promene zahteva tokom realizacije projekta negativno utiču na vreme realizacije i budžet projekta, kao i na već definisane i realizovane zahteve. Česti su slučajevi da se zahtevi realizuju, a da ih kasnije korisnici ne koriste.

Greške nastale usled lošeg razotkrivanja i definisanja zahteva očigledno uzrokuju značajne probleme, što zauzvrat dovodi do propadanja malih i velikih projekata. Pored mnogih tehnika za poslovne procese, generalizovanih zahteva i tehnika za analizu zahteva, još uvek postoji problem u razotkrivanju i definisanju zahteva. To se ogleda u nedovoljnom pregledu potreba korisnika, nepostojanju sistematizacije zahteva za određenu oblast i nepostojanju jednostavne procene kvaliteta zahteva. Sistematizacija zahteva daje osnovu korisnicima i stručnim licima da efikasno razotkriju i definišu sve zahteve neophodne za izgradnju softverskog proizvoda i time smanje rizik od definisanja nepotrebnih zahteva. Procena kvaliteta zahteva je bitan korak u verifikaciji zahteva jer omogućava smanjivanje rizika od loše definisanih zahteva koji su nerazumljivi i mogu prouzrokovati grešku u razvoju projekta. Dobro definisani zahtevi direktno utiču na kvalitet softverskog proizvoda i vreme realizacije projekta.

Upravo takav problem javlja se prilikom uspostave infrastrukture javnih ključeva (Public Key Infrastructure, PKI). PKI je složeni sistem koji se sastoji od hardvera, softvera, ljudi, politika i procedura potrebnih za kreiranje, upravljanje, distribuciju, korišćenje, čuvanje i opoziv elektronskih sertifikata i upravljanje kriptografijom javnog ključa. PKI sistem treba da omogući sveobuhvatnu funkcionalnost, jednostavnu integraciju sa aplikacijama, veliki broj korisnika, svakodnevni rad, pouzdanost i autoritet. PKI stvara pouzdano okruženje za prenos informacija u

distribuiranim sistemima koju obezbeđuje zahvaljujući sledećim svojim funkcijama: autentičnosti strana u komunikaciji, integritetu poruka, neporecivosti slanja i prijema i tajnosti poruka. Ova oblast je opisana u literaturi i standardima stručnim jezikom, pa korisniku nije lako da dođe do informacija na osnovu kojih bi definisao zahteve. Isto tako, obim materijala koji je potrebno proučiti oduzima mnogo vremena razvojnom timu za shvatanje oblasti i određivanja zahteva. Ovakva neuređenost donosi veliki rizik da neki zahtevi neće biti dobro definisani ili na vreme razotkriveni, a što može imati uticaj na razvoj i uspešan završetak projekta.

Uspešna izgradnja PKI sistema ne zavisi samo od mogućnosti sagledavanja i definisanja svih neophodnih zahteva, već zavisi i od kvaliteta zahteva. Kvalitet zahteva se određuje na osnovu indikatora koji proizilaze iz karakteristika dobrih zahteva.

Složenost PKI sistema predstavlja dodatni izazov za istraživanje, razotkrivanje i definisanje svih potrebnih zahteva za PKI. Istraživanje je sprovedeno prilikom razvoja i implementacije infrastrukture javnih ključeva Ministarstva odbrane i Vojske Srbije.

Literatura, standardi i preporuke iz oblasti PKI infrastrukture, razmatraju i opisuju funkcionalnost PKI, ali ne navode eksplicitno zahteve koji treba da dovedu do implementacije PKI sistema. Uglavnom se u literaturi opisuje suštinska funkcionalnost, a ne obuhvataju se i druge oblasti ovako složenog sistema. Složenost PKI sistema uslovljava neophodnost sagledavanja širokog skupa zahteva koji su raznovrsni i iz različitih oblasti (poslovanja, organizacije, održavanja). S obzirom da literatura, propisi i preporuke nisu struktuirani tako da iz njih korisnik i projektantski tim mogu efikasno sagledati, razotkriti i definisati zahteve za implementacijom PKI, potrebno je izvršiti klasifikaciju PKI zahteva. Klasifikacija zahteva treba da obuhvati sve oblasti PKI.

Klasifikacija zahteva daje radni okvir korisnicima i stručnim licima u razotkrivanju i definisanju zahteva. Međutim, klasifikaciona šema nije jedini uslov koji obezbeđuje uspešan završetak implementacije PKI. Bitan uslov je procena kvaliteta zahteva za PKI, odnosno da li je zahtev napisan i definisan tako da ga korisnici i inženjeri mogu shvatiti. Procena kvaliteta zahteva je subjektivni osećaj evaluatora. Kako bi se umanjila subjektivnost u proceni, primenjuje se fuzzy logika u proceni kvaliteta zahteva ocenjujući kvalitet svake izabrane karakteristike zahteva. Svrha ovog istraživanja je dizajniranje klasifikacione šeme i modela za procenu kvaliteta zahteva koji omogućavaju evaluatoru i korisniku zahteva da lako i brzo definišu kvalitetan zahtev za PKI.

Predmet naučnog istraživanja u predloženoj disertaciji je analiza i mogućnost unapređenja procesa razotkrivanja i definisanja zahteva za PKI primenom klasifikacije zahteva i procene kvaliteta zahteva. Fokus istraživanja je na izradi klasifikacione šeme za PKI zahteve i modela za procenu kvaliteta zahteva primenom fuzzy logike i njihova primena u praksi.

1.2. Cilj naučnog istraživanja

Istraživanja koja su obavljena u okviru predložene doktorske disertacije obuhvataju analizu klasifikacionih šema zahteva za softverom, analizu PKI arhitektura, analizu zahteva za Sertifikaciono telo MO i VS i mogućnosti procene kvaliteta zahteva.

Fokus istraživanja u ovoj doktorskoj disertaciji je bio na razvoju klasifikacione šeme zahteva za PKI i mogućoj primeni fuzzy logike za procenu kvaliteta zahteva. Za procenu kvaliteta zahteva koji najbolje zadovoljava data ograničenja kvaliteta zahteva primenjenje generalizovani problem zadovoljenja faza ograničenja sa prioritetima (Generalized Prioritized Fuzzy Constraint Satisfaction Problem, GPFCSP).

Akcenat je bio na analizi klasifikacionih šema i PKI, kao i na izradi klasifikacione šeme PKI zahteva. Osim navedenog, akcenat se stavlja i na izradu modela za procenu kvaliteta zahteva za PKI, a koji će se moći koristiti i za procenu kvaliteta zahteva drugih softverskih proizvoda.
Cilj istraživanja je razvijanje klasifikacije zahteva za PKI kako bi se na sistematičan način moglo pristupiti bržem i lakšem razotkrivanju i definisanju zahteva i time omogućiti potrebne i jasne zahteve za razvoj celokupnog PKI sistema. Nakon što se razvije klasifikaciona šema, cilj je bio da se razvije model koji će omogućiti procenu ispunjenosti traženog kvaliteta zahteva pre nego što se otpočne sa implementacijom zahteva, a kako bi se sprečilo propadanje implementacije PKI zbog loše i nepotpuno definisanih zahteva.

1.3. Očekivani rezultati naučnog istraživanja

Kao rezultat istraživanja očekuje se sledeće:

- klasifikaciona šema zahteva za PKI koja obezbeđuje konzistentan način klasifikovanja zahteva za PKI, brzo i jednostavno razotkrivanje PKI zahteva, a koju će moći koristiti organizacije koje imaju nameru da uvedu PKI u svoje poslovanje, kao i organizacije koje se bave razvojem i implementacijom PKI;
- usmerenja za razotkrivanje i definisanje PKI zahteva;

- sistematizacija postojećih PKI arhitektura i sprovođenje komparativne analize čiji bi rezultati pomogli u izboru najpovoljnije PKI arhitekture kao nosioca bezbednosti informacija u distribuiranim sistemima;
- razvoj modela za procenu kvaliteta zahteva zasnovan na rešavanju generalizovanog problema zadovoljenja fuzzi ograničenja sa prioritetima i dobrim karakteristikama zahteva;
- identifikacija, sistematizacija i kritička analiza postojećih klasifikacionih šema zahteva, PKI arhitektura i metoda za procenu kvaliteta zahteva;
- proširenje nivoa naučnih saznanja u pogledu inženjeringa zahteva.

Praktična primena rezultata doktorske disertacije je prikazana kroz proces nadogradnje Sertifikacionog tela MO i VS.

1.4. Primenjene naučne metode

U cilju izrade predložene doktorske disertacije korišćene su različite istraživačke metode koje treba da omoguće ispunjavanje zadatih ciljeva. Prikupljanje i sređivanje podataka o dostupnim relevantnim rešenjima na osnovu literature, Internet resursa, razmene informacija sa relevantnim subjektima u oblasti PKI, klasifikacionih šema i taksonomije zahteva.

Analitičko-sintetička metoda korišćena je za analizu podataka iz stručne literature i podataka prikupljenih u procesu razvoja infrastrukture javnih ključeva MO i VS. Takođe, izvršena je analiza PKI arhitektura, analiza klasifikacionih šema i taksonomije zahteva za softverom, analiza procesa identifikovanja i definisanja zahteva, kao i mogućnosti procene kvaliteta zahteva. Sintezom je izvršeno shvatanje procesa izbora PKI arhitekture, složenost zahteva i procena kvaliteta zahteva.

Metoda posmatranja je omogućila da se iz realnog sistema prikupi dovoljan broj podataka neophodan za analizu PKI zahteva postojeće PKI MO i VS. Korišćeni su i induktivni i deduktivni metod, kao osnovni logički metodi koji u toku istraživanja omogućavaju da se izvedu određeni zahtevi iz predmeta istraživanja.

Komparativna metoda je omogućila da se sagledaju prednosti i nedostaci do kojih se došlo u toku istraživanja. Takođe je korišćena i metoda modelovanja kao sistemski istraživački postupak pomoću koga je izrađen model za procenu kvaliteta zahteva za potrebe unapređenja definisanja zahteva.

Na krajuje korišćen i eksperimentalni metod kako bi se proverila klasifikaciona šema i metodologija za procenu kvaliteta zahteva prilikom nadogradnje Sertifikacionog tela MO i VS.

2. Infrastruktura javnih ključeva

2.1. Uvod u PKI

Brzi razvoj elektronskog poslovanja i globalne komunikacije uslovio je da bezbednost elektronskih transakcija dobije na značaju. Da bi se u potpunosti iskoristile prednosti Interneta i drugih računarskih mreža, kao i da bi se omogućio kontinuirani rast elektronskog poslovanja, potrebno je obezbediti pouzdane metode autentikacije, integriteta, poverljivosti, kontrole pristupa i neporecivosti.

Danas PKI predstavlja veliki potencijal koji može da omogući upotrebu navedenih metoda. To se postiže primenom elektronskog potpisa i šifrovanja zasnovanog na PKI. U principu, PKI predstavlja čvrstu tehničku i pravnu osnovu za sigurno elektronsko poslovanje i komunikacije.

PKI predstavlja skup entiteta, hardvera i softvera, pojedinaca koji učestvuje u sistemu, procesa, tehnologija, zapisa, politika i sporazuma koji omogućavaju korisnicima da koriste tehnologiju javnog ključa.

Uobičajeni entiteti koji učestvuju u PKI su [1, 2]:

Sertifikaciono telo (Certification Authority, CA). CA je entitet koji izvršava funkcije PKI sistema, kao što su: izdavanje sertifikata, održavanje informacija o statusima sertifikata i izdavanje liste opozvanih setifikata, objavljivanje aktivnih sertifikata i liste opozvanih sertifikata i održavanje arhive informacija o statusu izdatih sertifikata. CA izdaje elektronski sertifikat kojim garantuje vezu između javnog ključa i identiteta određenog subjekta, a za potrebe zaštićene razmene podataka u elektronskom poslovanju i komunikaciji između subjekata. CA vodi evidenciju o statusu svakog izdatog sertifikata kroz tekuću bazu ili arhivu. CA smešta sve sertifkate koji su u statusu "opozvan" u posebnu listu (lista opozvanih sertifikata, CRL) koju potpisuje svojim privatnim ključem. CA preko servisa za publikovanje informacija objavljuje tekuće sertifikate i listu opozvanih sertifikata.

Registraciono telo (Registration Authority, RA). Registraciono telo je poverljivi predstavnik CA odgovoran za autentikaciju identiteta podnosioca zahteva za sertifikat javnog ključa, određivanje atributa sertifikata, iniciranje opoziva sertifikata, kao i za odobravanje ili odbijanje zahteva za

obnovu sertifikata. RA proverava informacije podnosilaca zahteva za sertifikat i prosleđuje sertifikcionom telu zahtev za izdavanje sertifikata.

PKI repozitorijum (PKI Repository). PKI repozitorijum omogućava publikovanje, čuvanje i pristup sertifikatima i drugim PKI značajnim informacijama, kao i upravljanje nastalim promenama sertifikata. Sadrži informacije povezane sa digitalnim sertifiktima izdatim od strane CA. Svakom digitalnom sertifikatu, CA dodeljuje jedinstveni broj koji se čuva u repozitorijumu. Repozitorijum sadrži informacije o statusu digitalnih sertifikata koji može biti aktivan, opozvan ili suspendovan.

Arhiva. Arhiva omogućuje dugoročno čuvanje arhivskih informacije u ime CA i ima mehanizam kojim potvrđuje da je informacija bila dobra u vreme kada je primljena i da posle toga nije izmenjena. Arhiva štiti informacije nizom tehničkih mehanizama i odgovarajućim procedurama kako bi se obezbedila njihova zaštita.

PKI korisnici. PKI korisnici su organizacije ili pojedinci koji koriste PKI, ali ne izdaju sertifikte. Oni koriste komponente PKI za dobijnje sertifikata i proveru sertifikata drugih subjekata sa kojima posluju.

Politika sertifikacije (Certification Policy, CP). Politika sertifikacije propisuje opšte uslove koje PKI učesnici moraju ispuniti da bi radili u okviru PKI. CP najčešće opisuje koristi od sertifikata koji se izdaju i kategorije pojedinaca i organizacija koji mogu učestvovati u PKI.

Praktična pravila rada (Certification practice statements, CPS). CPS opisuje pravila i procedure rada koje primenjuje jedan ili više CA. Obuhvata ista poglavlja kao i CP, ali ih detaljno razrađuje kako bi se korisnik upoznao sa opisanim procedurama i primenjenim bezbednosnim mehanizmim i na taj način stekao poverenje u usluge CA.

Primarna funkcija PKI je da omogući distribuciju i upotrebu javnih ključeva i sertifikata za ostvarivanje ciljeva bezbednosti, kao što su: poverljivost, integritet, autentikacija, kontrola pristupa i neporecivost. Sistemi koji najčešće primenjuju bezbednosne mehanizame zasnovane na PKI su elektronska pošta, aplikacije koje koriste smart kartice, elektronsko bankarstvo i elektronski poštanski sistemi.

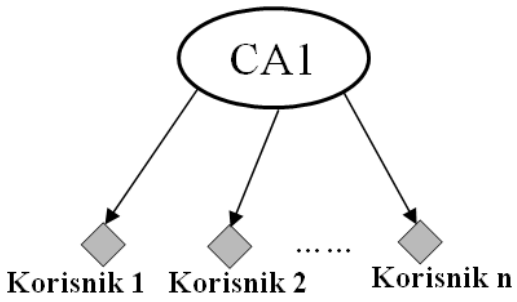
Postoji više PKI arhitektura, ali se sve one mogu svrstati u neku od sledećih [3, 4, 5, 6, 7]:

- jednostavne PKI arhitekture (Simple CA Architecture),
- Enterprise PKI arhitekture (Enterprise PKI Architecture),
- hibridne PKI arhitekture (Hybrid PKI Architecture).

2.2. Jednostavne PKI arhitekture

2.2.1. Arhitektura sa jednim CA

Arhitektura sa jednim CA je PKI arhitektura koja u svom sastavu ima jedan sertifikacioni autoritet koji pruža PKI usluge svim korisnicima. Na slici 1. prikazana je PKI arhitektura sa jednim CA.



Slika 1. PKI arhitektura sa jednim CA [7]

Podesna je za male organizacije sa ograničenim brojem korisnika. Arhitektura sa jednim CA ne može ispratiti širenje organizacije zbog povećanja poslovanja jer ne dozvoljava dodavanje novih CA u arhitekturu.

2.2.2. Basic Trust List arhitektura

Postoje različita tumačenja liste poverenja zato što ne postoji jedinstven način da se definiše ili formalizuje lista poverenja. Jedna od definicija je da je to lista sertifikata (npr. skup sertifikata u memorijskom prostoru koga koristi web pretraživač) ili da je to potpisana lista koja može sadržati bilo koju poverljivu informaciju (heševi ili imena fajlova sertifikata), kao u slučaju Microsoftove liste sertifikata (Certificate Trust List, CTL) [8]. Listu poverenja Certipost [9] definiše kao potpisani skup sertifikata sa informacijama koje definišu osobine i ograničenja kako se primenjuje poverenje.

U zavisnosti od toga ko upravlja listom poverenja mogu se razmatrati dve vrste:

- user trust lista ili basic trust list kojom upravlja korisnik i
- provider trust lista ili extended trust list kojom upravlja provajder od poverenja (trust provider).

User trust list je najrasprostranjenija PKI arhitektura koja je danas u upotrebi jer se proširuje preko operativnih sistema i web aplikacija. Krajni korisnici mogu modifikovati ovu listu dodajući ili brišući sertifikat CA. Ovaj model nije tehnički kompleksan, međutim korisnici nemaju način ili veštinu da pravilno održavaju svoje poverenje jer ne znaju da li dodavanje ili brisanje nekog sertifikata CA iz liste može prouzrokovati bezbednosni rizik.

Provider trust listu kreira i održava (upravlja) provajder od poverenja (TP, Trust Provider) koji predstavlja garanciju korisnicima da mogu verovati sertifikatima iz liste.

2.3. Enterprise PKI arhitekture

PKI sistemi sa jednim CA se mogu proširivati tako da se više CA povezuju u hijerarhijsku strukturu u kojoj se zna koji je podređeni, a koji nadređeni CA, ili se povezuju na ravnopravnoj osnovi svaki sa svakim (*peer-to-peer*). Teorijski gledano, svaka organizaciona struktura može da se realizuje preko jednog od navedenih načina. U ovom poglavlju, kao Enterprise PKI arhitekture razmatraju se dve PKI arhitekture [2]: hijerarhijska arhitektura (Hierarchical Architecture) i mrežna arhitektura (Mash Architecture).

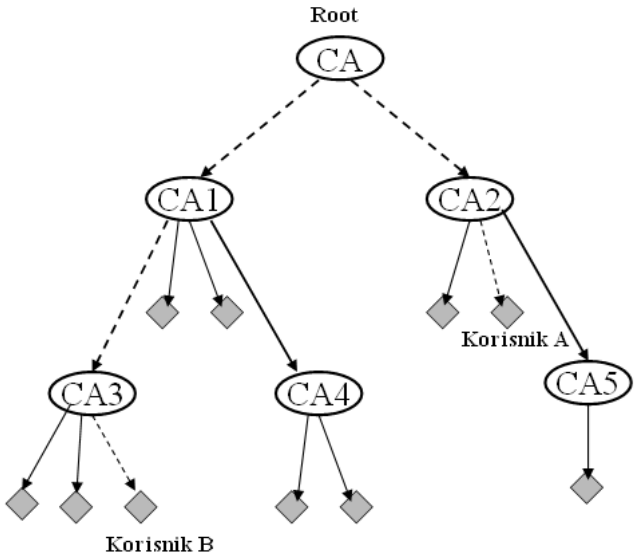
2.3.1. Hijerarhijska arhitektura

Ova PKI arhitektura izgrađena je na jednosmernim odnosima poverenja između nadređenog i podređenog CA. Na vrhu hijerarhije nalazi se jedan CA (root CA) koji predstavlja tačku poverenja za celu arhitekturu [10]. Root CA izdaje sertifikate svojim podređenim CA, dok oni mogi izdavati sertifikate svojim podređenim CA i korisnicima. Javnim ključem root CA inicira se poverenje u PKI tako što se distribuira do svih korisnika.

Potčinjeni CA izvršavaju sve funkcije CA, ali im nadređeni CA može delegirati ili uskratiti određene funkcionalnosti. Prilikom proširivanja hijerarhije dodavanjem novog CA, nadređeni CA mu izdaje digitalni sertifikat kroz koji mu proširuje ili uskraćuje osnovne funkcionalnosti. Potčinjeni CA ne mogu izdavati sertifikate svojim nadređenim CA ili root CA. Novi CA se može dodati na root CA ili bilo koji potčinjeni CA.

Na slici 2. je isprekidanim linijama prikazan lanac poverenja od korisnika A do korisnika B. Korisnik A i B su međusobno razmenili sertifikate da bi komunicirali. Korisnik A potvrđuje sertifikat korisnika B tako što verifikuje njegov potpis. Za verifikaciju sertifikata potreban mu je javni ključ korisnika B. Kako svi korisnici u ovoj arhitekturi veruju root CA i imaju njegov javni ključ, tako će korisnik A moći da verifikuje digitalni sertifikat CA1, a time i iskoristi njegov

javni ključ kako bi verifikovao digitalni sertifikat CA3. Javnim ključem CA3 potvrdiće digitalni sertifikat korisnika B i na taj način utvrditi da digitalni sertifikat koji je dobio od korisnika B zaista pripada njemu.

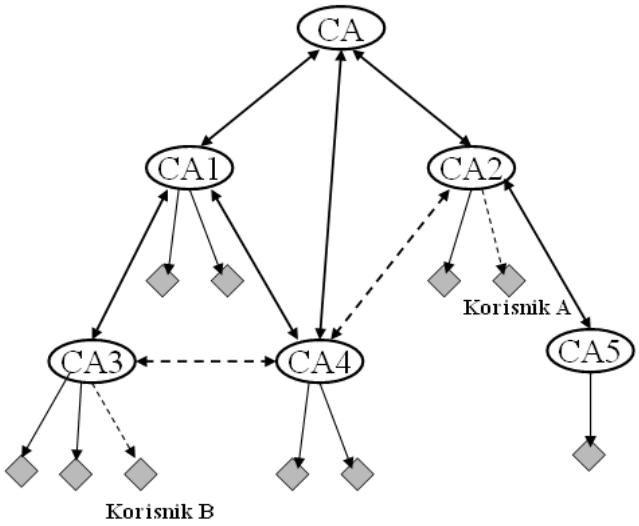


Slika 2. Hijerarhijska PKI arhitektura [7]

2.3.2. Mrežna arhitektura

Mrežna PKI arhitektura gradi bidirekcione odnose poverenja na ravnopravnoj osnovi (peer-to-peer) između ravnopravnih CA, tako što CA jedan drugom izdaju sertifikate. Mrežna arhitektura se s obzirom na broj relacija poverenja koje uspostavljaju međusobno sertifikaciona tela može podeliti na:

- full mash arhitekture, u kojoj svaki CA uspostavlja vezu poverenja sa više drugih CA.
- partial mash arhitektura u kojoj CA ne uspostavlja vezu poverenja sa svim ostalim CA.



Slika 3. Mrežna PKI infrastruktura

Na slici 3. prikazana je mrežna arhitektura sa korisnicima i međusobnim poverenjem između CA (linije sa dve strelice). Korisnik A i korisnik B treba da ostvare komunikaciju. Korisnik A zna javni ključ CA2 jer mu je CA2 izdao sertifikat. Da bi verifikovao sertifikat korisnika B, potrebno je da dobije javni ključ CA3. Postoji više lanaca međusobnog poverenja između korisnika A i B, a isprekidanim linijama označen je najkraći lanac poverenja. Kada korisnik A verifikuje digitalni certifikat CA4 pomoću njegovog javnog ključa koji je dobio od CA2, na isti način će verifikovati digitalni sertifikat CA3. Nakon uspešne verifikacije dobiće javni ključ CA3 pomoću koga će verifikovati digitalni sertifikat za koji smatra da je od korisnika B. Na isti način će korisnik B verifikovati digitalni sertifikat korisnika A.

U mrežnoj arhitekturi svaki korisnik se uzda u javni ključ jednog od CA u PKI, tj. onog CA koji mu izda sertifikat. Sada veze poverenja nisu nadređeni – podređeni, nego su veze poverenja istog prioriteta (nivoa). CA međusobno razmenjuju sertifikate u formi ukrštenih sertifikata.

2.4. Hibridne PKI arhitekture

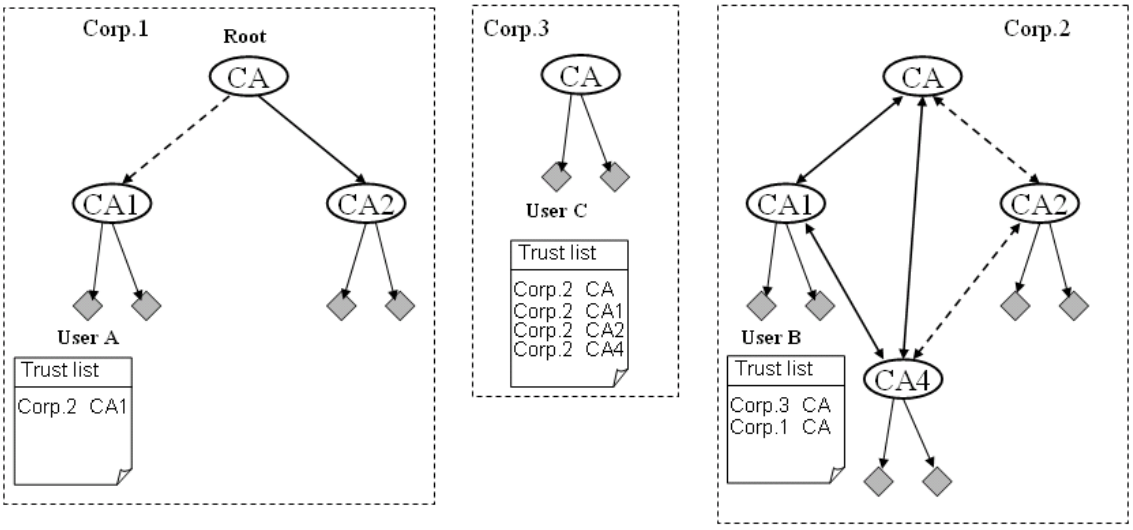
PKI arhitekture organizacija nisu uvek iste. Na primer, jedna organizacija može da ima hijerarhijsku arhitekturu, a druga, sa kojom treba da uspostavi bezbednu komunikaciju, da ima neku drugu arhitekturu. U ovakoj situaciji PKI treba da obezbedi rešenje koje omogućava organizacijama da međusobno bezbedno komuniciraju iako imaju različite PKI arhitekture. Rešenje koje se nameće je hibridna PKI arhitektura koja omogućava organizacijama sa više različitih PKI arhitektura da ostvare poverljivo okruženje za bezbednu razmenu informacija. Najčešće se razmatraju sledeće vrste hibridnih arhitektura: Extended Trust List arhitektura, Cross-certified PKI arhitektura i Bridge CA arhitektura.

2.4.1. Extended Trust List arhitektura

U svetu ne postoji jedan root CA niti jedan Bridge CA. Zbog toga aplikacije moraju podržati veliki broj različitih PKI arhitektura. Ovo se najčešće postiže ugradnjom tačke poverenja u aplikaciju. Liste poverenja se najčešće ugrađuju u aplikacije i na taj način se obezbeđuju jednostavna rešenja za problem upravljanja poverenjem. Primer takve arhitekture je web ili browser-oriented PKI gde su javni ključevi sertifikacionih tela preinstalirani u standardnom web pretraživaču [11]. Ključevi definišu skup CA koji korisniku služi kao početna tačka poverenja (kao root) za proveru sertifikata. Korisnik može menjati skup ključeva, ali mora da poštuje PKI i bezbednosna pitanja. Liste poverenja su, međutim, izložene kritikama zbog nepostojanja jasnog kriterijuma za unos tačaka poverenja u listu. Kriterijum je više zasnovan na komercijalnoj osnovi nego na bezbednosnoj analizi.

TERENA Academic CA Repository (TACAR) projekat započet je 2003. godine sa ciljem da se obezbedi repozitorijum poverenja koji će sadržati akreditovane root CA sertifikate za potrebe pretraživača i servera. Ovaj repozitojum treba da omogući jednostavno preuzimanje i importovanje liste poverenja.

Na slici 4. prikazana su tri različita PKI domena koja su povezana preko listi poverenja. Iz liste poverenja CA1 domena Corp.2. vidi se da je uspostavljeno poverenje sa hijerarhijskom PKI domena Corp.1. i sa CA iz domena Corp.3..



Slika 4. Extended trust list arhitektura

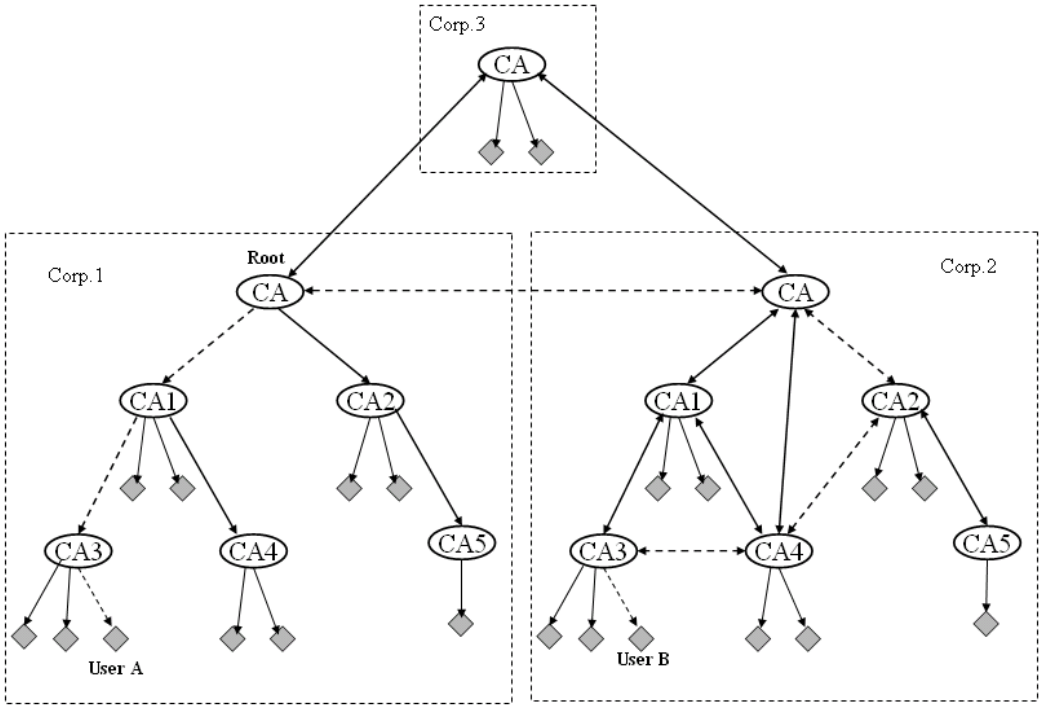
2.4.2. Cross-certified PKI arhitektura

Ova arhitektura omogućava povezivanje više različitih PKI arhitektura uspostavljanjem relacije poverenja ukrštenim sertifikatom. Entiteti jedne PKI arhitekture mogu potvrditi postojanje entiteta čiji sertifikat imaju iz druge PKI arhitekture.

U cross-certified PKI arhitekturi različiti korisnici konstruišu različite puteve za isti sertifikat krajnjeg entiteta. Sertifikacioni put počinje u tački poverenja koja je prirodna za tu PKI arhitekturu. Ako je korisnik deo hijerarhijske PKI arhitekture, onda sertifikacioni put počinje od root CA. Kada je korisnik deo arhitekture sa jednim CA ili mrežne arhitekture tada njegov sertifikacioni put počinje od CA koji mu je izdao sertifikat. U ovoj arhitekturi konstrukcija sertifikacione putanje zavisi od metoda koji se primenjuje u arhitekturama koje je sačinjavaju. Na primer, hijerarhijska arhitektura ima jednostavan metod konstrukcije sertifikacione putanje.

U mrežnoj arhitekturi konstrukcija sertifikacione staze je složenija jer se mora identifikovati jedan ili više ukrštenih sertifikata kako bi se došlo do tačke poverenja.

Na slici 5. je prikazana cross-certified arhitektura koja omogućava ostvarivanje poverenja između organizacija sa tri različite PKI arhitekture, odnosno poverenje između PKI arhitekture sa jednim CA, hijerarhijske i mrežne PKI arhitekture. Isprekidanim linijama na slici 5. prikazana je jedna od mogućih sertifikacionih staza.



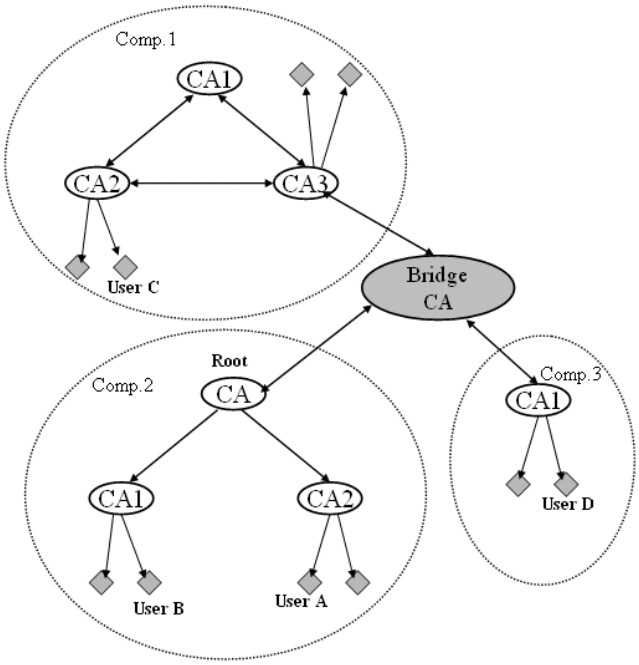
Slika 5. Cross-Certified Enterprise PKI arhitektura

Jedna od karakterističnih arhitektura za uspostavljanje poverenja između više CA u cross-certified arhitekturi je mrežna cross-certified arhitektura. U ovoj arhitekturi root CA različitih hijerarhijskih arhitektura mogu ostvariti međusobno peer to peer relacije, odnosno mogu razmeniti ukrštene sertifikacione parove kako bi ostvarili relacije poverenja i na taj način obezbedili međusobno poverenje između PKI arhitektura. U zavisnosti od broja ostvarenih relacija poverenja mrežnu cross-certified arhitekturu moženo podeliti na: full mash cross-certified i partial cross certified arhitekturu. U prvoj cross-certified arhitekturi svi root CA međusobno ostvaruju relacije poverenja kroz n^2 ukrštenih sertifikata za n root CA. U praksi se obično implementira partial mash cross-certified arhitektura u ostvaruje manje od n^2 relacija poverenja za n root CA

2.4.3. Bridge CA arhitektura

Jedno od rešenja koje olakšava povezivanje različitih PKI arhitektura zasnovano je na ukrštenoj sertifikaciji sa trećom stranom, odnosno Bridge CA. Ovo rešenje je dala U.S. Federal Government i ono omogućava povezivanje različitih PKI arhitektura tako što se uvodi novi CA (mostovni CA) koji uspostavlja peer-to-peer relacije poverenja sa CA drugih PKI arhitektura. Ova arhitektura se često naziva hub and spoke, a ovo ime proističe iz prostornog odnosa centralnog CA i CA PKI arhitektura sa kojima se uspostavlja poverenje [10]. Centralni CA (hub) predstavlja centar koji uspostavlja radijalne (spoke) relacije sa CA. Centralni CA uspostavlja poverenje sa CA u zavisnosti od vrste PKI arhitekture sa kojom uspostavlja poverenje. U slučaju hijerarhijske PKI arhitekture, na primer, relaciju poverenja uspostavlja sa root CA, a u slučaju mrežne PKI arhitekture sa bilo kojim CA.

Na slici 6. prikazan je mostovni CA koji uspostavlja relaciju sa tri kompanijske PKI, Comp.1, Comp.2 i Comp.3. Korisnik A i B hijerarhijske PKI arhitekture veruju glavnom CA Comp.1, a glavni CA Comp.1 je uspostavio sa mostovnim CA relaciju poverenja tako što mu je izdao digitalni sertifikat. Korisnik C veruje CA2 mrežne PKI arhitekture Comp.1 jer mu je izdao sertifikat, a veruje i mostovnom CA zato što postoji punovažna putanja sertifikata od CA2 do CA3 koji je izdao sertifikat mostovnom CA. Korisnik D veruje svom CA1 Comp.3 jer mu je direktno izdao sertifikat, a veruje i mostovnom CA jer je CA1 Comp.3 izdao sertifikat mostovnom CA. Sada korisnici iz različitih kompanija Comp.1, 2 i 3 mogu koristiti vezu poverenja koja postoji kroz mostovni CA i tako uspostave međusobnu komunikaciju.



Slika 6. Mostovna PKI arhitektura

Iako je ovaj model prilično jednostavan sa korisničke tačke gledišta, postoje brojne tehničke poteškoće jer je validacija sertifikacione staze kompleksna i vrši se nekoliko provera (ograničenje imena i politika, status sertifikata, mapiranje politika) kroz celu sertifikacionu stazu. FBCA (Federal Bridge Certification Authority) radila je na međusobnom povezivanju više Bridge CA, međutim konstatovane su brojni tehnički i operativni problemi [12]. NIST je razvio javni alat za testiranje [13] validnosti sertifikacione staze po X.509 pravilima [14], uključujući i Bridge CA.

Evropska unija radila je na projektu razvoja Bridge CA za svoje zemlje članice. Kako bi omogućili interoperabilnost, predlažu [15] kreiranje hibridne BCA koja kombinuje distribuciju sertifikata akreditovanog CA u obliku potpisane liste poverenja i omogućavanje ukrštene sertifikacije CA sa Bridge CA za one korisnike koji ne žele da preuzmu listu poverenja. Zaključak je da je ukrštena sertifikacija teže rešenje od modela liste poverenja.

2.5. Komparativna analiza PKI arhitektura

Izbor najpodesnije PKI arhitekture nije ni malo jednostavan zadatak. Razlog leži u tome što ne postoje čvrsta obavezujuća pravila za izbor PKI arhitekture, a ne postoji ni PKI arhitektura koja obezbeđuje rešenje za sve situacije. Da bi se izabrala što bolja PKI arhitektura potrebno je dobro poznavati njihove mogućnosti. Prvo je potrebno definisati pravila za izbor PKI arhitekture [16, 17] ili odgovarajućeg komercijalnog davaoca usluga sertifikacionog tela (Certification Service Providers). Takođe, u izboru PKI arhitekture značajno mesto ima sagledavanje istorijskog razvoja i problema realnih PKI arhitektura (npr EuroPKI) [18]. Potrebno je upoznati prednosti i nedostatke PKI arhitekture pre nego što se izabere odgovarajuća. To je najbolje uraditi kroz komparativnu analizu prednosti i nedostataka i kroz aspekt izabranih parametara koji najbolje definišu PKI arhitekturu.

2.5.1. Komparativna analiza na osnovu izabranih parametara

Komparacija PKI arhitektura izvršena je kroz sledeće izabrane parametre [7]: poverenje (relacija i tačka poverenja), sertifikaciona staza, skalabilnost i otkaz (tačku otkaza, težinu otkaza i oporavak od otkaza).

Relacija poverenja predstavlja vezu između sertifikata korisnika i CA, a u koju korisnik veruje pod pretpostavkom da je CA izdao odgovarajući važeći sertifikat [19]. Ključna uloga poverenja je da se opiše odnos između korisnika i CA ili između CA korisnika, kao i da su korisnici sigurni da mogu verovati CA koji je kreirao važeće i pouzdane sertifikate.

Tačka poverenja je tačka, odnosno CA, od koga korisnik sertifikata počinje validaciju sertifikacione staze. Tačka poverenja može biti root CA za hijerarhijsku arhitekturu, CA koji je korisniku izdao sertifikat ili bilo koji CA u mreži PKI kako je definisano politikom. Različite aplikacije oslanjaju se na različite tačke poverenja ili prihvataju sertifikacione staze od bilo kog CA iz skupa tačaka poverenja.

Sertifikaciona staza je lanac sertifikata koji je ostvaren preko relacija poverenja između sertifikacionih tela, a kako bi se odredilo da li je sertifikat koji se proverava potpisan od strane njegovog izdavača.

Korisnik (Relying party) je aplikacija ili strana koja obrađuje sertifikate za potrebe verifikovanja elektronskog potpisa, autentikaciju druge strane ili uspostavljanja poverljive komunikacije.

Obrada sertifikacione staze je proces kojim sistem za obradu sertifikata obrađuje sertifikate iz lanca sertifikata koji počinje od tačke poverenja i završava se ciljnim sertifikatom, odnosno sertifikatom koga proverava korisnik.

Skalabilnost predstavlja mogućnost PKI arhitektrure da se proširuje dodavanjem novih CA ili novih PKI, odnosno smanjuje isključivanjem jednog ili više CA iz PKI arhitekture, odnosno isključivanjem jedne ili više PKI arhitektura.

Tačka otkaza predstavlja najslabiju tačku u PKI arhitekturi čiji prestanak funkcionisanja dovodi u pitanje rad dela ili cele PKI arhitekture. U radu tačku otkaza predstavlja CA kome je kompromitovan privatni ključ.

Oporavak od otkaza predstavlja postupak ponovnog uspostavljanja poverenje u PKI arhitekturu [20].

Rezultati komparativne analize na osnovu izabranih parametara prikazani su u Prilogu br. 1a i Prilogu br. 1b i predstavljaju proširenje rezultata istraživanja prezentovanih u radu [7], a detaljnija analiza svakog izabranog parametra data je u nastavku teksta.

2.5.1.1. Poverenje u PKI

Poverenje u PKI razmatrano je kroz tačku poverenja i vrstu relacije poverenja koja se ostvaruje između CA.

PKI arhitektura sa jednim CA. U ovoj PKI arhitekturi CA ujedno predstavlja jedinu tačku poverenja (trust point), odnosno anker poverenja (trust anchor) kome svi korisnici veruju. PKI arhitektura sa jednim CA ne ostvaruje relacije poverenja sa drugim CA.

Basic Trust List arhitektura. U ovoj PKI arhitekturi ne postoje relacije poverenja između CA već entiteti održavaju poverljivost prema CA putem lista poverenja koje se nalaze kod njih. Ovi entiteti u listi poverenja imaju samo sertifikate i CRL onih CA kojima veruju. Postojanje liste poverenja omogućava da entiteti koji pripadaju različitim CA mogu međusobno bezbedno da komuniciraju, bez uspostavljanja relacija poverenja između CA.

Hijerarhijska PKI arhitektura. U hijerarhijskoj PKI arhitekturi svi korisnici zasnivaju poverenje na jednoj tački poverenja. Ta tačka poverenja predstavlja glavni CA (root CA). Root CA izdaje sam sebi sertifikat koji potpisuje (samopotpisani sertifikat) [21]. Javni ključ glavnog CA distribuira se do svih korisnika i na taj način se inicira poverenje u PKI. Relacije poverenja u ovoj PKI arhitekturi su jednosmerne i uspostavljaju se između glavnog i potčinjenih CA, počevši od glavnog do zadnjeg CA u hijerarhiji. Kroz uspostavljenu relaciju poverenja, potčinjeni CA izvršavaju sve dodeljene funkcije nadređenog CA. Nadređeni CA može uskratiti potčinjenim CA odgovarajuće funkcionalnosti, ali potčinjeni CA ne može uskratiti funkcionalnosti nadređenom CA.

Mash PKI arhitektura. Ova PKI arhitektura ima više tačaka poverenja. Svaki CA u mrežnoj PKI arhitekturi može biti tačka poverenja jer su povezani na ravnopravnoj osnovi (peer-to-peer). Relacija poverenja ostvaruje se parom sertifikata koji dva CA izdaju jedan drugom. Na ovaj način se opisuje njihov dvosmerni odnos poverenja, što rezultira mrežom veza poverenja između ravnopravnih CA. Pošto su u ravnopravnom odnosu, CA ne mogu da utiču na uslove i tipove sertifikata koje izdaje drugi CA. Ipak, odnos poverenja ne može da bude bezuslovan. Ako CA želi da ograniči poverenje, ta ograničenja se navode u sertifikatu koji izdaje. Ograničenja poverenja navode se u jednom ili više standardnih proširenja za ukršteni sertifikat u poljima *name constraints, policy constraints* i *path-length constraints*. [14]. Isto tako, relacija poverenja u ovoj arhitekturi može biti unilateralna kada jedan CA izda sertifikat drugom CA, odnosno ostvari relaciju poveranja, a drugi CA ne uzvrati sertifikatom.

Extended Trust List arhitektura. U Extended trust list arhitekturi CA različitih PKI arhitektura ne održavaju relacije poverenja međusobno nego to čine entiteti kroz održavanje liste poverenja. Ova lista sadrži više tačaka poverenja kojima entitet veruje. Ovakvo uspostavljanje poverenja

može se ostvariti sa drugim organizacijama koje imaju istu ili različitu PKI arhitekturu. To znači da se u proširenoj listi poverenja entiteta može nalaziti jedan ili više CA iz različitih PKI arhitektura. U nekim situacijama lista poverenja korisnika može sadržati sve CA jedne ili više PKI arhitektura sa kojima entitet želi da ostvari poverenja.

Cross-Certified Enterprise PKI. U ovoj arhitekturi ostvaruju se peer-to-peer relacije poverenja između istih ili različitih PKI arhitektura [22]. Najmanji oblik ove arhitekture je uspostavljanje relacija poverenja samo između dve arhitekture. Relacije poverenja koje se uspostavljaju ukrštenom sertifikacijom između CA različitih ili istih arhitektura može biti unilateralna i obostrana. Odnosi poverenja se mogu ograničiti kroz navođenje ograničenja u jednom ili više standardnih proširenja ukrštenog sertifikata [14]. U hijerarhijskoj arhitekturi root CA ili bilo koji potčinjeni CA može uspostaviti peer-to-peer relaciju poverenja sa bilo kojim CA mrežne arhitekture, arhitekture sa jednim CA ili sa drugom hijerarhijskom arhitekturom. Isto tako, mash arhitektura i arhitektura sa jednim CA mogu uspostaviti relaciju poverenja sa jednom ili više istih i različitih arhitektura.

Bridge CA arhitektura. Mostovni CA ne izdaje sertifikate korisnicima niti čini tačku poverenja, već ga svi korisnici smatraju posrednikom između različitih PKI arhitektura. Odnose poverenja uspostavlja stvarajući ravnopravne relacije i to sa hijerarhijskom PKI arhitekturom preko glavnog CA, a sa mrežnom PKI arhitekturom preko jednog od CA. CA koji ostvaruje relaciju poverenja sa bridge CA naziva se Principal CA. Novi CA ili enterprise PKI arhitektura razmenjuje digitalne sertifikate sa bridge CA ostvarujući ukršteni sertifikacioni par.

2.5.1.2. Sertifikaciona staza

Sertifikaciona staza se razmatra kroz dužinu i konstrukciju.

PKI arhitektura sa jednim CA. PKI arhitekturi sa jednim CA ne dozvoljava dodavanje novih CA u PKI okruženju, odnosno stvaranje bilo kakvog oblika poverenja između postojećeg CA i nekog drugog CA. Stoga sertifikaciona staza započinje i završava se istim sertifikatom, to jest sertifikatom koji je CA izdalo krajnjem korisniku. Dužina sertifikacione staze je jedan sertifikat, a njena validacija se odnosi na proveru jednog sertifikata.

Basic Trust List arhitektura. Kod ove PKI arhitekture ne uspostavljaju se relacije poverenja, pa i ne postoje sertifikacione staze. Sertifikaciona staza u ovoj arhitekturi je ista kao i u arhitekturi sa jednim CA i sadrži samo jedan sertifikat.

Hijerarhijska PKI arhitektura. Lanac poverenja do bilo kog korisnika u hijerarhiji uvek počinje od root CA, preko podređenih CA do korisnika. Svakom lancu poverenja odgovara određena sertifikaciona staza. Za svaki entitet (traženi sertifikat) postoji samo jedna sertifikaciona staza koja počinje sa sertifikatom root CA, ide preko sertifikata potčinjenih CA sve do sertifikata krajnjeg entiteta (sertifikata koji je potrebno poroveriti). U zavisnosti od dubine hijerarhijske PKI arhitekture zavisi i dužina sertifikacione staze. Najduža sertifikacioan staza jednaka je sumi sertifikata potčinjenih CA plus sertifikat krajnjeg entiteta. Validacija sertifikata zavisi od dužine sertifikacione staze i ograničenja u sertifikatu.

Mrežna PKI arhitektura. Konstrukcija sertifikacione staze u mrežnoj arhitekturi je kompleksnija nego u hijerarhijskoj PKI arhitekturi. U ovoj arhitekturi izgradnja sertifikacione staze od korisnika sertifikata do tačke poverenja nije deterministička. Konstrukcija sertifikacione staze počinje od tačke poverenja i kreće se preko CA koji ostvaruju relacije poverenja sa više drugih CA do CA koji je izdao sertifikat krajnjem korisniku. U mrežnoj arhitekturi veoma je teško konstruisati sertifikacionu stazu jer postoji više bidirekcionih relacija poverenja između CA što prouzrokuje više sertifikacionih staza između korisnika i tačke poverenja. Neke od sertifikacionih staza su dobre, a druge vode do beskorisnih krajeva ili stvaraju beskorisne petlje. Maksimalna dužina sertifikacione staze je jednaka broju CA u PKI. Validacija sertifikata je složena jer sertifikaciona staza može biti dugačka i sertifikati mogu imati ograničenja.

Extended Trust List arhitektura. Proširena lista poverenja može sadržati hijerarhijsku i mrežnu arhitekturu. Jedna stavka u listi poverenja može odgovarati root-u CA hijerarhije, a druga stavka može odgovarati nekom CA unutar mrežne arhitekture. U hijerarhijskoj arhitekturu se sertifikaciona staza konstruiše na jednostavan način, ali u slučaju mrežne arhitekture koristi se složeni algoritam konstrukcije. U ovoj arhitekturi se ne može iz sertifikata krajnjeg entiteta odrediti da li pripada hijerarhijskoj ili mrežnoj arhitekturi. Određivanje početne tačke sertifikacione staze je takođe teško zato što, osim u slučaju kada je sertifikat izdala jedna tačka poverenja, nije jasno od koje tačke poverenja sertifikaciona staza treba da počne. Da bi se rešili navedeni problemi oko konstrukcije sertifikacione staze ova arhitektura generiše keš sertifikata (certificate cache). Ovaj keš sadrži sve moguće sertifikacione staze, pa se umesto konstrukcije sertifikacione staze pretražuje keš. Nađenim sertifikacionim stazama određuje se vrednost. Ova vrednost predstavlja kompleksnost sertifikacione staze. Ona koja ima manju vrednosti predstavlja jednostavniju stazu.

Cross-Certified Enterprise PKI. U cross-certified PKI arhitekturi različiti korisnici konstruišu različite staze za isti sertifikat krajnjeg entiteta. Sertifikacionai staza počinje u tački poverenja koja je prirodna za tu PKI arhitekturu. Ako je korisnik deo hijerarhijske PKI arhitekture onda sertifikaciona staza počinje od root CA, a ako je korisnik deo mrežne PKI arhitekture počinje od CA koje je izdalo sertifikat.

Bridge CA arhitektura. Korisnici već znaju stazu do bridge CA i ostaje im samo da odrede stazu od bridge CA do sertifikata entiteta. Međutim, u zavisnosti dužine lanca sertifikata, obrada sertifikacione staze može biti komplikovana jer zahteva više provera (policy and name constraints, certificate status, policy mappings).

2.5.1.3. Skalabilnost PKI arhitektura

PKI arhitektura sa jednim CA. Pošto nema relacija poverenja između CA, ova arhitektura je ograničena na jedan CA i ne može se proširivati dodavanjem novih CA. Zato je ova PKI arhitektura podesna za male organizacije sa ograničenim brojem korisnika.

Basic Trust List arhitektura. Ova arhitektura se može jednostavno proširivati dodavanjem novih CA u liste poverenja. Međutim, iza navedene jednostavnosti krije se problem koji narasta sa proširenjem ove arhitekture. Uvođenje svakog novog CA zahteva ažuriranje liste poverenja svih entiteta koji treba da veruju novom CA. U ovoj arhitekturi lista poverenja sadrži vitalne informacije koje održava svaki korisnik za sebe. Ovakav način održavanja liste poverenja može dovesti do problema koji su prouzrokovani ubacivanjem lažnog CA ili kompromitovanjem bilo kog CA.

Hijerarhijska PKI arhitektura. Ovo je najčešća arhitektura koja se primenjuje u organizacijama jer prati hijerarhijski razvoj organizacije. Ova vrsta arhitekture je prilično skalabilna jer se mogu lako pratiti promene u rastu organizacije [23]. Arhitektura se proširuje uspostavljanjem relacije poverenja između root CA i novog CA ili nekog drugog CA (nadređenog CA) i novog CA. Glavni CA (root CA) izdaje sertifikate samo potčinjenim CA, a ne korisnicima. Međutim potčinjeni CA izdaju sertifikate svojim potčinjenim CA i korisnicima. Novi CA se može dodati na root CA ili bilo koji potčinjeni CA.

Mrežna PKI arhitektura. Ova PKI arhitektura se može jednostavno proširivati dodavanjem novog CA i uspostavljanjem veza poverenja sa drugim CA. Svakom novo pridodatom CA potrebno je odrediti sa kojim CA treba da uspostavi veze poverenja i njihova međusobna

ograničenja. Nakon toga CA međusobno razmenjuju sertifikate, tj izdaju sertifikate jedni drugima i kombinuju ih u ukršteni sertifikacioni par. Međutim, bez obzira na lakoću proširivanja, ova arhitektura, generalno gledano, ima lošu skalabilnost koja proizilazi iz složenosti sertifikata i problema u formiranju i validaciji sertifikacione staze.

Extended Trust List arhitektura. Ova arhitektura se lako može proširivati dodavanjem više CA iz različitih arhitektura u listu poverenja korisnika. U nekim situacijama može se dodati cela arhitektura. Način održavanja liste poverenja i problemi u vezi nje su isti kao u basic trust list modelu.

Cross-Certified Enterprise PKI. Ova arhitektura omogućava dodavanje istih i različitih PKI arhitektura jednostavnim uspostavljanjem ukrštenog sertifikacionog para. Pridodata arhitektura se može povezati sa jednom ili više drugih arhitektura. Zbog složene sertifikacione putanje ova mrežna arhitektura nije podesna za povezivanje više enterprise arhitektura, pa kada je reč o skalabilnosti možemo reći da joj je skalabilnost ograničena.

Bridge CA architecture. Proširivanje ove arhitekture novim enterprise PKI arhitekturama je jednostavno i ne usložnjava bitno otkrivanje sertifikacione staze i zato se može reći da je skalabilna. Bridge CA arhitekture mogu se međusobno povezivati, ali ovo povezivanje prate brojni tehnički i operativni problemi koji su opisanu u [12]. Svako proširenje bridge PKI arhitekture je transparentno za korisnike jer nema promene tačke poverenja.

2.5.1.4. Otkaz PKI

Otkaz PKI arhitekture razmatran je kroz tačku otkaza, težinu otkaza i oporavak od otkaza.

PKI arhitektura sa jednim CA. CA u ovoj arhitekturi predstavlja jedinu tačku poverenja i jedinu tačku otkaza zato što samo on drži sve informacije o ključevima entiteta. Kompromitovanje privatnog ključa CA prouzrokuje da svi sertifikati koje je izdao postaju nevažeći. Jedino rešenje da se u potpunosti povrati poverljivost u kompromitovani CA je da on sve sertifikate koje je izdao pre kompromitovanja oglasi nevažećim i da se potom uspostavi novi CA. Novi CA izdaje nove sertifikate koji se dostavljaju entitetima.

Basic Trust List arhitektura. Ova arhitektura nema jednu tačku otkaza koja bi prouzrokovala pad cele arhitekture. U suštini, ova arhitektura se sastoji od više nezavisnih sertifikacionih tela, odnosno od više arhitektura sa jednim CA, pa kompromitovanje jednog CA ne utiče na celu

arhitekturu, već može da utiče na neke korisnike drugih CA koji u listi poverenja imaju kompromitovani CA. Dok entitet ne izbaci kompromitovani CA iz liste poverenja on mu još uvek veruje. Ovo dovodi do toga da entitet smatra da i dalje može ostvariti bezbednu komunikaciju.

Hijerarhijska PKI arhitektura. Celokupno poverenje hijerarhijske arhitekture je u jednoj tački poverenja, root CA [10]. Ujedno ova tačka poverenja je veliki nedostatak jer njenim kompromitovanjem cela PKI arhitektura postaje neupotrebljiva. Potčinjeni CA takođe predstavljaju tačke poverenja za stablo kojima su oni „root CA“, ali su ujedno i potencijalne tačke otkaza. Kompromitovanjem potčinjenih CA samo deo arhitekture postaje neupotrebljiv. Značaj tačke otkaza raste od potčinjenih CA prema root CA. Što CA ima više podčinjenih CA to je šteta prilikom njegovog otkaza veća nego kada otkaže CA sa manjim brojem potčinjenih CA. Najznačajnija tačka otkaza je root CA. Kompromitovani potčinjeni CA relativno lako i brzo vraća poverljivost tako što opoziva sve sertifikate koje je izdao, generiše novi javni ključ i izdaje nove sertifikate korisnicima. Ako CA ima mnogo potčinjenih CA i korisnika onda je uspostavljanje poverenja sporije. Pošto je root CA na vrhu hijerarhije, gubitak poverenja root CA vodi kompletnom gubitku poverenja u celu PKI arhitekturu. Root CA se oporavlja na isti način kao i potčinjeni CA, ali uspostavljanje novog poverenja može dugo potrajati u zavisnosti od veličine arhitekture.

Mrežna PKI arhitektura. U ovoj arhitekturi postoji više tačaka poverenja tako da kompromitovanje bilo koje od njih neće uticati na funkcionalnost cele arhitekture. Ako dođe do kompromitovanja jednog CA onda entiteti drugih CA nastavljaju da komuniciraju sa drugim entitetima ako postoji sertifikaciona staza koja je validna. Kompromitovanom CA se poverljivost vraća tako što prvo opozove sve sertifikate koje je izdao, a zatim izdaje nove sertifikate potpisane novim javnim ključem. Izdaje ih za korisnike i druge CA sa kojima je ostvario relacije.

Extended Trust List arhitektura. Tačke otkaza možemo promatrati kada postoji više entiteta sa listom poverenja i kada postoji jedan entitet sa listom poverenja. Extended trust list arhitektura nema jednu tačku otkaza koja će prouzrokovati pad cele arhitekture kada postoji više entiteta sa listom poverenja. Međutim, postoji više potencijalnih tačaka otkaza i odnose se na CA pojedinačnih PKI arhitektura koje ulaze u ovu vrstu arhitekture. Ako se Extended Trust List arhitektura sastoji od više CA različitih arhitektura i dođe do kompromitovanja CA kome veruje korisnik (nalazi se u njegovoj listi poverenja) onda korisnik neće moći da pristupi korisnicima toga CA, ali će moći drugim CA koji se nalaze u njegovoj listi poverenja.

Cross-Certified Enterprise PKI. Kod jednostavnih Cross-Certified PKI arhitektura gde je poverenje uspostavljeno ukrštenim sertifikatima između CA dve PKI arhitekture, a gledano sa stanovišta bezbedne komunikacije između PKI arhitektura, otkaz CA preko koga je uspostavljeno poverenje dovodi do pada cele arhitekture. Kada se pogleda sa stanovišta pojedinačnih arhitektura otkaz CA preko koga se ostvaruje poverenje sa drugom arhitekturom imaće za posledicu pad cele pojedinačne arhitekture (hijerarhijske i singl CA arhitekture) ili pad dela arhitekture (mrežna arhitektura). Kada se radi o cross-certified PKI arhitekturi sa više enterprise PKI arhitektura, otkaz navedenih CA ima uticaj samo na pojedinačnu PKI arhitekturu i na korisnike drugih PKI arhitektura koji treba da u trenutku otkaza komuniciraju sa PKI arhitekturom čiji je CA otkazao. Kompromitovanom CA se poverljivost vraća na način kako je opisano za pojedinačne enterprise arhitekture s tim što novi CA mora da uspostavi relaciju poverenja sa CA druge PKI arhitekture.

Bridge CA architecture. U ovoj arhitekturi kompromitovanje Principal CA uticaće samo na nemogućnost te enterprise PKI arhitekture da ostvari bezbednu komunikaciju sa drugim PKI arhitekturama. Izuzetak je hijerarhijska PKI arhitektura i arhitektura sa jednim CA gde otkaz Principal CA prouzrokuje pad cele arhitekture. Razlog leži u tome što je Principal CA nosilac poverenja za tu arhitekturu. Bridge CA može biti kompromitovan u celosti ili pojedinačno. Kompromitovanje u celosti odnosti se na kompromitovanje svih tajnih ključeva kojima je brige CA potpisao sertifikat koji je izdao za Principal CA. Ako bridge CA koristi samo jedan tajni ključ za potpisivanje sertifikata kojima ostvaruje relaciju poverenja sa Principal CA onda kompromitovanje toga ključa prouzrokuje pad cele bridge PKI arhitekture. Kompromitovanje pojedinačnog tajnog ključa odnosi se samo na gubitak poverenja sa tom arhitekturom, dok i dalje postoji poverenje između preostalih arhitektura. Kada je kompromitovan Principal CA onda bridge CA opoziva njegov sertifikat. Na ovaj način druge relacije poverenja nisu ugrožene. U slučaju kada je kompromitovan bridge CA, Principal CA opoziva sertifikat koji mu je izdao taj CA. Otkaz hardverske ili softverske prirode takođe mogu srušiti celu PKI arhitekturu. Ukoliko bridge CA ne funkcioniše, korisnici PKI arhitektura ne mogu ostvariti međusobno poverenja.

Ponovno uspostavljanje poverljivost prilikom otkaza Principal CA ostvaruje se na način koji je već opisan u ovome radu za PKI arhitekture kojima pripada Principal CA. Pored toga, Principal CA mora povući sertifikat koji je izdao bridge CA i ponovno sa njim uspostaviti novu relaciju. Ponovno uspostavljanje poverljivosti bridge CA ostvaruje se uspostavljanjem novih relacija poverenja razmenom sertifikata sa Principal CA.

2.5.2. Prednosti i nedostaci PKI arhitektura

U praksi, postoje tehnički i politički problemi u izgradnji PKI. Svaka PKI arhitektura ima prednosti i nedostatke. Organizacije moraju izabrati arhitekturu koja najbolje ispunjava njihove zahteve. Kombinacijom različitih arhitektura mogu se razviti optimalne PKI arhitekture. Komparativni pregled prednosti i nedostataka između različitih PKI arhitektura dat je u Tabeli 1.

Tabela 1. Komparativni pregled prednosti i nedostataka PKI arhitektura [7]

Arhitektura	Prednosti	Nedostaci
Jednostavne PKI arhitekture		
Arhitektura sa jednim CA	- jednostavna arhitektura, - lako se implementira, - jednostavna obrada sertifikacione staze, - pogodna za male organizacije sa ograničenim brojem korisnika.	- nije skalabilana, - kompromitovanjem CA pada cela arhitektura, - ne ostvaruje relacije poverenja sa drugima CA.
Basic Trust List arhitektura	- omogućava bezbednu komunikaciju različitih Single CA, - omogućava proširenje arhitekture, - jednostavan način ostvarivanja poverljivosti, - jednostavna obrada sertifikacione staze.	- ne razmenjuje setifikate između CA, - vremenom može postati komplikovana, - problemi sa upravljanjem listom poverenja, - mogućnost poverenja u kompromitovani CA.
Enterprise PKI arhitektura		
Hijerarhijska arhitektura	- može se uskladiti sa hijerarhijom organizacije, - jednostavno određivanje i obrada sertifikacione staze, - sertifikacione staze su relativno kratke.	- ne može postojati jedan glavni CA u svetu, - nisu sve organizacije hijerarhijskog tipa, - kompromitovanjem root CA kompromituje se cela arhitektura.
Mrežna arhitektura	- flaksibilna arhitektura, - korisnik veruje CA koji mu je izdao sertifikat bez obzira gde se nalazi u PKI, - direktno ukrštanje sertifikata kako bi se skratio proces obrade sertifikacione staze, - jednostavna procedura oporavka jer se odnosi na manje korisnika.	- složen proces obrade sertifikacione staze, - postojanje zatvorenih staza, - loša skalabilnost jer povećanje broja CA degradira perfomanse, - politike sertifikata usložnjavaju sertifikat i obradu sertifikacione staze.
Hibridne PKI arhitekture		
Extended Trust arhitektura	- jednostavno uspostavljanje poverenja između organizacija sa različitim PKI arhitekturama, - lako proširivanje arhitekture,	- iz sertifikata krajnjeg korisnika ne može se odrediti kojoj arhitekturi pripada, - teškoće u određivanju početne tačke

Arhitektura	Prednosti	Nedostaci
	- potpuna kontrola korisnika nad listom poverenja.	sertifikacione staze, - vremenom može postati kompleksna, - teškoće u upravljanju listom poverenja, - moguća zloupotreba menjanja liste poverenja, - nemogućnost centralizovane administracije i primene validacionih politika unutar organizacije.
Cross-Certified Enterprise arhitektura	- može se sastojati od više istih ili različitih Enterprise arhitektura, - jednostavno dodavanje novih PKI arhitektura, - omogućuje bezbednu komunikaciju između entiteta različitih arhitektura, - poverenje između PKI arhitektura se može usloviti.	- ograničena skalabilnost, - složenost sertifikacione staze u zavisnosti od PKI arhitektura.
Bridge CA arhitektura	- otklanja nedostatke hijerarhijske i mrežne arhitekture, - jednostavno i transparentno proširivanje arhitekture, - pouzdanost prilikom kompromitovanja ključeva, - jednostavna obrada sertifikacione staze, - velika skalabilnost koja ne usložnjava sertifikacionu stazu, - centralizovana administracija i primena validacionih politika unutar organizacije.	- kompromitovanje bridge CA narušava se cela arhitektura, - otkrivanje sertifikacione staze je teže nego u hijerarhijskoj PKI, - dužina sertifikacione staze je duplo veća nego u hijerarhijskoj arhitekturi, - brojni problemi prilikom povezivanja bridge CA arhitektura.

3. Klasifikacione šeme i taksanomije zahteva

Prema globalnom istraživanju KPMG i AIPM (Australian Institute of Project Management) za 2020. godinu [26]:

- 64% ispitanika smatra da se složenost projekata povećala tokom protekle decenije,
- 65% ispitanika smatra da rukovodioci projekata imaju pozitivnu sliku o svojoj organizaciji,
- 64% ispitanika smatra da će veštine upravljanja projektima biti važnije u budućnosti i
- 53% ispitanika ne veruje da njihova organizacija čini dovoljno za poboljšanje veština i sposobnosti upravljanja projektima.

Jedan od primarnih razloga propadanja projekata (sa učešćem od 39%) su neodgovarajuće prikupljeni zahtevi [27]. Na globalnom nivou 70% projekata propadne iz razloga kao što su: netačni zahtevi, otkazi sponzora projekata, netačne procene, pomeranje ciljeva projekta i još mnogo toga [28]. U časopisu CIO Magazine [29] navodi se da 71% softverskih proizvoda propada zbog lošeg upravljanja zahtevima i to je, u stvari, jedan od primarnih razloga.

Kompanije sa dobrom praksom u definisanju zahteva prekorače budžet projekta za 21%, dok kompanije koje nemaju dobru praksu potroše znatno više, čak još jedan ceo budžet po projektu [30].

Nisu samo loše definisani zahtevi problem u realizaciji projekta, nego i dobro definisani zahtevi koji su realizovani, a korisnici ih ne koriste. Istraživanje Standish Group International ukazuje da se 45% implementiranih karakteristika softverskog proizvoda koji je u operativnoj upotrebi nikada ne koriste, dok se samo u 20% slučajeva uvek ili često koriste [31].

Iz prikazane statistike vidi se da loše definisani ili određeni zahtevi prouzrokuju značajne probleme u realizaciji i budžetiranju projekata, bilo velikih ili malih. Loše definisani sistemski zahtevi su uzrok propadanja 90% velikih softverskih projekta [32]. Samo 35% projekata se završi na vreme i u okviru budžeta, sa svim specificiranim karakteristikama i funkcijama, dok čak oko 20% projekata propada i posle multimilionerskih ulaganja.

Razumevanje korisničkih zahteva je sastavni deo dizajna informacionog sistema i predstavlja kritičnu tačku za njegovu uspešnu realizaciju. Životni vek uspešnog informacionog sistema i proizvoda počinje sa razumevanjem potreba i zahteva korisnika. Mnoge studije ukazuju da

greške nastale u definisanju zahteva značajno poskupljuju projekat i mogu dovesti do njovog odbacivanja kao neisplativog.

Da bi se prevazišli problemi upravljanja zahtevima, potrebno je zahtev razotkriti, dobro definisati i jasno zapisati. Ukoliko zahtev nije jasno i dobro definisan, neće biti realizovan i dovešće do neuspeha projekta. Dobro definisan zahtev treba da omogući razvojnom timu efikasno završenje projekta uz potpuno zadovoljenje potreba korisnika. Zahtevi treba da budu jasni i merljivi kako bi se moglo efikasno ustanoviti da li su ispunjeni.

Promene u toku razvoja su neminovne i uslovljavaju promene zahteva. Menjaju se zbog promena na tržištu, uvođenja nove tehnologije, nedostataka u dizajnu, propustima prilikom razotkrivanja zahteva, neuspeha prilikom testiranja ispunjenosti zahteva. Svaka promena zahteva u toku razvoja dodatno poskupljuje projekat i produžava vreme njegovog završetka. Zato je bitno da se promenama zahteva kvalitetno upravlja kako bi se smanjili troškovi.

Današnji projekti su multidisciplinarni, pa realizacija nekih zahteva podrazumeva razvoj više nezavisnih komponenti koje ostvaruju različiti izvršioci i alati. Zato je potrebno postojanje jednog izvora koji će nadgledati realizaciju zahteva. Praktično je nemoguće identifikovati celokupni uticaj zahteva kroz multidisciplinarni razvoj i testiranje ukoliko ne postoji jedan izvor koji ga nadgleda.

Prilikom definisanja zahteva potrebno je osmisliti kako da znamo da je zahtev ispunjen, odnosno kako testirati zahtev u krajnjem proizvodu. Ako ne postoji jasna veza između zahteva i testa teško je proceniti da li je zahtev efikasno implementiran.

Efikasno praćenje životnog ciklusa zahteva od trenutka definisanja do realizacije, omogućava da se lakše shvate potrebe za promenama zahteva u toku životnog ciklusa razvoja proizvoda.

3.1. Tehnike za analizu poslovnih procesa i generalizaciju zahteva

Bez obzira na mnogobrojne tehnike za analizu poslovnih procesa, poslovnih zahteva i tehnika za razotkrivanje zahteva, postoji problem u razotkrivanju i definisanju zahteva [33, 34, 35, 36]. Ovaj problem se ogleda kroz nedovoljno sagledavanje potreba korisnika, loše razotkrivanje, nejasno definisanje i definisanje nepotrebnih zahteva. Ovi problemi na direktan ili indirektan

način prouzrokuju teškoće u daljoj implementaciji koje mogu dovesti do produženja rokova i dodatnih finansijskih ulaganja, kao što se može videti iz gore navedene statistike.

3.1.1. Tehnike za analizu poslovnih procesa

Poslovni proces obuhvata skup povezanih aktivnosti kojima se ostvaruju određeni ciljevi ili zahtevi korisnika. Analiza poslovnih procesa je metodologija koja služi za razumevanje procesa poslovanja i poboljšanje efikasnosti i efektivnosti poslovanja u preduzeću. Ova metodologija opisuje procese, učesnike, razmenu informacija i dokumenta [37]. Pomoću ove metodologije postiže se dokumentovanje znanja o poslovnom procesu, uočavanje i evidentiranje manualnih ili nedokumentovanih procesa, analiziraju se pojedinačne akcije, dokumenti i podaci. Mogu se utvrditi problematična područja koja uzrokuju kašnjenje procesa i optimizovati dokumenta i smanjiti zahtevi za podacima.

Ovom analizom se opisuje i vizualizuje proces pomoću dijagrama ili slike koja je jednostavna za razumevanje procesa, a time i posla. Na osnovu analize mogu se identifikovati nepotrebni koraci, uska grla i mogućnosti da se proces jednostavno identifikuje i poboljša.

Generalno, sve metode analize poslovnog procesa imaju sledeće korake: identifikovanje procesa za analizu, prikupljanje podataka o procesu, analiziranje procesa („kakav jeste“), razvoj poboljšanog procesa („budući“).

Najčešće metode analize poslovnih procesa su [37]:

Gap analiza pronalazi i rešava neusklađenost između učinka koji se postiže i učinka koji se želi postići. Neusklađenost je sve ono što sprečava da proces ostvari efikasan rezultat. Otklanjanje neusklađenosti zahteva i akcioni plan za prevazilaženje prepreka i stvaranje uslova za poboljšanje. Ova analiza omogućava povezivanje sa ciljevima i preusmeravanje na pravac koji vodi njihovom ostvarivanju. Procena neusklađenosti se vrši sagledavanjem komponenti poslovnog procesa. Polazi se od odnosa ulaza i izlaza gde se može otkriti suvišnost, rasipanje aktivnosti, loše određeno vreme za zadatak, nedostajući koraci. Ispitivanjem uloge vodiča u ostatku procesa mogu se otkriti nedosledni i nedokumentovani koraci, preregulisani zadaci i nenamerno čuvanje znanja stečenog iskustvom.

Analiza dodate vrednosti podrazumeva ispitivanje suštine postojanja svake aktivnosti u svim fazama životnog ciklusa procesa (planiranje, izvršavanje, analiza i prilagođavanje) tako što se koraci imenuju jednostavnim oznakama i sortiraju kako bi se utvrdila svrha i otkrila prava vrednost. Vrednost se dodaje aktivnosti kroz planiranje, izvršavanje i prevenciju. Ova analiza omogućava objektivan pogled na nedostatke procesa.

Analiza osnovnog uzroka specijalizovana je za pronalaženje osnovnih razloga za probleme koje pokazuje svako od mogućih rešenja. Ovom tehnikom se istražuje odnos između postignutog efekta i mogućih uzroka. Problemi mogu sakriti dublja pitanja koja su manje vidljiva. Tabele su sredstvo koje se primenjuje u analizi za otkrivanje odnosa između uzroka i ispoljenog problema. *Ishikava dijagram* (dijagram „uzroka i posledice“) je vrlo pogodan za jasno utvrđivanje uzroka neželjenih ishoda. Svaka zainteresovana strana i jedinstvena situacija mogu imati ozbiljne skrivene probleme. Neki od njih se retko javljaju, pa se lako mogu prevideti. Stalno postavljanje pitanja je ključno za pronalaženje svih mogućih uzroka.

Analiza posmatranja daje analitičarima uvid u proces iz prve ruke u realnom vremenu. Kao kritična tačka prikupljanja informacija, posmatranje otkriva previđene ili potcenjene korake u procesu. Takođe, prikazuje sve aktivnosti koje su odsutne, uprkos tome što su dokumentovane ili se podrazumevaju kao aktivni deo procesa. Posmatrači takođe mogu da potvrde da li zaposleni tačno izvršavaju proces. Rezultati dobijeni primenom intervjua i mapiranja procesa mogu biti nepouzdani zbog neiskustva ili loše procene. Analitičari mogu zapaziti i dovesti u pitanje prepreke koje nisu uočene u kritičkom pogledu. Posmatrač može biti aktivan i pasivan. Pasivan izbegava interakciju kako bi proces ostao prirodan i nepromenjen, dok je aktivni promatrač u interakciji sa procesom kako bi ustanovio ponašanje u realnom vremenu. Posmatranjem se mogu uočiti teško objašnjivi procesi koji se analiziraju drugim metodama.

Analiza ispitivanja iskustva obuhvata analizu stečenog znanja o procesu dugogodišnjih zaposlenih. Posmatranjem se prikupljaju informacije o procesu iz perspektive početnika, dok se ispitivanjem iskustva prikupljaju informacije o procesu iz stečenog znanja zaposlenih. Iskustveno znanje nije dokumentovano i često se o njemu ne priča, stoga se jedino može na ovaj način prikupiti i analizirati njegov uticaj na proces. Ova analiza ima za cilj da otkrije nevidljive faktore koji proizilaze iz iskustva, a vremenom su uticali na modifikovanje procesa. Analiza iskustva je ključna za zadržavanje znanja u okviru firme u situacijama učestale fluktuacije kadra.

Ostale korisne i često korišćene tehnike su [38]: analiza kritičnog puta, analiza scenarija, analiza zahteva kupaca, analiza matrica, matrica korelacije, pareto analiza, analiza ograničenja procesa, analiza faktora kulture, fokusne grupe kupaca, povratne informacije dobavljača, poređenje dokumentovanih postupaka, igranje uloge.

Tehnike opisane u BABOK® Guide [33] Internacionalnog instituta za poslovnu analizu (International Institute of Business Analysis, IIBA) su najčešće i najrasprostranjenije tehnike koje se praktikuju za analizu poslovnih zadataka. U ovome vodiču opisano je pedeset tehnika.

3.1.2. Tehnike za analizu poslovnih zahteva

Analiza poslovnih zahteva odnosi se na identifikovanje, analizu i dokumentovanje ključnih zahteva povezanih sa poslovnim problemima koje treba rešiti ili ciljem organizacije koji treba ispuniti. Poslovni zahtevi su nešto što organizacija mora da uradi da bi ostala u poslu. Ovi zahtevi se ne odnose na nešto što sistem (nešto što podržava i omogućava poslovanje, softver) mora da uradi.

Analiza poslovnih zahteva obuhvata identifikaciju učesnika, prikupljanje zahteva zainteresovanih strana, kategorizaciju, analizu i dokumentovanje zahteva.

Postoji više različitih tehnika za analizu poslovnih zahteva, a najčešće korišćene su [39]:

Modeliranja poslovnih procesa označavanjem (Business process modeling notation, BPMN) je slična tehnici kreiranja dijagrama procesa pomoću posebnih simbola i elemenata. Koristi se za izradu grafikona za poslovni proces. Ovi grafikoni pojednostavljuju razumevanje poslovnog procesa i lakše razotkrivanje poslovnih zahteva. BPMN je široko popularan kao metodologija za poboljšanje procesa.

Objedinjeni jezik za modeliranje (Unified Modeling Language, UML) sastoji se od integrisanog skupa dijagrama koji su stvoreni za specificiranje, vizualizaciju, konstrukciju i dokumentovanje delova softverskog sistema. UML je korisna tehnika za kreiranje objektno orijentisanog softvera i proces razvoja softvera. U UML-u se grafički zapisi koriste da se predstavi dizajn softverskog projekta. UML takođe pomaže u verifikaciji dizajnirane arhitekture softvera.

Tehnika dijagrama toka (Flowchat technique): Dijagram toka prikazuje sekvencijalni tok i kontrolnu logiku skupa povezanih aktivnosti. Dijagrami tokova mogu biti linearni, višefunkcionalni i odozgo nadole. Dijagramom toka mogu se predstaviti sistemske interakcije, tokovi podataka itd. Grafikoni dijagrama toka se lako razumeju i mogu ih koristiti i tehnički i netehnički članovi tima. Tehnika dijagrama toka pomaže i u prikazivanju kritičnih atributa procesa.

Dijagram toka podataka (Data Flow Diagram, DFD) se koristi za vizuelno predstavljanje sistema i procesa koji su složeni i teško ih je opisati u tekstu. Dijagrami toka podataka predstavljaju protok informacija kroz proces ili sistem. Takođe, uključuju ulazne i izlazne podatke, skladišta podataka i razne potprocese kroz koje se podaci kreću. DFD opisuje različite entitete i njihove odnose pomoću standardizovanih notacija i simbola. Vizuelizacijom svih elemenata sistema lakše je identifikovati nedostatke koji se potom uklanjaju u pokušaju da se stvori kvalitetno rešenje.

Dijagrami aktivnosti uloga (Role Activity Diagrams, RAD) su modeli procesa orijentisani na ulogu. Sagledavaju zahteve na višem nivou organizacije kroz beleženje dinamike i strukture uloga organizacije. Uloge se koriste za grupisanje aktivnosti u jedinice odgovornosti. Aktivnosti su osnovni delovi uloge. Aktivnost se može obavljati izolovano ili u koordinaciji sa drugim aktivnostima u okviru uloge.

Gantov grafikon (Gantt Chart) se koriste u planiranju projekata, jer pruža vizuelni prikaz raspoređenih zadataka zajedno sa rokovima. Gantove tabele pomažu da se prikažu predviđeni zadaci i datumi planiranog završetka. Datumi početka i završetka svih zadataka u projektu mogu se videti u jednom prikazu.

Integrisana definicija za modeliranje funkcija (Integrated Definition for Function Modeling, IDEF): Ova tehnika predstavlja funkcije procesa i njihov odnos prema deci i roditeljskim sistemima uz pomoć okvira. Pruža šemu za shvatanje sistema organizacije.

Veliki problem u organizacijama je razotkrivanje poslovnih zahteva i određivanje prioriteta. Organizacije često imaju problem sa pronalaženjem pitanja koja bi omogućila izdvajanje poslovnih zahteva koji su jasni. Ovo prouzrokuje stvaranje liste zahteva koji nisu određeni i teško ih je pretvoriti u konkretne planove (implementacija). Sprovođenje efikasnih intervjua i

fokusnih grupa treba da otkrije specifične poslovne potrebe organizacije i da predvidi do kojih bi problema moglo doći, a koji bi se u suprotnom mogli prevideti ili ignorisati.

Tokom razmatranja zahteva u organizaciji svaki od njih može izgledati da je prioritetan. Budući da svaki nosilac zahteva vidi svoje potrebe kao glavne, potrebno je napraviti razliku između nečega što je zgodno imati da bi se zadovoljile neke želje i funkcionalnosti koje treba postići da bi se ostvario cilj. Uvođenjem nezavisne treće strane identifikovaće se takvi prioriteti poslovnih zahteva koji su orijentisani na postizanje poslovnih ciljeva [40].

3.1.3. Tehnike za analizu korisničkih zahteva

Analiza korisničkih zahteva nije jednostavan zadatak. Na analizu utiču složene situacije u organizaciji sa zainteresovanim stranama, tradicionalno razmišljanje korisnika i dizajnera koji nastoje da preslikaju aktuelni sistem i procese, korisnici koji ne znaju šta žele od budućeg sistema [41], smanjeno vreme za korisničku analizu zbog ubrzanog razvojnog ciklusa i predstavljanje zahteva korisnika u odgovarajućoj formi.

Kako bi se prevazišli navedeni problemi, potrebno je izabrati odgovarajuću tehniku za analizu zahteva u svakoj fazi. U ovom poglavlju razmatraju se tehnike za analizu korisničkih zahteva u sledećim fazama: prikupljanje informacija o korisnicima, drugim učesnicima i procesima, identifikovanje korisničkih potreba, predviđanje i procena kako bi korisnik dobio povratnu informaciju radi potvrde i preciziranja korisničkih zahteva i izrada specifikacije zahteva.

U Prilogu 2. prikazane su tehnike za analizu korisničkih zahteva po fazama, kao i njihove dobre i loše osobine [42].

3.2. Tipične situacije koje mogu uticati na definisanje zahteva

Problemi u definisanju zahteva proizilaze iz poteškoća koje se javljaju u inžinjeringu zahteva i mogu se svrstati u jednu od sledećih devet kategorija [43]:

- *Ljudski aspekti inžinjeringa zahteva* koji isključuju jednostavnu komunikaciju između projektanta i klijenta. Jedan od uzroka loše komunikacije je postojanje kognitivnih ograničenja za komunikaciju. Proceduralna uputstva za pitanja podstiču dublje razmišljanje pre odgovora, a time i veću verovatnoću da ispitanik neće adekvatno iskazati svoje mišljenje. Različite kulture, poreklo i jezik su znatna prepreka u razumevanju i

definisanju zahteva. Prevazilaženje ovog problema je približavanje kroz korišćenje jezika koji razumeju obe strane uz posmatrača. Raznolikost i bogatstvo jezika može uticati da jedna izjava zvuči dvosmisleno što dovodi do loše komunikacije. Velika količina informacija koje treba analizirati može isključiti komunikaciju kako se problem ne bi produbljivao ili došlo do međusobnog neslaganja.

- *Ljudski jezik nije uvek pogodan za tehnološko rešenje*. Mnogi izrazi koji se koriste u stvarnom svetu nemaju isto značenje u tehničkom smislu. Neke izjave o problemu zbog svog oblika ili jezika ne mogu se koristiti za iznalaženje rešenja. Metodologije koje se koriste imaju nedostatke koji ne mogu potuno pretočiti ono što se želi u tehničko rešenje. Ljudi u komunikaciji mogu problem predstaviti složenijim i većim nego što jeste.
- *Promene u zahtevima tokom napredovanja projekta*. Klijenti saznaju šta je moguće tokom projekta. Dinamičnost posla prouzrokuje da se zahtevi menjaju tokom trajanja projekta. Korisnici menjaju mišljenje o tome šta žele.
- *Zahtevi za kojima organizacija nema potrebe*. Klijenti će ponekad iznositi zahteve koji organizaciji nisu potrebni. Korisnik traži nešto što zaista nije potrebno ili nije u sklopu njegove odgovornosti ili posla.
- *Nemogućnost iskazivanja zahteva*. Korisnik ponekad ne može reći šta je preduzeću potrebno. Ovaj problem nastaje kada se smatra da korisnici razumeju svoje poslovne potrebe i kao takve ih iskazuju, a ispostavi se da su neosnovane. Ovi problemi obično nastaju kada klijent nešto prećuti u vezi zahteva ili korisnik zna samo deo posla koji obavlja.
- *Korisnik odbija da pomogne u projektu*. Neki klijenti ne žele da pomognu u projektu. Zahtevi mogu biti otežani za otkrivanje ako predstavnici korisnika nisu posvećeni projektu. Predstavnik korisnika ima interese koji su u suprotnosti sa drugima u projektu ili sa ciljevima projekta. Neki korisnici će koristiti taktiku otpora kako bi osujetili završetak razotkrivanja zahteva. Korisnici vide novi sistem kao deo borbe za moć u organizaciji.
- *Loše izveden inžinjering zahteva*. RE (requrement engeering) nije uspeo jer nije urađen kako treba. Ova vrsta problema nastaje zbog nedostatka obuke korisnika iz RE ili ponašanja u radu sa konsultantima i analitičarima. To znači da zahtevi korisnika nisu uvaženi ili RE nije sproveden u praksi.
- *Potenciranje simptoma koji ne predstavljaju problem*. Simptomi koji ne predstavljaju probleme se često prijavljuju. Nekompletan ili netačan skup zahteva rezultira nepotpunim RE. Pored navedenog, promena specifikacije i neuključivanje svih zahteva u gotov sistem predstavljaju problem tamo gde ga nema.

Omalovažavanje razvoja zahteva i upravljanja često dovodi do softverskih projekata koji se bore za opstanak ili propadaju. Deset najčešćih problema i situacija koji mogu dovesti do propadanja projekata su [44]:

- *Zabuna oko toga šta su zahtevi*. Reč zahtev za različite ljude može imati različito značenje. Tako rukovodilac pod pojmom zahteva može smatrati koncept proizvoda na visokom nivou ili poslovnu viziju. Programerima zahtevi mogu izgledati kao dizajn korisničkog interfejsa, dok su korisniku zahtevi zapravo rešenje problema.
- *Neadekvatno uključivanje korisnika*. Korisnici mogu odbaciti novi informacioni sistem kao neprihvatljiv na početku uvođenja. Ovo se dešava kada korisnici nisu bili uključeni u definisanja zahteva od samog početka ili smatraju da poslovni analitičari ili programeri već treba da znanju šta je njima potrebno. Jedan od prvih pokazatelja neadekvatnog uključivanja korisnika je kada menadžment ili programeri obezbeđuju ulazne zahteve.
- *Nejasni, dvosmisleni i neadekvatni zahtevi*. Ukoliko izjava zahteva ima nejasnoće može se tumačiti na više različitih načina. Najveći problem nastaje kada više čitalaca tumači zahtev na različite načine i smatra da je njegovo tumačenje tačno, a nejasnoće ostaju neotkrivene do trenutka kada ih je skuplje rešiti. Nedostajanje informacija koje su potrebne programerima je još jedan znak nejasnih ili nepotpunih zahteva. Ako se ne mogu kreirati testovi za proveru da li je svaki zahtev pravilno sproveden, to znači da zahtevi nisu jasno definisani. Krajnji simptom nejasnih zahteva je da programeri moraju postaviti mnogo pitanja poslovnim analitičarima ili korisnicima, ili moraju pogoditi šta se zahtevom traži.
- *Neprioritetni zahtevi*. Proglašavanje svih zahteva jednako bitnim i kritičnim onemogućava da se efikasno odgovori na bitne zahteve jer u ovom slučaju se može posvetiti više pažnje zahtevima koji nisu suštinski za projekat. Ukoliko se pre početka dizajna projekta ne definišu prioritetni zahtevi (ne odredi koje funkcije bi se mogle odgoditi) dolazi do brzog iscrpljivanja i neefikasne realizacije projekta. Različite zainteresovane strane mogu različito tumačiti „visoki“ prioritet, što dovodi do neusklađenih očekivanja o tome koja funkcionalnost prelazi u sledeće izdanje. Korisnici bi mogli oklevati sa davanjem prioriteta jer se plaše da stavke niskog prioriteta nikada neće biti realizovane.
- *Izgradnja funkcionalnosti koju niko ne koristi*. Često u toku realizacije projekta dizajneri ili programeri dodaju funkcije na zahtev korisnika ili na sopstvenu odgovornost sa ciljem poboljšanja proizvoda. Međutim često ovako dodate funkcionalnosti korisnici ne upotrebljavaju. Neke predložene funkcionalnosti nisu jasno povezane sa korisničkim

zadacima ili postizanjem poslovnih ciljeva. Sve naknadne funkcionalnosti oduzimaju vreme i mogu odvratiti tim od suštinskih funkcionalnosti.

- *Paraliza analize*. Nastaje kada analiza poslovnih zahteva postane preterano revnosna, pa se pokušavaju modelirati zahtevi ili prototip sistema pre nego što se potvrde zahtevi za primenu. Isti problem nastaje i ako se donosioci odluka ne mogu složiti oko osnovnih zahteva.
- *Iskrivljavanje prostora, proširivanje opsega (scope creep)*. Većina projekata se suočava sa pretnjom iskrivljavanja opsega, jer se tokom razvoja stalno dodaju novi zahtevi. Rokovi projekta se obično ne menjaju, ne obezbeđuje se više resursa i ništa se ne briše kako bi se prilagodilo novoj funkcionalnosti. Proširivanje opsega obično nastaje kada opseg projekta nije jasno definisan. Ako se predlažu novi zahtevi koji se zatim odbijaju, ali se kasnije ponovo pojavljuju - sa tekućim raspravama o tome da li pripadaju sistemu – tada je definicija opsega previše nejasna. Novi zahtevi koji se naknadno ubacuju sa strane, umesto kroz efikasnu promenu procesa dovode do prekoračenja u rasporedu realizacije projekta.
- *Neadekvatan proces promene*. Najizraženiji simptom je to što projektu nedostaje definisan proces za rešavanje promenljivih zahteva. Nova funkcionalnost može postati evidentna tek tokom testiranja sistema. Proces se često zaobilazi direktnim nalozima programerima o promenama koje se žele. Drugi problem koji ukazuje da je proces promene loš je kada nije jasno ko donosi odluke o predloženim promenama. Odluke o promenama se ne saopštavaju svima na koje to utiče, a status svakog zahteva za promenu nije uvek jasan.
- *Nedovoljna analiza uticaja promena*. Poslovni analitičari, programeri ili menadžeri projekata ponekad pristaju da unesu predložene promene bez pažljivog razmišljanja o implikacijama. Promena može biti složenija od predviđene, trajati duže od obećanog, biti tehnički ili ekonomski neizvodljiva ili u suprotnosti sa drugim zahtevima. Još jedan pokazatelj neadekvatne analize uticaja je da se programeri stalno susreću sa sve više pogođenim komponentama sistema dok primenjuju promenu.
- *Rešenja predstavljena kao zahtevi*. Korisnici često predstavljaju skice ekrana kao svoje zahteve, a diskusija o razotkrivanju zahteva fokusira se na dizajn korisničkog interfejsa, a ne na osnovne potrebe. Tim bi mogao očekivati da prototipovi zamene pisane specifikacije zahteva. Rasprave o zahtevima fokusiraju se na to kako će proizvod izgledati i njegove karakteristike, a ne na ono što će korisnici moći s njim da rade.

3.3. Pregled klasifikacionih šema i taksanomija zahteva

Definiciju zahteva koja se najčešće interpretira, dao je Internacionalni institut za poslovnu analizu (International Institute of Business Analysis, IIBA, www.IIBA.org) u [33], a zasnovana na [45]:

- zahtev je uslov ili mogućnost potrebna zainteresovanoj strani da reši problem ili dostigne cilj;
- zahtev je uslov ili mogućnost koja mora biti ispunjena ili je poseduju rešenja kroz komponentu ugovora, standarda, specifikacije ili drugog formalno nametnutog dokumenta;
- zahtev je dokumentovana forma uslova ili mogućnosti iz gore navedenih definicija.

Najjednostavnija podela zahteva je na funkcionalne i nefunkcionalne. Funkcionalni zahtevi opisuju funkcionalnosti sistema koje treba da omoguće željeno ponašanje sistema, dok se nefunkcionalni zahtevi odnose na kvalitet proizvoda. U oblasti softverskih zahteva, pojam nefunkcionalnih zahteva [46] koristi se za zahteve koji nisu povezani sa funkcionalnošću softvera, već sa kvalitetom sistema. Međutim, različiti autori na različite načine opisuju nefunkcionalne zahteve [47] i koriste termine ograničenja, kvalitativni atributi, kvalitativni ciljevi, kvalitet servisnih zahteva [48].

3.3.1. Klasifikacija zahteva po Davis-u

Davis [49] razmatra nefunkcionalne zahteve kao *non-behavioral* zahteve i identifikuje sedam kvaliteta. Non-behavioral zahtevi određuju kvalitet proizvoda i kao takvi su dobra osnova za testiranje gotovog proizvoda.

3.3.2. Klasifikacija zahteva po standardu IEEE 830-1998

IEEE standard “IEEE Std-830-1993” [50] i njegova revizija iz 1998. godine [51] su značajni primer pokušaja klasifikovanja i detaljnog opisa nefunkcionalnih zahteva. Takođe, ovi standardi uključuju i funkcionalne zahteve za razvoj softvera, kao i karakteristike koje treba ispuniti dobra softverska specifikacija zahteva.

Standard razmatra sledeće zahteve: zahteve za eksterni interfejs, funkcionalni zahteve, zahteve za perfomanse, za bazu podataka, za dizajn i za kvalitet sistema. Zahtevi za eksterni interfejs daju detaljan opis svih ulaza i izlaza softverskog sistema. Funkcionalni zahtevi treba da definišu osnovne radnje koje se moraju preduzeti u softveru pri prihvatanju i obradi ulaza, obradi i generisanju izlaza. Zahtevi za perfomanse navode statičke i dinamičke numeričke zahteve postavljene prema softveru ili prema ljudskoj interakciji sa softverom. Zahtevi za bazu podataka predstavljaju logičke zahteve za bilo koju informaciju koja se unosi u bazu podataka. Zahtevi za dizajnerska ograničenja određuju projektna ograničenja koja mogu nametnuti drugi standardi, hardverska ograničenja itd. Zahtevi za atribute sistema predstavljaju nefunkcionalne zahteve koji se odnose na kvalitet sistema (pouzdanost, raspoloživost, održivost, bezbednost, prenosivost,…).

3.3.3. Klasifikacija zahteva po Gilb-u

Gilb klasifikuje zahteve u sledeće kategorije: funkcionalnost (functions), kvalitet (qualities), troškovi (costs) i ograničenja (constraints) [52]. Kategorija zahteva funkcionalnost odnosi se na sve one specifikacije zahteva koje definišu šta sistem mora biti u stanju da uradi. U kategoriju kvalitet zahteva svrstavaju se specifikacije koje definišu koliko će se dobro izvršavati određena funkcionalnost. U kategoriju zahteva troškovi spadaju svi zahtevi koji se odnose na troškove (novac, kadar ili vreme) za stvaranje i održavanje funkcija i njihovog kvaliteta. Kategorija ograničenja odnosi se na zahteve ograničenja prema dizajnu ili funkcionalnosti.

3.3.4. Klasifikacija zahteva po Sommerville-u

Sommerville [53] u prvom nivou grupiše nefunkcionalne zahteve u zahteve proizvoda, organizacione zahteve (implementacije, standardi i zahtevi za isporuku) i spoljašnje zahteve.

Zahtevi proizvoda odnose se na moguće i željene osobine koje sistem treba da poseduje. Određuju ili ograničavaju ponašanje softvera. Uključuju zahteve performansi o tome koliko brzo sistem mora da se izvrši i koliko memorije mu je potrebno, zahteve pouzdanosti koji postavljaju prihvatljivu stopu grešaka, bezbednosne zahteve i zahteve upotrebljivosti.

Organizacioni zahtevi su izvedeni iz smernica i procedura organizacije zainteresovane strane i izvršioca posla (ko razvija i implementira sistem). Tu spadaju zahtevi operativnih procesa koji

definišu način na koji će se sistem koristiti, zahtevi razvojnog procesa koji određuju programski jezik, razvojno okruženje, kao i zahtevi za okruženje koji određuju operativno okruženje sistema.

Spoljašnji zahtevi su izvedeni iz spoljašnjih faktora koji utiču na sistem i razvojni proces. Može uključivati regulatorne zahteve koji određuju šta mora biti učinjeno da bi regulator odobrio sistem za upotrebu, zakonodavne zahteve koji se moraju poštovati kako bi se osiguralo funkcionisanje sistema u skladu sa zakonom i etičke zahteve koji garantuju da će sistem biti prihvatljiv za njegove korisnike i širu javnost.

3.3.5. Klasifikacija zahteva po Glinz-u

Glinz [54] predstavlja novo gledište koje prevazilazi nejasnoće tradicionalnih klasifikacija i grupiše zahteve prema četiri aspekta: vrsta, zadovoljstvo (satisfaction, sadržaj), zastupljenost (predstavljanje) i uloga.

Klasifikacija po vrsti odnosi se na zahteve koji opisuju zahtevanu funkcionalnost ili specificiraju zahtevano ponašanje perfomansu.

Zahtevi zastupljenosti odnose se na oblik njihovog predstavljanja kao operativnih ili kvantitativnih. Odnose se na to kako zahtev može biti verifikovan. Operativni zahtevi opisuju šta budući sistem treba da radi i proveravaju se pregledom, testiranjem ili formalnom verifikacijom. Zahtevi u pogledu performansi navode se u kvantitativnom obliku da bi bili precizni, nedvosmisleni i proverljivi. Kvantitativno određeni zahtevi se verifikuju merenjem.

Kada je reč o zadovoljenju zahteva, razlikuju se tvrdi i meki. Prilikom provere mora se utvrditi da li izabrano rešenje zadovoljava zahteve. Kada se ispituju kriterijumi koji se koristite za odlučivanje da li je zahtev zadovoljen, razmatraju se dva slučaja: zahtev je ili potpuno zadovoljen ili nije zadovoljen. Zahtevi ove vrste nazivaju se tvrdim. U drugom slučaju, zahtev se može delimično ispuniti, što znači da se stepen zadovoljstva meri na nekoj skali. U ovom slučaju govorimo o mekim zahtevima.

Klasifikacija prema ulozi razmatra tri uloge u specifikaciji zahteva. Prva uloga zahteva je da navodi svojstva budućeg sistema, druga uloga odnosi se na činjenice ili pravila u sistemskom

okruženju koja utiču na dizajn i implementaciju i treća uloga odnosi se na specificikaciju kako akter u sistemskom okruženju treba da se ponaša prilikom interakcije sa sistemom.

3.3.6. Klasifikacija zahteva po Lamsweerde -u

Lamsweerde klasifikuje nefunkcionalne zahteve u sledeće kategorije: zahtevi za kvalitet servisa, zahtevi za usklađenost sa normama, zahtevi za ograničenja arhitekture i zahtevi za ograničenja u razvoju [55].

Zahtevi za kvalitet servisa u ovoj klasifikaciji predstavljaju dodatna svojstva koja treba da ima funkcionalni deo softvera kao što su bezbednost, preformanse, raspoloživost, pouzdanost, tačnost, interfejs i drugi aspekti sistema koji utiču na kvalitet servisa (usluge).

Zahtevi usklađenosti propisuju da softverski efekti na okruženje budu u skladu sa nacionalnim zakonima, međunarodnim propisima, društvenim normama, kulturnim ili političkim ograničenjima i standardima.

Zahtevi za arhitekturu nameću strukturna ograničenja budućem softveru u skladu sa njegovim okruženjem. Obično su to ograničenja distribucije softverskih komponenti i ograničenja u instalaciji kako bi se osiguralo da će budući softver nesmetano raditi na ciljnoj platformi za implementaciju.

Zahtevi za razvoj određuju način razvoja softverskih proizvoda kako bi se zadovoljili funkcionalni zahtevi. U ovu kategoriju spadaju zahtevi troškova razvoja, rasporeda isporuke, promenljivosti karakteristika, održivosti, ponovnoj upotrebi, prenosivosti i slično.

3.3.7. Klasifikacija zahteva po Odeh -u

Klasifikaciona šema [56] inspirisana je Kotonia i Sommerville, ISO/IEC 9126 i Van Lamsveerde klasifikacijama nefunkcionalnih zahteva. Ova klasifikaciona šema zasniva se na inženjeringu usluga i softverskom inženjeringu orijentisanom na usluge kao dve različite kategorije na najvišem nivou klasifikacije iz kojih proizilaze dalje podklasifikacije.

Klasifikacija obuhvata zahteve koji su povezani sa željenim kvalitetom servisa, za razvojem proizvoda, za zakonskim regulativama i ograničenjima kao i zahteve kojima se ograničava arhitektura servisa.

Zahtevi koji su povezani sa kvalitetom servisa se odnose na željene karakteristike date usluge koja radi nezavisno, kao i kada su integrisane sa drugim servisima.

Zahtevi za razvoj odnose se na ograničenja u fazama procesa inženjeringa usluga, počevši od faze identifikacije, preko faze projektovanja i implementacije usluge i daljeg razvoja servisa.

Zahtevi povezani sa zakonskom regulativom i ograničenjima odnose se na standarde, zakone i pravila, organizacione propise, politička ograničenja itd. sa kojim razvijena usluga mora da bude u skladu.

Zahtevi kojima se ograničava arhitektura, odnose se na strukturna ograničenja u vezi sa dizajnom usluga, na primer, pridržavanje Erlovih principa servisno orjentisanog dizajna [57]: standardizovani ugovor o uslugama je princip koji obezbeđuje da svi servisi u jednom domenu budu u skladu sa istim standardima dizajna; princip slabog povezivanja podrazumeva da su usluge nezavisne tako da promene u jednoj usluzi neće uticati ni na jednu drugu; apstrakcija usluge je princip koji se odnosi na to da su informacije objavljene u ugovoru o uslugama ograničene na ono što je potrebno za efektivno korišćenje usluge; ponovna upotrebe usluge je princip koji se odnosi na kreiranje usluga koje se mogu ponovo koristiti u domenu; autonomija usluge je princip koji obezbeđuje usluge koje su nezavisne od okruženja izvršavanja; bezdržavnost usluge je princip dizajniranja skalabilnih servisa nezavisnih od podataka o stanju; otkrivljivost je stepen u kojem se nešto, posebno deo sadržaja ili informacija, može pronaći u pretrazi datoteke, baze podataka ili drugog informacionog sistema; ponovno korišćenje usluga je princip dizajna usluga koje se mogu ponovo koristiti u višestrukim rešenjima.

3.3.8. Klasifikacija zahteva po Comai-u

Kasifikaciona šema FOCUS-TBD (Functionality, Operativeness, Compliance, Usability, Security, Time, Budget, Documentation, Maintenance and Support) [58] sastoji se od osam kategorija: funkcionalni zahtevi, zahtevi operativnosti, saglasnosti, upotrebljivost, bezbednosti i

sigurnosti, vremenski zahtevi projekta, zahtevi za budžet projekta, za dokumentaciju, održavanje i podršku.

Funkcionalni zahtevi odnose se na to šta sistem treba da radi. Oni određuju koje funkcije sistem mora da obezbedi da bi zadovoljio navedene i podrazumevane potrebe zainteresovanih strana.

Zahtevi operativnosti odnose se na zahteve koje sistem treba da ispuni da bi pouzdano funkcionisao (raspoloživost, perfomanse, kapacitet, skalabilnost, prenosivost, instalacija) u cilju zadovoljenja potreba korisnika.

Zahtevi saglasnosti odnose se na poštovanje zakonske regulative, internih i eksternih standarda, poslovnih pravila, tehnologije, političkih i etičkih regulativa.

Zahtevi upotrebljivosti odnose se na zahteve okruženja u kome radi sistem, prilagođenosti korisnicima sa i bez invaliditeta, internacionalizacije sistema i posla, zahteve u vezi sa vremenom za učenje.

Zahtevi sigurnosti i bezbednosti su u vezi sa mogućim bezbednosnim efektima (gubitak i oštećenja), kontrolom pristupa, privatnošću privatnih i organizacionih podataka i integritetom podataka i sistema.

Vremenski zahtevi projekta odnosi se na zahteve ukupnog i etapnog trajanja projekta dok se zahtevi za budžet projekta odnose se na potrebna finansijska sredstva za realizaciju projekta.

3.3.9. Klasifikacija zahteva po standardu ISO/IEC 9126

Standard ISO/IEC 9126 je namenjen proceni kvaliteta softvera kroz klasifikaciju nefunkcionalnih zahteva. Klasifikacija nefunkcionalnih zahteva u ovom standardu obuhvata samo zahteve za softverski proizvod, a ne i zahteve za sistem u kome će funkcionisati softverski proizvod. Standard ISO 25010 [59] od 2011. godine zamenjuje gore navedeni standard, ali ni on ne obuhvata sve zahteve. Takođe, ne obuhvata funkcionalne zahteve, organizacione zahteve, zahteve za dokumentaciju, podršku, zakonske regulative. Ovaj standard klasifikuje nefunkcionalne zahteve u sledeće kategorije: funkcionalna podobnost, perfomanse, kompatibilnost, upotrebljivost, pouzdanost, bezbednost, održivost i prenosivost.

Funkcionalna podobnost predstavlja zahteve kojima se definiše stepen u kome proizvod ili sistem treba da pružaju funkcije koje zadovoljavaju navedene i podrazumevane potrebe kada se koriste pod određenim uslovima.

Zahtevi za perfomanse definišu koje perfomanse treba da ispunjava sistem u odnosu na količinu resursa koji se koriste pod navedenim uslovima.

Zahtevi za kompatibilnost definišu stepen do kojeg proizvod, sistem ili komponenta mogu razmenjivati informacije sa drugim proizvodima, sistemima ili komponentama i/ili obavljati potrebne funkcije dok dele isto hardversko ili softversko okruženje.

Zahtevi za upotrebljivost definišu stepen do kojeg određeni korisnici mogu da koriste proizvod ili sistem za efikasno postizanje određenih ciljeva u određenom kontekstu upotrebe.

Zahtevi za pouzdanost predstavljaju zahteve koji treba da omoguće da sistem, proizvod ili komponenta pouzdano obavlja određene funkcije pod određenim uslovima tokom određenog vremenskog perioda.

Zahtevi za bezbednost definišu kako proizvod ili sistem štiti informacije i podatke tako da osobe ili drugi proizvodi ili sistemi imaju stepen pristupa podacima koji odgovara njihovim vrstama i nivoima ovlašćenja.

Zahtevi za održivost definišu kako se proizvod ili sistem mogu modifikovati da bi se poboljšali, ispravili ili prilagodili promenama u okruženju i zahtevima.

Kategorija zahteva prenosivosti obuhvata zahteve koji određuju kako se sistem, proizvod ili komponenta mogu preneti iz jednog hardvera, softvera ili drugog operativnog ili upotrebnog okruženja u drugo.

3.3.10. Klasifikacija zahteva po Elese-u

FURPS je akronim koji predstavlja model za klasifikovanje kvaliteta osobina softvera, odnosno za klasifikovanje nefunkcionalnih zahteva. Ovaj model razvio je Robert Grady [60]. Znak +

dodat je kasnije tako da od tada FURPS+ predstavlja proširenu akronim koji ističe sledeće osobine [61]: funkcionalnost (functionality), upotrebljivost (usability), pouzdanost (reliability), perfomanse (perfomance) i podržanost (supportability), zahtevi za projektovanje, za implementaciju, za interfejs i fizički zahtevi. Funkcionalni zahtevi generalno predstavljaju karakteristike sistema.

Zahtevi za upotrebljivost se odnose na zahteve prema estetici i doslednosti u korisničkom interfejsu. Zahtevi za pouzdanost obuhvataju dostupnost, tačnost proračuna sistema i sposobnost sistema da se oporavi od kvara.

Zahtevi za performanse se odnose na propusnost, vreme odziva, oporavka, pokretanja i isključivanja. Zahtevi za podršku definišu testiranje, prilagodljivost, održavanje, kompatibilnost, konfigurabilnost, instalabilnost, skalabilnost i lokalizaciju.

Zahtevi za projektovanje određuju ograničenja dizajna, specificiraju ili ograničavaju opcije za projektovanje sistema. Zahtevi za implementaciju specificiraju ili ograničavaju kodiranje ili konstrukciju sistema.

Zahtevi za interfejs definišu spoljašnjost sa kojom sistem mora da stupi u interakciju, ili ograničenja u formatima ili drugim faktorima koji se koriste u okviru takve interakcije. Fizički zahtev specificira fizičko ograničenje koje se nameće sistemskom hardveru.

3.3.11. Klasifikacija zahteva po Roman-u

Postoje i druge klasifikacione šeme zasnovane na zahtevima za interfejs (interface), perfomanse (perfomance), operativnim zahtevima (operating), životnim ciklusom zahteva (lifecycle), političkim i ekonomskim zahtevima (political, economic) [62].

3.3.12. Klasifikacija zahteva po Shukla

Shukla [63] izdvaja sledećih vrste zahteva: poslovni, korisnički, sistemski i funkcionalni.

Sistemski zahtevi ili zahtevi rešenja definišu šta programeri koriste za konstruisanje sistema i šta sistem treba da radi. Poslovni zahtevi opisuju benifite koje treba da dobije organizacija ili njeni klijenti uvođenjem proizvoda.

Korisnički zahtevi opisuju potrebe korisnika u radu sa sistemom, dok funkcionalni zahtevi određuju šta će sistem raditi.

3.3.13. Klasifikacija zahteva po Internacionalnom institutu za poslovnu analizu

Jednu od najpoznatih klasifikacionih šema dao je IIBA u BABOK® Guide [33], a sastoji se od četiri vrste zahteva: poslovni (business requirements), zahtevi zainteresovanih strana (stakeholder requirements), zahtevi za proizvodom (zahtevi rešenja) i tranzicioni zahtevi. Poslovni zahtevi predstavljaju poslovne ciljeve koje navodi kupac. Mogu se primeniti na celo preduzeće, poslovnu oblast ili posebnu inicijativu. Ovi zahtevi predstavljaju izjave o ciljevima, ciljeve i ishode koji opisuju zašto je potrebno da dođe do promene. Poslovni zahtevi ne uključuju detalje o korisničkom interfejsu ili poslovnim pravilima.

Zahtevi zainteresovanih strana su zahtevi pojedinačnih zainteresovanih strana. Opisuju koje potrebe zainteresovanih strana moraju biti zadovoljene da bi se ispunili poslovni zahtevi. Mogu poslužiti kao most između zahteva poslovanja i zahteva za proizvod. Zainteresovane strane mogu prema svojim potrebama definisati zahteve specifične za projekat (odeljenje ili poslovna jedinica koju predstavljaju).

Zahtevi za proizvod predstavljaju svojstva i karakteristike koji se očekuju od razvijene softverske aplikacije. Ovi zahtevi opisuju sposobnosti i kvalitete rešenja koja ispunjavaju zahteve zainteresovanih strana. Pružaju odgovarajući nivo detalja koji omogućava razvoj i implementaciju rešenja. Zahtevi rešenja mogu se podeliti u dve potkategorije: funkcionalni i nefunkcionalni ili zahtevi kvaliteta usluga.

Tranzicioni zahtevi su potrebni za uspešnu implementaciju softverske aplikacije. Opisuju sposobnosti koje rešenje mora imati i uslove koje mora da ispuni kako bi se olakšao prelazak iz trenutnog u buduće stanje, ali koji nisu potrebni kada je promena potpuna. Razlikuju se od drugih vrsta zahteva jer su privremene prirode. Zahtevi za tranziciju obrađuju teme kao što su konverzija podataka, obuka i kontinuitet poslovanja.

3.3.14. Klasifikacija zahteva po Adams-u

Adams MacG. [64] se bavi širokim spektrom nefunkcionalnih zahteva i opisuje brojne taksonomije koje su korišćene za njihovo opisivanje.

Predstavlja nominalnu taksonomiju ili okvir za razumevanje nefunkcionalnih zahteva i njihovu ulogu kao deo svakog poduhvata u dizajnu sistema. Ova taksonomija ima 27 nefunkcionalnih zahteva razvrstanih u četiri kategorije: održivost, dizajn, adaptacija i sposobnost za funkcionisanje.

3.3.15. Klasifikacije bezbednosnih zahteva

Model CIA triada daje najosnovniju kalasifikaciju zahteva bezbednosti i to na: poverljivost, integritet i raspoloživost (confidentality, integrity, availability), dok Parker [65] ovu klasifikaciju poširuje sa dodatna tri zahteva: posedovanje, autentičnost i korisnost. U radu [66] se uvode novi zahtevi (pravična razmena, siguran protok informacija i zaštićen pristup) u klasifikaciju, a izostavljaju se osnovni zahtevi obuhvaćeni prethodnim klasifikacijama. U klasifikaciji zahteva bezbednosti [67] se više zahteva iz prethodnih klasifikacija integriše u jedan zahtev i uvode se novi zahtevi (praćenje bezbednosti i fizička zaštita). Klasifikacione šeme [68, 69, 70] uvode drugi nivo kategorije zahteva bezbednosti zasnovanih na kombinaciji drugih predloženih šema. Prvi nivo klasifikacije uglavnom obuhvata osnovne zahteve bezbednosti.

3.4. Analiza klasifikacionih šema i taksanomija zahteva

Kriterijumi na osnovu kojih je izvršena komparativna analiza klasifikacionih šema i taksanomija zahteva su:

- Sveobuhvatnost – podrazumeva da se klasifikaciona šema odnosi na široki spektar kategorija zahteva koji nisu samo nefunkcionalni i da obuhvata kategorije zahteva koji ne samo da definišu proizvod nego i sve neophodno za proizvod pre, za vreme i posle njegovog uvođenja.
- Sistematičnost – klasifikaciona šema je organizovana tako da potkategorije dobro oslikavaju kategoriju iz koje su proizašle. Kategorije i zahtevi su opisani.

- Jednostavnost – klasifikaciona šema je lako razumljiva i jednostavno se koristi za razotkrivanje i definisanje zahteva.
- Primenjivost – u kolikom delu se klasifikaciona šema možu primeniti za razotkrivanje i definisanje zahteva za PKI.
- Univerzalnost – primenjivost klasifikacione šeme za azotkrivanje i definisanje zahteva u raznim sistemima.
- Jasnoća (razumljivost) – klasifikaciona šema raspolaže jasnim zahtevima ili jasnim kategorijama zahteva.

Vrednosti koje poprimaju kriterijumi:

Sveobuhvatnost:

- Mala – klasifikaciona šema se odnosi na mali broj kategorija zahteva. Uglavnom obuhvata hardverske i softverske zahteve ili se odnosi na kvalitativne zahteve.
- Srednja – klasifikaciona šema obuhvata i druge kategorije zahteva, osim hardverskih i softverskih na prvom nivou i ima uglavnom dubinu dva nivoa zahteva.
- Velika - klasifikaciona šema obuhvata različite kategorije zahteva i dobro je razgranata u dubinu, najmanja tri nivoa, zahtevi su detaljno opisani.

Sistematičnost:

- Mala – klasifikaciona šema je slabo organizovana sa malim brojem kategorija zahteva.
- Srednja – klasifikaciona šema je dobro organizovana i daje dobar radni okvir za druge oblasti. Lako se ostvaruje uvid u kategorije zahteva i zahteve u većem delu klasifikacije. Zahtevi su kratko opisani.
- Velika – Dobro organizovana klasifikacija koja omogućuje jednostavan uvid u radni okvir u svim oblastima. Zahtevi su dobro opisani.

Jednostavnost:

- Mala – klasifikaciona šema je nejasna, nedorečena i teško se može primeniti za razotkrivanje i definisanje zahteva.
- Srednja – neke kategorije klasifikacione šeme su jednostavno opisane i mogu se primeniti za razotkrivanje zahteva.
- Velika – Klasifikaciona šema se može u većini kategorija i potkategorija primeniti za razotkrivanje i definisanje zahteva.

Primenjivost:

- Mala – klasifikaciona šema se manjim delom može primeniti za PKI. Obuhvata samo osnovne kategorije zahteva.

- Srednja – klasifikaciona šema se delimično može primeniti za PKI. U klasifikaciji postoje kategorije ili zahtevi koji se odnose na deo oblasti koju obuhvata PKI.
- Velika – većim delom se može primeniti za PKI.

Univerzalnost:

- Mala – klasifikaciona šema se ne može ili se manjim delom može primeniti i u drugim sistemima.
- Srednja – klasifikaciona šema se većim brojem zahteva, od kojih je većina nefunkcionalnih, može primeniti u drugim sistemima.
- Velika – klasifikaciona šema pored većine nefunkcionalnih zahteva ima i druge zahteve koji se takođe mogu primeniti za druge sisteme.

Jasnoća

- Mala – većina kategorija zahteva i zahtevi nisu jasno opisani.
- Srednja – manji broj kategorija zahteva i zahtevi nisu jasno opisani.
- Velika – veliki broj zahteva i kategorija i zahtevi su jasno opisani.

Poređenje klasifikacionih šema na osnovu izabranih kriterijuma prikazano je u Tabeli 2.

Tabela 2. Poređenje klasifikacionih šema na osnovu izabranih kriterijuma

Klasifika-ciona šema	Sveobu-hvatnost	Sistemati-čnost	Jednosta-vnost	Primenji-vost	Univerza-lnost	Jasnoća
IEEE 830-1998	Srednja (6)	Srednja (5)	Velika (9)	Srednja (5)	Srednja (5)	Srednja (4)
Gilb	Mala(1)	Mala (1)	Mala (1)	Mala (2)	Mala (1)	Mala (1)
Sommerville	Srednja (5)	Srednja (6)	Mala (3)	Velika (7)	Velika (7)	Mala (3)
Glinz	Mala (1)	Mala (1)	Mala (1)	Mala (3)	Velika (7)	Srednja (4)
Lamsweerde	Srednja (6)	Srednja (6)	Velika (7)	Velika (8)	Velika (7)	Velika (8)
Odeh	Srednja (6)	Srednje (4)	Srednja (4)	Srednja (6)	Velika (7)	Mala (2)
FOCUS-TBD	Velika (9)	Velika (8)	Velika (8)	Velika (8)	Velika (8)	Velika (8)
ISO/IEC 9126	Mala (3)	Srednja (6)	Velika (7)	Srednja (5)	Velika (8)	Velika (8)
FURPS+	Mala (3)	Srednja (5)	Velika (7)	Srednja (5)	Srednja (6)	Velika (8)
Roman	Srednja (4)	Srednja (4)	Srednja (5)	Mala (3)	Mala (3)	Mala (3)
Shukla	Mala (1)	Mala (1)	Mala (1)	Mala (2)	Mala (2)	Mala (1)
BABOK	Mala (3)	Mala (2)	Mala (2)	Mala (1)	Mala (3)	Mala (1)
Adams MacG.	Mala (2)	Velika (7)	Velika (8)	Srednja (6)	Srednja (6)	Velika (7)

3.4.1. Analiza klasifikacionih šema na osnovu kriterijuma sveobuhvatnosti

Klasifikacione šeme Gilb (M1), Shukla (M1), Glinz (M1), Adams (M2) i BABOK (M3) ne obuhvataju široki spektar kategorija i ne razvijaju se po dubini. Obično imaju prvi nivo klasifikovanja. Klasifikaciona šema ISO/IEC 9126 (M3) obuhvata nefunkcionalne zahteve koji se odnose na softverski proizvod i određuje dva nivoa klasifikacije, dok klasifikacija FURPS+ (M3) takođe klasifikuje nefunkcionalne zahteve, ali samo na prvom nivou klasifikovanja.

Glinz (M1) klasifikaciona šema ima drugačiji pristup nego ostale klasifikacione šeme, a definisana je tako da zahtev dobija po jednu vrednost iz svakog od četiri aspekta. Ova klasifikacija ne prikazuje različite kategorije zahteva.

Klasifikacione šeme čija je sveobuhvatnost srednje određena generalno obuhvataju širu kategoriju zahteva. Osim nefunkcionalnih zahteva, Roman (S4) razmatraju zahteve za organizaciju, regulativu i bezbednost (Sommervile (S6)), norme i standarde, ograničenja u skladu sa okruženjem, zahteve za vreme uvođenja sistema (Lamsweerde (S6)), ekonomske aspekte i održavanje (Odeh (S6)). U ovoj kategoriji se izdvaja IEEE klasifikaciona šema (S6) koja detaljno opisuje i dekomponuje zahteve koji se odnose na softver.

FOCUS-TBD (V9) klasifikaciona šema obuhvata različite kategorije zahteva i dobro je razgranata po horizontali i dubini. Zbog ovih osobina je kategorisana kao klasifikaciona šema koja ima veliku sveobuhvatnost.

3.4.2. Analiza klasifikacionih šema na osnovu kriterijuma sistematičnosti

Klasifikacione šeme (Glinz (M1), Shukla (M1), Gilb (M1), BABOK (M2)) nisu dovoljno sistematične za primenu u razotkrivanju i definisanju zahteva jer imaju samo jedan nivo klasifikacije koji je uopšten. Glinz klasifikacija ima četiri kategorije sa atributima koje zahtev može imati, odnosno zahtev pripada svakoj kategoriji iz koje mu je dodeljen odgovarajući atribut. Ova klasifikacija nema uticaja na razotkrivanje zahteva, nego već definisane zahteve svrstava u određenu kategoriju. Sistematičnost joj se ogleda u tačno definisanom postupku određivanja vrednosti svakog aspekta.

Klasifikacione šeme (Sommerville (S6), IEEE (S5), Lamsweerde (S6), Odeh (S4), Roman (S4), ISO/IEC 9126 (S6), FURPS+ (S5)) su dobro organizovane i sistematične pri razotkrivanju i definisanju zahteva. Kod ovih šema zahtevi su kratko i jasno opisani i pružaju dobar rani okvir. U ovoj kategoriji mogu se izdvojiti klasifikacije (Lamsweerde (S6), FURPS+ (S5), ISO/IEC 9126 (S6)) koje se ne zadržavaju samo na opisu zahteva na višim nivoima, nego opisuju zahteve i po dubini klasifikacije.

Klasifikacione šeme (FOCUS-TBD (V8), Adams (V7)) su dobro organizovane, sistematične i daju jasan okvir za razotkrivanje i definisanje zahteva. Zahtevi su jasno opisani kroz sve nivoe klasifikacije i dati su primeri iz prakse.

3.4.3. Analiza klasifikacionih šema na osnovu kriterijuma jednostavnosti

Klasifikacione šeme nije lako primeniti u razotkrivanju i definisanju zahteva jer su nejasne, nedorečene (Gilb (M1), Shukla (M1)) ili ne opisuje pojedinačne kategorije i zahteve (ne daju smernice i radni okvir) (Sommerville (M3), BABOK (M2)) ili su zasnovane na drugačijem principu kao Glinz (M1) gde je prvo potrebno definisati zahtev, pa ga potom klasifikovati shodno aspektima.

Klasifikacione šeme Roman (S5) i Odeh (S4) kratko opisuju osnovnu kategoriju zahteva na prvom nivou, a ostali zahtevi nisu opisani, što predstavlja nejasnoću u daljoj primeni klasifikacije. Stoga su ove klasifikacije svrstane u srednje jednostavne za razotkrivanje i definisanje zahteva.

Klasifikacione šeme koje su najjednostavnije za razotkrivanje i definisanje zahteva, odnosno koje daju najbolji radni okvir su IEEE (V9), FOCUS-TBD (V8), Adams (V8) jer su jednostavno opisane, dobro razumljive, daju smernice za definisanje zahteva. Klasifikacione šeme Lamsweerde (V7), ISO/IEC 9126 (V7), FURPS+ (V7) u većini kategorija se mogu primeniti za razotkrivanje zahteva. Zahtevi su opisani i kao takvi daju dodatno pojašnjenje.

3.4.4. Analiza klasifikacionih šema na osnovu kriterijuma primenjivosti

Klasifikacione šeme Roman (M3), Shukla (M2), Gilb (M2), BABOK (M1) i Glinz (M3) se malim delom mogu primeniti u razotkrivanju i definisanju zahteva za PKI zato što su previše uopštene. Glinz (M3) klasifikaciona šema je primenjiva za PKI, ali ne u kontekstu radnog okvira za razotkrivanje i definisanje zahteva nego za naknadno klasifikovanje zahteva, kada je već definisan.

Generalni nefunkcionalni zahtevi iz klasifikacionih šema (IEEE (S6), Adams S(6), ISO/IEC 9126 (S5)) koji se odnose na softverski proizvod ili klasifikacije (Odeh (S6), FURPS+ (S5)) koje imaju druge kategorije i zahteve pogodne za deo oblasti PKI, kao što je održavanje ili regulativa, mogu se primeniti u razotkrivanju i definisanju zahteva za PKI.

Klasifikacione šeme koje se najvećim delom mogu primeniti, odnosno mogu da obuhvate najveći deo zahteva u odnosu na ostale šeme su: Sommerville (V7), Lamsweerde (V8) i FOCUS-TBD (V8) jer osim nefunkcionalnih zahteva obuhvataju i zahteve koji su bitni za uspostavu PKI kao što su održavanje, regulativa, budžet, bezbednost.

3.4.5. Analiza klasifikacionih šema na osnovu kriterijuma univerzalnosti

Klasifikacione šeme Roman (M3), Shukla (M2), BABOK (M3) i Gilb (M1) mogu se primeniti u potpunosti u drugim sistemima jer su dovoljno opšte, ali kriterijum univerzalnost za njih je procenjena kao mali jer se ne mogu meriti po ovom kriterijumu sa složenijim klasifikacijama.

Adams (S6), IEEE (S5) i FURPS+ (S6) klasifikacione šeme imaju vrednost srednja za parametar univerzalan, jer se nefunkcionalni zahtevi mogu primeniti i u drugim sistemima, kao i funkcionalna specifikacija koja daje radni okvir za razotkrivanje i definisanje funkcionalnih zahteva u drugim sistemima.

Veliku univerzalnost imaju klasifikacione šeme Sommerville (V7), Lamsweerde (V7), Odeh (V7), FOCUS-TBD (V8), ISO/IEC 9126 (V8) jer pored većine nefunkcionalnih zahteva imaju i druge zahteve koji se takođe mogu primeniti za druge sisteme.

Karakteristična je klasifikaciona šema Glinz (V7) jer se može primeniti za klasifikovanje svakog zahteva iz svih sistema.

3.4.6. Analiza klasifikacionih šema na osnovu kriterijuma jasnoće

Klasifikacionim šemama Gilb (M1), Sommerville (M3), Odeh (M2), Roman (M3), BABOK (M1), Shukla (M1) data je ocena da je jasnoća mala jer kategorije zahteva nisu dovoljno opisane, a za klasifikacije sa zahtevima nema objašnjenja. Stoga ove klasifikacije namaju dovoljnu jasnoću da mogu poslužiti za razotkrivanje i definisanje zahteva.

IEEE klasifikaciona šema (S4) ima jasnoću u opisivanju radnog okvira u kome je potrebno tražiti zahteve, kao i opis nefunkcionalnih zahteva. Nema grafički prikaz nego je pisana tekstualno po poglavljima što umanjuje njenu jasnoću. Glinz (S6) je jasna za primenu, ali neupotrebljiva za potrebe definisanja zahteva kao radni okvir.

Klasifikacione šeme Lamsweerde (V8), FOCUS-TBD (V8), ISO/IEC 9126 (V8), FURPS+ (V7), Adams (V7) odlikuju se velikom jasnoćom jer su zahtevi jasno opisani i imaju smernice za razotkrivanje i definisanje zahteva.

4. Klasifikaciona šema zahteva za PKI

Pored tipičnih situacija [71] koje mogu omesti ili na drugi način uticati na proces razotkrivanja zahteva, autori izdvajaju značaj postojanja domena u kojem će se razotkrivati zahtevi. To podrazumeva postojanje klasifikacione šeme zahteva koja prestavlja granice domena u okviru kojih će menadžeri organizacije i tim za razotkrivanje i definisanje zahteva realizovati svoje zadatke.

Uspešno funkcionisanje PKI zavisi od međusobne interakcije komponenti, hardversko softverskih elemenata i ljudskih resursa u ostvarivanju predviđenog i željenog ponašanja. Preduslov za uspešno funkcionisanje PKI je postojanje dobro ustanovljenih i definisanih zahteva, počev od poslovno-organizacionih zahteva i zahteva za osnovnu finkcionalnost PKI, preko zahteva za održavanje, obuku, do tranzicionih zahteva za buduće unapređenje PKI.

Svrha klasifikacione šeme zahteva za PKI je obezbeđivanje korisnog i konzistentnog načina klasifikovanja zahteva sa ciljem sprečavanja pojave grešaka u njihovom razotkrivanju i definisanju. U literaturi su uglavnom opisani nefunkcionalni zahtevi za razvoj softvera, ali ne i zahtevi za PKI. Organizacije koja imaju potrebu za PKI, kao i one koje se bave razvojem PKI, mogu doći u konfuziju pri pokušaju definisanja potrebnih zahteva. Predložena klasifikacija zahteva za PKI je pokušaj da se ponudi takva klasifikacija koju će moći da koriste organizacije koje imaju nameru da uvedu PKI u svoje poslovanje, kao i organizacije koje se bave razvojem i implementacijom PKI. Predložena klasifikaciona šema ima za cilj da kreira kategorije zahteva koje treba da omoguće brže i lakše razotkrivanje i definisanje zahteva za PKI i tako otklone konfuziju u radu tima.

Drugi cilj predložene klasifikacione šeme je da se obezbedi takva klasifikacija PKI zahteva koja se ne odnosi samo na funkcionalne i nefunkcionalne zahteve vezane za razvoj softvera za PKI, već da se obuhvate i drugi zahtevi kao što su: poslovni zahtevi, zahtevi za održavanje, za primenu i poštovanje standarda i zakonskih regulativa i tranzicioni zahtevi. Ovakva klasifikacija nije ranije predložena, već se postojeće klasifikacione šeme ili taksonomije fokusiraju samo na poslovne ili IT zahteve iskazane kroz nefunkcionalne zahteve.

Predložena klasifikaciona šema ima za cilj da obezbedi, pored usmerenja za definisanje kvalitetnih i racionalnih zahteva, dobru i sveobuhvatnu osnovu za testiranje, verifikaciju i

validaciju gotovog proizvoda PKI. Ranije klasifikacione šeme i taksonomije, obzirom da su se odnosile na nefunkcionalne IT zahteve, mogu se u manjoj meri iskoristiti za testiranje i validaciju PKI.

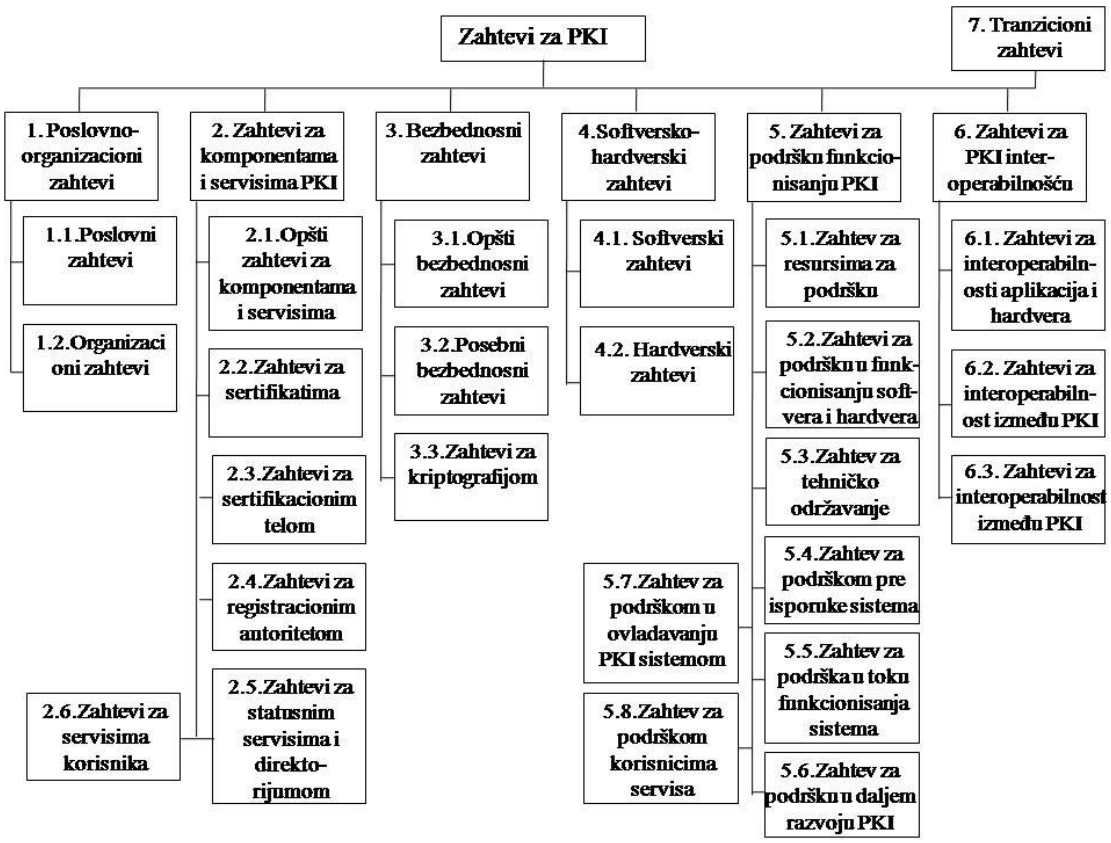
Definisanje zahteva za poslovno-informacione sisteme ne obuhvata samo definisanje zahteva za razvoj softvera, već i poslovnih, organizacionih, tehničkih, zahteva za obukom i za zakonskim regulativama. Ovakav pristup u definisanju zahteva omogućava da se sagledaju zahtevi od priprema za razotkrivanje do stavljanja proizvoda u funkciju i njegovo korišćenje.

Klasifikaciona šema zahteva za PKI izrađena je na osnovu analize sadržaja postojećih klasifikacija zahteva i prezentovana je u radu [72]. Ova klasifikaciona šema proširena je kategorijom zahteva za interoperabilnost PKI. Klasifikaciona šema prezentovana u ovom radu sastoji se od sedam glavnih kategorija zahteva:

- **Poslovno-organizacioni zahtevi.** Poslovni zahtevi za PKI organizacije moraju da poboljšaju stepen zaštite poslovnih informacija u elektronskom poslovanju. Organizacioni zahtevi za PKI pripremaju organizaciju, menadžment i zaposlene za PKI sistem kroz sve faze uvođenja PKI sistema.
- **Zahtevi za komponente i servise PKI.** Ovi zahtevi opisuju željeno ponašanje i osobine koje treba da ima PKI, a u skladu sa poslovnim zahtevima. Opisuju mogućnosti softverskog rešenja PKI koje će imati u eksploataciji, odnosno njegova ponašanja i izvršavanja kroz akcije i odgovore.
- **Hardversko-softverski zahtevi.** Ovi zahtevi opisuju kako pojedini softverski proizvodi u PKI sistemu treba da se ponašaju. Hardverskim zahtevima definisani su standardi i uslovi koje hardver mora da zadovolji kako bi se brzo i pouzdano izvršavao softver PKI sistema.
- **Bezbednosni zahtevi.** Bezbednosnim zahtevima definiše se bezbednost celog PKI sistema, a definišu se tako da se njihovim ispunjenjem dostignu bezbednosne osobine celokupnog PKI sistema.
- **Zahtevi za podršku u funkcionisanju.** Oni treba da obezbede podršku u radu svih komponenti svim korisnicima u PKI sistemu. Podrška funkcionisanju mora biti dobro definisana da ne bi došlo do zastoja u radu servisa i komponenti PKI, bilo iz funkcionalnih razloga ili neznanja korisnika.

- **Zahtevi za interoperabilnost.** Ovi zahtevi treba da obezbede neometano funkcionisanje hardvera i aplikacija, kao i komponenti i servisa PKI. Osim toga, treba da definišu saradnju između više domena PKI.
- **Tranzicioni zahtevi.** Ovi zahtevi nastaju u svim fazama analize PKI zahteva. Oni daju dodatni kavalitet PKI sistemu koji nije primećen u fazi razotkrivanja zahteva, već u drugim fazama izgradnje PKI sistema.

Predložena klasifikaciona šema prikazana je na slici 7.



Slika 7. Klasifikaciona šema za PKI zahteve

Navedene kategorije PKI zahteva dele se u potkategorije opisane u nastavku rada.

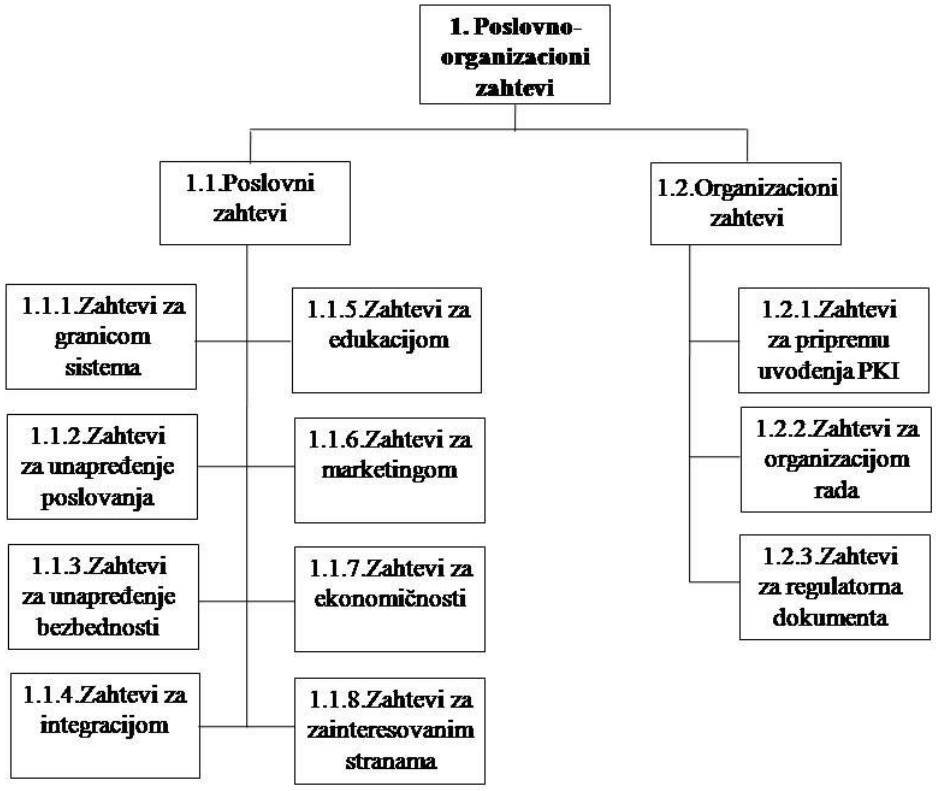
4.1. Poslovno-organizacioni zahtevi

Ova vrsta zahteva treba da omogući plansko uvođenje PKI u organizaciju uz optimalno korišćenje resursa. Potrebno ih je tako definisati da uvođenje nove tehnologije ne dovede do udaljavanja od poslovnih ciljeva organizacije, odnosno gubitka reputacije, partnera, kadra i finasijskih sredstava. Klasifikacija poslovno-organizacionih zahteva prikazana je na slici 8.

4.1.1. Poslovni zahtevi

Poslovni zahtevi za PKI treba da definišu poslovne potrebe za PKI i kriterijume za uspeh poslovanja PKI. Ovi zahtevi opisuju zašto je PKI potreban, kome će koristiti, kada i gde će se odvijati i koji standardi će se koristiti za njegovu procenu. Međutim, ne definišu način na koji će se projekat sprovesti i ne obuhvataju detalje njegove implementacije.

Poslovni zahtevi za PKI treba da podrže i omoguće ostvarivanje poslovnih ciljeva kroz bezbednost informacija u elektronskom poslovanju. Ova vrsta bezbednosti daje dodatni kvalitet organizaciji u elektronskom poslovanju i prednost nad konkurencijom. Poslovni zahtevi se razmatraju kroz sledeće potkategorije zahteva: granice PKI sistema, unapređenje poslovanja, unapređenje bezbednosti, marketing, ekonomičnost, integracija sa drugim PKI, edukacija, izbor stakeholdera, pravila, politike i regulative.



Slika 8. Klasifikacija poslovno-organizacionih zahteva

Zahtevi za granicu PKI. Ovi zahtevi treba da odrede šta PKI sistem treba da obuhvati i da definišu granice PKI proizvoda u elektronskom poslovanju. Isto tako, treba da odrede da li se usluge PKI koriste samo interno ili ih mogu koristiti i spoljašnji korisnici. Granice treba odrediti

shodno internom ili spoljašnjem okruženju, uslugama koje PKI treba da pruži i potrebama elektronskog poslovanja.

Zahtevi za unapređenje poslovanja. Ova vrsta zahteva treba da odredi koja funkcionalnost PKI unapređuje poslovanje unutar organizacije ili sa drugim poslovnim subjektima, kao i koliki će uticaj imati uvođenje novih funkcionalnosti na reorganizaciju. Potrebno ih je definisati tako da uvođenje nove tehnologije u što manjoj meri utiče na kvalitet funkcionisanja postojećih aplikacija i na prilagođavanje zaposlenih i korisnika.

Zahtevi za unapređenje bezbednosti. Zahtevi za unapređenje bezbednosti treba da odrede koja unapređenja PKI podižu nivo bezbednosti poslovnih informacija i u kojoj meri. Ova vrsta zahteva će se odrediti kroz sagledavanje potencijalnog rizika u postojećim aplikacijama od krađe identiteta, stepena rizika neprimenjivanja PKI tehnologije i složenosti u njenom implementiranju.

Zahtevi za marketing. Zahtevi za marketing treba da definišu kakav novi kvalitet u poslovanju organizacija treba da se ostvari kroz uvođenje PKI, a kako bi se zadobila bolja pozicija u odnosu na konkurenciju.

Zahtevi za ekonomičnost. Ova vrsta zahteva treba da odredi u kojoj meri je uvođenja PKI tehnologije ekonomično, kao i kako će uticati na elektronsku poslovnu strategiju.

Zahtevi za integraciju. Zahtevi za integraciju treba da odrede način poslovanja sa drugim kompanijama koje imaju drugačije bezbednosne politike, kao i ostvarenje poslovanja sa organizacijama koje već imaju svoju PKI.

Zahtevi za edukaciju. Treba da odrede profil korisnika koje je potrebno edukovati i sadržaj edukacije. Cilj ovog zahteva je razvoj svesnosti i potrebe za PKI, upoznavanje zaposlenih sa uticajem uvođenje PKI na postojeće poslovne funkcije i dobit od uvođenja PKI.

Zahtevi za zainteresovane strane. Ovi zahtevi određuje skup elementata koje je potrebno sagledati prilikom izbora prodavca PKI arhitekture. Neki od tih elemenata su: reference koje ima prodavac u poslu implementacije PKI arhitekture, njegova povezanost sa drugim softverskim kompanijama, fleksibilnost i potrebno vreme za implementaciju, iskustvo njegovih klijenata, udeo koji zauzima na tržištu i koliko je spreman na dalju saradnju posle implementacije.

4.1.2. Organizacioni zahtevi

Organizacioni zahtevi treba da pomognu u stvaranju sistema koji podržava struktura menadžmenta u organizaciji u svim fazama uvođenja PKI. Dobra organizacija treba da omogući racionalno korišćenje resursa, dobru komunikaciju, sigurno dovođenje projekta do cilja, stvaranje pozitivnog i motivisanog radnog okruženja, unapređenje i razvoj novih veština, sprečavanje haosa i kašnjenje. Ukoliko organizacija uvodi PKI sistem koji će organizaciono biti njen sastavni deo onda je potrebno definisati organizacionu strukturu i radna mesta u skladu sa regulativom za PKI. Organizacioni zahtevi za PKI razmatraju se kroz sledeće potkategorije: zahtevi za pripremu uvođenja PKI, zahtevi za organizaciju rada i zahtevi za regulatorna dokumenta.

Zahtevi za pripremu uvođenja PKI. Ova vrsta zahteva treba da odredi koje aktivnosti treba sprovesti da bi se organizacija pravovremeno pripremila za uvođenje PKI. Ova priprema se razmatra kroz sledeće zahteve: zahtev za organizaciju ljudskih, materijalnih, finansijskih i vremenskih resursa, za organizaciju razvoja dokumentacije, za organizaciju bezbednosti i za organizaciju planiranja uspostave PKI.

Zahtevi za organizaciju razvoja dokumentacije treba da definišu koja dokumenta je potrebno doneti za funkcionisanje PKI. Pod ovim zahtevom se podrazumeva razvoj modela ugovora o pružanju usluge, politika sertifikacije praktičnih pravila rada, internih pravila rada, dokumenata kojim se reguliše postupanje korisnika i pružaoca usluge.

Zahtevi za planiranje i uspostavljanje PKI treba da definišu opšte uslove za pružanje usluga (obaveze korisnika, ograničenja usluga i odgovornosti, vremenski period čuvanja zapisa, pravni okvir, način rešavanja sporova i prigovora), korišćenje pouzdanih uređaja i proizvoda, čuvanje relevantnih informacija, osiguranje, postupanje u slučaju teških incidenata, čuvanje podataka i postupak kod prestanka rada.

Zahtevi za organizaciju bezbednosti odnose se na zahteve za redizajniranu bezbednost u organizaciji uvođenjem PKI i zahteve za bezbednost PKI (akt o informacionoj bezbednosti).

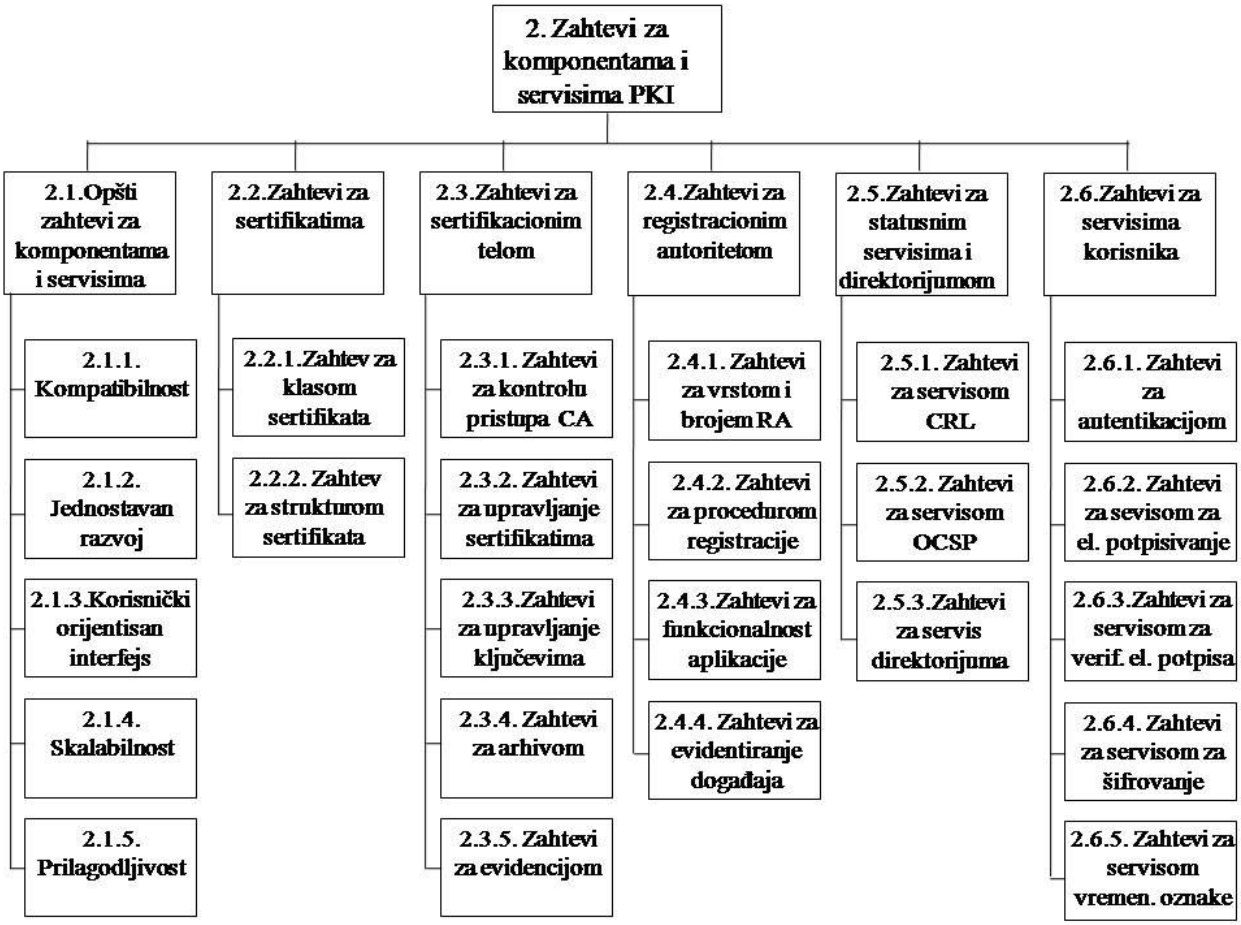
Zahtevi za organizaciju rada. Ova vrsta zahteva treba da omogući uspešno i optimalno funkcionisanje zaposlenih uz racionalno korišćenje resursa. Ovaj zahtev je složen i treba ga razmatrati kroz više faza uvođenja PKI, a treba da definiše organizaciju rada:

- u fazi razotkrivanja i definisanja zahteva gde treba formirati stručni tim, odrediti delokruge rada i odgovornosti, metodologiju rada, uspostaviti saradnju sa stakeholderom i odrediti plan aktivnosti za realizaciju zadatka;
- u fazi pripreme za uvođenje PKI treba planirati i organizovati edukaciju iz oblasti PKI, aktivnosti na uspostavi CA i RA i saradnju sa stakeholderom. U ovoj fazi treba da se odredi organizaciju rada u CA i RA kroz raspodelu posla (prihvatanje, unos i odobravanje zahteva za registraciju, kontrolu, distribuciju), vreme rada i određivanje lokacija CA i RA shodno geografskoj lokaciji korisnika;
- u fazi rada sertifikacionog tela kada treba obezbediti pouzdanu organizaciju rada kroz aktivnosti koje propiše zakonodavac ili u skladu sa međunarodnim preporukama ili standardima.

Zahtevi za regulatorna dokumenta. Ova vrsta zahteva treba da precizira koja regulatorna dokumenta će se poštovati prilikom uvođenja i funkcionisanja PKI, kao i koja lica moraju primenjivati i poštovati koja regulatorna dokumenta. Regulatorna dokumenta podrazumevaju dokumenta kojim organizacija uvodi PKI, uputstva i projektantsku dokumentaciju, CP, CPS [73], zakonske regulative, standarde, tehničke specifikacije i preporuke iz oblasti PKI.

4.2. Zahtevi za komponente i servise PKI

Zahtevi za komponente i servise PKI treba da odrede željenu funkcionalnost komponenti PKI. Ovi zahtevi razmatraju se po sledećim potkategorijama: opšti zahtevi za PKI, zahtevi za sertifikat, za CA, za RA, za statusne servise i direktorijum i zahtevi za korisničke servise. Ovi zahtevi treda da definišu kako komponente PKI treba da funkcionišu. Funkcionalni i nefunkcionalni zahtevi se ne razdvajaju. Na slici 9. prikazana je klasifikacija zahteva za komponente i servise PKI.



Slika 9. Klasifikacija zahteva za PKI komponente i servise

4.2.1. Opšti zahtevi za komponente i servise PKI

Ovi zahtevi daju opštu sliku o tome šta komponente i servisi PKI treba da zadovolje. Kao što svaki proizvod prate zahtevi za kompatibilnost, jednostavni razvoj, korisnički orjentisani interfejs, fleksibilnost, skalabilnost i prilagodljivost tako i ovi zahtevi prate PKI proizvod.

Kompatibilnost. Komponente i servisi PKI treba da su kompatibilni sa najnovim uređajima i aplikacijama nezavisno od njihovog proizvođača, a izvršavanje nadogradnje softvera mora da bude moguće na postojećoj softverskoj (operativni sistem, sistemski i aplikativni softver) i hardverskoj platformi.

Jednostavan razvoj. Zahtev za PKI rešenje treba da je takav da se može dodatno prilagoditi potrebama korisnika. Posebnu pažnju u razvoju PKI proizvoda treba usmeriti na bezbednost PKI operacija.

Korisnički orijentisan interfejs. Ovaj zahtev treba da odredi interfejs prema korisniku koji je lako shvatljiv i jednostavan za korišćenje. Interfejs ne treba da ima više funkcionalnosti nego što je korisniku potrebno za korišćenje i rad. Korisnički interfejs treba da omogući upotrebu prečica, da korisniku pruži odgovore na sprovedene akcije, omogući prevenciju i rukovanje greškama, dozvoli poništavanje akcije, da ima internu kontrolu unetog sadržaja, smanjeno opterećenje radne memorije.

Skalabilnost. Skalabilnost PKI rešenja treba da odgovori svim postojećim i planiranim zahtevima za proširenje. Neki od zahteva za proširenje su: povećanje broja korisnika, povećanje broja zahteva za izdavanje i opoziv elektronskih sertifikata, uvođenje novih tipova sertifikata, uvođenje više sertifikacionih i registracionih tela, podrška novim uređajima i aplikacijama.

Prilagodljivost. Neki zahtevi za prilagođavanje su: upis sertifikata i privatnog ključa na više različitih medija, primena više algoritama za potpisivanje sertifikata, podrška za neograničen broj RA i CA, ažuriranje informacija o korisnicima i drugim registrovanim uređajima.

4.2.2. Zahtevi za sertifikate

Zahtev za sertifikate treba da odredi klasu sertifikata i namenu korišćenja, a potom da za izabranu vrste sertifikata definiše njihovu strukturu.

Zahtevi za klasu sertifikata. Klasa sertifikata podrazumeva određivanje kako će se sertifikat koristiti (npr. sertifikati za sertifikaciona tela, za korisnike i za resurse). Svaka klasa sertifikata ima svoju namenu (npr. autentikacija TLS/SSL, zaštita elektronske pošte, elektronsko potpisivanje, elektronski pečat, autentikacija veb sajtova) i dodeljuje joj se bezbednosni nivo. Elektronski sertifikat može biti običan i kvalifikovan na osnovu propisane regulative. Bezbednosni nivo sertifikata usklađuje se na osnovu zakonske regulative ili ga definiše organizacija.

Zahtevi za strukturu sertifikata. Ovi zahtevi se dele na opšte, za sve tipove sertifikata, i dodatne. Opšti zahtevi proizilaze iz namene sertifikata i njegove strukture [14]. Dodatni zahtevi odnose se na specifičnosti svake klase sertifikata i specifičnosti bezbednosnih nivoa kojima pripadaju sertifikati. Primer dodatnog zahteva je zahtev da sertifikat bude kvalifikovan [74, 75].

4.2.3. Zahtevi za sertifikaciono telo

Zahtevi za sertifikaciono telo treba da omoguće da sertifikaciono telo formira sertifikate shodno definisanim zahtevima za sertifikate, da upravlja sertifikatima i ključevima i drugim podacima neophodnim za njegovo funkcionisanje.

Razmatraju se kroz sledeće potkategorije zahteva: zahtevi za kontrolu pristupa sertifikacionom telu, za upravljanje sertifikatima, za upravljanje ključevima, za arhivom i za evidenciju.

Zahtevi za kontrolu pristupa sertifikacionom telu. Ova vrsta zahteva treba da obezbedi ograničen pristup sistemu sertifikacije i obuhvata: kontrolu na mrežnom nivou, pouzdan pristup osetljivim podacima, efikasnu i pouzdanu administraciju korisničkih pristupa, ograničenja pristupa informacijama i aplikativnim funkcijama, razdvajanje bezbednosnih funkcija, pouzdanu identifikaciju i autentikaciju, mrežne komponente i uređaje za generisanje ključeva, kontinuirani monitoring i nadgledanje, kontrolisan pristup aplikaciji za opoziv sertifikata i aplikaciji za distribuiciju sertifikata, kontrolisan pristup ključevima i podacima.

Zahtevi za upravljanje sertifikatima. Upravljanje sertifikatima predstavlja jednu od najvažnih funkcionalnosti sertifikacionog tela. Zahteve za upravljenje sertifikatima treba razmatrati kroz životni ciklus sertifikata: inicijalizacija, izdavanje (obnavljanje), distribucija, suspenzija, opoziv i arhiviranje sertifikata. Zahtevi za inicijalizaciju treba da definišu procedure i potrebne parametre registracionog autoriteta koji će inicirati generisanje sertifikata. Zahtevi za izdavanje sertifikata treba da omoguće izdavanje sertifikata u skladu sa namenom i uslovima koje treba da ispune. Zahtevi za obnavljanje sertifikata treba da odrede događaje koji prouzrokuju obnavljanje sertifikata i para asimetričnih ključeva. Zahtevi za distribuciju sertifikata treba da definišu način dostavljanja sertifikata do korisnika: da li se sertifikat dostavlja preko direktorijuma, nosioca sertifikata ili na neki drugi način. Zahtevi za opoziv i suspenziju sertifikata podrazumevaju određivanje procedure za podnošenje zahteva i događaja koji prouzrokuju ove aktivnosti.

Zahtevi za arhiviranje treba da odrede postupak i uslove za arhiviranje, kao i preuzimanje sertifikata iz arhive.

Zahtevi za upravljanje ključevima. Ovi zahtevi treba da odrede proceduru koja će generisati par ključeva odgovarajuće dužine odgovarajućim algoritmom, shodno definisanim profilima. Procedura generisanja para ključeva mora biti bezbedno povezana sa generisanjem sertifikata. Svakoj vrsti ključa dodeljuje se rok važnosti. Takođe, potrebno je definisati da li se par ključeva za jednu namenu može koristiti za više sertifikata. Potrebno je definisati proceduru bezbednog dostavljanja privatnog ključa i njegovu zaštitu aktivacionim kodom. Procedura preuzimanja ključa treba da omogući pristup ključu iz arhive na siguran i pouzdan način. Isto tako, treba definisati situacije i vreme kada je potrebno izdati nove ključeve u skladu sa njihovom namenom.

Zahtevi za arhivu. Ovi zahtevi treba da odrede koji će se tekući i arhivski podaci čuvati (podaci o korisniku, sertifikatu, ključevima), tajnost i integritet podataka, životni vek, uslove za pristup podacima, kao i lica koja mogu pristupati podacima. Primeri informacija koje se čuvaju u arhivi su: zapisi o sertifikatima, registracione i druge informacije o korisniku, tačno vreme značajnih događaja u sertifikacionom telu, informacije o životnom ciklusu izdatog elektronskog sertifikata i ključeva.

Zahtevi za evidenciju. Treba da odrede vrste evidencija, nivo bezbednosti evidencije, sadržaj koji se upisuje u evidenciju, događaje koji prouzrokuju ažuriranje evidencije i mehanizam kontrole pristupa. Opšti zahtev za evidenciju je da budu tačne, ažurne i bezbedne. Primeri evidencija su: evidencija izdatih elektronskih sertifikata, nevažećih (opozvanih i suspendovanih) sertifikata, specifičnih događaja, događaja o registraciji korisnika, zahteva, izveštaja i aktivnosti koju se odnose na proceduru opoziva sertifikata, evidencija događaja u vezi životnog ciklusa ključeva, aktivnosti zaposlenih i evidencija događaja koji se odnose na pripremu sredstava za formiranje kvalifikovanog elektronskog sertifikata.

4.2.4. Zahtevi za registracioni autoritet

Registracioni autoritet sprovodi proceduru registracije korisnika i podnosi zahtev za izdavanje sertifikata. Zahtev za registracioni autoritet treba da odredi vrstu i broj RA, proceduru registracije korisnika, organizaciju rada, funkcionalnost RA aplikacije i evidentiranje događaja.

Zahtevi za vrstu i broj RA. Ovi zahtevi treba da odrede potreban broj registracionih autoriteta, vrstu (lokalni, spoljašnji, RA za korisnike, RA za resurse) i geografsku distribuiranost kako bi se ostvarila pokrivenost potencijalnih podnosilaca zahteva.

Zahtevi za proceduru registracije. Treba da omoguće postupak i način prijavljivanja korisnika, način dokazivanja i provere identiteta korisnika, propisivanje obrazaca za registraciju, vreme potrebno za registraciju, proveru podataka podnosioca, određivanje podataka koji se unose u RA aplikaciju i podataka koju se čuvaju u papirnom obliku. Korisnik može biti fizičko ili pravno lice koje zahteva izdavanje sertifikata. Način dokazivanja i provere identiteta zavisi od vrste i namene sertifikata koji korisnik potražuje.

Zahtevi za funkcionalnost aplikacije. Ova vrsta zahteva treba da odredi sledeće funkcionalnosti aplikacija registracionog autoriteta: unos podataka za registraciju, udaljenu identifikaciju korisnika (ako politika sertifikacionog tela to dozvoljava), unos pratećih elektronskih dokumenata, logičku proveru podataka, generisanje zahteva za izdavanjem sertifikata, suspenziju, aktivaciju i opoziv elektronskog sertifikata, praćenje svih aktivnosti koje se sprovode nad podnetim zahtevom korisnika, kontrolu kvaliteta nosioca elektronskih sertifikata (npr. eID), praćenje životnog veka izdatog elektronskog sertifikata i njegovog nosioca, promenu podataka podnosioca zahteva, evidentiranje podataka i pretraživanje po raznim kriterijumima.

Zahtevi za evidentiranje događaja. Kada je reč o ovom zahtevu potrebno je odrediti koji događaji u radu sa RA aplikacijom se beleže. Treba da odredi sledeće događaje: unos, modifikovanje, brisanje i odobravanje zahteva za registraciju, pregledanje zahteva, kontrolu podataka nosioca sertifikata, podnošenje zahteva za izdavanje sertifikata i promene u konfiguraciji aplikacije. Za svaki događaj potrebno je odrediti koji se podaci evidentiraju i osobu koja je izvršila događaj.

4.4.5. Statusni servisi i servis direktorijuma

Korisnički servisi, aplikacije i servisi drugih proizvođača koji koriste sertifikate mogu zahtevati proveru statusa sertifikata. Da bi se to omogućilo, potrebno je obezbediti statusne servise koji daju odgovore o statusu sertifikata, odnosno da li je sertifikat opozvan ili suspendovan. Razmatraju se sledeći statusni servisi: servis liste opozvanih sertifikata (CRL) i OCSP servis.

Servis direktorijuma objavljuje izdate sertifikate, a preporučeno je da to budu sertifikati koji se koriste za šifrovanje. Prilikom definisanja ove vrste zahteva potrebno je odrediti koji je servis za sertifikate obavezan, a koji je preporučen. Osnovni zahtev za ove servise je da su raspoloživi korisniku sertifikata u realnom vremenu.

Servis CRL. Zahtevi za servis liste opozvanih sertifikata treba da omogući izdavanje CRL u skladu sa X.509 regulativom [76], učestalost izdavanja CRL na najmanje 24 sata, struktru CRL u saglasnosti sa [14], način na koji se objavljuju liste (http, ldap ili na drugi način), ograničenja pristupa listi, metod verifikacije pristupa listi, dodatne distribucione tačke, raspoloživost CRL servisa, perfomanse za pristup CRL i proceduru za arhiviranje i čuvanje CRL.

OCSP servis. Prilikom određivanja zahteva za OCSP (Online Certificate Status Protocol) potrebno je definisati servis prema RFC 6960 [77], odrediti dozvoljeno vreme kašnjenja informacije o opozivu sertifikata, definisati ograničenje i tačke pristupa OCSP servisu, perfomanse, raspoloživost servisa i arhiviranje OCSP odgovora.

Servis direktorijuma. Prilikom definisanja zahteva za servis direktorijuma potrebno je razmatriti vrstu direktorijuma, interfejse za pristup direktorijumu, oblik i opcije pretraživanja, dodatne distribucione tačke direktorijuma, ograničenja i saglasnost sa pristupom, perfomanse pretraživanja, raspoloživost servisa, planirano vreme zastoja, obaveštenja o radu i postupak u slučaju prekida rada servisa ili prekida rada izdavača sertifikata.

4.4.6. Zahtevi za servis korisnika

Ovi zahtevi treba da odredi vrste servisa u PKI sistemu. Osnovne vrste servisa u PKI sistemu su: autentikacioni servis, servis za elektronski potpis, za šifrovanje i vremenske oznake.

Zahtevi za autentikaciju. Ovim zahtevom potrebno je odrediti vrstu autentikacije, protokol za autentikaciju, parametre za podešavanje kanala za autentikaciju, uslove za primenu tokena (npr. eID), proceduru dokumentovanja i verifikovanja izabranog protokola.

Zahtevi za servis za elektronsko potpisivanje. Ovaj zahtev treba da definiše u kom standardnom formatu (XML DSIG, PKCS #7 (RFC 2315) [78], CMS (RFC 8933) [79, 80], PADES PDF [81], XAdES [82], CAdES [83] će rezultirati operacija potpisivanja, postojanje sertifikata, CRL i

vrmenske oznake u SDO (signed data object), mogućnost integracije softvera sa drugim servisima i softverima, primenu ograničenja naznačenu u sertifikatu ili publikovanu u Opštim pravilima, autorizaciju prilikom upotrebe privatnog ključa, heš funkciju i asimetrični algoritam za potpisivanje [84], format prikaza i specifikaciju softvera za analizu potpisnikovog dokumenta ako se dizajnira namenski modul za prezentovanje dokumenta.

Zahtevi za servis za verifikaciju elektronskog potpisa treba da odredi: da li će servis biti integrisan sa softverom za elektronsko potpisivanje, da li verifikacija zahteva instalaciju posebnog softvera, da rešenje za verifikaciju bude u saglasnosti sa [85], prikaz dokumenta identičan kao u vreme potpisivanja, obaveštavanje korisnika o bilo kakvom dinamičkom sadržaju u dokumentu, prikaz statusa verifikacije potpisa. Servis za validaciju treba da obezbedi da se podatak koji je korišćen za potpis slaže sa podatkom prikazanim u toku verifikacije, da se ispravan i validan sertifikat koristi za svrhu verifikacije potpisa i vremenske oznake, da bilo kakva promena koja se odnosi na bezbednost bude otkrivena.

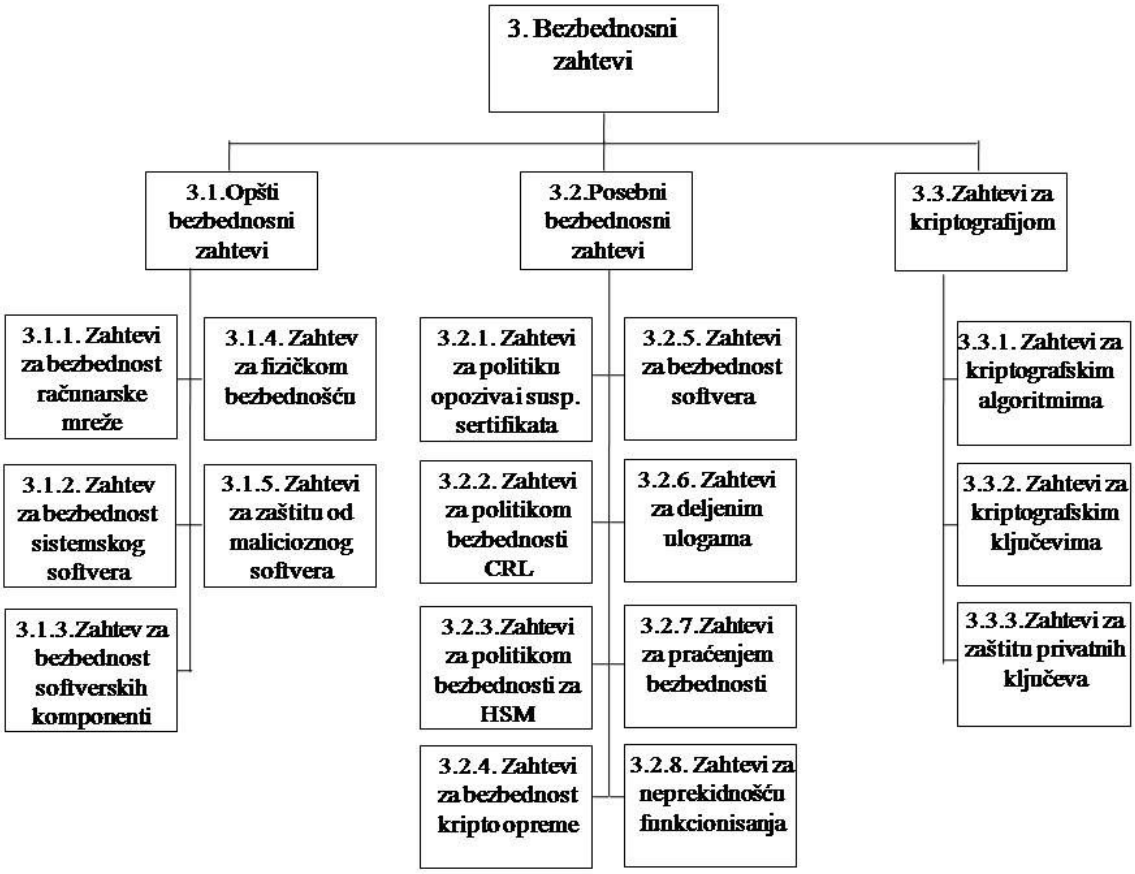
Zahtevi za servis za šifrovanje poruka treba da obezbede šifrovanje poruke na mestu nastanka javnim ključem, a dešifrovanje kod primaoca privatnim ključem koji korenspondira javnom ključu. Zahtevi za šifrovanje su sledeći: aplikacija za šifrovanje koja može da prihvati i obradi sertifikat, simetrični algoritama i dužina ključa shodno zahtevanom nivou bezbednosti. Zahtevi za dešifrovanje su sledeći: dešifrovanje poruka primenom privatnog ključa vlasnika sertifikata (eID ili na nekom drugom sigurnom medijumu) uz autentikaciju. Softver za šifrovanje treba da uzme u obzir sva ograničenja u korišćenju sertifikata koja su naznačena u samom sertifikatu, izvrši proveru važenja i status sertifikata korišćenjem statusnih informacija koje je odgovarajuće sertifikaciono telo javno publikovalo.

Zahtevi za servis vremenske oznake. Jedan od dodatnih servisa u PKI koji služi za obezbeđivanje jake neporecivosti je servis za izdavanja vremenske oznake (Time Stamping Authority, TSA). Ovaj servis treba definisati u skladu sa ETSI TS 319 421 [86] i odrediti zainteresovane strane koje će ga koristiti. Zahtevi za servis vremenske oznake treba da odrede: izbor servisa vremenske oznake (interni sopstveni servis, komercijalni ili javno dostupan servis), interfejs za servis vremenske oznake koji mora biti u saglasnosti sa RFC 3161 [87], politiku servisa vremenske oznake, format TSA sertifikata, ograničenja upotrebe TSA sertifikata, tačnost vremenske oznake, tačnost vremena (sata) i vreme važenja TSA. Javno dostupni servisi za izdavanje vremenske oznake imaju ograničenja u smislu brzine izdavanja vremenske oznake, neizdavanja

zbog opterećenosti, oscilacija u brzini izdavanja. Testiranje javno dostupnih besplatnih TSA dato je u radu [88].

4.3. Bezbednosni zahtevi

Bezbednosni zahtevi treba da odrede bezbednost PKI kroz opšte i posebne bezbednosne zahteve i zahteve za kriptografiju. Klasifikacija bezbednosnih zahteva prikazana je na slici 10.



Slika 10. Klasifikacija bezbednosnih zahteva

4.3.1. Opšti bezbednosni zahtevi

Opšti bezbednosni zahtevi za PKI odnose se na zahteve za bezbednost u organizacionoj celini sertifikacionog tela i softverskim komponentama koje omogućuju funkcionalnost sertifikacionog tela i registracionog autoriteta. Potrebno ih je razmatrati kroz sledeće zahteve:

Zahtevi za bezbednost računarske mreže treba da odrede mrežnu adresnu šemu, mere za komunikacione uređaje, potrebu za spoljašnjim mrežnim konekcijama, dolazni i odlazni saobraćaj kroz liste za kontrolu pristupa, vrstu i konfiguraciju zaštitnog zida, način i politiku za udaljeni pristup.

Zahtevi za bezbednost sistemskog softvera treba da odrede sledeće: odgovarajući izbor softvera, instalaciju samo proverenog softvera sa poslednjim verzijama zakrpa, omogućavanje rada samo potrebnih servisa, konfigurisanje bezbednosnih parametara, izbor lokacije u mrežnom okruženju.

Zahtevi za bezbednost softverskih komponenti treba da odrede odgovarajući autentikacioni mehanizam, bezbednu komunikaciju između komponenti, odgovarajuća prava pristupa, konfigurisanje bezbednosnih parametara, lokaciju u mrežnom okruženju, potreban broj portova za komunikaciju, izbor bezbednog smeštanja podataka u bazu podataka (šifrovani ili nešifrovani podaci), podatke za prijavljivanje i aktivnosti koje pokreću prijavljivanje.

Zahtevi za fizičku bezbednost sertifikacionog tela. Ovaj zahtev treba da odredi sledeće: fizičku zaštitu ključeva CA i sertifikacionog tela, sistem video nadzora, sistem kontrole pristupa prostoriji sertifikacionog tela, sistem protivpožarne zaštite i lokacije za čuvanje zaštitnih kopija, klimatizaciju i ventilaciju [89].

Zahtevi za zaštitu od malicioznog softvera. Zahtev za zaštitu od malicioznog softvera treba da je takav da se onemogući unos zlonamernog softvera u sertifikaciono telo. Ovaj zahtev treba da odredi vrstu antivirusnog softvera koji će se koristiti, postupak u radu sa prenosnim medijumima, postupak prilikom instalacije bezbednosnih zakrpa i nadogranje komponenti i servisa.

Bezbednosni zahtevi za zaposlene treba da odrede kriterijume za izbor osoblja, njihovu bezbednosnu proveru kod nadležnog organa, ugovorom definisane odgovornosti zaposlenog prema poverljivim informacijama i bezbednosti sistema za vreme rada i nakon prestanka rada, bezbednost u okviru zadataka zaposlenog, obučenost iz domena informacione bezbednosti [90] i odgovornosti prema nastalim bezbednosnim incidentima i nepravilnostima u radu.

4.3.2. Posebni bezbednosni zahtevi

Posebni bezbednosni zahtevi za sertifikaciono telo odnose se na bezbednosne mere koje sertifikaciono telo primenjuje u svom radu. Potrebno ih je definisati kroz razmatranje sledećih bezbednosnih zahteva: zahtev za politiku opoziva i suspenzije sertifikata, za politiku bezbednosti za CRL, za politiku bezbednosti za HSM, za fizičku bezbednost CA, za bezbednost softvera, za deljene uloge, za praćenje bezbednosti, za kripto opremu i za zaštitu CA u slučaju nepredviđenih situacija.

Zahtevi za politiku opoziva i suspenziju sertifikata. Ovim zahtevima je potrebno definisati uslove pod kojima će sertifikat biti opozvan pre isteka vremena validnosti, ko ima pravo da izvrši opoziv ili suspenziju sertifikata, u kojim slučajevima se može ukinuti suspenzija sertifikata, vrstu autentikacije i izbor koda za opoziv ili suspenziju sertifikata [14].

Zahtevi za politiku bezbednosti za CRL. Treba da odredi algoritam i dužinu ključa za potpisivanje CRL, vrstu autentikacije na servis za generisanje CRL, osobe koja vrši publikovanje i generisanje CRL, bezbedan pristup na lokaciju za publikovanje CRL, vreme generisanja i rok trajanja, arhiviranje CRL.

Zahtevi za politiku bezbednosti za HSM. Ovaj zatev treba da odredi sledeće: zaštitu HSM od neovlašćenog pristupa, izradu zaštitnih kopija nakon svake promene sadržaja tokena, raspodeljene uloge u radu sa uređajem, bezbedno čuvanje kopija ključeva i drugog sadržaja, princip M od N kontrole kod čuvanja ključa, razdvojeno čuvanje zaštićenog sadržaja i sredstva za pristup otvorenom sadržaju [91].

Zahtevi za bezbednost kripto opreme [92, 93] treba da odrede sledeće karakteristike opreme: postojanje mehanizma zaštite od falsifikovanja zaštićene memorije u kojoj se čuvaju ključevi, generator slučajnog niza i sat realnog vremena (real time clock), mehanizam za upravljanje ključevima (generisanje, čuvanje, brisanje i pravljenje zaštitne kopije ključa), krut bezbednosni mehanizam koji se ogleda u sprovođenju stroge autentikacije i kontrole pristupa kriptografskim servisima i ključevima, mehanizam raspodeljenih uloga, dvofaktorska autentikacija i mehanizam za zaštitu protiv falsifikovanja.

Zahtevi za bezbednost softvera. U toku razvoja treba da odrede autentikacione i autorizacione mehanizme koji će se implementirati, integraciju bezbednosti u svim fazama razvoja softvera [94]. Pored navedenog, komponente ne smeju da sadrže maliciozni kod, moraju biti razvijene na

pouzdanoj platformi (programski jezik, razvojni alati, biblioteke) i na razvoju mora da radi provereno osoblje.

Zahtevi za deljene uloge. Ova vrsta zahteva treba da definiše sledeće: uloge koje imaju zaposleni u različitim vrstama poslova, identifikovanje poslova i aktivnosti sa deljenim ulogama, opis uloga za svaku vrstu posla i radnog mesta, dokumentovanje i čuvanje uloga.

Zahtevi za praćenje bezbednosti. Svi bezbednosni događaji sertifikacionog tela moraju se beležiti (pratiti). Ovaj zahtev treba da odredi koji se bezbednosni događaji prate, proceduru bezbednog čuvanja, rok čuvanja zapisa, proceduru i učestalost pregledanja zapisa i osobe koje su zadužene za pregled.

Zahtevi za neprekidno funkcionisanje. Ovi zahtevi treba da odrede kako će se obezbediti neprekidnost funkcionisanja CA tela u slučaju nepredviđenih situacija, što podrazumeva postojanje preventivnih CRL lista, rezervne lokacije za rad CA i za kriptografske ključeve.

4.3.3. Zahtevi za kriptografiju

Zahtevi za kriptografiju treba da su takvi da algoritmi i dužina ključa omogućuju pouzdanu odbranu od kriptoanalitičkih napada. Ovi zahtevi se razmatraju kroz sledeće: kriptografski algoritmi, kriptografski ključevi, zaštita privatnih ključeva.

Zahtevi za kriptografski algoritam. Ova vrsta zahteva treba da odredi koji kriptografski algoritam će se koristiti za generisanje para ključeva za sva sertifikaciona tela i krajnje korisnike, heš funkciju i asimetrični kriptografski algoritam za potpisivanje sertifikata i statusnih informacija (CRL, OCSP) [84], vrstu i tip algoritma za zaštitu delova ključa za aktivaciju privatnog ključa sertifikacionog tela.

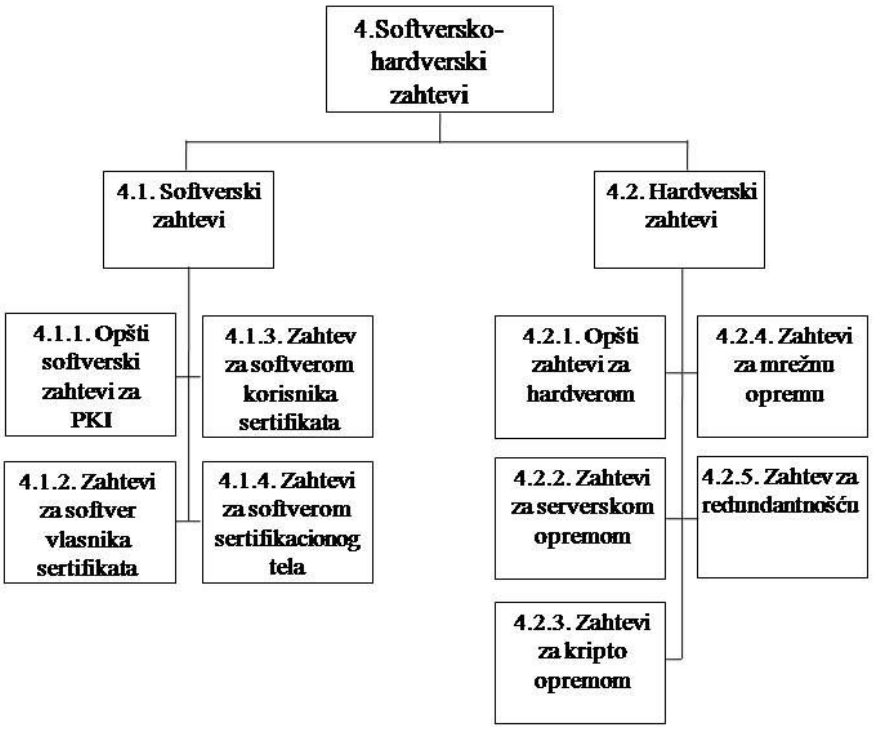
Zahtevi za kriptografski ključ. Ovim zahtevima je potrebno definisati dužinu para ključeva i efektivni životni vek ključeva za sva sertifikaciona tela i krajnje korisnike. Snagu i životni vek ključeva definisati shodno sa [84]. Zahtevi za dužinu javnog ključa koji služi za potpisivanje sertifikata i statusnih informacija (CRL, OCSP) moraju biti saglasni sa ETSI TS 102 176-1. Dužina simetričnog ključa mora biti dovoljna da zaštiti ključ za aktivaciju privatnog ključa sertifikacionog tela.

Zahtevi za zaštitu privatnih ključeva. Treba ih razmatrati kroz zaštitu privatnog ključa korisnika, privatnog ključa sertifikacionog tela i privatnog ključa za resurse. Ova vrsta zahteva treba da odredi sledeće: uređaj na koji će biti smešteni privatni ključevi, pristup privatnom ključu (npr. dvofaktorska autentikacija), postojanje autorizacije svake operacije koja obuhvata korišćenje privatnog ključa, mehanizam za uništavanje privatnih ključeva takav da se privatni ključ ne može naknadno rekonstruisati, mehanizam i proceduru za bezbedno generisanje ključeva, autorizaciju osoblja i proceduru za izradu i čuvanje rezervnih kopija.

4.4. Softversko-hardverski zahtevi

4.4.1. Softverski zahtevi

Softverski zahtevi treba da odrede softverske karakteristike komponenti PKI sistema takve da se može izvršavati na potojećoj softverskoj platformi, u postojećem informacionom sistemu ili sa standarnim aplikacijama elektronske pošte, internet pretraživačima. Softverski zahtevi se razmatraju kroz opšte zahteve za softverske komponente PKI, zahteve za softver vlasnika sertifikata, za softver korisnika sertifikata i za softver sertifikacionog tela. Klasifikacija softversko-hardverskih zahteva prikazana je na slici 11.



Slika 11. Klasifikacija softversko-hardverskih zahteva

Opšti softverski zahtevi za PKI. Treba definisati: perfomanse, modularnost, skalabilnost, upravljivost, održavanje, upotrebljivost, jezičku podršku, raspoloživost, dnevničke zapise i konfigurabilnost. Zahteve za perfomanse je potrebno definisati shodno trenutnom broju korisnika i planiranom proširenju PKI tako da se omogući rad svih korisnika bez zastoja. Zahtev za modularnost i skalabilnost treba da odredi softverske module, način komuniciranja između modula, proširivanje ili ukidanje postojećih funkcionalnosti, povećanje broja relacija poverenja, dodavanje novih funkcionalnosti [95]. Zahtev za upravljivost treba da omogući jednostavno upravljanje svim poslovnim funkcijama sertifikacionog tela i registracionog autoriteta. Zahtev za održivost (maintainability) treba da definiše jednostavno modifikovanje softvera kako bi se ispravila greška, poboljšale perfomanse i osobine ili prilagodio izmenjenom okruženju. Zahtev za upotrebljivost treba da definiše sledeće: način informisanja korisnika o dešavanjima u sistemu, kvalitet i jednostavnu interakciju sa korisnikom, konzistentnost i standardizaciju fraza, prevenciju greške kroz višestruke upite, prepoznavanje umesto prisećanja, estetiku i minimalni dizajn dijaloga za komunikaciju i jasne poruke o greškama. Softver treba da ima mogućnost lokalizacije jezika korisnika. Zahtev za raspoloživost treba da definiše raspoloživost u procentima, odnosno prihvatljivo vreme otkaza softvera u toku godine, meseca i nedelje. Zahtev za izradu dnevničkih zapisa definiše koje aktivnosti u radu sertifikacionog tela i registracionog autoriteta je potrebno pratiti, odnosno evidentirati i koje informacije zapis treba da sadrži. Zahtev za konfigurabilnost treba da je takav da osoblje može da komponente instalira, konfiguriše i što pre dovede u operativno stanje. Ovaj zahtev predviđa i omogućavanje bekapa konfiguracije, kao i mehanizam za kontrolu pristupa ovim elementima i podacima.

Zahtevi za softver vlasnika sertifikata. Ova vrsta zahteva definše platformu na kojoj će se izvršavati softver vlasnika sertifikata, tehnologiju koja će se koristiti za pristup nosiocu sertifikata i privatnog ključa, potrebu za integracijom sa softverom trećih lica, podešavanja na opremi krajnjeg korisnika da bi se omogućilo korišćenje elektronske kartice, rad u on-line ili u off-line režimu, namenu softvera (šifrovanje, potpisivanje, ili oba) i licencu za korišćenje (vremenska, po broju korisnika, trajna).

Zahtevi za softver korisnika (primaoca) sertifikata. Korisnik sertifikata treba da je u mogućnosti da primi i obradi sertifikate bez bilo koje druge dodatne opreme koju bi trebalo integrisati u postojeći sistem. Ova vrsta zahteva treba da odredi potrebu za integracioni modul za saradnju sa partnerima (namena modula, okruženje u kome će da radi, koje interfejse treba da podržava, kao i pod kojim operativnim sistemom treba da radi i u kom programskom okruženju),

dokumentovanje koje omogućava drugim programerima da ih koriste, licence i načine regulisanja korišćenja licence.

Zahtevi za softver sertifikacionog tela. Ovim zahtevima definiše se interfejs prema administratoru sistema za konfigurisanje neophodnih bezbednosnih parametara, parametara za konfigurisanje sertifikata, mehanizama za upravljanje sertifikacionim telima i korisnicima, servisima za nadgledanje i olakšavanje rada administratora.

4.4.2. Hardverski zahtevi

Hardverski zahtevi treba da odrede karakteristike opreme koje će podržati funkcionisanje softvera za PKI sisteme. Prevashodno se misli na hardver u samom sertifikacionom telu. Hardverski zahtevi se razmatraju kroz sledeće zahteve: opšti zahtevi za hardver, zahtevi za serverversku opremu, za kripto opremu, za mrežnu opremu i za redudantnost.

Opšti zahtevi za hardverom. Ova vrsta zahteva treba da odredi funkcionalnost uređaja, pouzdanost uređaja (raspoloživost, srednje vreme između kvarova (MTBF-mean time between failures), srednje vreme dovođenja uređaja u radno stanje (MTTF – mean time to repair), tačnost (accuracy) rada uređaja, učestalost grešaka ili defekata u radu uređaja, perfomanse uređaja (vreme odgovora za jednu transakciju, propusna moć, kapacitet, prihvatljiv mod rada uređaja kada je sistem degradiran na neki način, korišćenje resursa), mogućnost podrške ili održavanja, pristup dokumentaciji, kompatibilnost i interoperabilnost komponenti uređaja, interfejse i portove (hardverske, komunikacione, korisničke), protokole, licence i standarde (pravni, kvalitativni i regulacioni standardi, industrijski standardi za usability i interoperabilnost).

Zahtevi za serversku opremu. Ovi zahtevi treba da odrede sledeće: opterećenje servera shodno procenjenom broju zahteva i operacija koje server treba izvrši za realizaciju jednog zahteva, mogućnost proširivanja hardverskih kapaciteta, kao što su procesorska snaga i memorijski kapacitet (radne memorije i hard diskova).

Zahtevi za kripto opremu. Kripto oprema treba da zadovoljava sledeće zahteve: da je u skladu sa standardom, level 3 [91], ili ekvivalentnim standardima [96] ili [97] ili [98], da može generisati zahtevane kriptografske ključeve i ključeve za projektovani broj zahteva bez kašnjenja, da je oprema zaštićena od kompromitovanja u toku transporta i od neovlašćenog modifikovanja.

Prodavac treba da dostavi i dokumentuje proceduru za bezbednu distribuciju sredstva za formiranje kvalifikovanog elektronskog potpisa i aktivacioni kod.

Zahtevi za mrežnu opremu. Mrežna oprema koja povezuje hardverske komponente sertifikacionog tela mora da zadovolji najviše standarde. Ova vrsta zahteva treba da definiše brzinu uređaja, vreme odgovora na ulazni podatak, da radi na L3 i višem nivou OSI modela, da ima ugrađen zaštitni zid, određenu vrstu autentikacije, operativni sistem koji ima mogućnost podešavanja i generisanja dnevničkih zapisa, ekspanzione slotove za nadogradnju u budućnosti.

Zahtevi za redundantnost. Bezbednost i sigurnost rada sertifikacionog tela je potrebno obezbediti u slučaju hardverskih otkaza uređaja ili komponenti. Ovaj zahtev treba da odredi potencijalne tačke otkaza uređaja, odgovarajuće uređaje za redundantno napajanje, redundantni aktivni elemenat za hlađenje, redundantne hard diskove (RAID), redundantnu mrežnu karticu i rezervnu opremu.

4.5. Zahtevi za podršku funkcionisanja PKI

Podrška funkcionisanju PKI predstavlja jedan uređen i sistematičan pristup u planiranju, organizovanju, nadgledanju i praćenju funkcionalnosti PKI sistema. Organizovana podrška funkcionisanju PKI je dobra preventiva za dobro funkcinisanje PKI.

Prilikom definisanja zahteva za PKI infrastrukturu potrebno je razmatrati zahteve za podršku funkcionisanja PKI. Ovaj zahtev treba da obuhvati: planiranje resursa za podršku, podršku u funkconisanju hardvera i softvera PKI, u ovladavanju PKI sistemom i podršku korisnicima servisa. Klasifikacija zahteva za podršku funkcionisanju PKI prikazana je na slici 12.

Slika 12. Klasifikacija zahteva za podršku funkcionisanju PKI

4.5.1. Zahtev za resurse za podršku

Ova vrsta zahteva treba da odredi sledeće resurse za svaku vrstu podrške: kadrovske, materijalne, finansijske resurse i vremenski resurs. Kadrovske resurse treba definisati za svaku vrstu podrške: profil kadra po oblastima koje treba da obuhvate, kao i da li se radi o kadru iz organizacije ili su u pitanju spoljnji saradnici. Materijalni resursi određuju se prema vrsti održavanja, a podrazumavaju sredstva koja će biti korišćena i lokaciju na kojoj će se realizovati podrška. Finansijski resursi se određuju po vrsti održavanja i angažovanim kadrovskim i materijalnim resursima. Vremenski resursi se određuju kroz vreme odziva podrške. Potrebno je odrediti vreme reakcije podrške po nivoama, vreme za rešavanje problema po vrstama podrške, postupke i odredbe u slučaju prekoračenja vremena, postupak evidentiranja vremena.

4.5.2. Zahtevi za podršku u funkcionisanju softvera i hardvera

Ovu vrstu zahteva potrebno je definisati tako da podrže neprekidan rad i funkcionalnosti PKI sistema. Osnovni zahtev za ovu vrstu podrške je postojanje korisničke dokumentacije za podršku koja jasno i detaljno opisuje svaku funkcionalnost softvera, postupke i procedure za korisničko održavanje softvera i hardvera, postupke za rešavanja problema, procedure za prikupljanje informacija o problemu, postupke za prijavljivanje problema.

4.5.3. Zahtevi za tehničko održavanje

Ovi zahtevi treba da odrede vrste i plan održavanja. Prema Standardu ISOIEC 14764 korisnik može da odredi sledeće vrste održavanja: korektivno održavanje (reaktivno održavanje) koje podrazumeva modifikacije u softveru i hardveru sa ciljem rešavanja problema, preventivno održavanje (proaktivna podrška) što znači modifikaciju hardvera i softvera sa ciljem da se unapred otklone potencijalni problemi u radu, adaptivno održavanje tj. modifikovanje gotovog softverskog proizvoda kako bi se prilagodio novom ili izmenjenom okruženju i perfektivno održavanje sa ciljem poboljšanja perfomansi isporučenog sistema.

4.5.4. Zahtevi za podršku pre isporuke sistema

Ovi zahtevi treba da odrede aktivnosti za pripremu uvođenja novog sistema. Primeri aktivnosti su: instalacija računarske mreže, fizička zaštita, obuka korisnika PKI, obuka menadžmenta, obezbeđivanje potrošnih sredstava i materijala.

4.5.5. Zahtevi za podršku u toku funkcionisanja sistema

Ova vrsta zahteva treba da odredi aktivnosti u toku funkcionisanja sistema sa ciljem održavanja njegove funkcionalnosti. Ove aktivnosti obuhvataju održavanje, pružanje stručne podrške, ažuriranje i dopune uputstava i dokumentacije, ažuriranje i dopuna izvornog koda nakon izvršenih ispravki u softveru, podrška korisnicima na više načina (telefonom, elektronskom poštom).

4.5.6. Zahtevi za podršku u daljem razvoju PKI

Ovaj vid podrške treba da unapredi PKI sistem kroz uvođenje novih rešenja i servisa. Najčešće se definišu po završetku uvođenja PKI kada se javlja potreba za: podrškom osoblju PKI, podrškom IT osoblju novoizabranog stakeholdera, primenom sertifikata u informacionim sistemima organizacije, nadogradnjom i poboljšanjima. Ova vrsta zahteva treba da odredi koji softver ili hardver je potrebno poboljšati, koje nove funkcionalnosti se uvode, vreme potrebno za realizaciju, ko izvodi poboljšanja, dokumentovanje izmena u programskom kodu, pružanje podrške IT osoblju u daljem razvoju.

4.5.7. Zahtevi za podršku u ovladavanju PKI sistemom

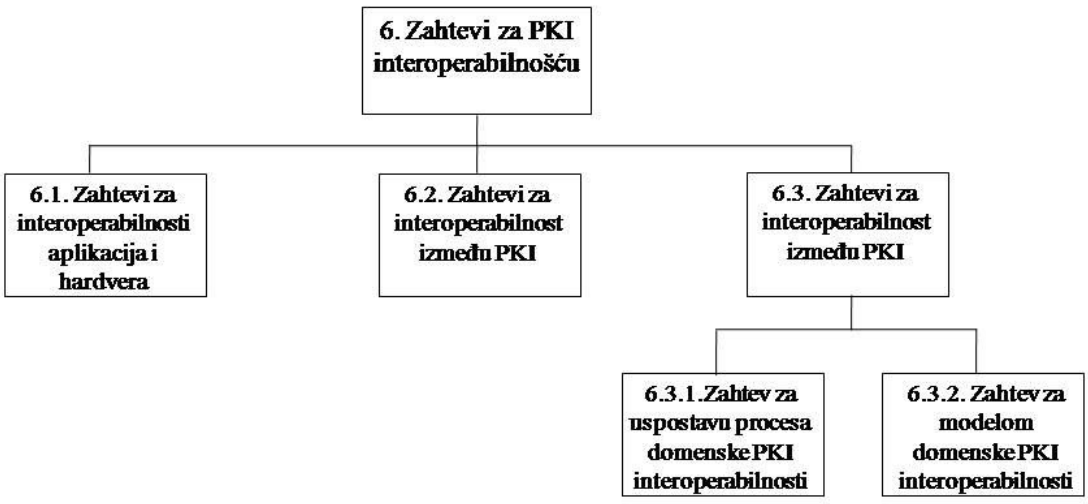
Uvođenje PKI sistema povlači za sobom mnogo novina za IT osoblje koje treba usvojiti i primenjivati u daljem radu. Zbog složenosti PKI potrebno je da isporučilac sistema pruži podršku IT osoblju za vreme operativnog rada PKI. Ovu vrstu podrške je potrebno omogućiti telefonskim putem, elektronskom poštom ili dolaskom na lokaciju korisnika.

4.5.8. Zahtevi za podršku korisnicima servisa

Ova vrsta zahteva treba da odredi uputstvo za korisničku podršku, okvir korisničke podrške i servise za pozivanje podrške. Uputstvo treba da sadrži sledeće: opis servisa, način njihovog funkcionisanja, redosled izvršavanja postupaka, vreme potrebno za odgovor korisniku i način pristupa servisu (telefonom, elektronskom poštom ili web interfejsom). Okvir korisničke podrške treba da odredi da li je ova vrsta podrške u sklopu neke druge podrške ili nije, kao i na koji hardver, softver ili servis korisnika sertifikata se odnosi ova podrška. Servisom za pozivanje podrške potrebno je specificirati ko obezbeđuje servis i koje oblasti takav servis obezbeđuje u prikladnom vremenu.

4.6. Zahtevi za PKI interoperabilnost

Uspostava PKI interoperabilnosti omogućava povezivanje dva ili više istih ili različitih aplikacija i hardvera, komponenti ili PKI domena. Na ovaj način se omogućava funkcionalnost između različitih softverskih aplikacija i hardvera kao osnove za funkcionalnost različitih komponenti PKI. Interoperabilnost PKI domena omogućuje korišćenje elektronskih sertifikata za elektronske servise izdate od različitih sertifikacionih tela iz različitih PKI domena. PKI interoperabilnost za PKI se promatra u tri kategorije, slika 13: interoperabilnost aplikacija i hardvera, interoperabilnost komponenti PKI i domenska interoperabilnost PKI.



Slika 13. Klasifikacija zahteva za PKI interoperabilnost

4.6.1. Zahtevi za interoperabilnost aplikacija i hardvera

Ovi zahtevi se odnose na omogućavanje da različite aplikacije PKI i hardver budu interoperabilni jedni sa drugim bez obzira ko ih je proizveo. Prilikom razvoja aplikacija njihovi proizvođači, da bi ostvarili interoperabilnost u PKI okruženju, razmatraju način smeštanja kredencijala, kompatibilnost između različitih fajlova i formata poruka (npr. veličina ključa i algoritmi treba da su kompatibilni između različitih aplikacija) i komunikaciju između različitih aplikacija.

4.6.2. Zahtevi za interoperabilnost PKI komponenti

Ovi zahtevi omogućavaju da brojne PKI komponente funkcionišu zajedno pružajući celokupnu funkcionalnost PKI rešenju. Dobro definisani zahtevi su od značaja za ovu interoperabilnost jer greške u komunikaciji između komponenti vode prekidu funkcionalnosti PKI. Potrebno je definisati protokole i formate poruka za komunikaciju između različitih komponenti, kao što su CA, RA i klijenti. Takođe, potrebno je definisati i mehanizme za davanje informacija o opozvanim sertifikatima, kao što su: protokol za online proveru sertifikata (Online Certificate Status Protocol, OCSP) i lista opozvanih sertifikata (Certificate Revocation List, CRL). Ništa manje značajno nije ni definisanje autentikacionih metoda i kriptografskih algoritama koji će se koristiti.

4.6.3. Zahtevi za domensku interoperabilnost PKI

Ova interoperabilnost fokusira se na uspostavljanje relacija poverenja između različitih PKI domena. Prilikom razmatranja ove vrste interoperabilnosti potrebno je sagledati raspoloživost javnog ključa između domena i opštih politika PKI domena. Pored toga, svaki domen treba da ostane veran skupu politika koje upravljaju njegovim procesom sertifikacije. Ova kategorija zahteva razmatra se kroz uspostavljanje procesa domenske PKI interoperabilnosti i model domenske PKI interoperabilnosti.

Zahtevi za uspostavu procesa domenske PKI interoperabilnosti. Ovaj zahtev definiše političke ili ugovorne procese uspostave međusobnog priznanja i tehničko rešenje za prenošenje međusobnog priznanja. Prvi zahtev treba da definiše merila kojima bi se utvrdilo da li učesnici interoperabilnosti ispunjavaju određene tehničke, bezbednosne i upravljačke zahteve za interoperabilnošću, pre nego što se pristupi tehničkoj realizaciji. Tehničko rešenje za prenošenje

međusobnog priznanja definiše uslove za automatsko odlučivanje da li se prihvata ili ne prihvata sertifikat iz drugog PKI domena.

Zahtevi za model domenske PKI interoperabilnosti. Treba da definišu način razmene poverenja u transakciji. Postoji više modela interoperabilnosti kao što su: hijerarhijski model, model ukrštene sertifikacije, prepoznavanja, mostovni model, model listi poverenja sertifikata i model sertifikata o akreditaciji. Zahtevi treba da proizađu iz sagledavanja dobrih i loših osobina modela [99] i potreba poslovanja. Prilikom definisanja zahteva potrebno je razmotriti sledeće:

- proces obrade sertifikacione staze, odnosno njeno razotkrivanje i validacija od krajnjeg korisnika do tačke poverenja,
- utvrđivanje osobina sertifikata iz politike sertifikacije i
- utvrđivanje da li je sertifikat pouzdan za predviđenu namenu.

4.7. Tranzicioni zahtevi

Ovi zahtevi rešenja za prelazak sa tekućeg stanja organizacije na buduće željeno stanje. Tranzicioni zahtevi su razlikuju od drugih tipova zahteva zato što su privremeni i mogu nastati u pojedinim fazama razvoja sistema ili nakon nekog vremena rada sistema. Ne nastaju samo u pojedinim fazama razvoja PKI već i nakon stavljanja PKI sistema u operativnu upotrebu. Tranzicioni zahtevi, u zavisnosti od vremena nastanka u toku životnog ciklusa razvoja PKI, mogu da se podele u sledeće grupe: zahtevi u toku razotkrivanja, dizajna, implementacije i prijema sistema i u toku operativnog rada. Zahtevi za tranziciju treba da odrede kojom detaljnošću se definišu zahtevi, vreme i bitnost realizacije zahteva i prioritet zahteva.

4.8. Međusobni uticaj zahteva za PKI iz klasifikacione šeme

Zahtevi iz različitih kategorija mogu imati u uticaj jedni na druge. To znači da prilikom definisanja zahteva treba uzeti u obzir ovaj uticaj i prilagoditi zahteve kako bi se umanjio rizik od naknadnog redefinisanja zahteva za vreme projektovanja i razvoja PKI. Međusobni uticaj zahteva za PKI prikazan je u Tabeli 3 i Prilogu 3.

Tabela 3. Međusobni uticaj zahteva iz klasifikacione šeme

	1. Poslovno-organizacioni zahtevi	2. Zahtevi za komponentama i servisima PKI	3. Bezbednosni zahtevi	4.Softversko-hardverski zahtevi	5. Zahtevi za podršku funkcionisanju PKI	6. Zahtevi za PKI interoperabilnošći
1. Poslovno-organizacioni zahtevi	-	2.2., 2.4., 2.6.	3.1.	4.1., 4.2.	5.1-5.8	6.3.
2. Zahtevi za komponentama i servisima PKI	1.1.	-	3.1., 3.2., 3.3.	4.1., 4.2.	5.2., 5.3., 5.5., 5.7., 5.8.	6.1., 6.2.
3. Bezbednosni zahtevi	1.	2.	-	4.1., 4.2.	5.4., 5.5., 5.7., 5.8.	6.1., 6.2., 6.3.
4.Softversko-hardverski zahtevi	1.1.2., 1.1.3., 1.1.5., 1.1.7., 1.1.8.	2.1., 2.3. 2.6.	3.3.	-	5.2., 5.3., 5.5.	6.1.
5. Zahtevi za podršku funkcionisanju PKI	1.1.2., 1.1.6., 1.1.7., 1.1.8., 1.2.2.	2.	3.1.	4.1., 4.2.	-	6.1.
6. Zahtevi za PKI interoperabilnošću	1.1.5., 1.1.6., 1.2.1., 1.2.3.	2.3. 2.4. 2.5. 2.6.	3.1., 3.2., 3.3.	4.1.1., 4.2.4., 4.2.2., 4.2.3.	5.2., 5.3., 5.5.	-

4.8.1. Uticaj poslovno-organizacionih zahteva na zahteve iz klasifikacione šeme

Poslovno-organizacioni zahtevi imaju uticaj na formiranje zahteva PKI komponenti i servisa tako što određuju namenu sertifikata (sertifikat za autentikaciju, elektronsko potpisivanje, ...) i

servisa (servis za elektronsko potpisivanje, servisi za autentikaciju, ...) shodno potrebama poslovanja. Zahtev za organizaciju rada uslovljava određivanje zahteva za registracioni autoritet koji omogućavaju organizaciju i procese rada u skladu sa propisima zakonodavca i međunarodnim standardima.

Uticaj poslovno-organizacionih zahteva na opšte i posebne zahteve bezbednosti proizilazi iz cilja koje ima poslovanje, a to je unapređenje bezbednosti u organizaciji i bezbednosti poslovnih transakcija. Zahtev ekonomičnosti ima direktan uticaj na zahteve bezbednosti. Ovaj zahtev treba da bude takav da se za planirana finansijska sredstva mogu implementirati najbolje mere koje će omogućiti zahtevanu bezbednost PKI sistema. Zahtevi za integraciju poslovnih sistema sa drugim kompanijama ne smeju da utiču na odustajanje od nekih zahteva bezbednosti PKI.

Poslovni zahtevi utiču na zahteve za hardver i softver PKI kroz potrebu da se unapredi poslovanje i bezbednost primenom hardvera i softvera boljih perfomansi i bezbednosnih karakteristika, a u granicama ekonomičnosti. Ovi zahtevi ne treba da ograničavaju hardversko – softverske zahteve na štetu perfomansi i bezbednosti PKI sistema.

Uvođenje PKI sistema u organizaciju zahteva dobro dizajniran i implementiran sistem podrške funkcionisanja. Zahtev ekonomičnosti ograničava potpuno ispunjavanje zahteva za podršku funkcionisanja i dovodi u pitanje ne samo funkcionisanje PKI sistema nego i poslovanje. Razlog leži u lošoj podršci fukcionisanja sistema (kašnjenje prilikom uvođenja sistema, nedostupnost funkcionalnosti zbog zastoja u radu PKI komponenti i servisa, neodgovarajuća podrška korisnicima i sistemu,...) prouzrokovanoj restriktivnim merama ekonomičnosti.

Uvođenje PKI u organizaciju osim podizanja nivoa bezbednosti elektronskog poslovanja utiče i na proširivanje poslovanja preko granica sistema, pa je potrebno obezbediti interoperabilnost sa drugim organizacijama kroz uspostavu međudomenske interoperabilnosti.

4.8.2. Uticaj zahteva za PKI servise i komponente na zahteve iz klasifikacione šeme

Zahtevi za PKI komponente i servise utiču na poslovno-organizacione zahteve koji se odnose na: unapređenje poslovanja i organizacije, bezbednost, izbor prodavca PKI, edukaciju i primenu PKI. Međusobna interakcija navedenih zahteva utiče na poboljšanje bezbednosti i podizanje perfomansi poslovnog sistema (bezbedno elektronsko poslovanje).

Najveći međusobni uticaj imaju zahtevi za PKI komponente i servise i zahtevi za bezbednost. Da bi PKI sistem ostvario bezbednost poslovnog sistema (integritet, poverljivost, autentičnost, neporecivost i raspoloživost) mora, pre svega, sam da bude bezbedan i pouzdan. Gotovo svaki zahtev za PKI komponente i servise na direktan ili indirektan način utiče na zahteve za bezbednost jer postojanje zahteva za PKI komponente i servise povlači postojanje odgovarajućih zahteva bezbednosti.

Implementacijom zahteva za komponente i servise stvara se infrastruktura koja zahteva podršku od trenutka stavljanja u funkcionalnost. Sistem od koga zavisi bezbednost poslovnog sistema mora biti bezbedan i funkcionalan u svakom trenutku. Zato je neophodan dobro razvijen sistem podrške funkcionisanja koji je potrebno definisati prilikom razotkrivanja i definisanja zahteva za PKI komponente i servise. Npr. zahtevi za servis za šifrovanje poruka ostvariće uticaj na zahteve za podršku ovladavanja PKI sistemom, za podršku korisnicima servisa i za podršku u toku funkcionisanja.

Zahtevi za PKI komponente i servise su blisko povezani sa hardversko-softverskim zahtevima jer uslovljavaju odgovarajuću hardversku i softversku platformu na kojoj će se izvršavati bezbedno i sa maksimalnim perfomansama.

Da bi PKI komponente mogle da komuniciraju i funkcionišu kao jedna celina potrebno je da se izaberu odgovarajući protokoli. Isto tako je potrebno izabrati protokole i za međusobno funkcionisanje aplikacija i hardvera, kao i komponenti koje se izvršavaju na odgovarajućim aplikacijama.

4.8.3. Uticaj zahteva za bezbednost na zahteve iz klasifikacione šeme

Zahtevi za opšte i posebne mere bezbednosti uglavnom će se odraziti na poslovno-organizacione zahteve i to one koji se odnose na finansije i organizaciju. Bez obzira na uticaj zahteva bezbednosti, potrebno je definisati poslovne zahteve tako da se omogući ispunjenje zahteva za bezbednost PKI sistema i na taj način podigne nivo bezbednosti poslovnog sistema.

Ovi zahtevi imaju uticaj na zahteve za PKI komponente i servise tako što utiču da se prilagode tako da njihovu funkcionalnost učine bezbednijom.

Bezbednosni zahtevi utiču na određivanje zahteva za hardver, npr. na zahteve za specijalne bezbednosne uređaje (Hardware Security Modul, HSM) i smart kartice, a sa druge strane zahtevi za bezbednosni hardver utiču na zahteve za razvoj bezbednosnih procedura. Zahtevi za kriptografske algoritme i ključeve imaće uticaj na razvoj softvera koji ih koristi, kao i na zahteve za aplikativni i sistemski softver.

Zahtevi za bezbednost su povezani sa zahtevima za podršku funkcionisanja tako što utiču na zahteve za podršku pre isporuke (priprema bezbednosne infastrukture u organizaciji), za podršku u toku funkcionisanja sistema (održavanje kripto opreme), za podršku u ovladavanju sistemom (obuka u primeni bezbednosnih mehanizama) i za podršku korisnicima servisa (uticaj na korisnika da primenjuje i poštuje mere bezbednosti).

Zahtev za bezbednost ima uticaj na zahteve interoperabilnosti prilikom izbora aplikacija i hardvera tako što aplikacije i hardver moraju da se definišu tako da ispunjavaju zahteve za bezbednost. Bezbednost je bitna i prilikom projektovanja i implementacije komponenti PKI jer njihova interoperabilnost mora da ispunjava bezbednosne zahteve. Cilj domenske interoperabilnosti je uspostavljanje viskokog nivoa bezbednosti između dva PKI domena, pa bezbednost utiče na izbor najboljeg rešenja za interoperabilnost PKI domena.

4.8.4. Uticaj softversko-hardverskih zahteva na zahteve iz klasifikacione šeme

Ovi zahtevi ostvaruju uticaj na druge PKI zahteve. U klasi poslovno organizacionih zahteva najviše utiču na zahteve za ekonomičnost, a takođe i na zahteve za unapređenje poslovanja i bezbednosti, za edukaciju i za izbor poslodavca.

Opšti hardverski i softverski zahtevi ne bi smeli bitno da utiču na zahteve za PKI komponente i servise, dok specifični zahtevi za hardver (zahtev za kripto opremu) i softver (zahtev za softver serifikacionog tela, za softver vlasnika ili korisnika sertifikata) utiču na zahteve za PKI komponente i servise. Najveći uticaj se ostvaruje na opšte zahteve za komponente i servise, zahteve za sertifikaciono telo i za servise korisnika.

Zahtevi za softver i hardver ne bi trebali da ostvare bitan uticaj na zahteve bezbednosti i tako naruše politiku bezbednosti. Uticaj zahteva za hardver i softver na bezbednosne zahteve može se

uvažiti samo ako poboljšavaju bezbednost i perfomanse PKI sistema. Izbor odgovarajuće kripto opreme uticaće na bezbednost servisa za elektronsko potpisivanje ili širovanje kroz snagu generisanog kriptografskog ključa (dužina i kvalitet algoritma za generisanje ključeva), a time i na bezbednost poslovnih transakcija.

Zahtevi za hardver i softver ostvaruju najveći uticaj na zahteve za podršku u funkcionisanju i to u potkategorijama koj se odnose na održavanje i funkcionisaje PKI sistema u operativnoj upotrebi. Oprema i softver moraju biti funkcionalni sa minimalnim vremenom otkaza.

Softverski i hardverski zahtevi mogu da traže opremu i softver od različitih proizvođača, ali moraju imati mogućnost međusobnog funkcionisanja. To znači da utiču na zahteve interoperabilnosti softvera i hardvera.

4.8.5. Uticaj zahteva za podršku funkcionisanja PKI na zahteve iz klasifikacione šeme

Zahtevi za podršku funkcionisanja utiču na poslovno-organizacione zahteve i to na: zahtev za ekonomičnost, za marketing, zahtev unapređenje poslovanja, organizacione zahtev i zahteve za izbor isporučioca PKI sistema.

Zahtevi za podršku funkcionisanja utiču i na zahteve za PKI komponente i servise. Ukoliko nije moguće razviti podršku funkcionisanja u skladu sa klasifikacionom šemom potrebno je da se u toku definisanja zahteva za komponente PKI i servise odrede i zahtevi koji će uticati na razvoj proizvoda koji ne traži složen sistem podrške, ali u granicama pouzdane funkcionalnosti i bezbednosti.

Sama podrška funkcionisanja sistema ne treba da ima direktan uticaja na postavljanje zahteva za bezbednost u fazama razvoja i implementacije sistema, jer svojim delovanjem treba da omogući sprovođenje mera bezbednosti. Može ostvariti indirektan uticaj kroz uočavanje bezbednosnih problema u toku pružanja podrške koji će uticati na defnisanje zahteva za nadogradnju PKI sistema.

Zahtevi za podršku funkcionisanja ne bi trebalo da utiču na zahteve za hardver i softver jer su oni prevashodno određeni zahtevima za PKI komponente i servise i zahtevima za bezbednost. Mogu da utiču ako izabrana oprema ne zadovoljava zahteve podrške i da traže da se obezbedi druga

oprema ili softver koji neće narušiti zahtevano izvršavanje komponenti i servisa, kao i definisane mere bezbednosti. U toku pružanja podrške funkcionisanja mogu se pojaviti novi zahtevi za hardver i softver koji bi PKI sistem učinili efikasnijim i bezbednim.

Zahtevi za podršku funkcionisanja PKI mogu imati uticaj na zahteve interoperabilnosti aplikacija i hardvera iz klase zahteva za interoperabilnost.

4.8.6. Uticaj zahteva za interoperabilnost na zahteve iz klasifikacione šeme

Domenska interoperabilnost omogućuje organizaciji da proširi bezbedno elektronsko poslovanje prema organizacijama iz drugih PKI domena. Međutim, domenska interoperabilnost utiče na poslovne zahteve u oblasti marketinga i edukacije. Uticaj na oblast marketinga je ta što je vrednost uticaja domenske interoperabilnosti potrebno predstaviti postojećim i novim klijentima i organizacijama. Uvođenje ovakve novine zahteva dodatnu edukaciju zaposlenih. Domenska interoperabilnost utiče i na organizacione zahteve u oblasti zahteva za pripremu uvođenja PKI i zahteva za regulatorna dokumenta.

Interoperabilnost ima uticaja i na zahteve za komponente jer moraju zajedno da funkcionišu. Ima uticaja i na izbor protokola preko kojih će komponente međusobno razmenjivati podatke. Najveći uticaj ima na komponente sertifikacionog tela i registracionog autoriteta jer su to komponente koje međusobno najviše komuniciraju. Interoperabilnost ima uticaja i unutar samih komponenti, npr. komponenta sertifikacionog tela utiče na izbor protokola za razmenu podataka i protokola za upravljanje statusom sertifikata.

Zahtevi za interoperabilnost imaju uticaj na zahteve za softver i hardver, jer komponente koje će se na njima izvršavati moraju da efikasno funkcionišu jedne sa drugima.

Zahtevi za interoperabilnost aplikacija, hardvera, komponenti ne smeju da narušavaju definisane zahteve za bezbednost, kako u međusobnoj komunikaciji tako i u komunikaciji delova unutar iste kategorije.

Interoperabilnost utiče na softversko-hardverske zahteve jer definisanje ovih zahteva mora da omoguću neometanu saradnju softvera i hardvera.

Zahtevi za interoperabilnost aplikacija i hardvera i za interoperabilnost PKI komponenti mogu uticati na zahteve održavanje koji se odnose na održavanja hardver i softvera različitih proizvođača.

4.8.7. Uticaj tranzicionih zahteve na ostale zahteve iz klasifikacione šeme

Tranzicioni zahtevi nastaju u svim fazama razvoja PKI sistema i oni ne utiču na zahteve iz klasifikacione šeme prilikom razvoja sistema nego već tek kada dođe do nadogradnje PKI sistema. Cilj tranzicionih zahteva je da se PKI sistem unapredi, učini efikasnim i bezbednim.

4.9. Prednosti i nedostaci klasifikacione šeme

Predložena klasifikacija je dobra početna osnova za klasifikaciju zahteva PKI sistema. U radu, pored zahteva za PKI proizvode (softver, servisi), određene su i kategorije zahteva koji treba da omoguće lakše uvođenje PKI sistema i njegovo kasnije funkcionisanje. Posebno je izdvojena kategorija bezbednosnih zahteva na koju treba obratiti posebnu pažnju jer obuhvata bezbednosne zahteve za ceo PKI sistem. Predložena klasifikacija ima svoje prednosti i nedostatke. Prednosti predložene kasifikacije zahteva za PKI sistemom su:

- klasifikacija zahteva ukazuje menadžmentu na potrebne radnje i promene koje je potrebno uraditi pre, za vreme implementacije i u toku rada PKI sistema,
- omogućava timu za razotkrivanje zahteva da definiše granice u kojima se zahtevi razotkrivaju,
- detaljnost i sveobuhvatnost koja omogućava projektantima sistema da zadovolje zahteve korisnika, kao i timu za testiranje da proveri da li je proizvod ispunio zahteve korisnika,
- pomoć projektantskom timu da obuhvati sve značajne zahteve u procesu razotkrivanja i definisanja zahteva,
- omogućava rukovodećoj strukturi da bolje i lakše sprovede pripremne aktivnosti za uvođenje PKI sistema, kao i aktivnosti na njegovom održavanju u funkcionisanju,
- primena zahteva za PKI (poslovno-organizacioni zahtevi, zahtevi za podršku, tranzicioni zahtevi) u drugim projektima,
- u procesu razotkrivanja i definisanja zahteva učestvuju različiti izvori (npr. menadžeri, zaposleni, stručni timovi korisnika, dokumentacija) specijalizovani za određenu oblast,

- omogućava korisniku uvid u PKI sistem kroz zahteve koje je potrebno razotkriti i definisati,
- brz razvoj PKI sistema kroz smanjenje vremena za pripremu organizacije, za razotkrivanje i definisanje zahteva i za podršku funkcionisanja,
- smanjuje mogućnost kašnjenja uvođenja PKI sistema u organizaciju,
- smanjuje mogućnost naknadnog definisanja zahteva u narednim razvojnim fazama projekta,
- smanjuje troškove i produženje vremena realizacije projekta zbog loše ili naknadno definisanih zahteva,
- sprečava konfuziju u radu tima prilikom razotkrivanja i definisanja zahteva,
- daje dobru osnovu za testiranje i validaciju implementiranog PKI sistema.

Nedostaci predložene klasifikacije zahteva za PKI sistemom su:

- predložena kalsifikacija može predstavljati problem projektantskom timu koji ima svoju razvijenu metodologiju u razotkrivanju i definisanju zahteva za razvoj softvera,
- odbacivanje od strane izvođača projekta jer je usmeren samo na razvoj softverskog rešenja proizvoda, a ne na uvođenje celokupnog PKI sistema,
- ne objašnjavaju se elementarni zahtevi veće se samo nabrajaju,
- detaljnost može navesti rukovodstvo organizacije da odustane od uvođenja PKI sistema jer na osnovu navedene klasifikacije može zaključiti da se radi o suviše složenom sistemu,
- funkcionisanje tima za razotkrivanje i definisanje zahteva „linijom manjeg otpora“ zbog velikog broja zahteva.

5. Kvalitet zahteva

5.1. Osnovno o kvalitetu zahteva

Pojam zahtev se koristi u softverskom inženjeringu još od 1960-ih godina [100]. Internacionalni institut za poslovnu analizu (International Institute of Business Analsys, IIBA) u svom vodiču *Guide to the Business Analysis Body of Knowledge*® version 2 [33] zahtev definiše na sledeći način:

1) Uslov ili sposobnost potrebna zainteresovanoj strani da reši problem ili postigne cilj.
2) Uslov ili sposobnost koju mora da ispuni ili poseduje rešenje ili komponenta rešenja da bi se zadovoljio ugovor, standard, specifikacija ili drugi formalno nametnuti dokumenti.
3) Dokumentovani prikaz stanja ili sposobnosti kao u (1) ili (2).

Navedena definicija je zasnovana na IEEE 610.12-1990: IEEE Standardni rečnik terminologije softverskog inženjerstva [45].

Procena kvaliteta softverskog proizvoda uglavnom se fokusira na završetak faze implementacije kada se radi testiranje. Procena kvalitata softvera treba da počne ranije i to u fazi identifikovanja i definisanja zahteva. Loše identifikovani i definisani zahtevi mogu uticati na druge zahteve, a isto i na naknadne nedostatke u arhitekturi, dizajnu, kodiranju i testiranju.

Kvalitet zahteva zavisi od konteksta u kome se posmatra. Kontekst može biti idealistički, odnosno da se kvalitet smatra nečim čemu uvek težimo kao idealu. Međutim, idealan zahtev se nikada ne može u potpunosti dostići.

Drugi kontest je korisnički. Zahtevi se promatraju kroz kvalitet softverskog proizvoda koji treba da ih ispuni. Kroz ovaj kontekst definišu se zahtevi koji treba da opišu šta korisnik zahteva od konačnog proizvoda.

Treći kontekst odnosi se na pridržavanje standarda i proceni da li je proizvod izrađen pravilno i pravovremeno. Zahteve treba definisati na način koji omogućava efektan i efikasan razvoj proizvoda kroz sve životne faze.

Četvrti kontekst odnosi se na sagledavanje proizvoda i ustanovljavanju unutrašnjih kvaliteta proizvoda koji se mogu meriti. Inženjeri zahteva moraju da prate određene standarde kada određuju zahteve kako bi obezbedili kvalitet zahteva od samog početka.

Peti kontekst zasniva se na vezi između kvaliteta i cene, odnosno smatra se da je kvalitet nešto za šta je kupac spreman da plati. Kupci moraju da odluče o vrednosti svakog zahteva, kao i da li je trošak implementacije opravdan [101].

Standardi su početna tačka za definisanje kvaliteta zahteva i specifikacije zahteva. Nisu samo standardi dovoljni da bi se definisali kvalitetni zahtevi nego i postupak kako sprovesti dobar inžinjering zahteva. Potrebno je postići optimalan kompromis između željenog kvaliteta i raspoloživih resursa s obzirom na specifičan kontekst zahteva i potrebom za kvalitetom PKI.

5.2. Tehnike i metode za procenu kvaliteta zahteva

U radu [102] je predstavljen okvir za dobijanje indikatora kvaliteta „niskog nivoa“ za tekst zahteva, kao što su veličina zahteva, broj dvosmislenih termina, imperativni glagolski oblici, preklapanje zahteva i tako dalje. Rad se fokusira na analizi kvaliteta teksta zahteva, a ne na značaj ili sadržaj zahteva, niti na proces definisanja šta zainteresovane strane zaista žele. Metrike niskog nivoa ne mogu zameniti stručnu procenu o kvalitetu sadržaja zahteva, ali mogu da obezbede usmerenja za njihovo poboljšanje.

U radu [103] autori sistematizuju listu poželjnih indikatora koje treba da ispuni specifikacija zahteva. Razrađuju teorijski okvir koji služi kao osnova za dizajn i konstrukciju praktičnog alata: definišu merljive indikatore, taksonomiju indikatora i njihov međusobni odnos, određuju indekse kvaliteta zahteva i globalnog kvaliteta. Potom, predstavljaju alat za procenu kvaliteta zahteva, Analizator kvaliteta zahteva [103]. Alat izračunava metriku kvaliteta na potpuno automatizovan način, a mogu ga koristiti inženjeri zahteva, menadžeri kvaliteta, itd. jer apstrahuje složenost obrade prirodnog jezika.

U radu [104] autori koriste industrijski pristup za analizu procene kvaliteta zahteva. Pristup je implementiran u alatu za analizu kvaliteta sistema kompanije „The Reuse Company” koji podržava analizu kvaliteta zahteva kroz indikatore kvaliteta: korektnost, kompletnost i konzistentnost. Pristup se zasniva na kreiranju preseka o statusu specifikacije zahteva u datom

trenutku. Kolekcija preseka pokazuje kako je kvalitet tokom projekta evoluirao kao rezultat promena u skupu zahteva ili u skupu indikatora kvaliteta za procenu. Automatizovana podrška olakšava analizu evolucije kvaliteta zahteva.

U radu [105] autori integrišu tehnike NLP (Natural Language Processing) i GQM (Goal-Question-Metric) u jednom modelu za merenje kvaliteta zahteva i predlažu prototip alata za automatizovanu validaciju zahteva za ruski jezik. Tekst softverskih zahteva napisan na prirodnom jeziku se može analizirati pomoću NLP alata kako bi se identifikovale reči i fraze koje izjavu čine dvosmislenom. Primena pristupa cilj-pitanje-metrika u modelu kvaliteta pomaže u odabiru najvažnijih atributa kvaliteta i kreiranju indikatora. Koriste sledeće indikatore kvaliteta: dvosmislenost, jedinstvenost, subjektivnost, potpunost i čitljivost. Model kvaliteta je implementiran u prototip koji koristi tehniku obrade prirodnog jezika za zahteve napisane na ruskom jeziku uz podršku eksternog API-ja. Identifikovani indikatori kvaliteta treba da ukažu na konkretne nedostatke i da daju predloge za poboljšanje. Predloženi prototip alata kombinuje sve ove indikatore i izračunava stepen kvaliteta na potpuno automatizovan način.

U radu [106] je predstavljena strukturirana metodologija za merenje pojedinačnog i kolektivnog kvaliteta zahteva. Zahtevi su okarakterisani sa deset faktora kvaliteta, od kojih svaki ima pridruženu individualnu metriku i metriku kvaliteta opštih zahteva. Individualne metrike kvaliteta su: ispravnost, potpunost, doslednost, jasnoća, nedvosmislenost, povezanost, jedinstvenost, proverljivost, promenjivost i izvodljivost.

U radu [107] je predstavljen metod za objektivnu procenu kvaliteta specifikacije softverskih zahteva kroz upotrebu prirodnog jezika u specifikaciji zahteva i strukturi dokumenata. Razmatraju se tri karakteristike dokumenta: nedvosmislenosti, proverljivost i mogućnost modifikacije, kako bi se ukazalo na kvalitet dokumenta i nedostatke koji se pojavljuju tokom inženjeringa softverskih zahteva. Model procene procesa se primenjuje kao okvir za procenu kvaliteta specifikacije softverskih zahteva, a model procesa merenja i model informacija o merenju se koriste kao pristupi za predlaganje metode za procenu kvaliteta specifikacije i definisanje metrike, respektivno, korišćenjem Pirsonovog koeficijenta korelacije kao kriterijuma za proveru validnosti rezultata dobijenih procenom specifikacije primenom predloženog metoda, koji ukazuje da rezultati dobijeni procenom kvaliteta odražavaju kvalitet SRS, kao i očigledne nedostatke.

5.3. Karakteristike dobrih zahteva

Autori karakteristike dobrih zahteva različito navode, pri čemu neki autori naglašavaju karakteristike koje su najprikladnije njihovoj opštoj diskusiji ili specifičnom tehnološkom domenu koji se obrađuje. Opšte su priznate sledeće karakteristike [49, 51]: jedinstvenost ili kohezivnost, kompletnost, konzistentnost, nekonjugovanost ili atomičnost, sledljivost, aktuelnost, nedvosmislenost i proverljivost.

U radu [108] dat je pregled dobrih karakteristika koje utiču na zahtevani kvalitet. A to su:

- Kompletnost (potpunost) znači da zahtev mora biti u potpunosti deklarisan bez nedostajućih informacija, kao i da sadrži sve što zainteresovana strana traži.
- Dosledan znači da zahtev ne sme biti u suprotnosti ni sa jednim drugim zahtevom i mora biti u potpunosti u skladu sa dokumentacijom.
- Korektnost (ispravnost) znači da zahtev mora biti u skladu sa potrebom o kojoj su se zainteresovane strane dogovorile, odnosno predstavlja ono što je zainteresovana strana tražila.
- Nedvosmislenost znači da se zahtev može protumačiti na jedan i samo jedan način, da je jasan i ne zbunjuje.
- Proverljivost znači da se implementirani zahtev može proveriti u sistemu kroz jedan od sledećih načina: inspekcija, analiza, demonstracija ili testiranje kako bi se utvrdilo da sistem ispunjava zahtev.
- Gradabilnost (gradacija) znači da se zahtev može klasifikovati na osnovu značaja klijenta i nekog drugog kriterijuma.
- Promenljivost znači da promene u zahtevu ne utiču na strukturu i stil zahteva.
- Sledljivost se odnosi na to da li se može pronaći izvor nastanka zahteva i da li se zahtev može jedinstveno identifikovati i pratiti.
- Razumljivost znači da korisnici i razvojni tim mogu razumeti zahtev.
- Izvodljivost znači da se zahtev može realizovati u okviru postojećih ograničenja (npr. vremena i (ili) finansijskih sredstava.
- Jasnost se odnosi na činjenicu da zahtev mora biti jasan i jednostavan kako bi inženjer mogao lako da razume potrebe korisnika.
- Nezavisnost znači da zahtev ne zavisi od drugog zahteva kako bi se u potpunosti razumeo.
- Neredundantnost znači da zahtev ne bi trebalo da sadrži duple informacije.

- Sažetost se odnosi na to da zahtev mora sadržati relevantne informacije kako bi se razumele potrebe zainteresovane strane.
- Nevezanost za implementaciju. To znači da zahtev ne sme da sadrži informacije o implementaciji i dizajnu.
- Neophodnost. Odnosi se na to da zahtev ne sadrži nepotrebne informacije, odnosno informacije koje nisu u vezi sa potrebama zainteresovane strane.

Navedena lista može se proširiti sledećim dobrim karakteristikama: tačnost, prioritet, jedinstvenost [109], kohezivnost, spoljna posmatranost, obaveznost, relevantnost, upotrebljivost, validbilnost [110]. Pregled kvaliteta zahteva različitih autora data je u radu [111] kako bi se inženjerima pružila konzistentna podrška prilikom definisanja specifikacije zahteva. Rezultati rada se mogu uzeti za budući razvoj alata za podršku automatizovanoj ili poluautomatskoj evaluaciji kvaliteta specifikacije zahteva.

5.4. Generalizovani problem zadovoljenja fazi ograničenja sa prioritetima

Generalizovani problem zadovoljenja fazi ograničenja sa prioritetima ili GPFCSP (Generalized Prioritized Fuzzy Constraint Satisfaction) predstavlja proširenje PFCSP (Prioritised Fuzzy Constraint Satisfaction Problem) [112] koje se odnosi na upotrebu disjunkcije i negacije. PFCSP sistemi omogućavaju upotrebu konjukcije, odnosno t-norme nad ograničenjima. Da bi se PFCSP proširio na GPFCSP, za disjunkciju se uzima t-konorma dualna t-normi izabranoj za konjunkciju, dok se za negaciju koristi standardna negacija: N(x) = 1−x. Proširenje se realizuje kroz proširenje treće i četvrte aksiome PFCSP-a, dok ostale aksiome nema potrebe proširivati jer se odnose na konjunkciju. Izmene kod treće aksiome se odnose na dodavanje disjunkcije, dok se četvrta aksioma generalizuje tako da monotonost važi samo u slučaju kada se ne upotrebljava negacija. Proširena definicija i njene aksiome dati su u nastavku i preuzete iz [113, 114].

Definicija 1. Neka su *X, D,* C^f*,* ρ *,* g definisani kao:
1. Skup $X = \{x_i \mid i = 1, 2, \dots, n\}$ je konačan skup promenljivih.
2. Skup $D = \{D_i \mid i = 1, 2, \dots, n\}$ je konačan skup domena. Svaki domen D je skup elemenata koji može uzimati promenljive x iz skupa X.
3. Fuzzy skup ograničenja C^f predstavljen je fuzzy relacijama čije se funkcije pripadnosti definišu na sledeći način:

$$\mu_{R_i^f}: \left(\prod_{x_j \in var\left(R_i^f\right)} D_j\right) \rightarrow [0,1], \tag{5.1}$$

gde $var\left(R_i^f\right)$ predstavlja skup promenjivih u navedenim ograničenjima R_i^f.

4. ρ je funkcija prioriteta $\rho: C^f \rightarrow (0, \infty]$.

5. Funkcija g agregira prioritete svakog ograničenja sa vrednošću tog ograničenja, pri čemu se tako agregirane vrednosti uz pomoć operatora agregacije $\oplus$ agregiraju u globalni stepen zadovoljenja ograničenja,

a GPFCSP predstavlja devetorku $(X, D, C^f, \rho, g, \wedge, \vee, \neg)$.

Elementarna formula je uređen par $\left(x, \rho\left(R_i^f\right)\right)$ gde je $R_i^f \in C^f$, a $x \in Dom\left(R_i^f\right)$ je stepen zadovoljenja u navedenom ograničenju R_i^f, dok je $\rho\left(R_i^f\right)$ njegov prioritet.

Formula GPFCSP-a definisana je na sledeći način:

1. Elementarna formula je formula.
2. Ako su f_1 i f_2 formule, onda su i $\wedge(f_1, f_2)$, $\vee(f_1, f_2)$ i $\neg(f_1)$ takođe formule.

Stepen zadovoljenja ograničenja $\alpha_F(\vartheta_X)$ za neku valuaciju ϑ_X se izračunava u odnosu na interpretaciju veznika.

Sistem je GPFCSP ako važi:

1. Ako je $F = \wedge_{i \in (1,\ldots,n)} f_i$ GPFCSP formula, gde su f_i, $i \in \{1, \ldots, n\}$ elementarne formule i neka je C^F skup ograničenja koji se pojavljuje u formuli i ako za fuzzy ograničenje R_{max}^F važi $\rho_{max} = \rho_{max}(R_{max}^F) = max\{\rho(R^F | R^F \in C^F)\}$, tada za svaku formulu F važi i $\mu_{R_{max}^f}\left(\vartheta_{var\left(R_{max}^f\right)}\right) = 0$ sledi $\alpha_F(v_x) = 0$.
2. Ako je $\exists \rho_0 \in [0,1]$ takvo da je $\forall R^f \in C^f$ važi da je $\rho(R^f) = \rho_0$, onda je globalni stepen zadovoljenja ograničenja dat sa: $\alpha_F(\vartheta_x) = F_\wedge(\vartheta_x)$, gde je $F_\wedge$ interpretacija logičke formule F u fuzzy logici.
3. Pretpostavimo da za $R_i^f, R_j^f \in C^f$ važi $\rho\left(R_i^f\right) \geq \rho\left(R_j^f\right)$, neka je dato $\delta > 0$ i neka su date dve kombinovane valuacije ϑ_x i ϑ'_x, takve da za $\forall R^f \in C^f$ važi:
    a. ako $R^f \neq R_i^f$ i $R^f \neq R_j^f$, onda $\mu_{R^f}\left(\vartheta_{var(R^f)}\right) = \mu_{R^f}\left(\vartheta'_{var(R^f)}\right)$
    b. ako $R^f = R_i^f$, onda $\mu_{R^f}\left(\vartheta_{var(R^f)}\right) = \mu_{R^f}\left(\vartheta'_{var(R^f)}\right) + \delta$
    c. ako $R^f = R_j^f$, onda $\mu_{R^f}\left(\vartheta_{var(R^f)}\right) = \mu_{R^f}\left(\vartheta'_{var(R^f)}\right) + \delta$

Tada, ako važi:

$F = \wedge_{k=1,\dots,n} \left(x_k, \rho\left(R_k^f\right)\right),\ x_k \in Dom(R_k)$

$F = \vee_{k=1,\dots,n} \left(x_k, \rho\left(R_k^f\right)\right),\ x_k \in Dom(R_k)$

sledi da je:

$\alpha_F(\vartheta_X) \geq \alpha_F(\vartheta'_x)$.

4. Neka su date dve različite kombinacije valuacije ϑ_x i ϑ'_x sa osobinom da $\forall R^f \in C^f$ važi $\mu_{R^f}\left(\vartheta_{var(R^f)}\right) \geq \mu_{R^f}\left(\vartheta'_{var(R^f)}\right)$. Tada ako formula *F* ne sadrži negaciju, važi $\alpha_F(\vartheta_X) \geq \alpha_F(\vartheta'_x)$.
5. Ako postoji kombinovana valuacija ϑ_x takva da $\forall R^F \in C^F$ važi $\mu_{R^F}\left(\vartheta_{var(R^F)}\right) = 1$ i ako je F formula oblika $F = \wedge_{i\in\{1,\dots,n\}} f_i$ ili $F = \vee_{i\in\{1,\dots,n\}} f_i$, gde su $f_i,\ i \in \{1, \dots, n\}$ elementarne formule, tada sledi da je $\alpha_F(\vartheta_X) = 1$.

Takači u radu [115] opisuje i dokazuje jedan specijalni GPFCSP sistem.

Teorema 2. Sledeći sistem $(X, D, C^f, \rho, g, \wedge, \vee, \neg,)$ gde je $\wedge = T_L, \vee = S_L, \neg = N_S$ i, konačno, $\Diamond\,(x_i, p_i) = S_p(x_i, 1 - p_i)$ je GPFCSP. Globalni stepen zadovoljenja ograničenja valuacije v_x za formulu F se računa na sledeći način:

$$\alpha_x(\vartheta_x) = \Phi\left\{\Diamond\left(v_{X_i}\right)\frac{\rho\left(R_i^f\right)}{\rho_{max}} | R^f \in C^f\right\} \tag{5.2}$$

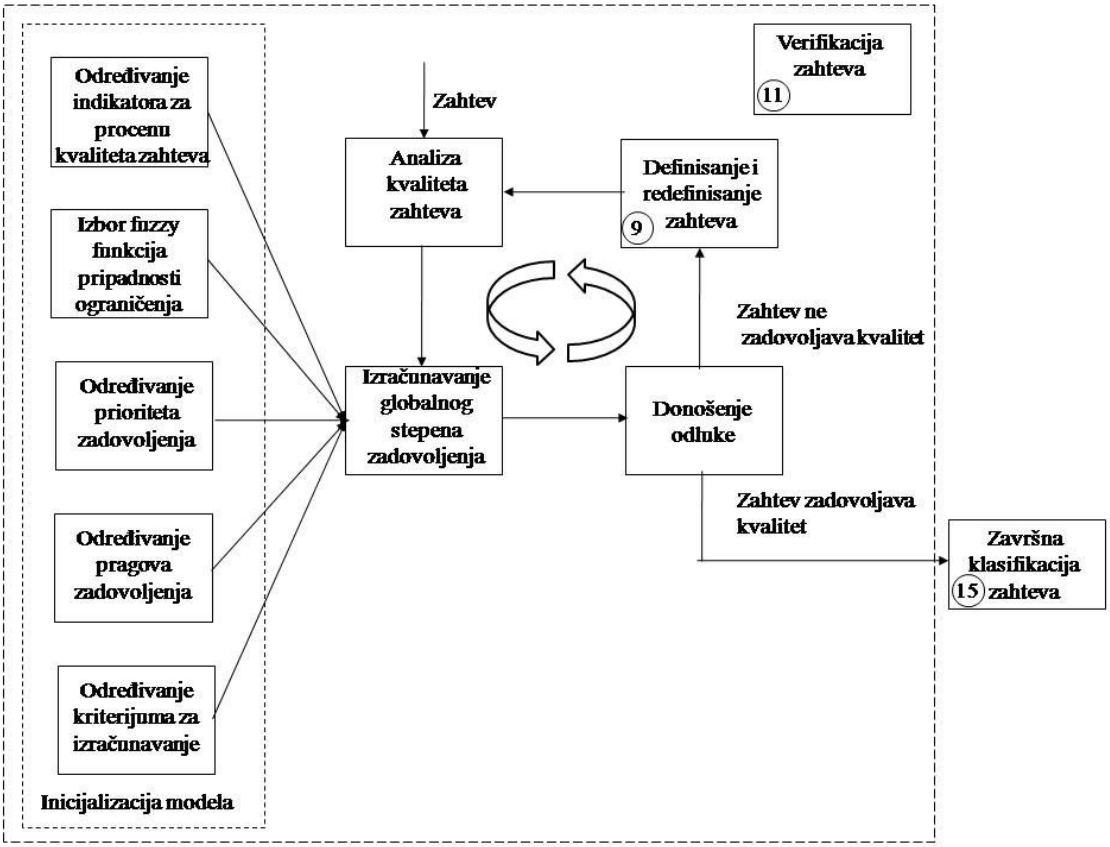
Gde je C^f skup ograničenja formule F, ρ_{max}=max$\left\{\rho\left(R_i^f\right), R^f \in C^f\right\}$, a Φ je interpretacija formule F u GPFCSP.

5.5. Model za procenu kvaliteta zahteva zasnovan na GPFCSP

Model za određivanje kvaliteta zahteva zasnovane je na modelu iz rada [113]. Model je proizašao kao rešenje za unapređenje procesa definisanja zahteva u cilju smanjenja loše definisanih zahteva za PKI kako bi se umanjili potencijalni problemi: razumevanja zahteva u toku dizajna i implementacije, krajnje rešenje koje nije želeo korisnik, usporavanje realizacije projekta PKI. Na osnovu modela datog na slici 14, evaluatori kvaliteta zahteva ili lice koje definiše i redefiniše zahteve, može proceniti da li zahtev ispunjava karakteristike dobrih zahteva, odnosno da li je zahtev dovoljno kvalitetan da neće prouzrokovati probleme. Ukoliko zahtev ne ispunjava zadati kvalitet, takav zahtev se redefiniše sve dok ne ispuni zadati kvalitet.

Model se primenjuje kroz sledeće faze:

- Faza inicijalizacije – u ovoj fazi se određuju indikatori za procenu kvaliteta, definišu se fuzzy funkcije pripadnosti ograničenja, određuju prioriteti i pragovi zadovoljenja i određuje se kriterijum za izračunavanje.
- Faza provere kvaliteta zahteva – u ovoj fazi se izračunava globalni stepen zadovoljenja (stepen kvaliteta zahteva) na osnovu koga se donosi odluka o ispunjenosti traženog kvaliteta zahteva. Ako zahtev ne ispunjava traženi kvalitet potrebno je izvršiti redefinisanje zahteva. Redefinisani zahtev se podvrgava analizi kvaliteta na osnovu koje se izračunava stepen kvaliteta zahteva. Proces se ponavlja sve dok zahtev ne zadovolji definisani kvalitet iz faze inicijalizacije.



Slika 14. Model za procenu kvaliteta zahteva

5.5.1. Određivanje indikatora za odlučivanje o kvalitetu zahteva

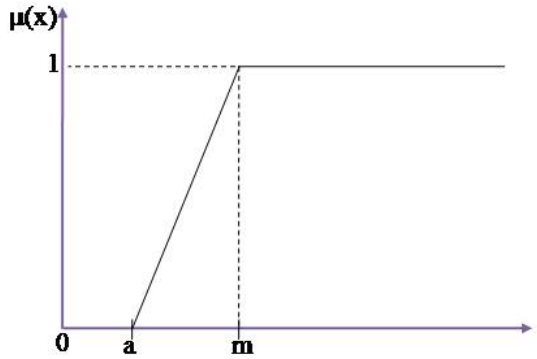
Indikatori za odlučivanje o kvalitetu zahteva biraju se iz karakteristika dobrih zahteva. U literaturi [108, 109, 110] postoji više različitih listi karakteristika za definisanje dobrih zahteva. Izbor više karakteristika uticaće na bolju procenu kvaliteta zahteva, ali će prouzrokovati veću složenost u postupku i proračunu kvaliteta zahteva. Izabrani indikatori, odnosno karakteristike dobrih zahteva, predstavljaju lingvističke varijable kada se primeni fuzzy logika [113].

5.5.2. Izbor fuzzy funkcija pripadnosti ograničenja

Funkcije pripadnosti predstavljaju se kao karakteristične funkcije koje u osnovi definišu fuzzy skup. Cilj ove funkcije je pridruživanje stepena članstva svakom elementu iz domena korenspondirajućeg fuzzy skupa. Postoje različite vrste funkcija pripadnosti, kao što su trapezna, trouglasta, gausaova, logička. Funkcije pripadnosti se konstruišu shodno dobijenim istraživanjima. Eksperti najčešće slobodno izabiraju ili konstruišu funkcije pripadnosti za potrebe rešavanja problema, tako da zadovoljavaju sledeće uslove:

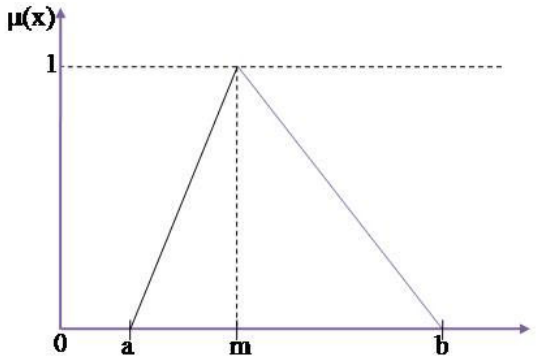
- Domen funkcije pripadnosti je u opsegu (range) [0,1]. Domen funkcije pripadnosti nikad nije negativan.
- Injektivnost, odnosno svaki element x iz fuzzy skupa X funkcija $\mu_A(x)$ se preslikava u različite vrednosti. Isti element fuzzy skupa ne može imati različite stepene pripadnosti za isti fuzzy skup.

U zavisnosti od vrste funkcije pripadnosti, dobijaju se različiti fazi skupovi. Zadeh u radu [116] klasifikuje ove funkcije u dve kategorije: linearne i nelinearne. Najčešće korišćene funkcije pripadnosti prikazane su na slikama 15, 16, 17, 18 i 19.



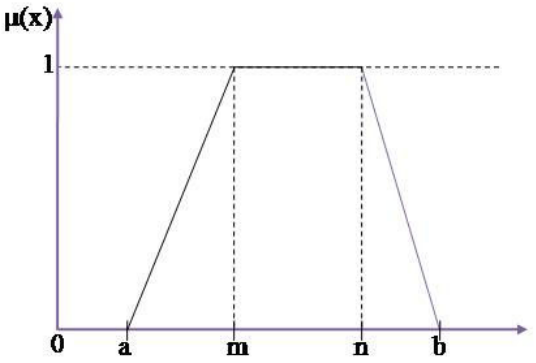
$$\mu_A(x) = \begin{cases} 0, x \in (0, a], \\ \dfrac{(x-a)}{(m-a)}, x \in (a, m) \\ 1, x \in [m, \infty) \end{cases}$$

Slika 15. Sigma funkcija pripadnosti



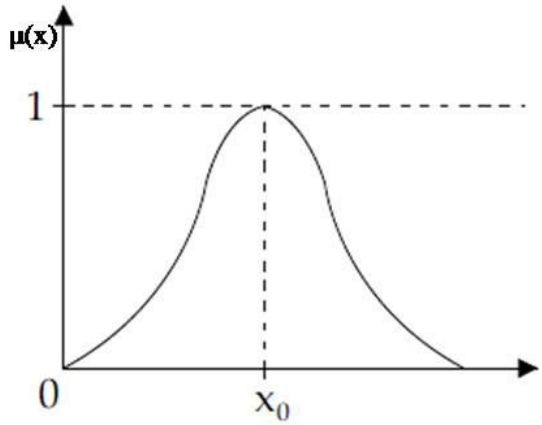
$$\mu_A(x) = \begin{cases} 0, x \leq a, x \geq b \\ \dfrac{(x-a)}{(m-a)}, x \in (a,m) \\ \dfrac{(b-x)}{(b-m)}, x \in [m,b) \end{cases}$$

Slika 16. Trougaona funkcija pripadnosti



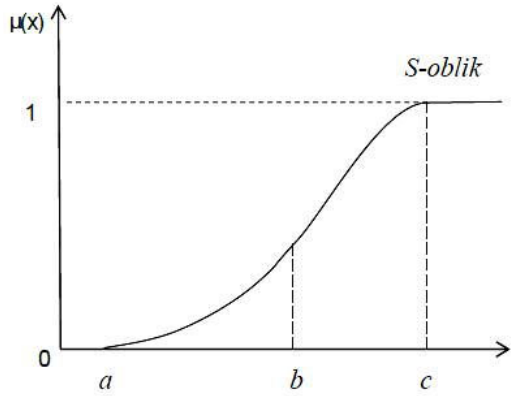
$$\mu_A(x) = \begin{cases} 0, x \leq a, x \geq b \\ \dfrac{(x-a)}{(m-a)}, x \in (a,m) \\ 1, x \in [m,n] \\ \dfrac{(b-x)}{(b-n)}, x \in (n,b) \end{cases}$$

Slika 17. Trapezoidna funkcija pripadnosti



$$\mu_A(x) = e^{\frac{-(x-x_0)^2}{d}}$$

Slika 18. Gausova funkcija pripadnosti



$$\mu_A(x) = \begin{cases} 0, x < a \\ 2\left(\frac{x-a}{c-a}\right)^2, a \le x \le b \\ 1 - 2\left(\frac{x-c}{c-a}\right)^2, b < x \le c \\ 1, x > c \end{cases}$$

Slika 19. S-funkcija pripadnosti

Parametri za procenu kvaliteta zahteva predstavljaju lingvističke varijable kada se prevedu u fuzzy logiku. Da bi se izračunala lingvistička varijabla, potrebno je odrediti funkcije pripadnosti za svaku lingvističku vrednost. Evaluatori na osnovu iskustva mogu definisati svoje funkcije pripadnosti.

5.5.3. Određivanje prioriteta i pragova zadovoljenja

U modelu, indikatori za procenu kvaliteta zahteva nemaju isti uticaj na donošenje odluke. Indikatore nije dovoljno podeliti na bitne i one manje bitne, nego je potrebno definisati stepen uticaja indikatora na krajnji rezultat. Stepen uticaja izražava se u procentima. Zato se u donošenju odluke za svaki indikator određuje prioritet. Manje bitni indikatori, čiji je uticaj na rezultat uglavnom zanemarljiv, imaju granične vrednosti koje se ne smeju prekoračiti. Granica ispod koje ne sme da se ide naziva se prag zadovoljenja (*threshold*) i poput prioriteta se izražava u procentima.

Prioriteti i prag zadovoljenja navode se neposredno posle fuzzy vrednosti u uglastim zagradama [P_vrednost, T_vrednost], a odnose se na samu fuzzy vrednost. Navedene vrednosti mogu biti iz intervala [0,1]. Ako prioritet za neku fuzzy vrednost nije naveden, podrazumevana vrednost je 1. Ukoliko ne postoji nikakvo ograničenje, prag zadovoljenja se ne navodi, a podrazumevana vrednost je 0. Ako prioritet i prag zadovoljenja za fuzzy lingvističku promenjivu prikažemo kao [P_0.7, T_0.4] to znači da promenjiva ima prioritet od 70% i prag zadovoljenja od 40%.

Stepen zadovoljenja ograničenja izračunava se upotrebom t-konormi S_p, gde je $S_p\left(\mu_{R_x^f}(\vartheta), 1 - \rho Rxf\right)$. ϑ je posmatrana vrednost, sa stepenom pripadanja $\mu Rxf\vartheta$ i prioritetom ρRxf [113].

5.5.4.Određivanje kriterijuma i izračunavanje globalnog stepena zadovoljenja ograničenja

Pre nego što se počne sa izračunavanjem globalnog stepena zadovoljenja ograničenja, potrebno je odrediti zavisnost između skupova ograničenja, odnosno indikatora. Skupovi ograničenja mogu biti konjunktivno ili/i disjunktivno povezani. Primer formule za izračunavanje globalnog stepena zadovoljenja gde postoji konjunktivna i disjunktivna povezanost između tri skupa ograničenja je $\left(R_1^f \vee R_2^f\right) \wedge R_3^f$.

$$\alpha = T_L\left(S_L\left(S_P\left(\mu_{R_1^f}(\vartheta), 1 - \rho\left(R_1^f\right)\right), S_P\left(\mu_{R_2^f}(\vartheta), 1 - \rho\left(R_2^f\right)\right)\right), S_P\left(\mu_{R_3^f}(\vartheta), 1 - \rho\left(R_3^f\right)\right)\right) \quad (5.3)$$

Globalni stepen zadovoljenja ograničenja α u slučaju konjunktivne zavisnosti izračunava se kao t-norma T_L, a u slučaju disjunktivne zavisnosti kao S_L dualna t-konorma od T_L [113] .

Formula se dalje rešava:

$$S_P(x, y) = x + y - xy \quad (5.4)$$

$$T_L(x, y) = max\ (x + y - xy, 0) \quad (5.5)$$

$$S_L(x, y) = min\ (x + y, 1) \quad (5.6)$$

5.5.5. Donošenje odluke o kvalitetu zahteva

Odluka o kvalitetu zahteva donosi se na osnovu izračunatog globalnog stepena zadovoljenja ograničenja i određenog stepena zadovoljenja za svaku varijablu. Definiše se minimalna granica kvaliteta. Ako je izračunati stepen zadovoljenja ispod granice kvaliteta onda zahtev treba redefinisati. U suprotom specifikacija zahteva zadovoljava traženi kvalitet.

Kada globalni stepen zadovoljenja ograničenja prelazi granicu kvaliteta, potrebno je proveriti da li je ispunjen stepen zadovoljenja za svaku varijablu (indikator) da bi se donela konačna odluka.

Ako bilo koji parametar nije ispunio stepen zadovoljenja, tada je potrebno redefinisati zahtev tako da parametri zadovolje traženi stepen.

Nakon redefinisanja zahteva, ponovo se vrši preocena zahteva u celosti, a ne samo za parametre kvaliteta koje je bilo potrebno poboljšati [113].

5.5.6. Analiza kvaliteta zahteva na osnovu izabranih parametara

Kvalitet zahteva određuje se procenom svakog izabranog indikatora tako što se odgovara na pitanja za procenu kvaliteta parametara. U literaturi [110, 117] postoji više različitih listi pitanja za procenu ispunjenosti karakteristika kvalitetnog zahteva.

Na osnovu odgovora, zahtev za razmatrani parametar može da ne ispunjava, delimično ispunjava, ispunjava ili delimično ne ispunjava kvalitet. Kada parametar delimično ispunjava kvalitet, to znači da ga većim delom ne ispunjava, a manjim ispunjava. U slučaju da parametar delimično ne ispunjava, to znači da većim delom zadovoljava kvalitet, a manjim delom ne zadovoljava. Delimičnu ispunjenost ili neispunjenost kvaliteta parametra evaluator izražava u procentima. Npr., parametar ne ispunjava, ali sa 20% ispunjava kvalitet, ili parametar ispunjava kvalitet zahteva, ali sa 10% ne ispunjava.

Ovakve situacije u određivanju nivoa ispunjenosti parametra nastaju kada evaluator na osnovu datih odgovora iz liste pitanja ne može tačno da proceni da li parametar u potpunosti ispunjava ili ne ispunjava.

Evaluator kvaliteta zahteva za procenu može koristiti Tabelu 4 tako što procenjuje u kojoj meri je zadovoljen parametar za svako pitanje. Ukoliko odgovor evaluatora nije jedna od vrednosti „ispunjava“ ili „ne ispunjava“, tada odgovor može biti jedna od delimičnih vrednosti. Evaluator tada procenjuje u kom procentu odgovor zadovoljava pitanje. Na primer, ako je odgovor da većim delom ispunjava, a manjim delom ne ispunjava, tada evaluator u koloni (4) unosi procenat odgovora (npr. 10%) što znači da vrednost 10% ne ispunjava. Nakon datih odgovora, evaluator donosi krajnju odluku o ispunjenosti parametra. Na primer, parametar delimično ispunjava 30% što znači da većim delom ne ispunjava, a manjim delom ispunjava.

Tabela 4. Tabela za procenu parametra kvaliteta zahteva

Zahtev: _____			Parametar:_____	
Pitanja	Ne ispunjava	Delimično ispunjava	Ispunjava	Delimično ne ispunjava
	(1)	(2)	(3)	(4)
Pitanje_1				
Pitanje_2				
Pitanje_3				
...				
Pitanje_n				
Procena parametra:				

6. Unapređenje definisanja zahteva za PKI

Zbog nedostataka okvira za usmeravanje definisanja zahteva, modeli su postali jedno od glavnih pitanja. Istraživači predlažu mnoge detaljne i fokusirane metode za razvoj zahteva. Međutim, većina ovih metoda je suviše složena za praktičnu primenu, pogotovo kada je primenjuje tim koji nije dovoljno upoznat sa problematikom pronalaženja i definisanja zahteva. Isto tako, neke metode su složene i komplikovane da bi ih u praksi primenjivali timovi koji se bave inženjeringom zahteva. Čak i primena metoda ili modela kroz specijalizovane alate stvara korisniku poteškoće da iskaže i definiše zahteve za svoje potrebe. Primena takvih alata stvara jaz između korisnika i projektantskog tima u pronalaženju i definisanju zahteva.

Za PKI sistem, iako je složen, mogu se primeniti četiri glavne aktivnosti inžinjeringa zahteva: utvrđivanje (elicitation) zahteva, modeliranje i analiza zahteva, osiguranje kvaliteta zahteva (validacija i verifikacija zahteva) i upravljanje i evolucija zahteva. Na slici 20. su prikazane navedene aktivnosti.

Slika 20. Glavne aktivnosti inžinjeringa zahteva

Utvrđivanje zahteva ima za cilj da otkrije potrebe zainteresovane strane, ciljeve sistema sa različitih gledišta (gledište kupaca, korisnika, ograničenja, okruženja za rad sistema, trgovine, marketinga i standarda, itd.), kao i da se razume kontekst u kome će budući sistem funkcionisati. Faza utvrđivanja zahteva počinje identifikacijom zainteresovane strane i prikupljanjem zahteva sa različitih stanovišta. Ovi zahtevi su neobrađeni jer nisu analizirani i nisu zapisani u notaciji koja se odnosi na dobro formiran zahtev. Faza elicitacije ima za cilj prikupljanje zahteva sa raznih gledišta kao što su poslovni zahtevi, zahtevi kupca, korisnika, ograničenja, bezbednosni zahtevi, zahtevi za informacije, standardi, itd. Glavne tehnike za utvrđivanje zahteva po Zowghi i Coulin [118] su: **tehnike prikupljanja podataka** (background study – prikupljanje informacija o sistemu, intervjui), **kolaborativne tehnike** (brainstorming, Joint Application Development (JAD) Workshops – radionice za zajednički razvoj aplikacije), **kognitivne tehnike** (card sorting - razvrstavanje kartica, repertory grids – mreža repertoara [119]), **kontekstualne tehnike** (posmatranje i analiza protokola), **kreativne tehnike** (radionice kreativnosti [120], ContraVision [121]).

Modeliranje i analiza zahteva. Prikupljeni zahtevi moraju biti precizno opisani na način razumljiv stručnjacima iz određene oblasti, programerima i drugim zainteresovanim stranama. Širok spektar neformalnih, poluformalnih i formalnih tehnika i notacija se mogu koristiti za specifikaciju zahteva i dokumentaciju. Izbor odgovarajuće metode često zavisi od vrste analize ili razloga. Analiza zahteva se odnosi na proces izgradnje specifikacije sistema koja zadovoljava zahteve kupca u odnosu na sistem i pruža dovoljno informacija za izgradnju sistema. Glavni cilj analize zahteva je da obezbedi formalni ili poluformalni opis sistema koji se gradi. Modeliranje zahteva odnosi se na proces izgradnje specifikacije sistema koju će na isti način razumeti i kupac (koji želi da se sistem izgradi i plaća za razvoj) i programer (koji je odgovoran za njegovu izgradnju). U fazi elicitacije se identifikuju zahtevi, osobine domena i druge pridružene specifikacije, dok modeliranje zahteva daje specifikaciju zahteva koja omogućava zainteresovanim stranama da se saglase o tome šta se razvija. Svakodnevni jezik je dobar način predstavljanja zahteva u ranoj fazi RE procesa, dok se poluformalne i formalne tehnike često koriste za sprovođenje sistematičnije i rigoroznije analize. Ova analiza takođe može dovesti do stvaranja dodatnih zahteva. Tehnike za modelovanje i analizu zahteva su: **tehnike za poboljšanje kvaliteta iskaza zahteva izraženih svakodnevnim jezikom** [122, 123, 124], **tehnike strukturalnog modelovanja** [125, 126], **modelovanje ponašanja** [127, 128], **modelovanje ciljeva** [129, 130].

Osiguranje kvaliteta zahteva. Da bi se obezbedio kvalitet zahteva potrebno je da se identifikuju, prijave (saopšte), analiziraju i poprave nedostaci u zahtevima. To uključuje i validaciju i verifikaciju. Validacija ima za cilj da proveri da li su specificirani i modelirani zahtevi i pretpostavke domena adekvatni stvarnim očekivanjima zainteresovanih strana, tj. validacija proverava da li traženi zahtevi odražavaju stvarne potrebe zainteresovanih strana, da li su realni i dosledni sa ograničenjima domena. Zainteresovanoj strani je bitno da zahtevi ispune očekivanja od samog početka. Da bi se to ostvarilo potrebno je koristiti tehnike koje se fokusiraju na proveru svakog **zahteva pojedinačno** (Quality gateway [131]) ili da se posmatra **specifikacija zahteva kao celina** (Walkthroughs [132]). Verifikacija pokriva širok opseg provera, uključujući kriterijume kvaliteta specificiranih i modeliranih zahteva (npr. doslednost). Takođe, verifikacijom se proverava da li zahtevi ispunjavaju neka svojstva (npr. konzistentnost) i da li specifikacija softvera ispunjava zahteve u datom domenu. Neke tehnike za verifikaciju su: argumentacija [133] i provera modela [128].

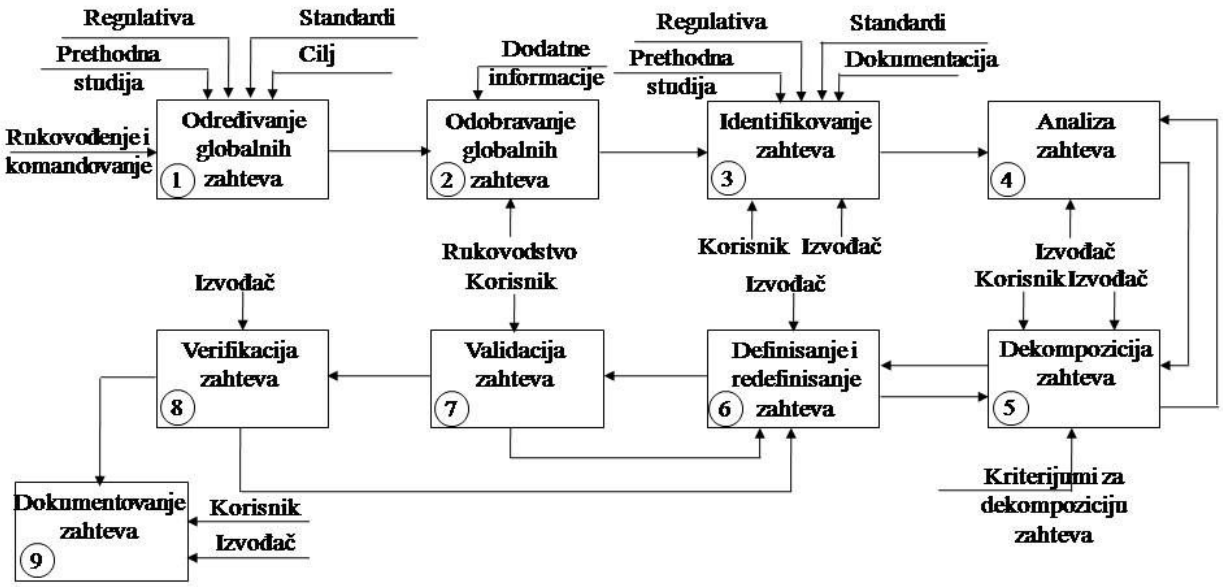
Upravljanje i evolucija zahteva. Upravljanje zahtevima odnosi se na rukovanje promenama zahteva, pregled i postizanje dogovara o zahtevima i njihovim prioritetima, kao i održavanje sledljivosti između zahteva i drugih softverskih artefakata. Tehnike koje se koriste za upravljanje i evoluciju zahteva su: **pregovaranje i određivanje prioriteta** (WinWin [134], MoSCoW [135], **komparacija parova zahteva i AHP metoda** kako bi se utvrdila njihova relativna vrednost prema kupcima ili korisnicima [136], **prioritizacija zahteva na osnovu kriterijuma poslovne vrednosti, cene, zadovoljstva korisnika** [123] **i rizika** [137]), **agilne metode** koje se primenjuju u svim aktivnostima inžinjeringa zahteva, a podstiču kontinuiranu saradnju sa zainteresovanim stranama [138], **ponovno korišćenje zahteva** [95, 139, 140, 141, 142]), **tehnike adaptacije** [143, 144, 145]), **tehnike sledljivosti** ([146, 147, 148]).

6.1. Primenjeni model definisanja zahteva za PKI MO i VS

Prihvatanje i uvođenje novih i savremenih dostignuća u sistem koji funkcioniše predstavlja izazov za rukovodstvo, zaposlene i izvođača radova. Pre nego što je rukovodstvo donelo odluku o uvođenju PKI infrastrukture u MO i VS sprovoden je pilot projekat da bi se demonstrirale mogućnosti primene elektronskih sertifikata. Sagledavajući efekte praktičnog prikaza, postojeću regulativu o elektronskom dokumentu i elektronskom potpisu, standarde, prethodnu studiju o uvođenju elektronskih identifikacionih dokumenata u Ministarstvo odbrane, a sve u cilju poboljšanja telekomunikaciono-informatičkog obezbeđenja MO i VS rukovodstvo je donelo odluku da se uvede PKI sistem i odredilo globalne zahteve.

Nakon donete odluke pristupilo se utvrđivanju i definisanju zahteva po sledećem modelu (slika 21):

- Odobravanje globalnih zahteva. Nakon definisanja globalnih zahteva rukovodstvo ih je odobrilo i dalo saglasnost za uvođenje PKI.
- Identifikovanje zahteva. Razmatrajući globalne zahteve, dokumentaciju, standarde, regulative i potrebe krajnjih korisnika, u saradnji sa izvođačem projekta, identifikovani su zahtevi.
- Analiza zahteva. Koristeći identifikovane zahteve, izvođač je izvršio njihovu analizu i napravio je specifikaciju sistema koja zadovoljava potrebe korisnika i pruža dovoljno informacija za izgradnju PKI. U ovoj fazi, izvođač je formalizovao opis sistema koji se gradi. Ovakav opis je više svojstven izvođaču nego korisniku, koji nije poznavao UML u dovoljnoj meri.
- Dekomponavanje zahteva. Dobijene i formalno opisane zahteve korisnik i izvođač dekomponuju u jednostavnije zahteve ili korisnik daje saglasnost na već predložnu dekompoziciju zahteva.
- Definisanje i redefinisanje zahteva. U ovoj fazi izvođač formuliše zahteve na jeziku svojstvenom korisniku, odnosno definiše ih u formi koju će moći da razumeju korisnik i programer koji bude radio dizajn i implementaciju.
- Validacija zahteva. Korisnik sagledava definisane zahteve nastojeći da utvrdi da li su u skladu sa globalnim zahtevima, ciljem i pravnom regulativom, da li odražavaju stvarne potrebe, da li su realni i u skladu sa ograničenjima. Svi zahtevi koji ne prođu validaciju izvođač treba sa redefiniše.
- Verifikacija zahteva. Verifikovanje zahteva rade zajedno korisnik i izvođač da bi se ustanovile eventualno nejasnoće za obe strane.
- Dokumentovanje zahteva. U ovoj fazi se zahtevi dokumentuju u formi tehničke i funkcionalne specifikacije.



Slika 21. Model identifikovanja i definisanja zahteva prilikom uvođenja CA MO i VS

6.2. Analiza zahteva PKI MO i VS nakon implementacije

Kroz faze životnog ciklusa razvoja PKI MO i VS izdvojili su se karakteristični zahtevi. To su zahtevi za koje se u toku razvoja PKI proizvoda pokazalo da je potrebno izvršiti određenu akciju nad njima kako bi se doveli na određeni nivo za implementaciju. Isto tako, prilikom razvoja su ustanovljeni novi zahtevi koji nisu uočeni i definisani tokom ustanovljavanja potreba sistema. Činjenica je da su postojali i zahtevi koji su preambiciozno postavljeni, pa ih nije bilo moguće uopšte implementirati ili njihova implementacija nije isplativa. Ovi zahtevi su svrstani u pet kategorija: redefinsani, naknadno definisani, odbačeni, pogrešno realizovani i tranzicioni.

Redefinisani zahtevi su oni koje je u nekoj od faza životnog razvojnog ciklusa trebalo ponovo definisati, a nastali su kao posledica nedovoljnog sagledavanja i razumevanja sistema.

Naknadno definisani zahtevi su svi oni koji su se pojavili u nekoj fazi životnog razvojnog ciklusa. Uzrok za naknadno definisanje zahteva je nedovoljno sagledavanje i razumevanje sistema.

Odbačeni zahtevi su oni od kojih se odustalo zbog toga što su nerealni, nepotrebni, prezahtevni, nije ih moguće izvesti ili su preskupi za realizaciju.

Pogrešno realizovani zahtevi su implementirani, ali su korisnici ustanovili da sama realizacija zahteva nije ono što su podrazumevali. Ova vrsta zahteva nastaje kao posledica lošeg razumevanja zahteva od strane izvođača ili različitog tumačenja zahteva od strane izvođača i korisnika.

Tranzicioni zahtevi su oni za koje su se korisnik i izvođač usaglasili da ih u ovoj fazi implementacije nije potrebno ili se ne mogu implementirati, ali da su značajni i da ih je potrebno planirati za neku drugu fazu dogradnje sistema.

Tabela 5. Pregled karakterističnih zahteva i njihov procentualni udeo u ukupnom broju zahteva

Vrsta zahteva	Broj zahteva nakon implementacije	Procentualni udeo karakterističnih zahteva u ukupnom broju zahteva (%)
Redefinisani zahtevi	56	14,25
Naknadno definisani zahtevi	100	25,45
Pogrešno realizovani zahtevi	42	10,69
Odbačeni zahtevi	23	5,85
Tranzicioni zahtevi	29	7,38
Ukupan broj zahteva	393	
Ukupno loših zahteva	250	63,61

Uspostava Sertifikacionog tela MO i VS i sistema za personalizaciju realizovana je implementacijom funkcionalne specifikacije. U definisanju zahteva učestvovali su stručni tim MO i VS i tim izvođača. Zbog prethodno navedenih problema u razotkrivanju i definisanju zahteva izvršena je analiza implementirane specifikacije. Problemi su uticali na pojavu velikog broja loših zahteva, Tabela 5. Od ukupnog broja zahteva 63,61% otpada na loše zahteve. Na zahteve koje je trebalo redefinisati otpada 14,25%, na zahteve koji su naknadno definisani 25,45%, na pogrešno realizovane zahteva 10,69%, na odbačene zahteve 5,85% i na zahteva koje bi trebalo implementirati u nekoj narednoj fazi 7,38%.

Problemi koji su se izdvojili prilikom razotkrivanja i definisanja zahteva za uspostavu Sertifikacionog tela MO i VS i sistema za personalizaciju eID:

- Organizacioni problemi. Učešće članova tima za razotkrivanje i definisanje zahteva bilo je ograničeno i opterećeno drugim poslovima i obavezama. Koordinacija tima MO i VS i tima izvođača realizovana je kroz sastanke, brain storming kada su se usaglašavale aktivnosti, razotkrivali i definisali zahtevi.
- Raznorodnost sastava tima. Ogledala se u različitim nivoima znanja članova tima iz oblasti inžinjeringa zahteva kao i PKI.
- Nedovoljno znanje iz oblasti PKI. Članovi tima su se susreli sa novom oblašću za koju je bilo potrebno definisati zahteve. Nisu imali dovoljno vremena da prouče i sagledaju oblast kako bi mogli da uoče i definišu zahteve za potrebe sistema.
- Nespremnost rukovodstva. Rukovodstvo nije bilo spremno za uvođenje nove tehnologije koja bi omogućila elektronsku razmenu dokumenata i elektronsko potpisivanje i ako su preko Pilot projekta upoznati sa prednostima i nedostacima uvođenja PKI. Osim toga, Pilot projekat je u potpunosti pokazao opravdanost uvođenja PKI i elektronskog potpisa.
- Komunikacija. Na razotkrivanju i definisanju zahteva pored stručnog tima agažovana je treća strana, softverska firma. Prilikom definisanja i verifikacije zahteva korišćen je UML koji pojedini članovi stručnog tima nisu dovoljno poznavali. Zato je verifikacija zahteva bila spora i sa dosta nerazumevanja.
- Rokovi. Dati rokovi za definisanje zahteva bili su kratki što je prouzrokovalo dodatni pritisak na članove tima, pored redovnih obaveza.
- Finansijska sredstva. Finansijska sredstva su bila ograničena tako da se često morala raditi korekcija zahteva izvođača ili stručnog tima.
- Oslanjanje na izvođača radova. Stručni tim se uglavnom oslanjao na zahteve koje je definisao izvođač, a pod pritiskom kratkih rokova, iako mu nisu bili u potpunosti jasni, kao takve ih je verifikovao.

Sagledavajući uticaj problema na ovako veliki broj zahteva ustanovljeno je da najveći uticaj ima problem nedovoljnog znanja iz PKI i oblasti inžinjeringa zahteva, a zatim oslanjanje na izvođača radova i komunikacija. Navedeni problemi su međusobno povezani i u zajedničkoj interakciji su uticali na pojavu velikog broja karakterističnih (loših) zahteva.

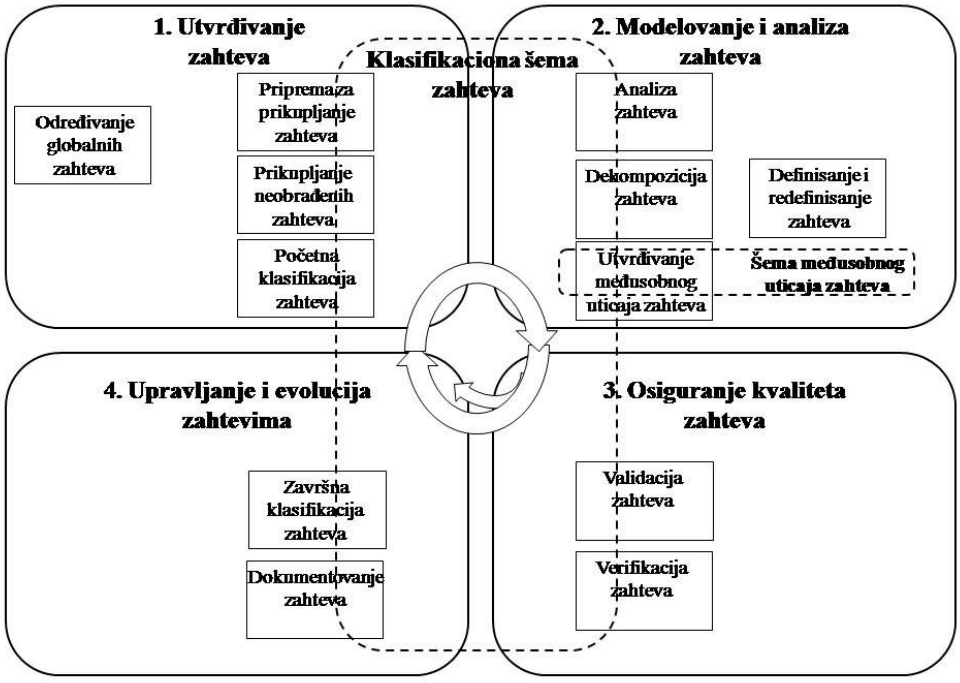
Kako bi se otklonio ili umanjio uticaj navedenih problema na buduća definisanja zahteva Sertifikacionog tela MO i VS, izrađena je klasifikaciona šema zahteva za PKI. Šema je stručnom timu i timu izvođača dala radni okvir i smernice za razotkrivanje i definisanje zahteva, zajednički jezik komunikacije i suštinsko znanje timu o zahtevima za PKI.

6.3. Unapređenje modela sa klasifikacionom šemom

6.3.1. Opis modela identifikovanja i definisanja zahteva primenom klasifikacione šeme

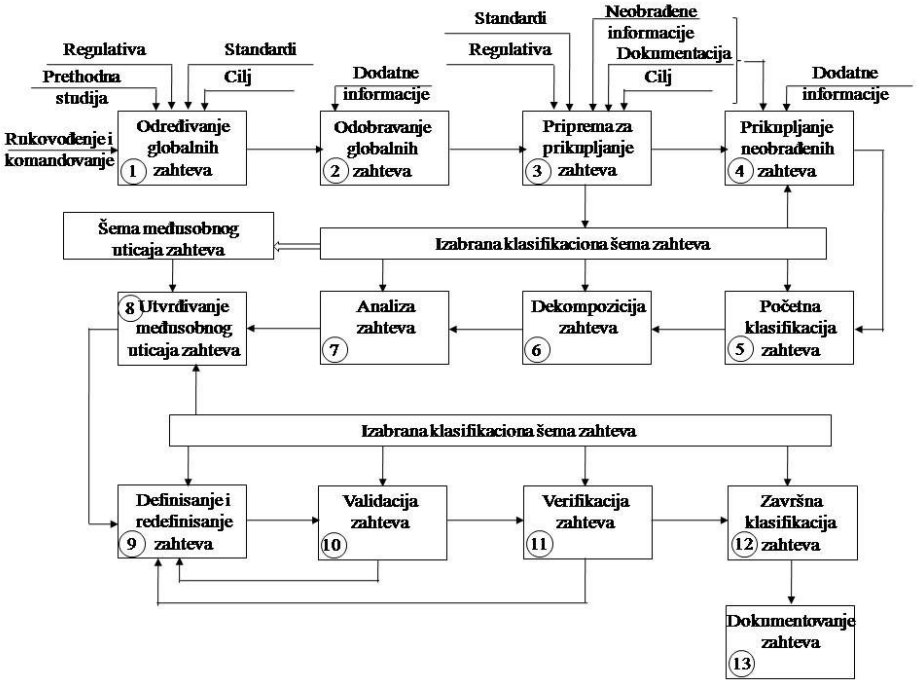
Unapređeni model identifikovanja i definisanja zahteva primenom klasifikacione šeme osmišljen je tako da klasifikaciona šema ima uticaja na identifikovanje i definisanje zahteva u svim fazama. Klasifikaciona šema predstavlja domen u kome korisnik i izvođač radova treba da traže zahteve. Osim toga, usmerava u kojim kategorijama treba tražiti zahteve. Klasifikacina šema se razmatra od opšteg ka pojedinačnom, odnosno sagledavajući potrebe sistema, kategorija i potkategorija sve do najnižeg nivoa klasifikacije. Korisnik ili izvođač radova identifikuju i definišu zahteve. Klasifikacije mogu biti opšte ili specijalizovane. Opšte klasifikacione šeme obično rade klasifikaciju nefunkcionalnih zahteva i generalno nisu povezane ni sa jednim sistemom. Specijalizovane klasifikacione šeme su namenske klasifikacije zahteva u određenoj oblasti i na poslednjem nivou daju usmerenja za definisanje i identifikovanje zahteva. Primena specijalizovanih klasifikacija daje bolje rezultate nego opšte klasifikacione šeme.

Klasifikaciona šema primenjuje se u svim fazama (aktivnostima) inžinjeringa zahteva, slika 22. U svakoj od ovih faza sprovode se procesi koje uključuju klasifikacionu šemu u svoju aktivnost.



Slika 22. Unapređenje modela klasifikacionom šemom

Detaljan model unapređenja sa klasifikacionom šemom dat je na slici 23.



Slika 23. Model za identifikovanje i definisanje primenom klasifikacione šeme

Model se sastoji iz sledećih procesa [149]:

Određivanje i odobravanje globalnih zahteva. Rukovodstvo određuje globalne zahteve za uvođenje novog ili dogradnju postojećeg sistema. Globalni zahtevi određuju šta sve treba ispuniti da bi se stiglo do cilja. Oni iniciraju dalje procese identifikovanja i definisanja zahteva. Pre nego što se otpočne sa procesom, rukovodstvo mora da verifikuje globalne zahteve.

Priprema za prikupljanje zahteva. Priprema obuhvata prikupljanje i kategorizaciju svih neobrađenih informacija koje korisnik može da pruži. Informacije se mogu dobiti iz prethodnih studija projekata, propisa, standarda, strategija, dokumentacije. Osim toga, u toku pripreme se određuju i tehnike koje će se koristiti za identifikovanje zahteva i odlučuje se o izboru odgovarajuće klasifikacione šeme.

Prikupljanje neobrađenih zahteva podrazumeva prikupljanje informacija iz dokumentacije, standarda, regulativa, intervjua i informacija na koje ukazuje klasifikaciona šema. Klasifikaciona šema predstavlja domen u kome treba tražiti zahteve. Tokom tog procesa se sagledavaju ograničenja u sistemu u smislu uticaja na sistem (nema uticaja, ima uticaja, može imati pozitivan uticaj na sistem ili nije neophodan za sistem). Uočena ograničenja i prikupljene informacije daju osnovu za utvrđivanje zahteva koji se nakon kreiranja označavaju stepenom značaja i (ili) stepenom hitnosti (neohodnost da se zahtev realizuje). Prikupljanje neobrađenih zahteva se ne

izvodi odjednom. Svaki put kada korisnik iznese dodatne informacije one se moraju proveriti i eventualno uvrstiti u dodatne zahteve.

Početna klasifikacija zahteva. Nakon identifikacije nobrađenih zahteva vrši se klasifikacija kako bi se veliki skupovi dekomponovali na logički povezane podskupove, što pojednostavljuje dalji rad sa zahtevima. Izabrana klasifikaciona šema predstavlja okvir za klasifikovanje zahteva. Osim toga, prema izabranoj klasifikacionoj šemi može se izvršiti klasifikovanje i po drugim kriterijumima kako bi se omogućio različit pogled na isti skup zahteva.

Dekompozicija zahteva uspostavlja odnos nadređeni/podređeni između zahteva. Koristi se za zahteve koji se odnose na više aspekata sistema. Sagledavanjem klasifikacione šeme ostvaruje su uvid u postojanje zahteva iz drugih aspekata sistema. Dekomponovanjem složenog zahteva na jednostavnije olakšava se njihovo razumevanje i realizacija. Skup dekomponovanih zahteva obuhvata ista ograničenja kao i originalni (složeni) zahtev.

Analiza zahteva. Prikupljeni zahtevi moraju biti precizno opisani na način razumljiv stručnjacima iz određene oblasti, programerima i drugim zainteresovanim stranama. Postoji širok spektar tehnika i notacija koje mogu specifikaciju zahteva predstaviti na neformalne, poluformalne ili formalne načine. Specifikacije treba da zadovolje zahteve korisnika u odnosu na sistem i pruže dovoljno informacija za izgradnju sistema. Klasifikaciona šema omogućava usmerenjima za definisanje zahteva izradu kvalitetne specifikacije i omogućava bolje razumevanje zahteva.

Utvrđivanje međusobnog uticaja zahteva. Zahtevi nisu nezavisni jedni od drugih. Prvi vid povezanosti proizilazi iz klasifikacije zahteva, gde nadređeni zahtev pruža opšti kontekst, a njegovi podređeni zahtevi se bave konkretnim pitanjima unutar tog konteksta. Drugi vid povezanosti dolazi iz međusobnih uticaja zahteva iz različitih kategorija. Utvrđivanjem međusobnog uticaja zahteva se izbegava njihov sukob i pravovremeno se utvrđuje interakcija koju treba uzeti u obzir prilikom dizajna sistema.

Definisanje i redefinisanje zahteva [150]. Ova aktivnost formuliše, odnosno uobličava zahteve tako da sadrže sve karakteristike dobrih zahteva. Određuju se prioritet zahteva i njegova merljivost. Sve zahteve koji ne ispunjavaju uslove validacije i verifikacije potrebno je redefinisati, odnosno definisati tako da zadovolje kriterijume.

U definisanju je potrebno opisati zahteve što jasnije. U toku ove faze ne samo da se definiše šta je to zahtev već i šta nije zahtev. Da bi se razumela međusobna povezanost zahteva i omogućio efikasan rad sa njima u narednim fazama potrebno je izvršiti klasifikaciju prema klasifikacionoj šemi. Takođe, radi se prioritizacija zahteva u skladu sa poslovnim potrebama, jer ne mogu da se implementiraju svi odjednom.

Validacija zahteva. Validacija ima za cilj da uporedi adekvatnost specificiranih i modeliranih zahteva i pretpostavki domena sa stvarnim očekivanjima zainteresovanih strana. Validacija zapravo proverava da li traženi zahtevi odražavaju stvarne potrebe zainteresovanih strana, da li su realni i dosledni sa ograničenjima domena. Zainteresovanoj strani je bitno da zahtevi ispune očekivanja od samog početka.

Verifikacija zahteva. Verifikacija pokriva širok opseg provera uključujući kriterijume kvaliteta specificiranih i modeliranih zahteva (npr. doslednost). Ima za cilj da proveri da li zahtevi ispunjavaju neka svojstva (npr. konzistentnost) ili da li specifikacija softvera ispunjava zahteve u datom domenu.

Završna klasifikacija zahteva. Po potrebi se mogu uspostaviti dodatne klasifikacije skupa zahteva, kao što su:

- Klasifikacija po inkrementu: za sistem koji se razvija inkrementalno zahtevi se mogu klasifikovati prema inkrementima koji će biti implementirani
- Klasifikacija prema komponentama: koristi se kada je softverski sistem baziran na komponentama, pa je potrebno sve zahteve koji se odnose na komponentu staviti u jednu klasu.
- Klasifikacija prema odgovornosti: podrazumeva klasifikovanje zahteva prema stepenu odgovornosti osobe ili tima zaduženih za njihovu implementaciju.

Dokumentovanje zahteva. Zahtevi se mogu dokumentovati u različitim formama. Obično se dokumentuju u formi liste i mogu uključiti slučajeve korišćenja, korisničko uputstvo ili specifikaciju procesa.

6.3.2. Klasifikaciona šema zahteva implementirane PKI MO i VS

Reverznim inžinjeringom iz funkcionalne specifikacije i specifikacije iz ugovora za uvođenje Sertifikacionog tela MO i VS i sistema za personalizaciju eID kreirana je klasifikaciona šema zahteva za PKI MO i VS.

Klasifikaciona šema sastoji se od sledećih grupa zahteva i prikazana je na slici 24:

- **Zahtevi za registracioni autoritet** definišu rad registracionog autoriteta u smislu provere podataka i vođenja evidencije o korisnicima, kao i rad aplikacije registracionog autoriteta. Ovi zahtevi sastoje se od dve grupe i to: zahteva za funkcionalnost RA i zahteva za aplikaciju RA. Zahtevi za funkcionalnost RA odnose se na rad sa korisnicima (kreiranje, opozivanje, izmene i pretraživanje korisnika) i na upravljanje životnim ciklusom sertifikata korisnika. Zahtevi za aplikaciju RA definišu izdavanje eID kao nosioca elektronskih i optičkih podataka korisnika i kriptografski materijal za potrebe elektronskog poslovanja. Ovi zahtevi definišu sadržaj eID, proces izdavanja, rada i pretraživanja eID, kao i kriptografski materijal sadržan u eID.
- **Zahtevi za sertifikaciono telo** obuhvataju zahteve za arhitekturu CA, za uspostavu CA i instaliranje komponeti CA, kao i zahteve za sertifikate koje će izdavati CA. Zahtevi za arhitekturu CA definišu međusobni odnos sertifikacionih tela potrebnih za funkcionisanje sistema. Zahtevi za uspostavu CA i instaliranje komponenti CA definišu postupke instalacije kriptografskih modula i softvera CA, određivanje profila krajnjih korisnika i postupak uspostave arhitekture CA. Zahtevi za sertifikate određuju namenu, vrstu i strukturu sertifikata.
- **Zahtevi za bezbednost sistema** služe za uspostavu i održavanje bezbednosti sistema i to kroz opšte bezbednosne i specifične zahteve za upravljanje pravima pristupa sistemu, kao što su zahtevi za identifikaciju korisnika, nadležnosti i uloge u sistemu.
- **Zahtevi za hardver i softver** se odnose na zahteve za servere, mrežnu opremu i kriptografske module, dok se softverski zahtevi odnose na vrstu aplikativnog i sistemskog softvera i softvera baze podataka koji treba da podrže rad namenski izrađenog softvera sertifikacionog tela i sistema za personalizaciju.
- **Zahtevi za personalizaciju eID** definišu vrstu personalizacije eID (optička i elektronska) i proceduru za proizvodnju eID (zahtevi za proizvodnju eID). Navedena procedura definiše se kroz zahteve za proizvodnju eID koji obuhvataju potvrdu prijema zahteva za proizvodnju, otpočinjanje, opoziv i odbijanje prozvodnje, kao i pretragu ovih zahteva.

Slika 24. Klasifikaciona šema zahteva za Sertifikaciono telo MO i VS i sistem za personalizaciju

Nakon izvršene analize zahteva ustanovljeno je sledeće:

- Većina zahteva odnosi se na registracioni autoritet i to na aplikaciju registracionog autoriteta u delu kojim se upravlja izdavanjem eID;
- Zahtevi za softver i hardver nisu eksplicitno definisani, ali se u ugovoru navodi koji je softver i hardver potrebno obezbediti da bi sistem funkcionisao. Na osnovu tih specifikacija iz ugovora urađena je klasifikacija ove kategorije zahteva.
- Bezbednosni zahtevi su delimično definisani i uglavnom se odnose na zahteve za upravljanje pravima pristupa. Jedan manji deo opštih zahteva definisan je kroz zahteve iz ugovora.
- Zahtevi za održavanje nisu definisani, osim u ugovoru gde je definisan zahtev za rešavanje reklamacije i rešavanje problema nastalih u radu u toku jedne godine.
- Organizacioni zahtevi nisu eksplicitno definisani nego je na osnovu zakonske regulative formirana organizaciona celina koja obavlja poslove sertifikacionog tela.
- Nisu definisani zahtevi za interoperabilnost sertifikacionog tela sa drugim sertifikacionim telima. Generalno, interoperabilnost se u tom trenutku nije razmatrala jer je sertifikaciono telo razvijano za sopstvene potrebe, odnosno za potrebe u zatvorenom sistemu.

- Zahtevi su uglavnom definisani u sklopu funkcionalne specifikacije ili su implementirani u sklopu ugovora. Iz ovakvog načina definisanja zahteva, koji je usko usmeren na funkcionalnost, zanemaruju se drugi nefunkcionalni zahtevi neophodni za jedan ovako složen sistem.
- Zahtevi su definisani kroz više sesija od strane izvođača radova uz primenu metoda sastanaka, intervjua, ali karakteristično je da korisnik u većini slučajeva nije bio nosilac zahteva već je uglavnom odobravao zahteve koje je definisao izvođač.

6.3.3. Izbor klasifikacione šeme za izradu PKI u MO i VS

U cilju detaljnijeg sagledavanja zahteva u narednim dogradnjama PKI, a kako bi se smanjio broj karakterističnih zahteva (loših) i obezbedio domen u kome treba utvrđivati zahteve, rešenje je traženo u klasifikacionim šemama. Postojeće klasifikacione šeme nisu kompletne i ne obuhvaju sve potrebe za zahteve PKI sistema.

Razmatrana je klasifikacina šema zahteva za PKI dobijena reverznim inžinjeringom iz funkcionalne i tehničke specifikacije za izgradnju Sertifikacionog tela MO i VS. Ova klasifikacija je većim delom bila usmerena na registracioni autoritet (rad sa osobama, dokumentima, izveštajima), a manjim delom, ali dovoljnim, na sertifikaciono telo. Šema nije uzimala u detaljnija razmatranja bezbednosni aspekt, održavanje, organizaciju, poslovanje.

Izrađena klasifikaciona šema za PKI je robusna i obuhvata svaki aspekt PKI. S obzirom da je specijalizovana, predstavlja prvi izbor za primenu u modelu identifikovanja i definisanja zahteva za PKI.

Kako se ne bi favorizovala jedna klasifikaciona šema za PKI, urađeno je poređenje izabranih klasifikacionih šema na osnovu sledećih kriterijuma [72]: sveobuhvatnost (K1), sistematičnost (K2), jednostavnost (K3), primenjivost (K4), univerzalnost (K5) i jasnoća (K6).

Korišćena je AHP (Analytic Hierarchy Process) metoda za višekriterijumsko odlučivanje. Ova metoda izračunava stepen konzistentnosti na osnovu kojeg se utvrđuje uticaj subjektivnosti prilikom merenja.

Problem odlučivanja je definisan u skladu sa konceptom AHP. Na najvišem nivou hijerarhije nalazi se cilj, zatim kriterijumi i alternative (potencijalna rešenja).

Cilj je izbor najpogodnije klasifikacione šeme zahteva za identifikovanje i definisanje PKI zahteva.

Alternative su: IEEE 830 klasifikacija (A1), klasifikacija po Sommervillu (A2), klasifikacija po Lamsweerde (A3), klasifikacija po Odehu (A4), FOCUS-TDB klasifikacija (A5), ISO IEC 9126 klasifikacija (A6), FURPS klasifikacija (A7), PKI MO i VS klasifikacija (A8) i PKI klasifikaciona šema (A9).

Poređenje svih parova kriterijuma u odnosu na cilj, Tabela 7, i parova alternativa u odnosu na kriterijum (matrice poređenja, Prilog 4) urađen je pomoću Satijeve skale (Tabela 6).

Tabela 6. Satijeva skala vrednovanja (relativni značaj) [151]

Značaj	Definicija	Objašnjenje
1	Istog značaja	Dva elementa su identičnog značaja u odnosu na cilj.
3	Slaba dominantnost	Iskustvo ili rasuđivanje neznatno favorizuju jedan element u odnosu na drugi.
5	Jaka dominantnost	Iskustvo ili rasuđivanje znatno favorizuju jedan element u odnosu na drugi.
7	Demonstrirana dominantnost	Dominantnost jednog elementa potvrđena u praksi.
9	Apsolutna dominantnost	Dominantnost najviseg stepena.
2, 4, 6, 8	Međuvrednosti	Potreban kompromis ili dalja podela.

Vektori sopstvenih vrednosti, *W*, (Tabela 7) izračunati su po formuli (6.1). Na osnovu izračunatog vektora sopstvenih vrednosti svaki kriterijum dobija odgovarajući težinski koeficijent kojim se definiše njegova relativna vrednost u odnosu na cilj.

Vektor težinskih koeficijenata *w* može se dobiti normalizacijom recipročnih vrednosti suma kolona, formula (6.1).

$$\sum_{i=1}^{n} \frac{W_i}{W_j} = \frac{1}{W_j}\left(\sum_{i=1}^{n} \frac{1}{W_i}\right) \qquad (6.1)$$

$\boldsymbol{j = 1, \ldots, n}$ (po kolonama), gde je *n* red matrice poređenja, a W_i predstavlja relativan težinski koeficijent elementa *i*.

Poređenje parova kriterijuma u odnosu na cilj i izračunati vektor sopstvenih vrednosti (težinski vektor) prikazani su u Tabeli 7.

Tabela 7. Matrica poređenja kriterijuma u odnosu na cilj i težinski vektori

Cilj	Sveobuhvatnost (K1)	Sistematičnost (K2)	Jednostavnost (K3)	Primenjivost (K4)	Univerzalnost (K5)	Jasnoća (K6)	Težinski vektor
Sveobuhvatnost (K1)	1	2	1	1/2	5	1/3	0,145
Sistematičnost (K2)	1/2	1	1	1/3	7	1	0,149
Jednostavnost (K3)	1	1	1	1/2	7	1/2	0,142
Primenjivost (K4)	2	3	2	1	7	1/2	0,247
Univerzalnost (K5)	1/5	1/7	1/7	1/7	1	1/7	0,028
Jasnoća (K6)	3	1	2	2	7	1	0,289
				CR=0,0608173<0,10			

Stepen konzistentnosti (*CR*) računa se prema formuli (6.2).

$$CR = \frac{CI}{RI} \tag{6.2}$$

Indeks koegzistencije (*CI*) izračunava se prema formuli (6.3)

$$CI = \frac{\lambda_{max} - n}{n-1} \tag{6.3}$$

gde je λ_{max} maksimalna sopstvena vrednost matrice poređenja.

λ_{max} izračunavamo tako što matricu sopstvenih vrednosti pomnožimo sa vektorom težinskih koeficijenata. Svaki elemenat dobijenog vektora *b* delimo sa korenspondirajućim elementom vektora *W*. Zatim sabiramo sve elemente dobijenog vektora *c* i podelimo sa *n* [149].

Slučajni indeks (*RI*) određuje se iz Tabele 8, a na osnovu reda matrice poređenja.

Tabela 8. Slučajni indeksi [151]

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
RI	0,0	0,0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,48	1,56	1,57	1,58

Red matrice poređenja kriterijuma je n=5 kome odgovara RI=1,12, dok je red matrice poređenja alternativa n=9 kome odgovara RI=1,45.

Izračunati stepeni koegzistencije za poređenje kriterijuma i poređenje alternativa dat je u Tabeli 9.

Tabela 9. Stepeni konzistentnosti

Matrica	CR
Cilj - K	0,060817331
K1-A	0,031314884
K2-A	0,015425217
K3-A	0,078214798
K4-A	0,010383099
K5-A	0,006995164
K6-A	0,024337736

Izračunati stepen konzistentnosti (*CR*) za sve matrice je manji od 0,10, što znači da ne premašuje dozvoljenu granicu, a time i da je vrednovanje kriterijuma i alternativa sprovedeno sa minimumom subjektivnosti.

Konačnu odluku koja alternativa je najbolja za ostvarivanje cilja, dobijena je izračunavanjem otežane sume (aditivne težine) tako što je formirana matrica težinskih vektora alternativa po svim kriterijumima i pomnožena sa težinskim vektorom kriterijuma, Tabela 10. Dobijeni rezultat je uticaj kriterijuma na izbor alternative koja predstavlja najbolje rešenje za izbor klasifikacione šeme, Tabela 11.

Tabela 10. Težinski vektori alternativa i kriterijuma

Alternative	Sveobuhva-tnost (K1)	Sistemati-čnost (K2)	Jednosta-vnost (K3)	Primenji-vost (K4)	Univerza-lnost (K5)	Jasnoća (K6)
Wc	0,145	0,149	0,142	0,247	0,028	0,037
IEEE 830	0,092	0,049	0,214	0,044	0,046	0,037
Sommerville-u	0,048	0,078	0,021	0,119	0,122	0,026
Lamsweerde -u	0,074	0,069	0,081	0,186	0,124	0,080
Odeh -u	0,074	0,030	0,053	0,073	0,115	0,020
FOCUS-TBD	0,269	0,229	0,145	0,174	0,191	0,110

ISO/IEC 9126	0,031	0,090	0,096	0,051	0,205	0,110
FURPS	0,031	0,049	0,096	0,051	0,065	0,173
PKI MO i VS	0,145	0,162	0,174	0,117	0,017	0,173
PKI klasifikacija	0,235	0,244	0,119	0,186	0,115	0,272

Tabela 11. Vektor prioriteta i rang

Alternative (klasifikacione šeme)	Vektor prioriteta	Rang
IEEE 830 (A1)	0,07378	7
Sommerville-u (A2)	0,06183	8
Lamsweerde -u (A3)	0,10504	4
Odeh -u (A4)	0,04962	9
FOCUS-TBD (A5)	0,17381	2
ISO/IEC 9126 (A6)	0,08168	6
FURPS (A7)	0,08979	5
PKI MO i VS (A8)	0,14922	3
PKI klasifikacija (A9)	0,21525	1

Iz Tabele 11. vidi se da alternativa A9 predstavlja najdominantniju klasifikaciju koju treba primeniti prilikom identifikovanja i definisanja zahteva za dogradnju PKI MO i VS. Alternativa A5 je druga po rangu što znači da je klasifikaciona šema PKI najpovoljnija za primenu u nadogradnji PKI MO i VS.

Na osnovu izračunatog vektora prioriteta i dodeljenog ranga, klasifikaciona šema PKI MO i VS predstavlja treću dominantnu klasifikaciju, dok klasifikacija zahteva po Lamsweerde–u (A3) predstavlja četvrtu po rangu klasifikaciju za proces identifikovanja i definisanja zahteva za PKI. Rezultati ostalih alternativa nisu u rangu prve četiri, pa nisu razmatrane za moguću primenu u toku dogradnje.

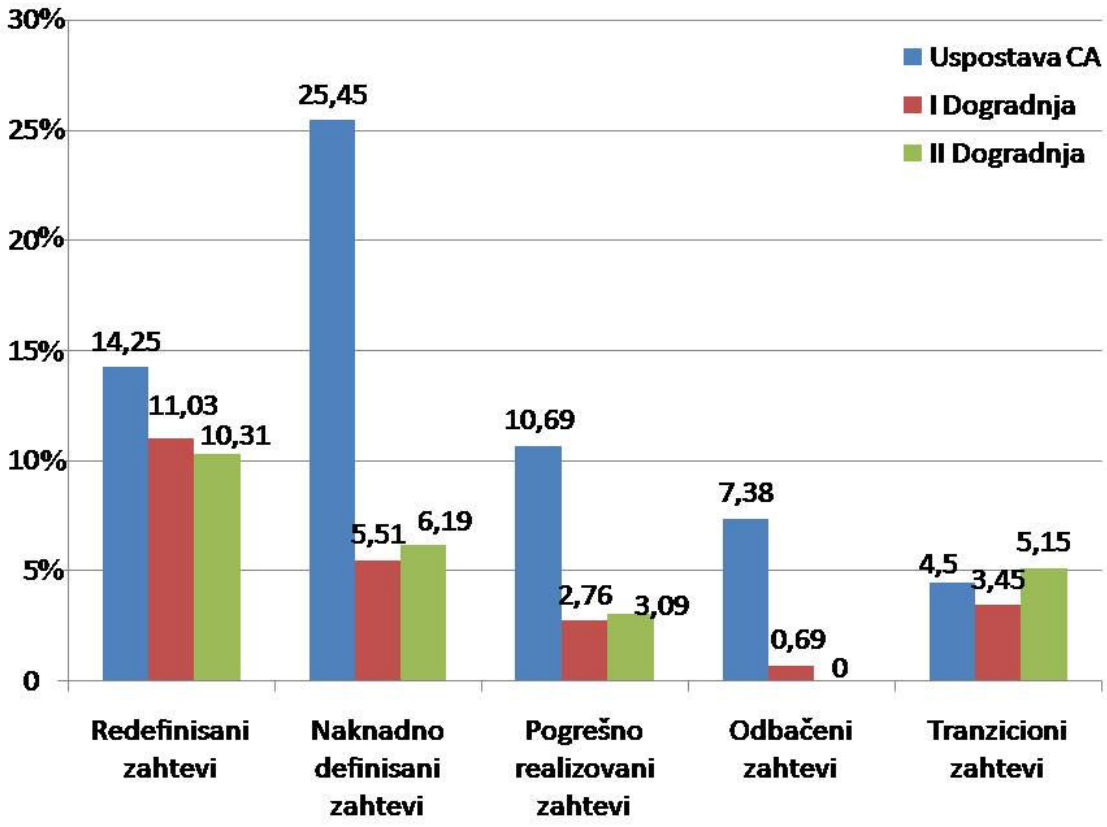
6.3.4. Rezultati primene klasifikacione šeme

Izabrana klasifikaciona šema primenjena je u naredne dve dogradnje za razotkrivanje i definisanje zahteva. Pored primene klasifikacione šeme i dalje su se pojavljivali loši zahtevi. U prvoj dogradnji procenat loših zahteva u odnosu na ukupan broj zahteva je znatno manji u

odnosu na uspostavu sistema i iznosi 23,45%, odnosno 2,7 puta manji nego procenat u toku uspostave sistema (63,61% loših zahteva).

Primena klasifikaciona šeme ostvarila je naveći efekat na naknadno definisane zahteve. Efekat se ogleda u smanjenju naknadno definisanih zahteva za 4,6 puta u donosu na prvu dogradnju. Kada je reč o redefinisanim zahtevima i ovde je ostvareno poboljšanje tako da ih je u prvoj nadogradnji procentualno za 3% manje nego prilikom uspostave sistema. Značajnija poboljšanja su ostvarena kod pogrešno realizovanih zahteva, tako da ih je u prvoj dogradnji 3,8 puta manje nego prilikom uspostave sistema. U prvoj dogradnji odbačenih zahteva gotovo da nije bilo (0,69%) za razliku od uspostave sistema kada ih je bilo 5,85% od ukupnog broja zahteva. Broj tranzicionih zahteva u toku prve dogradnje smanjen je dvostruko u odnosu na uspostavu sistema.

Primena klasifikacione šeme za definisanje zahteva u toku druge dogradnje sistema, a u odnosu na uspostavu sistema, ostvarila je znatna smanjenja svih kategorija loših zahteva. Međutim, smanjenje svih kategorija loših zahteva zadržalo se na istom nivou kao i za vreme prve dogradnje, slika 25.



Slika 25. Efekat primene klasifikacione šeme ostvaren kroz I i II dogradnju

6.4. Model sa klasifikacionom šemom unapređen ocenom kvaliteta zahteva

6.4.1. Analiza kvaliteta karakterističnih zahteva Sertifikacionog tela MO i VS i sistema za personalizaciju

Primena klasifikacione šeme prilikom identifikovanja i definisanja zahteva za prvu dogradnju dala je pozitivne efekte koji se ogledaju kroz smanjenje redefinisanih zahteva za 1,29 puta, naknadno definisanih zahteva za 4,62 puta, pogrešno realizovanih zahteva za 3,87 puta, odbačenih zahteva za 10,70 puta i tranzicionih zahteva za 1,30 puta u odnosu na broj navedenih vrsta zahteva nakon uspostave Sertifikacionog tela MO i VS.

Klasifikaciona šema je primenjena u toku identifikovanja i definisanja zahteva za drugu dogradnju. Rezultati primene klasifikacione šeme neznatno su bolji (u proseku za 0,71%) ili neznatno lošiji (u proseku za 0,9%) u odnosu na dobijene rezultate u toku prve dogradnje. Pošto se ponovnom primenom klasifikacione šeme nije ostvarilo značajnije smanjenje karakterističnih (loših zahteva) izvršena je analiza zahteva. Analizom su obuhvaćeni loši zahtevi za uspostavu Sertifikacionog tela MO i VS i zahtevi iz dogradnji.

Analizom zahteva za razvoj softvera za sertifikaciono telo ustanovljeno je da je najveći problem bio sa zahtevima koji su se morali ponovo razmotriti i/ili redefinisati (pogrešno realizovani), slika 25.

Analiziran je kvalitet na osnovu karakteristika dobrih zahteva na uzorku od 20 zahteva iz grupe redefinisanih i pogrešno realizovanih zahteva, Prilog 5. Analizom je ustanovljeno sledeće:

- ima zahteva koji su nepotpuni, odnosno nisu potpuno navedeni. Iz ovih zahteva se ne može zaključiti šta je sve potrebno uraditi jer nedostaju informacije. Zahtevi su previše uopšteni;
- polovina zahteva nije korektno definisana tj. ne mogu se lingvistički dobro razumeti ili postoje pravopisne greške i greške u podacima;
- izvodljivost je pokazala da četvrtinu zahteva nije moguće realizovati zbog finansijskih ili vremenskih ograničenja;
- četvrtina razmatranih zahteva pri implementaciji ne bi stvorili bitnu vrednost za korisnika (iskoristivost), dok ostali zahtevi stvaraju neophodnu vrednost za korisnika;

- da je 55 % zahteva teško konzistentno tumačiti sa strane korisnika i inženjera (nedvosmislenost). Veliki stepen neispunjenosti karakteristika nepotpun i korektnost utiče na to da je zahteve teško protumačiti i razumeti (šta se htelo postići zahtevom ili kako zahtev realizovati);
- karakteristika proverljivost nakon analize pokazala je iste rezultate kao i karakteristika nedvosmislenost. Veoma je teško proveriti zahtev nakon implementacije ako on nije potpuno definisan sa svim podacima. Generalno se zahtevi mogu testirati, ali je pitanje završne ocene da li zahtev zadovoljava ako nisu navedeni prilikom definisanja svi relevantni podaci.
- ostale analizirane karakteristike zahteva (doslednost, razumljivost, jasan, nezavisan, neophodnost) najviše sa 20 % učestvuju kao uzrok koji utiče na nastanak loših zahteva. Uglavnom su indirektne posledice prethodno analiziranih karakteristika dobrih zahteva. Ovi zahtevi se neće razmatrati kao indikatori za procenu kvaliteta zahteva.

Sagledavanjem kvaliteta zahteva došlo se do zaključka da najveći uticaj na kvalitet ima nepoštovanje sledećih dobrih karakteristika:

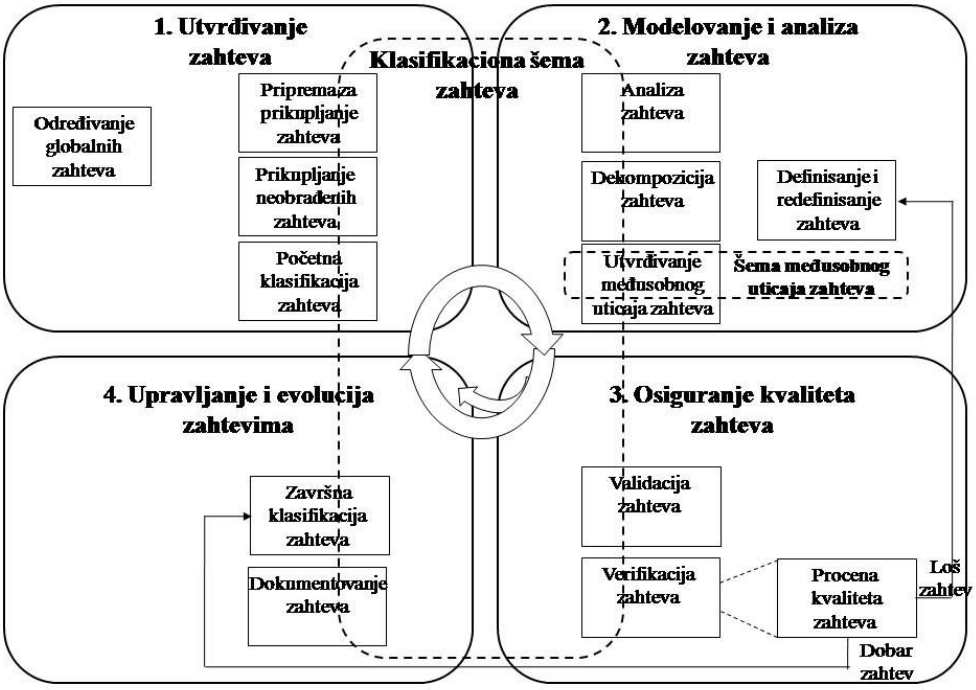
- *Kompletnost.* Kompletnost podrazumeva da zahtev u potpunosti opisuje funkcionalnost sistema koji se želi implementirati, odnosno da zahtev sadrži sve informacije neophodne za dizajniranje i implementaciju funkcionalnosti. Zahtev mora biti kompletan pre otpočinjanja dela životnog ciklusa razvoja proizvoda na koji se odnosi.
- *Korektnost.* Zahtev tačno opisuje funkcionalnost koja treba da se implementira. Nekorektnosti u zahtevima dovode do nedostataka u realizovanoj arhitekturi i implementaciji.
- *Izvodljivost*. Ova karakteristika odnosi se na mogućnost implementacije zahteva unutar poznatih ograničenja sistema i radnog okruženja. Da bi pojedinačni zahtevi bili izvodljivi treba imati u vidu sva relevantna ograničenja.
- *Iskoristivost*. Zahtev implementacijom treba da stvori vrednost koja korisniku zaista treba ili je potrebna za usaglašavanje sa zahtevima spoljašnjeg sistema, spoljnim interfejsom ili standardom.
- *Nedvosmislenost*. Svi koji tumače specifikaciju zahteva treba da dođu do jedinstvenog, konzistentnog tumačenja. Zahteve treba napisati jednostavnim, konciznim, razumljivim i jasnim jezikom. Korisnici specifikacije zahteva moraju biti u stanju da shvate na šta se zahtev odnosi.
- *Proverljivost*. Zahtev treba tako specificirati da se nakon implementacije može testirati i dokazati njegova ispunjenost. Ako se zahtev ne može verifikovati onda je upitno da li se

može realizovati kroz implementaciju. Zahtevi koji su nepotpuni, nedosledni, neizvodljivi ili dvosmisleni nisu proverljivi.

Ostale karakteristike dobrih zahteva su manje zastupljene u analiziranom uzorku. U analizi nisu razmatrane karakteristike dobrih zahteva gradacija, promenjivost i sledljivost jer se ove karakteristike više odnose na upravljanje zahtevima. Karakteristika nevezan za implementaciju nije razmatrana jer je ustanovljeno da svi analizirani zahtevi ne sadrže informaciju o implementaciji i dizajnu.

6.4.2. Unapređenje modela ocenom kvaliteta zahteva

Ovaj model unapređuje definisanje zahteva u aktivnosti "osiguranje kvaliteta" i to u toku verifikacije zahteva. Cilj ovog modela je da u toku verifikacije omogući procenu kvaliteta zahteva na osnovu indikatora kvaliteta. Ukoliko je u toku verifikacije izvršena takva ocena kvaliteta da je zahtev loš, odnosno da ne ispunjava indikatore kvaliteta, takav zahtev se vraća na doradu, odnosno redefinisanje. Nakon redefinisanja, zahtev ponovo dolazi na procenu kvaliteta. Ovaj postupak se ponavlja sve dok zahtev ne ispuni traženi kvalitet. Ako se u bilo kom krugu provere kvaliteta ustanovi da zahtev ispunjava tražene uslove kvaliteta, prosleđuje se u narednu aktivnost, odnosno zahtev se klasifikuje i dokumentuje. Detaljan model unapređenja sa klasifikacionom šemom i procenom kvaliteta zahteva dat je na slici 26.



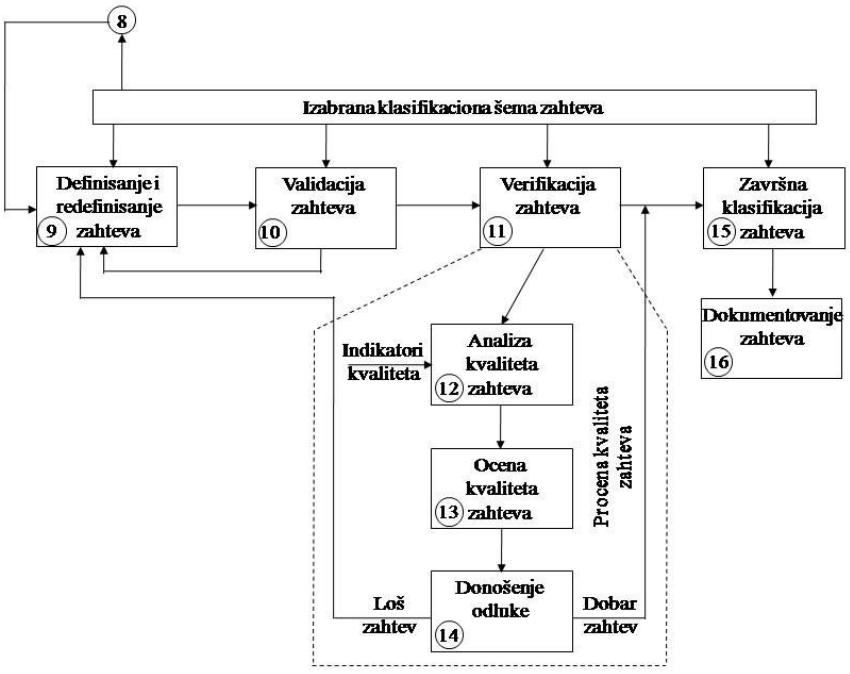
Slika 26. Unapređenje modela procenom kvaliteta zahteva

Model za procenu kvaliteta, slika 27, daje informaciju da li su definisani zahtevi za PKI dovoljno kvalitetni za implementaciju. Takođe, omogućuje korisnicima koji nemaju dovoljno znanja iz oblasti inženjeringa zahteva, kao i iskusnim inžinjerima da na jednostavan način procene kvalitet zahteva.

U toku verifikacije vrši se prvo analiza zahteva na osnovu indikatora za ocenu kvaliteta. U toku aktivnosti procesa identifikacije i definisanja zahteva evaluatori (korisnici ili inženjeri) ocenjuju u kojoj meri je ispunjen svaki indikator. S obzirom da ima više indikatora na osnovu koji se vrši ocena kvaliteta, veoma je teško doneti odluku da li je kvalitet zahteva zadovoljen. Stoga u aktivnosti procena kvaliteta zahteva je potrebno da postoji mehanizam koji će objediniti sve procene ispunjenosti indikatora i dati rezutat na osnovu kojega će se doneti odluka.

U aktivnosti „Donošenje odluke“ na osnovu dobijenog rezultata iz aktivnosti ocene kvaliteta i unapred određenog stepena traženog kvaliteta se donosi odluka da li zahtev ispunjava zadati kvalitet (dobar zahtev) ili ne (loš zahtev).

Model za ocenu kvaliteta zahteva zasnovan je na fuzzy logici i to na GPFCSP pomoću koje se izračunava globalni stepen zadovoljenja, a dobijeni rezultat određuje da li definisani zahtev zadovoljava traženi kriterijum kvaliteta. Model za procenu kvaliteta zahteva zasnovan na GPFCSP opisan je u glavi 5.5. Model za procenu kvaliteta zahteva zasnovan na GPFCSP.



Slika 27. Model za procenu kvaliteta definisanih zahteva

6.5. Primena modela za procenu kvaliteta zahteva koji je zasnovan na GPFCSP

6.5.1. Izbor indikatora za procenu kvaliteta zahteva

Analizom kvaliteta karakterističnih zahteva Sertifikacionog tela MO i VS i sistema za personalizaciju je ustanovljeno koje karakteristike dobrih zahteva najčešće nisu ispunjene. U literaturi postoji preko trideset opisanih karakteristika dobrih zahteva. Međutim, razmatranje ispunjenosti svih karakteristika dobrih zahteva u analizi kvaliteta predstavlja složen proces, pogotovo za korisnika. Na osnovu prethodne analize izabrane su karakteristike dobrih zahteva čije neispunjenje je najviše uticalo na kvalitet zahteva u procesu izgradnje i dve dogradnje Sertifikacionog tela MO i VS. Ove karakteristike upravo predstavljaju indikatore kvaliteta zahteva (kompletnost, korektnost, izvodljivost, iskoristivost, nedvosmislenost, proverljivost).

S obzirom da je cilj procene kvaliteta zahteva stvaranje modela koji će moći da koriste korisnici koji nemaju iskustva sa inženjeringom zahteva, potrebno je u proceni ispunjenosti kvaliteta zahteva za svaki indikator dati bliža usmerenja za procenu.

Za izabrane indikatore kvaliteta zahteva data su usmerenja za procenu svakog kroz pitanja koja verifikatoru zahteva treba da pomognu u proceni kvaliteta. U proceni kvaliteta korišćena su pitanja [113] iz Priloga 6.

6.5.2. Ocenjivanje indikatora kvaliteta

Vrednost indikatora se određuje na osnovu odgovora na pitanja za procenu. Indikatori mogu da imaju sledeće vrednosti: “ne ispunjava“, „malo ispunjava“, „gotovo ispunjava“ i „ispunjava“. Vrednosti i opseg indikatora prikazan je u Tabeli 12. Evaluator procenjuje ispunjenost indikatora kvaliteta zahteva tako što mu dodeljuje vrednost od 0 do 100. Do konačne vrednosti dolazi se na osnovu odgovora na pitanja za procenu ispunjenosti kvaliteta zahteva za određeni indikator.

Tabela 12. Vrednosti indikatora

Vrednost indikatora	Opseg vrednosti
Ne ispunjava	0-30
Malo ispunjava	31-60

Gotovo ispunjava	61-85
Ispunjava	86-100

Evaluator kvaliteta zahteva za procenu koristi Tabelu 13 tako što procenjuje u kojoj meri je zadovoljen indikator za svako pitanje. Nakon datih odgovora, izračunava srednju vrednost koja predstavlja vrednost indikatora za posmatrani zahtev.

Tabela 13. Tabela za procenu indikatora kvaliteta zahteva

Zahtev: _____			Indikator:_____	
Pitanja	Ne ispunjava (0-30)	Malo ispunjava (31-60)	Gotovo ispunjava (61-85)	Ispunjava (85-100)
Pitanje_1				
Pitanje_2				
Pitanje_3				
...				
Pitanje_n				
Procena indikatora:	$=\frac{\sum_{i=1}^{n}\sum_{j=1}^{k} a_{ij}}{n}$, gde je *n* broj pitanja, a *k* broj vrednosti indikatora.			

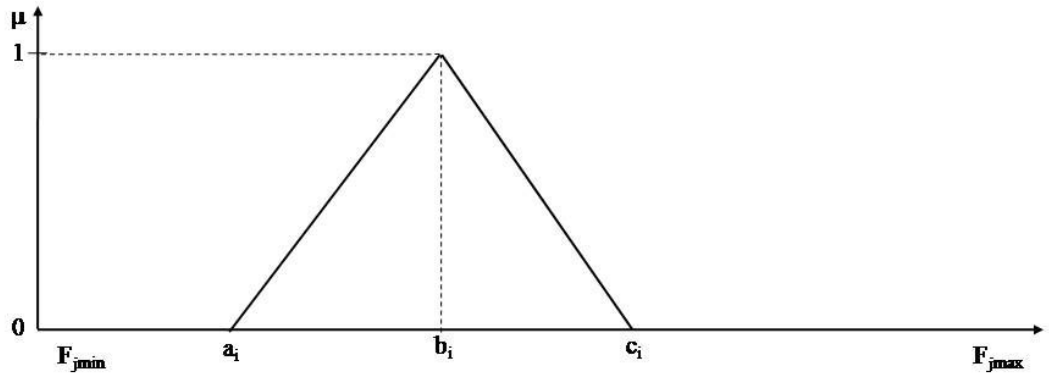
6.5.3. Određivanje fuzzy funkcije pripadnosti ograničenja

Podaci na osnovu kojih je izvršeno određivanje fuzzy funkcija dobijeni su na osnovu procene 30 zahteva tri nezavisna evaluatora. Procenjivan je stepen ispunjenosti indikatora nad 30 zahteva koji su označeni kao loše definisani u procesu izrade i dogradnje Sertifikacionog tela MO i VS i sistema za personalizaciju eID. Procena je vršena tako što je odgovarano na pitanja za svaki parametar. Ocenjivanje zahteva dato je u Prilogu 7. Na osnovu dobijenih podataka izvršena je konstrukcija funkcija pripadnosti ograničenja za svaki indikator kvaliteta zahteva.

6.5.3.1. Konstrukcija funkcije pripadnosti ograničenja

Konstrukcija funkcija pripadnosti ograničenja indikatora za procenu kvaliteta zahteva rađena je na osnovu tehnike iz rada [152] koja je modifikovana i dorađena za ovu potrebu.

Neka S predstavlja skup od N indikatora (F_1, F_2, ..., F_j,..., F_n), a F_j posmatrani indikator. Indikator F_j ima n vrednosti v_{1i}, v_{2i}, ...,v_{nj}. F_{jmin} i F_{jmax} predstavljaju minimalnu i maksimalnu vrednost (ocenu) indikatora F_j, slika 28.



Slika 28. Trougaona funkcija članica

Kada se odrede kvantitativne vrednosti (ocene) za indikator, sprovode se sledeći koraci za formiranje funkcije članice ograničenja:

Korak 1. Sortirati vrednosti indikatora F_j u rastućem redosledu.

Korak 2. Uraditi normalizaciju vrednosti indikatora F_j pomoću formule $v'_{1i} = \frac{v_{1i} - v_{maxi}}{v_{maxi} - v_{mini}}$, gde je v'_{1i} nova normalizovana vrednost, v_{1i} trenutna stvarna vrednost koju je potrebno normalizovati, v_{mini} minimalna vrednost indikatora F_j, v_{maxi} maksimalna vrednost indikatora F_j.

Korak 3. Odrediti *k* klastera pomoću K-means algoritma ili nekim drugim načinom grupisanja svojstven problemu koji se rešava, odnosno određivanje tačke grupisanja za indikator F_j. Indikator F_j se deli u k klastera (y_1, y_2, ..., y_i, ... y_k) gde $y_{i\,min}$ i $y_{i\,max}$, predstavljaju minimalnu i maksimalnu vrednost i-tog klastera.

Korak 4. Odrediti klaster centar (b_1, b_2, ..., b_i, ... b_k) svakog klastera (y_1, y_2, ..., y_i, ... y_k).

Korak 5. Odrediti vrednosti funkcije članice za dve granične tačke svakog klastera.

Korak 5.1. Izračunati razliku između susednih podataka. Za svaki par v'_i i v'_{i+1} gde je (i=1, 2, ..., n-1) izračunati razliku $diff_i = v'_{i+1} - v'_i$.

Korak 5.2. Izračunati sličnost (vrednost) između susednih podataka kvantitativnih vrednosti indikatora F_j. Sličnost između susednih podataka dobija se prema sledećoj formuli [153]:

$$S_m = \begin{cases} 1 - \dfrac{diff_i}{C * \sigma_s} \; za \; diff_i \leq C * \sigma_S \\ 0, inače \end{cases} \tag{6.4}$$

Gde je

S_m vrednost sličnosti između susednih vrednosti,

σ_S standardna devijacija od $diff_i$,

C kontrolni parametar koji utiče na izbor oblika funkcija članica.

Korak 5.3. Minimalna vrednost S_m od i-tog klastera je vrednost koju ima funkcija članica u krajnjima tačkama $y_{i\,min}$ i $y_{i\,max}$ i-tog klastera.

Korak 6. Odrediti interpolacijom leve granične tačke funkcije, (a_i, 0), na sledeći način:

$$a_i' = b_i - \frac{b_i - y_{imin}}{1 - \mu(y_{imin})} \tag{6.5}$$

$$a_i = \begin{cases} 0, \;\; a_i' \leq 0 \\ b_{i-1}, \; 0 < a_i' \leq b_{i-1} \\ a_i', \; a_i' \geq b_{i-1} \end{cases} \tag{6.6}$$

Korak 7. Odrediti interpolacijom desne granične tačke funkcije, (b_i, 0), na sledeći način:

$$c_i' = b_i + \frac{y_{imin} + b_i}{1 - \mu(y_{imax})} \tag{6.7}$$

$$c_i = \begin{cases} c_i', \; c_i' \leq b_{i+1} \\ b_{i+1}, \; c_i' > b_{i+1} \end{cases} \tag{6.8}$$

Korak 8. Odrediti tačke preseka funkcija članica, (d_i,0), i vrednosti funkcije u tački preseka.
Korak 8.1. Odrediti tačke preseka po x-koordinati, odnosno tačke (d_i,0):

$$d_i = \frac{(a_{i+1} - c_i)(b_i - c_i)}{b_i - c_i + a_{i+1} - b_{i+1}} + c_i \tag{6.9}$$

ako je $c_{i+1} < c_i$. Za $c_{i+1} \geq c_i$ ne određuje se tačka preseka. Funkcije članice u tim tačkama imaju vrednost 0.

Korak 8.2. Odrediti vrednosti funkcije u tački preseka, (d_i,0).

$$\mu(\vartheta) = \mu(d_i) = \frac{a_{i+1} - c_i}{b_i - b_{i+1} + a_{i+1} - c_i} \tag{6.10}$$

ili

$$\mu(\vartheta) = \mu(d_i) = \frac{d_i - a_{i+1}}{b_{i+1} - a_{i+1}} \tag{6.11}$$

Korak 9. Prevesti trougaone funkcije u trapezoidnu pomoću ograničavanja funkcija pripadnosti.

Korak 9.1. Odrediti maksimalnu vrednost funkcije članice ($\mu(\vartheta_1)$, $\mu(\vartheta_2)$, ..., $\mu(\vartheta_i)$, ... $\mu(\vartheta_k)$) svakog klastera (y_1, y_2, ..., y_i, ... y_k).

Korak 9.2. Odrediti interval ograničenja maksimalne vrednosti funkcije članice svakog klastera

$$v_{Li} = \mu(\vartheta_i) \cdot (b_i - a_i) + a_i \tag{6.12}$$

$$v_{Ri} = c_i + \mu(\vartheta_i) \cdot (c_i - b_i) \tag{6.13}$$

Korak 10. Pronaći vrednosti funkcije članice za kvantitativne vrednosti indikatora F_j,

$$\mu(\vartheta) = \begin{cases} \dfrac{v - a_i}{b_i - a_i}, & a_i \leq v < v_{Li} \\ k_i, & v_{Li} \leq v \leq v_{Ri} \\ \dfrac{c_i - v}{c_i - b_i}, & v_{Ri} < v < d_i \\ \dfrac{v - a_{i+1}}{b_{i+1} - a_{i+1}}, & v = d_i \\ \dfrac{v - a_{i+1}}{b_{i+1} - a_{i+1}}, & d_i < v < v_{Li+1} \end{cases} \tag{6.14}$$

gde je k_i vrednost ograničenja funkcije pripadanja za i-ti indikator kvaliteta.

6.5.3.2. Konstrukcija funkcije ograničenja za indikator kvaliteta kompletnost

U ovom poglavlju je prikazana konstrukcija funkcije članice za indikator kvaliteta kompletnost. Funkcije članice za indikatore korektnost, izvodljivost, iskoristivost, nedvosmislenost i proverljivost prikazane su u Prilogu 8.

Skup podataka za konstrukciju funkcija članica dobili smo na osnovu rezultata analize ocene trideset loših zahteva koju su izvršila tri evaluatora. Ocenjivanje ispunjenosti indikatora kvaliteta izvršeno je ocenama od 0 do 100. Što je ocena veća to je zahtev kompletniji. Primena predloženog algoritma prikazana je u Tabeli 14 i Tabeli 15.

Korak 1. Izvršeno je sortiranje vrednosti indikatora kompletnost u rastućem redosledu, kao u Tabeli 14.

Korak 2. Koristeći formulu za normalizaciju izvršena je normalizacija podataka indikatora kompletnost, kao u Tabeli 14.

Tabela 14. Indikatori vrednosti za kompletnost i izračunavanje parametara

Vrednost	Normaliza-cija	Klasteri (y_i)	$diff_i$ (v_{i+2}-v_i)	Vrednost sličnosti (S_m)
10	0	y_1	0	1
10	0	y_1	0,055556	0,381121
15	0,055556	y_1	0,055556	0,381121
...				
30	0,222222	y_1	0	1
30	0,222222	y_1	0,055556	0,381121
35	0,277778	y_2	0	1
35	0,277778	y_2	0	1
...				
60	0,555556	y_2	0	1
60	0,555556	y_2	0,055556	0,381121
65	0,611111	y_3	0	1
65	0,611111	y_3	0,055556	0,381121
...				

85	0,833333	y_3	0	1
85	0,833333	y_3	0,055556	0,381121
90	0,888889	y_4	0	1
90	0,888889	y_4	0	1
...				
100	1	y_4	0	1
100	1	y_4	0	1

Tabela 15. Osnovni parametri za izračunavanje funkcije članice kompletnost

Standardna devijacija (σ_S)	Konstanta (C)	Centar Klastera 1 (b_1)	Centar Klastera 2 (b_2)	Centar Klastera 3 (b_3)	Centar Klastera 4 (b_4)
0,022441	4	0,1496	0,4106	0,7375	0,9556

Korak 3. Podaci su grupisani u četiri klastera, Tabela 15. Klaster "ne ispunjava" od 0 do 30, klaster "malo ispunjava" od 31 do 60, klaster "gotovo ispunjava" od 61 do 85 i klaster "ispunjava" od 86 do 100. Klaster y_1 (ne ispunjava) sadrži 13 podataka, klaster y_2 (malo ispunjava) sadrži 23 podatka, klaster y_3 (gotovo ispunjava) sadrži 29 podataka, a klaster y_4 (ispunjava) sadrži 25 podataka.

Korak 4. Centri klastera određeni su izračunavanjem srednje vrednosti podataka svakog klastera. Centri b_1, b_2, b_3, b_4, klastera y_1, y_2, y_3, y_4 su 0,1496, 0,4106, 0,7375, 0,9556 respektivno.

Korak 5. U ovom koraku određene su granične tačke funkcije članice. Prvo je izračunata razlika susednih podataka indikatora kompletnost (v_2-v_1=0-0=0; v_3-v_2=0,05556-0=0,05556...), kao u Tabeli 14.

Izračunata je sličnosti između susednih podataka, S_m, po formuli (6.4). Standardna devijacija je 0,022442, dok je izabrani parametar C=4.

$$S_1 = 1 - \frac{0}{4 \cdot 0{,}022442} = 1$$

$$S_2 = 1 - \frac{0.05556}{4 \cdot 0{,}022442} = 0{,}38112$$

.....

$$S_{89} = 1 - \frac{0}{4 \cdot 0{,}022442} = 1$$

$$S_{90} = 1 - \frac{0}{4 \cdot 0{,}022442} = 1$$

Minimalna sličnost za klastere y_1, y_2, y_3, y_4 je 0,38112, a to znači da je vrednost dve krajnje tačke y_{imin} i y_{imax}, za i=1,2,3,4, jednaka 0,38112.

Korak 6. Izračunavanje interpolacijom leve granične tačke funkcije, (a_i, 0).

Za klaster y_1, b_1=0,1496, y_{1min}=0, $\mu(y_{1min}) = 0{,}38112$; za klaster y_2, b_2=0,4106, y_{2min}=0,27778, $\mu(y_{2min}) = 0{,}38112$; za klaster y_3, b_3=0,7375, y_{3min}=0,61111, $\mu(y_{3min}) = 0{,}38112$; za klaster y_4, b_4=0,9556, y_{4min}=0,8889, $\mu(y_{4min}) = 0{,}38112$. Vrednosti leve granične tačke izračunavaju se pomoću formula (6.5) i (6.6).

$$a_1' = 0{,}1496 - \frac{0{,}1496 - 0}{1 - 0{,}38112} = -0{,}09211 < 0$$

a_1=0

$$a_2' = 0{,}4106 - \frac{0{,}4106 - 0{,}27778}{1 - 0{,}38112} = 0{,}19596 > 0{,}1496$$

a_2=0,19596

$$a_3' = 0{,}7375 - \frac{0{,}7375 - 0{,}61111}{1 - 0{,}38112} = 0{,}53324 > 0{,}4106$$

a_3=0,53324

$$a_3' = 0{,}9556 - \frac{0{,}9556 - 0.8889}{1 - 0{,}38112} = 0{,}84783 > 0{,}7375$$

a_4=0,84783

Korak 7. Izračunavanje interpolacijom desne granične tačke funkcije, (c_i, 0).

Za klaster y_1, b_1=0,1496, y_{1max}=0,22222, $\mu(y_{1max}) = 0{,}38112$; za klaster y_2, b_2=0,4106, y_{2max}=0,55556, $\mu(y_{2max}) = 0{,}38112$; za klaster y_3, b_3=0,7375, y_{3max}=0,83333, $\mu(y_{3max}) = 0{,}38112$; za klaster y_4, b_4=0,9556, y_{4max}=1, $\mu(y_{4max}) = 0{,}38112$. Vrednosti desne granične tačke izračunavaju se pomoću formula (6.7) i (6.8).

$$c_1' = 0.1496 + \frac{0{,}22222 - 0{,}1496}{1 - 0{,}38112} = 0{,}26696 < 0{,}4106$$

c_1=0,26696

$$c_2' = 0{,}4106 + \frac{0.55556 - 0{,}4106}{1 - 0{,}38112} = 0{,}64480 < 0{,}7375$$

c_2=0,64480

$$c_3' = 0{,}7375 + \frac{0{,}83333 - 0{,}7375}{1 - 0{,}38112} = 0{,}89232 < 0{,}9556$$

c_3=0,89232

$$c_4' = 0{,}9556 + \frac{1 - 0{,}9556}{1 - 0{,}38112} = 1{,}02737$$

c_4=1,02737

Korak 8. Određene su tačke preseka funkcija članica, (d_i,0), odnosno presek funkcija članica klastera pomoću formule (6.9).

Tačka preseka, (d_1,0) između prvog i drugog klastera:

$$d_1 = \frac{(0{,}19596 - 0{,}26696) \cdot (0{,}1496 - 0{,}26696)}{0{,}1496 - 0{,}26696 + 0{,}19596 - 0{,}4106} + 0{,}26696$$

d_1=0,241843

Tačka preseka, (d_2,0) između drugog i trećeg klastera:

$$d_2 = \frac{(0{,}53324 - 0{,}64480) \cdot (0{,}4106 - 0{,}64480)}{0{,}4106 - 0{,}64480 + 0{,}53324 - 0{,}7375} + 0{,}64480$$

d_2=0,585195

Tačka preseka, (d_3,0) između trećeg i četvrtog klastera:

$$d_3 = \frac{(0{,}7375 - 0{,}89232) \cdot (0{,}7375 - 0{,}89232)}{0{,}7375 - 0{,}89232 + 0{,}7375 - 0{,}9556} + 0{,}89232$$

d_3=0,866068

Korak 9. Ograničavanje vrednosti funkcija pripadnosti. Na primer, određena je maksimalna vrednost funkcije članice prvog, drugog i trećeg klastera na 0,9, ($\mu(\vartheta_1)$= $\mu(\vartheta_2)$=$\mu(\vartheta_3)$=0,9), a funkcije članice četvrtog klastera na 1 za v > b_4, $\mu(\vartheta_4)$ =1. Granični interval ograničenja funkcija članica računamo prema formulama (6.12) i (6.13).

Prvi klaster

$$v_{L1} = 0{,}9 \cdot (0{,}1496 - 0) + 0$$

v_{L1}=0,13464

$$v_{R1} = 0{,}26696 - 0{,}9 \cdot (0{,}26696 - 0{,}1496)$$

v_{R1}=0,16133

Drugi klaster

$$v_{L2} = 0{,}9 \cdot (0{,}4106 - 0{,}19596) + 0{,}19596$$

v_{L2}=0,38914

$$v_{R2} = 0{,}64480 - 0{,}9 \cdot (0{,}64480 - 0{,}4106)$$

v_{R2}=0,43402

Treći klaster

$$v_{L3} = 0{,}9 \cdot (0{,}7375 - 0{,}53324) + 0{,}53324$$

v_{L3}=0,71707

$$v_{R3} = 0{,}89232 - 0{,}9 \cdot (0{,}89232 - 0{,}7375)$$

v_{R3}=0,75298

Četvrti klaster

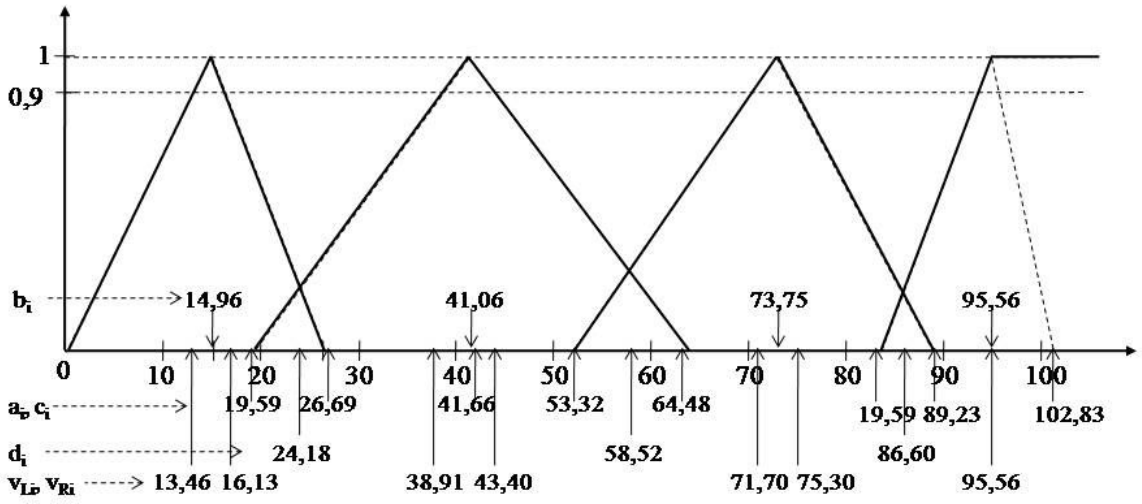
Iz uslova da je ograničenje funkcije $\mu(\vartheta_4)$=1 za sve vrednosti veće od b_4, tada su v_{L4}= v_{R4}= b_4. To znači da v_{L4} i v_{R4} imaju vrednost 0,9556.

Nakon sprovedenih koraka za konstrukciju funkcije članice u Tabeli 16 prikazani su dobijeni rezultati za izradu funkcije članice za indikator kompletnost. Na slici 29 prikazana je funkcija članica za indikator kompleksnost. Svi rezultati su pomnoženi sa 100 kako bi se lakše prikazali na grafiku.

Tabela 16. Dobijeni rezultati za konstrukciju funkcije pripadnosti

	a_i	b_i	c_i	d_i	v_{Li}	v_{Ri}
Klaster 1 (y_1)	0	0,1496	0,26696	0,241843	0,13464	0,16133
Klaster 2	0,19596	0,4106	0,64480	0,585195	0,38914	0,43402

(y_2)						
Klaster 3 (y_3)	0,53324	0,7375	0,89232	0,866068	0,71707	0,75298
Klaster 4 (y_4)	0,84783	0,9556	1,02737	-	0,9556	0,9556



Slika 29. Funkcija članica za indikator kvaliteta kompletnost

6.5.3.3. Određivanje funkcija pripadnosti ograničenja

Nakon konstrukcije funkcija pripadnosti ograničenja za indikatore kvaliteta određuje se skup optimalnih ograničenja, odnosno optimalne funkcije pripadnosti ograničenja.

Definiše se skup ograničenja:

$R_1^f = "Optimalna\ kompletnost"$, funkcija pripadnosti ograničenja indikatora kompletnost u delu ispunjava;

$R_2^f = "Optimalna\ korektnost"$, funkcija pripadnosti ograničenja indikatora korektnost u delu delimično ispunjava i u delu ispunjava;

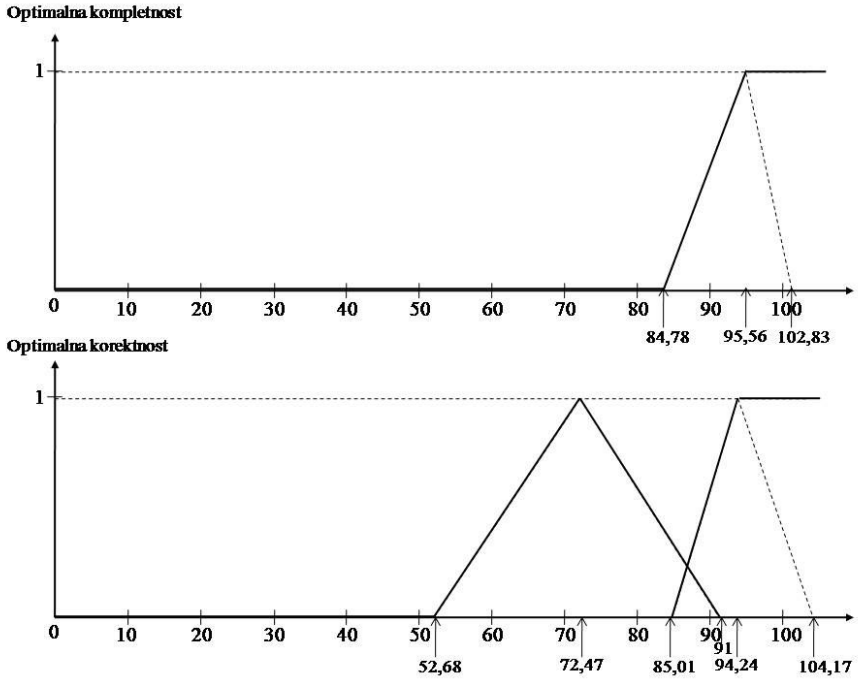
$R_3^f = "Optimalna\ izvodljivost"$, funkcija pripadnosti ograničenja indikatora izvodljivost u delu ispunjava;

$R_4^f = "Optimalna\ iskoristivost"$, funkcija pripadnosti ograničenja indikatora iskoristivost u delu delimično ispunjava i u delu ispunjava;

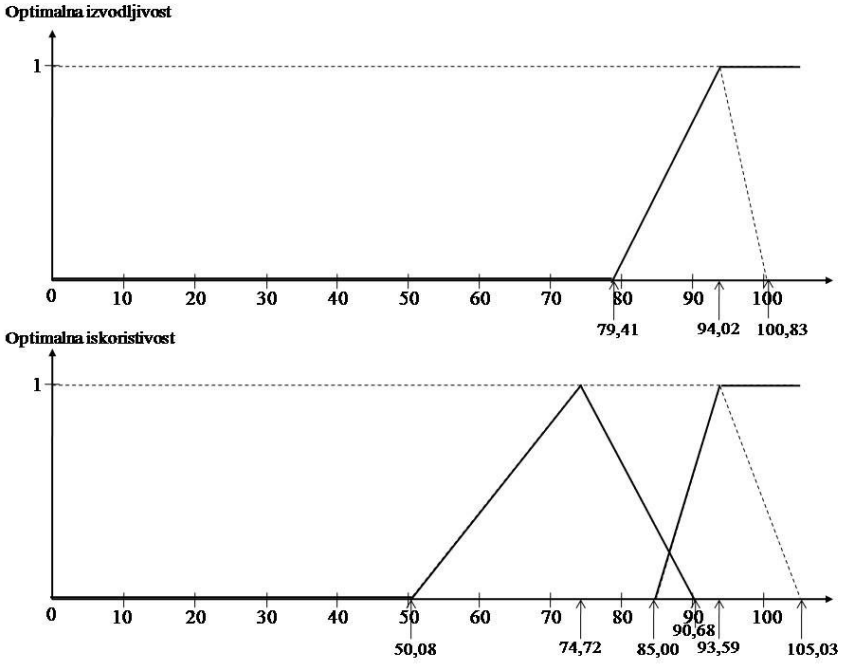
$R_5^f = "Optimala\ nedvosmislenost"$, funkcija pripadnosti ograničenja indikatora nedvosmislenost u delu ispunjava;

$R_6^f = "Optimalna\ proverljivost"$, funkcija pripadnosti ograničenja indikatora proverljivost u delu ispunjava;

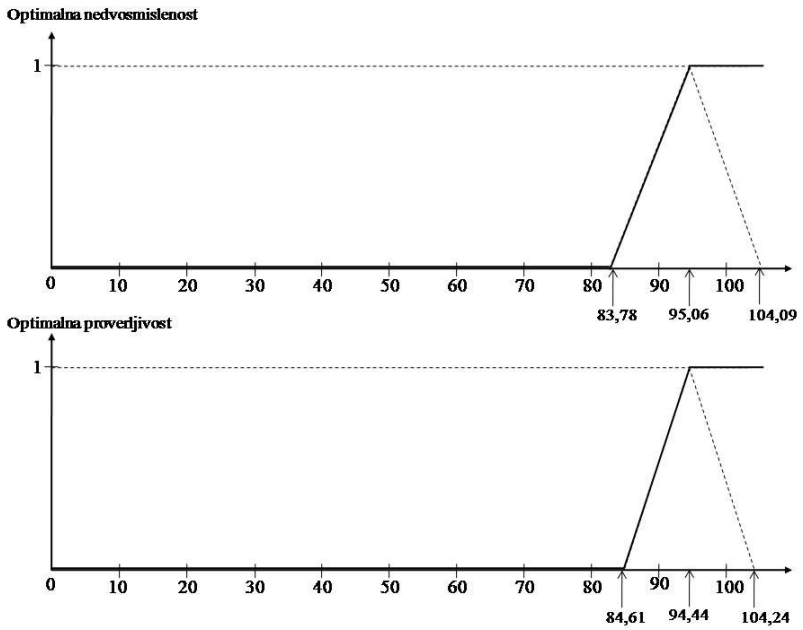
Optimalne funkcije pripadnosti ograničenja za ove skupove prikazane su na slikama 30, 31 i 32.



Slika 30. Optimalna funkcija pripadnosti ograničenja za kompletnost i korektnost



Slika 31. Optimalna funkcija pripadnosti ograničenja za izvodljivost i iskoristivost



Slika 32. Optimalna funkcija pripadnosti ograničenja za nedvosmislenost i proverljivost

6.5.4. Prioriteti i pragovi zadovoljenja

Nakon što su definisane funkcije pripadnosti ograničenja određeni su prioriteti i pragovi zadovoljenja za indikatore kvaliteta:

- "Optimalna kompletnost",[P_0.8, T_0], odnosno [$\rho(R_1^f) = 0.8$, T_0];
- "Optimalna korektnost", [P_0.85, T_0], odnosno [$\rho(R_2^f) = 0.85$, T_0];
- "Optimalna izvodljivost", [P_0.9, T_0], odnosno [$\rho(R_3^f) = 0.9$, T_0];
- "Optimalna korisnost", [P_0.9, T_0], odnosno [$\rho(R_4^f) = 0.9$, T_0];
- "Optimalana nedvosmislenost", [P_0.85, T_0], odnosno [$\rho(R_5^f) = 0.85$, T_0];
- "Optimalna proverljivost", [P_0.9, T_0], odnosno [$\rho(R_6^f) = 0.9$, T_0];

6.5.5. Izračunavanje globalnog stepena zadovoljenja i određivanje kriterijuma

Pre nego što se počne sa izračunavanjem globalnog stepena zadovoljenja ograničenja određuje se zavisnost između skupova ograničenja, odnosno parametara. Skupovi ograničenja mogu biti konjuktivno ili/i disjunktivno povezani.

Kvalitet zahteva zavisi od ispunjenosti uslova ograničenja svih varijabli, tako da je izabrana konjuktivna zavisnost između skupova ograničenja.

Formula za izračunavanje globalnog stepena zadovoljenja ograničenja za šest skupova ograničenja povezanih konjukcijom, $R_1^f \wedge R_2^f \wedge R_3^f \wedge R_4^f \wedge R_5^f \wedge R_6^f$, je složena. Radi lakšeg izračunavanja, a zahvaljujući asocijativnosti, skupove ograničenja povezaćemo na sledeći način:$\left(R_1^f \wedge R_2^f\right) \wedge R_3^f \wedge \left(R_4^f \wedge R_5^f\right) \wedge R_6^f$. Sada formula za izračunavanje globalnog stepena zadovoljena ograničenja kvaliteta zahteva izgleda ovako:

$\alpha = \mathrm{T_L}(\alpha_1, \alpha_2)$, gde je:

$$\alpha_1 = T_L\left(T_L\left(S_P\left(\mu_{R_1^f}(\vartheta), 1-\rho\left(R_1^f\right)\right), S_P\left(\mu_{R_2^f}(\vartheta), 1-\rho\left(R_2^f\right)\right)\right), S_P\left(\mu_{R_3^f}(\vartheta), 1-\rho\left(R_3^f\right)\right)\right)$$

$$\alpha_2 = T_L\left(T_L\left(S_P\left(\mu_{R_4^f}(\vartheta), 1-\rho\left(R_4^f\right)\right), S_P\left(\mu_{R_5^f}(\vartheta), 1-\rho\left(R_5^f\right)\right)\right), S_P\left(\mu_{R_6^f}(\vartheta), 1-\rho\left(R_6^f\right)\right)\right)$$

Za svaku vrednost ϑ izračunava se njen stepen pripadanja $\mu_{R_x^f}(\vartheta)$ koji se dobija kao presek funkcije pripadnosti i trenutne vrednosti, na osnovu formule (6.14).

Testiranjem modela ustanovljeni su sledeći kriterijumi za određivanje kvaliteta zahteva:

I) Ako je $\mu_{R_2^f}(\vartheta)$<0,60 ili $\mu_{R_4^f}(\vartheta)$<0,60 kriterijum nije ispunjen;
II) Ako je barem jedan od $\mu_{R_i^f}(\vartheta)$=1, $(i = 1, 2, \dots, 6)$ i svaki $S_{P2i4} > 0{,}69$ i $S_{P1,3,5i6} > 0{,}13$, i $\alpha > 0{,}94$ tada je ispunjen traženi kvalitet zahteva, u suprotnom nije ispunjen;
III) Ako je barem jedan $\mu_{R_i^f}(\vartheta)$=0, $(i = 1, 2, \dots, 6)$ tada nije ispunjen traženi kvalitet;
IV) Ako je S_{Pi}=1 za svaki $(i = 1, 2, \dots, 6)$ ispunjen je traženi kvalitet zahteva;
V) Zahtev zadovoljava traženi kvalitet kada je $\alpha > 0{,}94$ i ako su ispunjeni kriterijumi od I do IV.

Kada kriterijum I nije ispunjen potrebno je izvršiti redefinisanje zahteva težišno za indikatore korektnost i iskoristivost. To znači da oba ili jedan od navedenih indikatora ili malo ispunjava(ju) i teži(e) da pređu u kategoriju gotovo ispunjavaju ili iz kategorije gotovo ispunjavaju teže kategoriji ispunjavaju. Shodno navedenom zahteve treba redefinisati tako da im se poveća kvalitet.

Kada kriterijum II nije ispunjen potrebno je izvršiti redefinisanje zahteva za sve indikatore kod kojih nije ispunjen S_P.

Ako kriterijum III nije ispunjen, odnosno ako je vrednost bilo kog ili više indikatora nula tada je potrebno redefinisati zahtev tako da se podigne kvalitet za indikatore koji ne zadovoljavaju.

6.5.6. Donošenje odluke o kvalitetu zahteva

Donošenje odluke o kvalitetu zahteva zasniva se na izračunatom globalnom stepenu zadovoljenja i ispunjenosti kriterijuma.

Primer a): Primena kriterijuma I.

Ocene indikatora i vrednosti funkcija članica ograničenja date su u Tabelama 17 i 18, red a).

Ako vrednosti za izračunati stepen pripadanja svakog $\mu_{R_x^f}(\vartheta)$ i vrednosti prioriteta $\rho(R_x^f)$ uvrstimo u jednačinu za izračunavanje globalnog stepena zadovoljenja ograničenja α dobijamo sledeći rezultat:

$$\alpha_{1a} = T_L\Big(T_L\big(S_P(0{,}020408163, 1-0.8), S_P(0{,}115653041, 1-0.85)\big), S_P(0{,}382614648, 1-0.9)\Big)$$

$$\alpha_{1a} = T_L(T_L(0{,}216326531, 0{,}248305085), 0{,}444353183)$$

$$\alpha_{1a} = T_L(0{,}410916638, 0{,}444353183) = 0{,}672677705$$

$$\alpha_{2a} = T_L\Big(T_L\big(S_P(0{,}657635468, 1-0.9), S_P(0{,}108156028, 1-0.85)\big), S_P(0{,}039674466, 1-0.9)\Big)$$

$$\alpha_{2a} = T_L(T_L(0{,}691871921, 0{,}241932624), 0{,}135707019)$$

$$\alpha_{2a} = T_L(0{,}766418156, 0{,}135707019) = 0{,}798116852$$

$$\alpha_a = T_L(0{,}672677705, 0{,}798116852) = 0{,}933919145$$

Izračunata vrednost za $\mu_{R_2^f}(\vartheta)$=0,12 što je manje od 0,60. To znači da na osnovu kriterijuma I treba izvršiti redefinisanje zahteva tako da se ovaj indikator kvaliteta poveća. Ovo je neophodno jer se na osnovu ocene i vrednosti vidi da ovaj indikator kvaliteta više pripada kategoriji "malo ispunjava" nego kategoriji "gotovo ispunjava".

Tabela 17. Proračun stepena pripadanja za indikatore kompletnost, korektnost, izvodljivost

	Specifikacija zahteva					
Primer	X_1- Kompletnost	$\mu_{R_1^f}(\vartheta)$	X_2-Korektnost	$\mu_{R_2^f}(\vartheta)$	X_3-Izvodljivost	$\mu_{R_3^f}(\vartheta)$
a)	85	0,020408163	55	0,115653041	85	0,382614648
b)	85	0,020408163	80	0,602409639	85	0,382614648
c)	85	0,020408163	70	0,863409771	90	0,724845996
d)	70	0	70	0,863409771	80	0,040383299
e)	85	0,020408163	70	0,863409771	95	1

Tabela 18. Proračun stepena pripadanja za indikatore iskoristivost, nedvosmislenost i proverljivost

		Specifikacija zahteva				
	X_4- Iskoristivost	$\mu_{R_4^f}(\vartheta)$	X_5- Nedvosmislenost	$\mu_{R_5^f}(\vartheta)$	X_6- Proverljivost	$\mu_{R_6^f}(\vartheta)$
a)	80	0,657635468	85	0,108156028	85	0,039674466
b)	80	0,657635468	85	0,108156028	85	0,039674466
c)	75	0,965517241	85	0,108156028	85	0,108156028
d)	65	0,612479475	90	0,55141844	100	1

Primer b): Izračunavanje globalnog stepena zadovoljenja nakon redefinisanja zahteva i poboljšanja kvaliteta indikatora korektnost iz primera a).

Ocene indikatora i vrednosti funkcija članica ograničenja date su u Tabelama 17 i 18, red b).

$$\alpha_{1b} = T_L\Big(T_L\big(S_P(0{,}020408163, 1-0.8), S_P(0{,}602409639, 1-0.85)\big), S_P(0{,}382614648, 1-0.9)\Big)$$

$$\alpha_{1b} = T_L(T_L(0{,}216326531, 0{,}662048193), 0{,}444353183)$$

$$\alpha_{1b} = T_L(0{,}735156135, 0{,}444353183) = 0{,}852840349$$

$$\alpha_{2b} = T_L\left(T_L\left(S_P(0{,}657635468, 1-0.9), S_P(0{,}108156028, 1-0.85)\right), S_P(0{,}039674466, 1-0.9)\right)$$

$$\alpha_{2b} = T_L(T_L(0{,}691871921, 0{,}241932624), 0{,}135707019)$$

$$\alpha_{2b} = T_L(0{,}766418156, 0{,}135707019) = 0{,}798116852$$

$$\alpha_b = T_L(0{,}852840349, 0{,}798116852) = 0{,}970290946$$

Vrednosti $\mu_{R_2^f}(\vartheta)$=0,602 i $\mu_{R_4^f}(\vartheta)$=0,657 su veće od 0,60 što znači da kriterijum I ispunjava. Globalni stepen zadovoljenje α je 0,97 što je veće od zahtevanog globalnog stepena kvaliteta 0,94, te analizirani zahtev zadovoljava traženi kvalitet.

Primer c): Primena kriterijuma I i V kada su svi indikatori kvaliteta ispunjeni.

Ocene indikatora i vrednosti funkcija članica ograničenja date su u Tabelama 17 i 18, red c).

$$\alpha_{1c} = T_L(0{,}909014182, 0{,}752361396) = 0{,}977468399$$

$$\alpha_{2c} = T_L(0{,}976473771, 0{,}135707019) = 0{,}979666445$$

$$\alpha_c = T_L(0{,}977468399, 0{,}979666445) = 0{,}999541852$$

Izračunati globalni stepen zadovoljenja, α_c, je veći od zahtevanog, a kriterijum I je zadovoljen stoga zahtev ispunjava traženi kvalitet.

Primer d): Primena kriterijuma III.

Ocene indikatora i vrednosti funkcija članica ograničenja date su u Tabelama 17 i 18, red d).

U ovom primeru stepen pripadanja indikatora kompletnost je nula, dok je globalni stepen zadovoljenja $\alpha_d > 0{,}94$. Ovakav globalni stepen zadovoljenja pokazuje da kvalitet zahteva ispunjava definisani kvalitet. Međutim, u ovom slučaju potrebno je uzeti u obzir kriterijum III jer je $\mu_{R_1^f}(\vartheta)$=0. Na osnovu primene kriterijuma III ovaj zahtev ne ispunjava traženi kvalitet. Zahtev je potrebno redefinisati tako da indikator kvaliteta kompletnost ima vrednost $\mu_{R_1^f}(\vartheta)$>0.

$$\alpha_d = T_L(0{,}91978255, 0{,}945940811) = 0{,}99566351$$

Primer e): Primena kriterijuma II.

Ocene indikatora i vrednosti funkcija članica ograničenja date su u Tabelama 17 i 18, red e).

$$\alpha_{1e} = T_L\left(T_L\left(S_P(0{,}020408163, 1-0.8), S_P(0{,}863409771, 1-0.85)\right), S_P(1{,}1-0.9)\right)$$
$$\alpha_{1e} = T_L(T_L(0{,}216326531, 0{,}883898305), 1)$$
$$\alpha_{1e} = T_L(0{,}909014182, 1) = 1$$

$$\alpha_{2e} = T_L\left(T_L\left(S_P(0{,}612479475, 1-0.9), S_P(0{,}55141844, 1-0.85)\right), S_P(1{,}1-0.9)\right)$$
$$\alpha_{2e} = T_L(T_L(0{,}651231527, 0{,}618705674), 1)$$
$$\alpha_{2e} = T_L(0{,}86701656, 1) = 1$$

$$\alpha_e = T_L(1, 1) = 1$$

U ovom primeru $\alpha_e = 1 > 0{,}94$, što znači da je ispunjen traženi kvalitet zahteva. Međutim, primenjujući kriterijum II vidi se da je uslov $S_{P4} = 0{,}651231527 < 0{,}69$. Pošto je navedeni kriterijum manji od navedene granice ukupni kvalitet zahteva ne ispunjava traženu vrednost.

6.6. Rezultati primene unapređenog modela

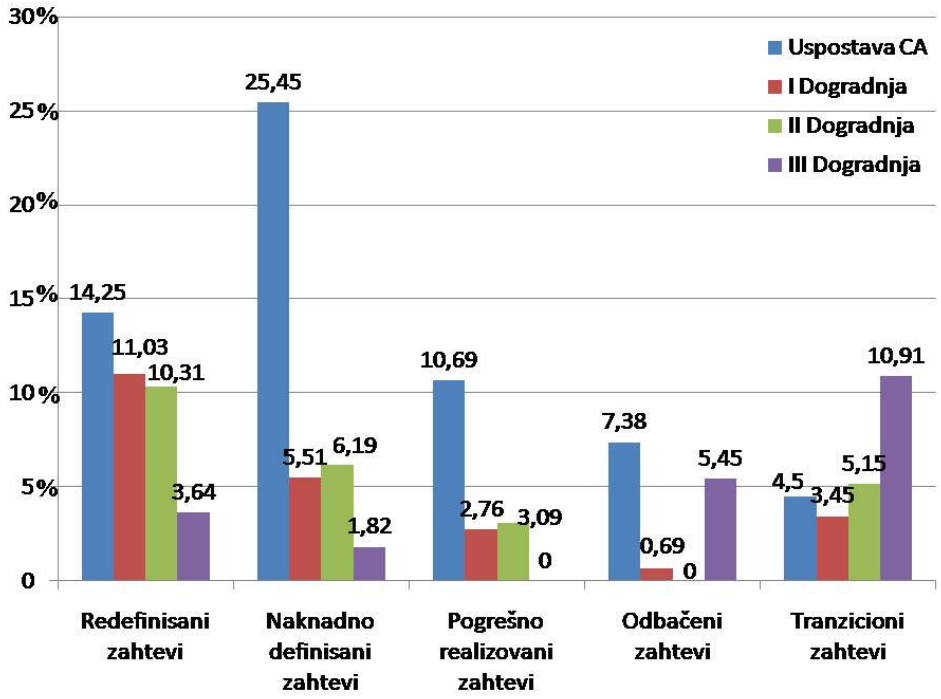
Prilikom identifikovanja i definisanja zahteva za dogradnju Sertifikacionog tela MO i VS (treća dogradnja) primenjen je postupak ocene kvaliteta zahteva, odnosno primenjen je unapređeni model sa klasifikacionom šemom i ocenom kvaliteta. Nakon završene implementacije zahteva izvršena je analiza uspešnosti njihove realizacije. Analiza je pokazala sledeće rezultate: redefinisanih zahteva u odnosu na ukupan broj zahteva je bilo 3,64%, naknadno definisanih je bilo 1,82%, nije bilo pogrešno realizovanih, odbačenih zahteva je bilo 5,45%, a tranzicionih je bilo 10,91%.

Primena modela za ocenu kvaliteta direktno je uticala na smanjenje loših zahteva iz kategorije redefinisanih i kategorije pogrešno realizovanih zahteva. Potreba za naknadnim redefinisanjem

zahteva smanjila se 2,38 puta u odnosu na druge dogradnje. Pogrešno realizovanih zahteva nije bilo, dok ih je u drugoj nadogradnji bilo 3,09% u odnosu na ukupan broj loših zahteva.

Procenat odbačenih zahteva je u odnosu na ukupan broj zahteva bio na nivou uvođenja sistema. Uzrok nastanka odbačenih zahteva u trećoj dogradnji je nedostatak finansijskih sredstava za njihovu realizaciju.

Veliki procenat tranzicionih zahteva od 10,91% koji je veći nego za vreme uvođenja sistema posledica su nemogućnosti implementacije zbog zastarelosti aplikativnog i sistemskog softvera i hardvera.



Slika 33. Uporedni pregled loših zahteva nakon primene modela sa klasifikacionom šemom i unapređenog modela

Primena unapređenog modela sa klasifikacionom šemom i ocenom kvaliteta zahteva doprinela je procentualnom smanjenju loših zahteva u odnosu na uvođenje i prethodne dogradnje Sertifikacionog tela MO i VS i sistema za personalizaciju. Uporedni pregled loših zahteva za vreme uvođenja sistema, nakon primene model sa klasifikacionom šemom i primene unapređenog modela prikazano je na slici 33.

7. Zaključak

Utvrđivanje i definisanje zahteva predstavlja prvi korak u razvoju ne samo PKI nego i drugih softverskih proizvoda. Dobro utvrđeni i definisani zahtevi su osnova za kvalitetan proizvod izrađen na vreme i u granicama budžeta. Da bi se utvrdili i kvalitetno definisali svi zahtevi potrebno je dobro poznavati procese koji se žele unaprediti ili sistem koji se želi uvesti. Sa jedne strane, korisnik treba da iskaže svoje potrebe i želje, a sa druge strane te potrebe treba da razumeju inženjeri koji treba da realizuju sistem. Što je sistem složeniji, kao što je PKI, to je teže utvrditi i definisati kvalitetne zahteve. Sistematizacija PKI arhitektura, njihova komparativna analiza i komparativna analiza prednosti i nedostataka pružaju korisnicima i stručnim licima da bolje razumeju i sagledaju PKI, a time i da bolje iskažu potrebe.

Klasifikaciona šema zahteva za PKI daje radni okvir za utvrđivanje zahteva i smernice za njihovo definisanje. Prilagođena je tako da je mogu iskoristiti i korisnici i stručna lica kako bi se što lakše usaglasili oko zahteva za PKI. Integracija klasifikacione šeme za PKI u modelu za definisanje zahteva, kao i sama primena takvog modela prilikom dogradnji Setifikacionog tela MO i VS i sistema za personalizaciju doprinela je smanjenju broja loših zahteva. Efekti primene modela sa klasifikacionom šemom direktno su se odrazili na smanjenje broja redefinisanih, naknadno definisanih i pogrešno realizovanih zahteva. Broj redefinisanih zahteva u nadogradnjama PKI se smanjio jer su smernice iz klasifikacione šeme uticale da se zahtevi jasnije definišu. Efekat klasifikacione šeme izražen je i u smanjenju potrebe za naknadnim definisanjem zahteva jer je obuhvaćen širok spektar kategorija zahteva za oblast PKI što je uticalo na njihovo pravovremeno pronalaženje i definisanje. Na smanjenje pogrešno realizovanih zahteva klasifikaciona šema je uticala tako što ja doprinela smanjenju broja zahteva koje je potrebno redefinisati, odnosno smanjenje broja zahteva koji nisu dovoljno jasni, a što je čest uzrok pogrešne realizacije.

Model za definisanje zahteva sa klasifikacionom šemom doprinosi smanjenju rizika od nedovoljnog sagledavanja potreba korisnika i potreba za redefinisanjem i definisanjem novih zahteva u odmaklim životnim fazama razvoja proizvoda. Međutim, primena klasifikacione šeme ne utiče u dovoljnoj meri na kvalitet zahteva, tako da mogu postojati nejasnoće kod korisnika i inženjera u toku implementacije zahteva. Model sa klasifikacionom šemom unapređen je modelom za procenu kvaliteta zahteva. Ovaj model omogućava korisnicima i inženjerima

zahteva (stručnim licima) da na jednostavan način u toku validacije zahteva, ocenjivanjem indikatora, ustanove da li zahtev poseduje dovoljan kvalitet za implementaciju.

Sinergija modela sa klasifikacionom šemom i modela za ocenu kvaliteta zahteva u unapređeni model za definisanje zahteva daje efikasan postupak za utvrđivanje i definisanje zahteva za PKI i smanjuje rizik od propadanja projekta za uvođenje ili dogradnju PKI.

7.1. Ostvareni doprinosi

U ovoj disertaciji ostvareni su sledeći doprinosi:

- izrađena je klasifikaciona šema zahteva za PKI koja obezbeđuje konzistentan način klasifikovanja zahteva za PKI, brzo i jednostavno identifikovanje PKI zahteva, a koju mogu koristiti organizacije koje imaju nameru da uvedu PKI u svoje poslovanje, kao i organizacije koje se bave razvojem i implementacijom PKI;
- izrađen je model za identifikovanje i definisanje zahteva primenom klasifikacione šeme koji unapređuje aktivnosti inžinjeringa zahteva;
- određena su usmerenja za identifikovanje i definisanje zahteva za svaku kategoriju klasifikacione šeme PKI;
- postignuta je univerzalnost klasifikacione šeme zahteva za PKI. Klasifikaciona šema se u većini svojih kategorija može primeniti i u drugim oblastima razvoja softverskog proizvoda, a u nekim svojim kategorijama i u definisanju zahteva bilo kog proizvoda (organizaciono-poslovni zahtevi, održavanje, bezbednost);
- izvršena je sistematizacija postojećih PKI arhitektura. Ova sistematizacija, kao i urađena komparativna analiza daju čvrstu osnovu za izbor najpovoljnije PKI arhitekture kao osnovnog zahteva za dalje određivanje i definisanje zahteva;
- razvijen je model za procenu kvaliteta zahteva zasnovan na rešavanju generalizovanog problema zadovoljenja fuzzy ograničenja sa prioritetima i indikatorima zasnovanim na dobrim karakteristikama zahteva;
- unapređene su aktivnosti inženjeringa zahteva kroz unapređeni model za definisanje zahteva zasnovan na klasifikacionoj šemi i proceni kvaliteta zahteva;
- izvršena je identifikacija, sistematizacija i kritička analiza postojećih klasifikacionih šema zahteva, PKI arhitektura i identifikovane su metode za procenu kvaliteta zahteva.

7.2. Oblast primene

Unapređeni model za definisanje zahteva za PKI primenjiv je u oblasti inženjeringa zahteva za PKI. Međutim, primenjeni modeli mogu se koristiti i u drugim oblastima.

Model za definisanje zahteva zasnovan na klasifikacionoj šemi može se primeniti za definisanje zahteva u drugim oblastima uz prilagođavanje klasifikacione šeme konkretnoj oblasti.

Model za procenu kvaliteta zahteva zasnovan na rešavanju generalizovanog problema zadovoljenja fuzzy ograničenja sa prioritetima može se primeniti za procenu kvaliteta zahteva u drugim oblastima. Model za procenu kvaliteta se lako može prilagoditi tako što će se izabrati odgovarajući indikatori za procenu kvaliteta i funkcije članice. Koristeći opisan postupak za konstrukciju funkcija članica na osnovu postojećih rezultata mogu se konstruisati funkcije ograničenja u primenjenoj oblasti. Ovaj model može se primeniti i prilikom donošenja odluke za izbor najbolje opcije za rešavanje nekog problema u različitim oblastima.

7.3. Pravci daljeg razvoja

Unapređeni model za definisanje zahteva za PKI dalje treba razvijati kroz pojedinačna poboljšanja modela zasnovanog na klasifikacionoj šemi i modela za procenu kvaliteta zahteva.

Prvi model treba razvijati kroz unapređenja klasifikacione šeme. Klasifikacionu šemu zahteva treba razvijati u pravcu proširenja novim kategorijama zahteva, kao što je kategorija "verifikacija zahteva". Dalja unapređenja treba sprovoditi u pravcu ispunjavanja regulative iz oblasti PKI i tehničko tehnološkim promenama.

Model za procenu kvaliteta zahteva treba unapređivati kroz uvođenje analize kvaliteta teksta zahteva, odnosno procene indikatora kvaliteta „niskog nivoa" za tekst zahteva, kao što su veličina zahteva, broj dvosmislenih termina, imperativni glagolski oblici, preklapanje zahteva, i tako dalje.

Unapređeni model za definisanje zahteva je potrebno proveriti u drugim okruženjima uz navedena prilagođavanja modela i izradu odgovarajućeg softverskog rešenja.

8. Literatura

[1] American Bar Association. PKI Assessment Guidelines, PAG v 1.0.Guidelines Information Security Committee. USA. 2003;

[2] Kuhn DR, Hu VC, Polk WT, Chang S-J. Introduction to Public Key Technology and the Federal PKI Infrastructure. NIST Special Publication SP 800-32. NIST. 2001.

[3] Linn J. Trust Models and Management in Public-Key Infrastructures. RSA Laboratories. 2000. Pristupan 18.09.2021. godine. Raspoloživo na: http://networkdls.com/Articles/PKIPaper.pdf.

[4] Polk WT, Hastings NE. Bridge Certification Authorities: Connecting B2B Public Key Infrastructures. National Institute of Standards and Technology. 2000.

[5] Perlman R. An Overview of PKI Trust Models. IEEE Network. 1999; vol. 13: 38-43.

[6] Choudhury S, Bhatnagar K, Haque W. Public Key Infrastructure Implementation and Design. M&T Books; 2002.

[7] Prodanović R, Vulić I, Tot I. A survey of PKI architecture, 5th International Scientific Conference on Knowledge Based Sustainable Development – ERAZ 2019; 23 May 2019; Budapest, Hungary. 2019.

[8] Microsoft. Certificate Trust List Overview. 2021. Pristupano 18.09.2021.godine. Raspoloživo na: http://msdn.microsoft.com/en-us/library/windows/desktop/aa376545%28v=vs.85%29.aspx.

[9] Certipost. Trust List Usage Recommendations for a European IDABridge/Gateway CA Pilot for Public Administrations. IDA PKI II / EBGCA /WP1.2. 2004.

[10] Moses T. PKI trust models. Draft. 2003. Pristupano 21.02.2022. godine. Raspoloživo na: https://www.scribd.com/document/140586360/PKI-Trust-Models.

[11] Adams C, Lloyd S. Understanding PKI: Concepts, Standards, and Deployment Considerations. Second Edition .Addison Wesley; 2002.

[12] Blanchard D. I-CIDM Bridge to Bridge Interoperations. In: 5th Annual PKI R&D Workshop Making PKI Easy to Use. 2006.

[13] NIST. Public Key Interoperability Test Suite (PKITS), Certification Path Validation, Version 1.0.1. 2011. Pristupano 19.09.2021. godine. Raspoloživo na: https://csrc.nist.gov/CSRC/media/Projects/PKI-Testing/documents/PKITS.pdf.

[14] Cooper D, Santesson S, Farrell S, Boeyen S, Housley R, Polk W. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280. 2008.

[15] Murphy PE. A bridge CA for Europe's Public Administrations - Feasibility study. Intertchange of Data between Administrations. EESSI. Rome. 2003.

[16] Casola V, Mazzeo A, Mazzocca N, Rak M. An Innovative Policy-Based Cross Certification Methodology for Public Key Infrastructures. Second European PKI Workshop: Research and Applications, EuroPKI 2005, Canterbury, UK, June 30 - July 1; 2005. p. 100–117. DOI 10.1007/11533733_7.

[17] Lopez J, Oppliger R, Pernul G. Classifying Public Key Certificates. 2nd European PKI Workshop: Research and Applications (EuroPKI05). LNCS. 2005; 3545: 135-143.

[18] Lioy A, Marian M, Moltchanov N, Pala M. PKI past, present and future. International Journal of Information Security. Heidelberg. 2006; 5(1): 18-29. DOI 10.1007/s10207-005-0077-9.

[19] Shirey R. Internet Security Glossary, Version 2. RFC 4949. IETF. 2007.

[20] Prodanović R, Vulić I. Failure Points in the PKI Architecture. Vojnotehnički glasnik/Military Technical Courier. 2017; 65 (3):771-784.

[21] Liping H, Lei S. Research on Trust Model of PKI. Fourth International Conference on Intelligent Computation Technology and Automation. 2011; 232-235, DOI 10.1109/ICICTA.2011.67.

[22] Turnbull J. Cross-Certification and PKI Policy Networking. Version: 1.0. Entrust. 2000. Pristupano: 19.09.2021. godine. Raspoloživo na: http://au-kbc.org/bpmain1/PKI/cross_ certification.pdf.

[23] Burr WE. Public Key Infrastructure (PKI) technical Specification: Part A –Technical Concept of Operations.Working Draft. TWG-98-59. 1998.

[24] Guo Z, Okuyama T, Finley MR. A New Trust Model for PKI Interoperability. Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services - (icas-isns'05). 2005; 37-37. DOI 10.1109/ICAS-ICNS.2005.6.

[25] Hat-hong E, HaClong UU, Song M, Zhang H. A trans-domain convergence architecture trust model for network trust. The Journal of China Universities of Posts and Telecommunlcatlons. 2007; vol.14.

[26] Project Delivery Performance: AIPM and KPMG Project Management Survey 2020. Pristupano: 25.09.2021. godine. Raspoloživo na: https://home.kpmg/au/en/home/insights/ 2020/08/australian-project-delivery-performance-survey-2020.html.

[27] Lim R. Top 10 Main Causes of Project Failure. 2021. Pristupano 15.12.2021. godine. Raspoloživo na: https://project-management.com/top-10-main-causes-of-project-failure/.

[28] TeamStage. 31 Pivotal Project Management Statistics for 2021. Pristupano 15.12.2021. godine. Raspoloživo na: https://teamstage.io/project-management-statistics/.

[29] Lindquist C. Fixing the Software Requirements Mess. 2005. Pristupano 20.12.2021.godine. Raspoloživo na: https://www.cio.com/article/255253/developer-fixing-the-software-requirements-mess.html.

[30] Ellis K. The Impact of Business Requirements on the Success of Technology Projects. IAG Consulting. 2009.

[31] Standish Group International Inc.2002. CHAOS Summary 2009 The 10 Laws of CHAOS. 2009. Pristupano: 12.09.2021. Raspoloživo na: http://edocs.nps.edu/licensed/ CHAOSSummary2009.pdf.

[32] Davis CJ, Fuller RM, Tremblay M C, Berndt D J. Communication challenges in requirements elicitation and the use of the repertory grid technique. Journal of Computer Information Systems. 2006; 78.

[33] Wick MA, Iem E, Burns MAJ, et al. A Guide to the Business Analysis Body of Knowledge,v3., International Institute of Business Analysis. 2015. Pristupano 03.08.2021. godine. Raspoloživo na: https://book.akij.net/eBooks/2018/September/5b8a80dd494ce/BABOK_Guide_v3_Member.pdf.

[34] Souter N. Creative Business Solutions: Breakthrough Thinking: Brainstorming for Inspiration and Ideas. Sterling. 2007.

[35] Yu, E.S.K., "Modelling Organizations for Information Systems Requirements Engineering," Proc. REP3 – 1st International Symposium on Requirements Engineering, IEEE, 1993, pp. 34–41.

[36] van Lamsweerde A. Goal-Oriented Requirements Engineering: A Guided Tour. Proceedings RE'01, 5th IEEE International Symposium on Requirements Engineering, Toronto, August 2001. p. 249–263.

[37] White D. 5 Business Process Analysis Techniques to Know., ProcessMaker. 2021. Pristupano: 27.07.2021. godine. Raspoloživo na: https://www.processmaker.com/blog/5-business-process-analysis-techniques-to-know/.

[38] Long KA. Overview of Common Process Analysis Techniques. Business Rules Journal. 2012;13 (12). Pristupano: 27.07.2021. godine. Raspoloživo na: URL: http://www.brcommunity.com/a2012/b679.html.

[39] ReQtest. Requirements Analysis – Understanding the Process & Techniques. ReQtest. 2018. Pristupano: 27.07.2021. godine. Raspoloživo na: https://reqtest.com/requirements-blog/requirements-analysis/.

[40] Enginess. The Insider`s Guide to Enterprise. Technology Procurement. Chapter 01 Business Requirements Analysis. An Enginess Business Guide. Pristupano 28.07.2021. godine. Raspoloživo na: https://www.enginess.io/guides/technology-procurement/business-requirements-analysis.

[41] Olphert CW, Damodaran L. Getting what you want, or wanting what you get? - beyond user centred design. Proceedings of the Third International Conference on Design and Emotion. Loughborough, UK, 1-3 July 2002.

[42] Maguire M, Bevan N. User Requirements Analysis. In: Hammond J, Gross T, Wesson J, editors. Usability. IFIP WCC TC13 2002. IFIP — The International Federation for Information Processing. Springer, Boston, MA; 2002. 99. DOI 10.1007/978-0-387-35610-5_9

[43] Damian D. Challenges in Requirements Engineering. University of Calgary. PRIMS. 2000. DOI 10.11575/PRISM/31288. Pristupano 30.03.2022.godine. Raspoloživo na: https://prism.ucalgary.ca/handle/1880/46566.

[44] Wiegers K, Joy B. Software Requirements (Developer Best Practices). 3rd Edition. Microsoft Press; 2013. ISBN-10: 0735679665.

[45] IEEE 610.12-1990: IEEE Standard Glossary of Software Engineering Terminology. 1990. E-ISBN: 0-7381-0391-8.

[46] Yeh RT, Zave P, Conn AP, Cole GE. Software Requirements Analysis — New Directions and Perspectives. In: Vick CR, Ramamoorthy CV, editors. Handbook of Software Engineering. Van Nostrand Reinhold Co.;1984.

[47] Glinz, M. On Non-Functional Requirements. In: 15th IEEE International Requirements Engineering Conference (RE 2007); 2007. 21–26.

[48] Stellman A, Greene J. Applied Software Project Management . O'Reilly Media; 2005. p. 113. ISBN 978-0-596-00948-9.

[49] Davis A. Software Requirements: Objects, Functions and States. Prentice Hall, Upper Saddle River; 1993. ISBN 978-0-13-805763-3.

[50] IEEE. IEEE Recommended Practice for Software Requirements Specification. IEEE standard 830-1993. 1993.

[51] IEEE. IEEE Recommended Practice for Software Requirements Specification. IEEE standard 830-1998. 1998.

[52] Gilb T. Towards the Engineering of Requirements. Requirements Engineering Journal. 1997; 2(3):165-169.

[53] Sommerville I. Software Engineering.Ninth Edition. Addison-Wesley; 2011. ISBN 13: 978-0-13-703515-1.

[54] Glinz M. Rethinking the Notion of Non-Functional Requirements. In Proceedings of the 3rd World Congress for Software Quality, Munich, Germany. 2005; 55-64.

[55] Van Lamsweerde A. Requirements Engineering: From System Goals to UML Models to software specifications. John Wiley & Sons Ltd, Chichester, England; 2009, Reprinterd 2012.

[56] Odeh Y, Odeh M. A new classification of non-functional requirements for service-oriented software enineering. 2011.

[57] Erl T. SOA: Principles of Service Design. Prentice Hall, Upper Saddle River; 2007.

[58] Comai A. A Guide for the Discovery of Software Requirements. Version 1.0. 2007. Pristupano 11.08.2021. godine. Rapoloživo na: https://analisi-disegno.com/wp-content/uploads/2013/08/requirementsbyexample.pdf.

[59] ISO/IEC. ISO/IEC 25010. Pristupano 11.08.2021. godine. Raspoloživo na: https://iso25000.com/index.php/en/iso-25000-standards/iso-25010?start=0

[60] Grady R. Practical Software Metrics for Project Management and Process Improvement. Prentice-Hall; 1992.

[61] Eeles P. Capturing Architectural Requirements. JOUR. 2001. Pristupano 11.08.2021.godine. Raspoloživo na: https://www.researchgate.net/publication/329760910_Capturing_Architectural_ Requirements.

[62] Roman GC. A Taxonomy of Current Issues in Requirements Engineering. Computer. 1985; 18(4): 14–23. DOI 10.1109/MC.1985.1662861.

[63] Shukla V, Pandey D, Shree R. Requirements Engineering: A Survey, Communications on Applied Electronics (CAE). Foundation of Computer Science FCS, New York, USA. 2015; 3(5).

[64] Adams MacG K. Non-functional Requirements in Systems Analysis and Design, Springer International Publishing. 2015; 45-72.

[65] Jule H, Kees H, Hans B, Smulders A. Foundations of Information Security Based on Is027001 and Is027002. Best Practice. Van Haren Publishing. 2015. ISBN 90-8753-568-6.

[66] Alam M. Software Security Requirements Checklist. Int.J. of Software Engineering. USE. 2010; 3(1).

[67] Firesmith D. Specifying Reusable Security Requirements. Journal of Object Technology. Published by ETH Zurich, Chair of Software Engineering. 2004; 3(1).

[68] Caideron C, Marta E. A Taxonomy of Software Security Requirements. Avances en Sistemas e Informatica. 2007; 4 (3):47-56.

[69] Travis C. Security Requirements Reusability and the SQUARE Methodology. No. CMU/SEI-2010-TN-027. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst. 2010.

[70] Rjabibi N, Rabai BA. Developing a Novel Holistic Taxonomy of Security Requirements, Procedia Computer Science. 2015; 62: 213–220.

[71] Wiegers K. Karl Wiegers Describes 10 Requirements Traps to Avoid, Software Testing & Quality Engineering. 2000.

[72] Prodanović R, Vulić I. Classification as an Approach To Public Key Infrastructure Requirements Analysis. IET Software. 2019;13. DOI: 10.1049/iet-sen.2018.5286.

[73] Chokhani S, Ford W, Sabett R, at. al. Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework. RFC 3647. 2003.

[74] IETF RFC 3739: Internet X.509 Public Key Infrastructure: Qualified Certificates Profile. 2004.

[75] ETSI EN 319 412 - 5 – Electronic Signatures and Infrastructure (ESI); Certificate Profiles; Part 5: QCStatements, v2.1.1. 2016.

[76] ISO/IEC, The Directory: Public key and attribute certificate frameworks Internationali Standard ISO/IEC 9594-8. Recommendation ITU-T X.509. 2019.

[77] Santesson S, Myers M, Ankney R, Malpani A, at. al. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. RFC 6960. 2013. ISSN: 2070-1721.

[78] Kaliski B. PKCS #7: Cryptographic Message Syntax, Version 1.5. 1998.

[79] Housley R. Cryptographic Message Syntax (CMS). RFC 5652. 2009.

[80] Housley R. Update to the Cryptographic Message Syntax (CMS) for Algorithm Identifier Protection. RFC 8933. 2020.

[81] ETSI. ETSI TS 103 172 - Electronic Signatures and Infrastructures (ESI); PadES Baseline Profile, v2.2.2. ETSI. 2013.

[82] ETSI. ETSI TS 101 903 – Electronic Signatures and Infrastructures, XML Advanced Electronic Signatures (XAdES), v1.4.2. ETSI. 2010.

[83] ETSI. ETSI TS 101 733 - Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES), v2.1.1. ETSI. 2012.

[84] ETSI. ETSI TS 102 176-1 – Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash Functions and Asymmetric Algorithms, v2.0.0. ETSI. 2007.

[85] CWA. CWA 14171 – General guidelines for electronic signature verification. CWA. 2004.

[86] ETSI. Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. ETSI TS 319 421 v.1.1.1. 2016.

[87] Adams C, Cain P, Pinkas D, Zuccherato R. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). RFC 3161. 2001.

[88] Prodanović R, Sarang S, Rančić D, Vulić I, Stojanović GM, Stankovski S, Ostojić G, Baranovski I, Maksović D. Trustworthy Wireless Sensor Networks for Monitoring Humidity and Moisture Environments. Sensors, 2021: (21):3636. DOI 10.3390/s21113636.

[89] ANSI/TIA-942-A Telecommunication Infrastructure Standard for Data Centers. 2010.

[90] ISO/IEC. Information technology – Security techniques – information security management systems – Requirements. ISO/IEC 27001:2013.2013.

[91]NIST. FIPS 140-3 Announcing the Standard for Security Requirements for Cryptographic Modules. National Institute of Standards and Technology. 2019.

[92] SafeNet. ProtectServer Gold Non-Proprietary Security Policy FIPS140-2 Level 3. Document number: CR-2970 Revision: 1. SafeNet. Pristupano 19.08.2021. godine. Raspoloživo na: https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/ security-policies/140sp739.pdf.

[93] Gemalto. Level 3 Non-Proprietary Security Policy for ProtectServer Internal Express 2 (PSI-E2). Gemalto. 2018. Pristupano: 19.08.2021. godine. Raspoloživo na: https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3231.pdf.

[94] Goertzel MK, Winograd T, et al. Enhancing the Development Life Cycle to Produce Secure Software: A Reference Guidebook on Software Assurance, Data and Analysis Center for Software (part of the Defense Technical Information Center). 2008. Pristupano 19.08.2021. godine. Raspoloživo na: https://www.seas.upenn.edu/~lee/09cis480/papers/ DACS-358844.pdf.

[95] Withall S. Software Requirement Patterns (Best Practices). Microsoft Press. Redmond, WA, USA. 2007. ISBN: 0735623988.

[96] ETSI. ETSI TS 101 456 – Policy requirements for certification authorities issuing qualified certificates, v1.4.3. ETSI. 2007.

[97] CWA. CEN Workshop Agreement 14169: Secure Signature-Creation Device (EAL 4+). CWA. 2002.

[98] CWA. CEN Workshop Agreement 14167-3: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Modules for CSP Key Generation Services - Protection Profile (CMCKG-PP). CWA. 2004.

[99] Prodanović R, Vulić I. Model for PKI Interoperability in Serbia. Vojnotehnicki glasnik/ Military Technical Courier. 2017; 65(2):530.

[100] Boehm B. A view of 20th and 21st century software engineering. ICSE '06 Proceedings of the 28th international conference on Software engineering. University of Southern California, University Park Campus, Los Angeles, CA: Association for Computing Machinery, ACM New York, NY, USA. 2006;12–29. ISBN 1-59593-375-1.

[101] Denger C, Olsson T. Quality Assurance in Requirements Engineering. In: Aurum, A., Wohlin C, editors. Engineering and Managing Software Requirements. Springer, Berlin, Heidelberg. 2005. DOI 10.1007/3-540-28244-0_8.

[102] Génova G, Fuentes JM, Llorens J, et al. A framework to measure and improve the quality of textual requirements. Requirements Eng. 2013;18: 25–41. DOI 10.1007/s00766-011-0134-z.

[103] The Reuse Company. RQA Requirements Quality Analyzer. Pristupano 14.03.2022. godine. Raspoloživo na: http://www.reusecompany.com/index.php?option =com_content&view=category& layout=blog&id=171&Itemid=75&lang=en.

[104] Parra E, de la Vara J L, Alonso L. Poster: Analysis of Requirements Quality Evolution. 2018 IEEE/ACM 40th International Conference on Software Engineering: Companion (ICSE-Companion). 2018;199-201.

[105] Timoshchuk E V. Assessing the quality of the requirements specification by applying GQM approach and using NLP tools. Proceedings of ISP RAS. 2020; 32(2):15–28. DOI 10.15514/ISPRAS-2020-32(2)-2.

[106] Halligan R J. Requirements Quality Metrics: The Basis of Informed Requirements Engineering Management. Presented at the 1993 Complex Systems Engineering Synthesis and Assessment Technology Workshop (CSESAW ’93).Calvados, MD, USA. 1993.

[107] Thitisathienkul P, Prompoon N. Quality Assessment Method for Software Requirements Specifications Based on Document Characteristics and Its Structure. 2015 Second International Conference on Trustworthy Systems and Their Applications. 2015; 51-60. DOI 10.1109/TSA.2015.19.

[108] Wong LR, Mauricio D S. Qualities that the Activities of the Elicitation Process Must Meet to Obtain a Good Requirement. Journal of Engineering Science and Technology. 2019; 14(5):2883 – 2912.

[109] Koelsch G. Requirements Writing for System Engineering. Springer Science+Business Media New York, New York. 2016. DOI 10.1007/978-1-4842-2099-3.

[110] Firesmith D. Specifying Good Requirements. Journal of Object Technology. 2003; 2(4).

[111] Saavedra R, Ballejos L, Ale M. Software Requirements Quality Evaluation: State of the art and research challenges. 14th Argentine Symposium on Software Engineering. ASSE 2013. 2013; 240-257.

[112] Luo X, Lee J, Leung H, Jennings N. Prioritised Fuzzy Constraint Satisfaction Problems: Axioms, Instantiation and Validation. Fuzzy Sets and Systems. 2003;136(2): 151–188.

[113] Prodanović R, Rančić D, Vulić I, Bogićević D. The Approach to Measurement of Requirement Quality by Application of Generalized Prioritized Fuzzy Constraint Satisfaction Problem. Facta Universitatis, Series: Automatic Control and Robotics. 2020;19(3):175-190.

[114] Panić G. Razvoj namenskog sistema fazi logike za primenu u sistemima za upravljanje XML dokumentima. Doktorska disertacija. Prirodno-matematički fakultet, Univerzitet u Novom Sadu; 2013.

[115] Takači A. Trougaone norme prioriteta i njihova primena na modeliranje ispunjenja fazi ograničenja. Doktorska disertacija. Prirodno-matematički fakultet, Univerzitet u Novom Sadu; 2006.

[116] Zadeh L. Fuzzy Sets. Information and Control. 1965; 8(3):338-353.

[117] NASA. Appendix C: How to Write a Good Requirement. NASA. 2019. Pristupano 20.06.2020.godine. Raspoloživo na: https://www.nasa.gov/seh/appendix-c-how-to-write-a-good-requirement.

[118] Zowghi D, Coulin C. Requirements Elicitation: A Survey of Techniques, Approaches, and Tools. Springer Berlin Heidelberg, Berlin, Heidelberg. 2005;19–46.

[119] Niu N, Easterbrook SM. So, you think you know others' goals? A repertory grid study. IEEE Software. 2007; 24(2):53–61. DOI 10.1109/MS.2007.52.

[120] Maiden NAM, Gizikis A, Robertson S. Provoking creativity: Imagine what your requirements could be like. IEEE Software. 2004; 21(5): 68–75. DOI 10.1109/MS.2004.1331305.

[121] Mancini C, Rogers Y, Bandara AK, Coe T, Jedrzejczyk L, Joinson AN, Price BA.,Thomas, K, Nuseibeh B. Contravision: exploring users' reactions to futuristic technology. In: Proceedings of the 28th International Conference on Human Factors in Computing Systems, CHI 2010, Atlanta, Georgia, USA; April 10-15, 2010. p. 153–162.

[122] Alexander IF, Stevens R. Writing Better Requirements. Pearson Education. 2002.

[123] Robertson S, Robertson J. Mastering the Requirements Process. ACM Press/Addison-Wesley Publishing Co., New York, NY, USA. 1999.

[124] Mavin A, Wilkinson P, Harwood A, Novak M. Easy approach to requirements syntax (EARS). In: Proc. of the 17th IEEE International Requirements Engineering Conference, RE; 2009. p. 317–322. DOI 10.1109/RE.2009.9.

[125] Jackson M. Problem Frames: Analyzing and Structuring Software Development Problems. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA. 2001.

[126] Eichelberger H, Wolff von Gudenberg J. UML Class Diagrams - State of the Art in Layout Techniques. VISSOFT. 2003.

[127] Alexander I. Gore, sore, or what? IEEE Software. 2011; 28(1): 8–10. DOI 10.1109/MS.2011.7.

[128] Clarke EM, Wing JM. Formal methods: State of the art and future directions. ACM Computing Surveys. 1996; 28(4):626–643.

[129] van Lamsweerde A. Requirements engineering: from craft to discipline. In: Proceedings of the 16th ACM SIGSOFT International Symposium on Foundations of Software Engineering, 2008, Atlanta, Georgia, USA, November 9-14, 2008; p. 238–249. DOI 10.1145/1453101.1453133.

[130] Yu ESK. Towards modeling and reasoning support for early-phase requirements engineering. In: 3rd IEEE International Symposium on Requirements Engineering (RE'97), January 5-8, 1997, Annapolis, MD, USA. IEEE Computer Society;1997. p. 226–235. DOI 10.1109/ISRE.1997.566873.

[131] Robertson S, Robertson J. Mastering the requirements process: Getting requirements right. Addison-wesley. 2012.

[132] Alexander IF, Maiden N. Scenarios, Stories, Use Cases: Through the Systems Development Life-Cycle. John Wiley & Sons. 2005.

[133] Besnard P, Hunter A. Elements of Argumentation. The MIT Press. 2008.

[134] Boehm BW, Grünbacher P, Briggs RO. Developing groupware for requirements negotiation: Lessons learned. IEEE Software. 2001;18(3):46–55. DOI 10.1109/52.922725.

[135] Dai Clegg and Richard Barker. 1994. Case Method Fast-Track: A Rad Approach. Addison-Wesley Longman Publishing Co., Inc., USA.

[136] Karlsson J, Ryan K. A cost-value approach for prioritizing requirements. IEEE Software.1997; 14(5):67–74. DOI 10.1109/52.605933.

[137] Yu Y, Franqueira VNL, Tun TT, Wieringa R, Nuseibeh B. Automated analysis of security requirements through risk-based argumentation. Journal of Systems and Software. 2015; 106: 102–116. DOI 10.1016/j.jss.2015.04.065.

[138] Ramesh B, Cao L, Baskerville R. Agile requirements engineering practices and challenges: an empirical study. Inf. Syst. J. 2010; 20(5):449–480. DOI 10.1111/j. 1365-2575.2007.00259.x.

[139] Jackson M. The name and nature of software engineering. In: Revised Tutorial Lectures in Advances in Software Engineering. Lipari Summer School, 2007, p. 1–38. DOI 10.1007/978-3-540-89762-0_1.

[140] Moon M, Yeom K, Chae HS. An approach to developing domain requirements as a core asset based on commonality and variability analysis in a product line. IEEE Trans. Software Eng. 2005; 31(7):551–569. DOI 10.1109/TSE.2005.76.

[141] Tun TT, Boucher Q, Classen A, Hubaux A, Heymans P. Relating requirements and feature configurations: a systematic approach. In: Proc. of the 13th International Conference on Software Product Lines, SPLC; 2009, p. 201–210 . DOI 10.1145/1753235.1753263.

[142] Viana T, Bandara A, Zisman A. Towards a Framework for Managing Inconsistencies in Systems of Systems. In: Colloquium on Software-intensive Systems-of-Systems at 10th European Conference on Software Architecture, 29 Nov 2016, Copenhagen, ACM.; 2016. DOI 10.1145/3175731.3176177.

[143] Silva Souza VE, Lapouchnian A, Robinson WN, Mylopoulos J. Awareness requirements for adaptive systems. In: Proceedings of the 6th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, SEAMS ’11, ACM, New York, NY, USA; 2011. p. 60–69. DOI 10.1145/1988008.1988018.

[144] Filieri A, Maggio M, Angelopoulos K, D’Ippolito N, Gerostathopoulos I, Hempel AB, Hoffmann H, Jamshidi P, Kalyvianak E, Klein C, Krikav, F, Misailovic S, Papadopoulos AV, Ray S, Sharifloo AM, Shevtsov S, Ujma M, Vogel T. Software engineering meets control theory. In: 2015 IEEE/ACM 10th International Symposium on Software Engineering for Adaptive and Self-Managing Systems; 2015.p. 71–82. DOI 10.1109/SEAMS.2015.12.

[145] Jureta I, Borgida A, Ernst NA, Mylopoulos J. The requirements problem for adaptive systems. ACM Trans. Management Inf. Syst. 2014; 5(3):17. DOI 10.1145/2629376.

[146] Cleland-Huang J, Gotel O, Hayes JH, Mäder P, Zisman A. Software traceability: trends and future directions. In: Proc. of the Future of Software Engineering, FOSE@ICSE; 2014. p. 55–69. DOI 10.1145/2593882.2593891.

[147] Furtado F, Zisman A. Trace++: A traceability approach for agile software engineering. In: Proc. of the 24th International Requirements Engineering Conference, RE (2016); 2016.

[148] Mirakhorli M, Cleland-Huang J. Tracing non-functional requirements. In: Software and Systems Traceability. Springer; 2012. p. 299–320. DOI 10.1007/978-1-4471-2239-5_14.

[149] Prodanović R, Rančić D, Pronić-Rančić O, Vulić I. Model za identifikovanje i definisanje zahteva za PKI zasnovan na klasifikacionoj šemi zahteva. YUINFO 2022. U štampi 2022.

[150] Prodanović R, Vulić I, Jovančić D. Jedan pristup u analizi PKI zahteva. INFOTECH 2013 ICT Conference & Exhibition. 2013. ISBN: 978-86-82831-19-8.

[151] Saaty TL. The Analytic Hierarchy Process. McGraw-Hill, Inc.. 1980.

[152] Yadav HB, Yadav DK. Construction of Membership Function for Software Metrics. Procedia Computer Science. 2015; 46:933 – 940.

[153] Hattori K, Tor Y. Effective algorithm for the nearest neighbour method in the clustering problem. Pattern Recognitions. 1993; (26):741– 746.

9. Spisak slika

10. Spisak tabela

11. Prilozi

11.1. Prilog br. 1a. Komparativna analiza PKI arhitektura na osnovu izabranih parametara - prvi deo

		Jednostavne PKI arhitekture		Enterprise PKI arhitekture	
		Arhitektura sa jednim CA	Basic Trust List arhitektura	Hijerarhijska arhitektura	Mrežna arhitektura
Poverenje	Tačka poverenja.	CA koje je ujedno i root.	CA iz liste poverenja.	Root CA.	Svaki CA u arhitekturi koji je izdao sertifikat.
	Relacija poverenja.	Ne ostvaruje relacije poverenja	Lista poverenja.	Jednosmerna.	Dvosmerna i jednosmerna.
Sertifikaciona staza	Dužina sert. staze.	Jedan sertifikat.	Jedan sertifikat.	Suma sertifikata potčinjenih CA i sertifikata EE.	Suma sertifikata svih CA u izabranoj stazi i sertifikat EE.
	Konstrukcija sert. staze.	Jednostavna.	Jednostavna.	Jednostavna.	Složena.
Otkaz	Tačka otkaza.	Single CA.	Otkaz liste poverenja ili mehanizma za obradu sert. staze.	Root CA.	Nema jednu tačku otkaza koja utiče na otkaz cele arhitekture, osim kada u arhitekturu postoje dva CA.
			Pojedinačni CA iz liste poverenja.	Otkaz potčinjenog CA.	
	Težina otkaza.	Otkaz cele arhitekture, svi korisnici ne mogu koristi arhitekturu.	Nemogućnost korisnika da ostvari poverenje sa korisnicima čiji je CA u listi.	Gubitak poverenja u celu arhitekturu, svi korisnici ne mogu da koristiti arhitkturu.	Otkaz se odnosi na nemogućnost komuniciranja korisnika tog CA sa korisnicima drugih CA i obrnuto. Korisnici ostalih mogu da komuniciraju ako postoji
			Nemogućnost da svi korisnici ostvare poverenje sa korisnicima čiji je CA kompromitovan .	Gubitak poverenja u deo arhitekture, korisnici sertifikacionog tela koje je kompromitovano i	

		Jednostavne PKI arhitekture		Enterprise PKI arhitekture	
				korisnici svih njemu potčinjenih CA tela ne mogu koristiti arhitekturu.	validna sertifikaciona staza.
	Oporavak od otkaza	Uspostavljanje novog CA.	Ponovno uspostavljenje liste poverenja i mehanizma za obradu sert staze.	Ponovno uspostavljanje tačke poverenja, root CA.	Ponovno uspostavljanje CA, izdavanje sertifikata korisnicima i uspostavljanj relacija poverenja sa drugm CA.
			Uspostavljanje novog CA i njegov upis u listu korisnika.	Ponovno upostavljanje otkazanog potčinjenog CA i svih ostalih CA iz tog stabla.	
Skalabilnost		Loša	Loša	Srednja	Loša

11.2. Prilog br. 1b. Komparativna analiza PKI arhitektura na osnovu izabranih parametara - drugi deo

		Hibridne PKI arhitekture		
		Extended Trust arhitektura	Cross-Certified Enterprise arhitektura	Bridge CA arhitektura
Poverenje	Tačka poverenja	Svaki CA iz liste poverenja.	Tačke poverenja PKI arhitekture kojoj pripada EE.	Tačke poverenja PKI arhitekture kojoj pripada EE.
	Relacija poverenja	Ne ostvaruje relacije poverenja.	Jednosmerna i dvosmerna.	Jednosmerna i dvosmerna.
Sertifikaciona staza	Dužina sert. staze	Jedan sertifikat.	Suma najdužih sertifikacionih staza PKI arhitektura kojim pripadaju EE + sertifikaciona CA preko kojih se uspostavlja arhitektura i sertifikat EE.	Suma najdužih sertifikacionih staza PKI arhitektura kojim pripadaju EE i sertifikat bridge CA.
	Konstrukcija sert. staze	Jednostavna.	Složena.	Srednje složena.
Otkaz	Tačka otkaza	Lista poverenja ili mehanizma za obradu sert. staze.	karakteristična tačka otkaza arhitektura koje se povezuju.	bridge CA, potpuno, svi privatni ključevi
				bridge CA, delimično, neki privatni ključevi
		Svaki CA iz arhitektura od kojih je sačinjena ova arhitektura.	Bilo koji CA u arhitekturama između kojih je uspostavljeno poverenje.	Otkaz Principal CA, karakteristična tačka otkaza arhitektura koje se povezuju.
	Težina otkaza	Nemogućnost korisnika da ostvari povernje sa korisnicima CA iz liste.	Nemogućnost korisnika drugih arhitektura da komuniciraju sa korisnicima arhitekture otkazanog CA.	Gubitak poverenja u celu PKI, nemogućnost međusobnog komuniciranja korisnika svih arhitektura.
				Delimičan gubitak poverenja, nemogućnost komuniciranja korisnika samo delom arhitektura.
		Korisnik neće moći ostvariti poverenje sa	U zavisnosti od arhitekture, kako je već opisano za	U zavisnosti od arhitekture čiji je

		Hibridne PKI arhitekture		
		korisnicima otkazanog CA ili cele arhitekture.	enterprise arhitekture.	Principal CA, kako je već opisano za enterprise CA.
	Oporavak	Uspostavljananje liste poverenja i mehanizma za obradu staze.	Ponovno uspostavljanje CA i ostvarivanje relacija poverenja sa izabranim CA drugih arhitektura.	uspostavljanje novog Bridge CA i relacija poverenja sa Principa CA.
				Uspostavljanje relacija poverenja sa Principal CA.
		Uspostavljanje poverenja otkazanog CA ili poverenja u celu PKI.	Kako je već opisano za enterprise arhitekture i uspostavljanje relacija poverenja sa ostalim arhitekturama.	U zavisnsti od arhitekture, kako je već opisano za enterprise arhitekture i uspostavljanje poverenja sa Bridge CA.
Skalabilnost		Loša.	Loša.	Velika.

11.3. Prilog br. 2. Tehnike za analizu korisničkih zahteva po fazama i njihove dobre i loše osobine

Tehnika	Prednosti	Nedostaci
Prikupljanje informacija o korisnicima		
Analiza zainteresovanih strana - identifikovanje svih korisnika i zainteresovanih strana na koje sistem može uticati.	Obezbeđuje razmatranje svih relevantnih zainteresovanih strana.	-
Sekundarno istraživanje tržišta - istraživanje objavljenih izvora.	Dobar pregled tržišta.	Informacije mogu biti generalne i zastarele.
Analiza konteksta upotrebe – prikupljanje i analiza informacija iz okruženja povezanih sa radom korisnika.	Radni okvir za dokumentovanje svih faktora koji mogu uticati na projekat.	Proces može biti dugotrajan. Ne može se sve primeniti na projekat.
Analiza zadataka – analiza šta korisnik treba da uradi (radnja i ili kognitivni proces) da bi postigao zadatak.	Definiše i modelira zadatke koji mogu da istaknu direktne potrebe korisnika.	Može biti previše formalna za jednostavne zadatke ili zadatke otvorenog tipa.
Detaljne slike – mapiranje prostora problema radi lakšeg istraživanja i razumevanja.	Identifikovanje potencijalnih zahteva iz složenih korisničkih okruženja.	Slike mogu naglasiti postojanje nekih pokazatelja, ali bez dovoljno detalja.
Metoda terenskog proučavanja i posmatranja – promatranje korisnike dok rade i beleženje aktivnosti koje se odvijaju.	Omogućava pregled onoga što korisnici zaista rade i mogu otkriti nezapažene procese.	Zahteva mnogo vremena. Komentari korisnika i posmatranje analitičara mogu poremetiti zadatke.
Vođenje dnevnika – evidentiranje ponašanja korisnika u određenom vremenu.	Omogućava korisniku beleženje aktivnosti tokom dana.	Korisnici mogu zaboraviti da popune dnevnike ili sažete aktivnosti na kraju. Podsetnici analitičara mogu biti dosadni.
Video snimanje – snimanje procesa rada radi boljeg razumevanja i definisanja pitanja.	Beleženje trenutnih aktivnosti bez nametanja i ličnog kontakta.	Zahteva mnogo vremena. Zahteva od korisnika da objasne aktivnosti nakon posmatranja.
Identifikovanje potreba korisnika		
Anketiranje korisnika – prikupljanje informacija davanjem odgovora na pitanja u pisanoj formi.	Relativno brza metoda za određivanje prioritetnih potreba kod velikih grupa korisnika.Omogućuje statističku analizu.	Ne obuhvata detaljne komentare i možda neće dozvoliti nastavak ankete.

Tehnika	Prednosti	Nedostaci
Fokusne grupe – diskusiona grupa korisnika ili zainteresovanih strana istog profila.	Omogućava analitičaru da brzo dobije ideje i saglasnost od korisnika	Nagovaranje radi okupljanja grupa. Dominantni učesnici mogu nesrazmerno uticati na grupu.
Intervju – prikupljanje informacija razgovorom o potrebama i zahtevima u vezi sa novim sistemom.	Intervjui omogućavaju brzo iznošenje ideja i koncepata.	Treba dogovarati pristup i kombinovati niz mogućih mišljenja različitih korisnika.
Scenariji i slučajevi upotrebe - daju detaljne realne primere kako korisnici mogu izvršavati svoje zadatke u određenom kontekstu sa budućim sistemom.	Efikasan način razmišljanja o budućoj upotrebi sistema u kontekstu.	Scenariji mogu previše povećati očekivanja.
Radionice o budućnosti – diskutovanje o ostvarenom sistemu i njegovom uticaju na organizaciju u budućnosti.	Način da se misli kreativno.	Rezultati mogu izgledati previše ambiciozno za trenutne potrebe.
Procena postojećeg ili analiza konkurentnog sistema.	Efekasan način za identifikovanje trenutnih problema, mogućih novih karakteristika i kriterijuma za novi sistem.	Može dovesti do uključivanja previše novih funkcija ili učiniti sistem previše sličnim konkurentima.
Predvidjanje i procena		
Brainstorm – generisanje novih ideja.	Brzo razotkrivanje i inovativno razmišljanje.	Ne pokriva aspekte detaljnog dizajna.
Sortiranje kartica i dijagrami afiniteta – otkrivanje organizacione strukture.	Efikasno prikazivanje organizacione strukture sistema.	Potreban je način za kombinovanje rezultata ako ih pojedinci ili grupe izvode odvojeno.
Scenariji prezentacije – prikazivanje odnosa između radnji korisnika ili ulaza i izlaza sistema.	U ranom razvojnom ciklusu jednostavno demonstrira softverske interakcije i moguće korisničke interfejse.	Nedostaje interaktivni kvalitet izrade prototipova.
Prototip – kreiranje simulacija sistema.	Brzo se gradi i poboljšava. Omogućava rano otkrivanje problema upotrebljivosti kao odgovor na povratne informacije korisnika.	Izrađeni prototopi ne mogu se iskoristiti za gotov proizvod, a izgradnja oduzima dosta vremena. Ne podržavaju procenu finih detalja.
Dodela funkcija i analiza troškova i koristi – podela funkcija koje obavljaju ljudi i tehnologija. Procena isplativosti.	Identifikuje interes za zadatak. Pomaže da se definiše zadovoljstvo poslom i smanji rizik od nezadovoljnog osoblja.	Potreban je dobar pregled celog sistema. Mnoge opcije raspodele mogu izazvati zabunu. Ponekad je teško proceniti isplativost.
Dizajniranje uputstava i standarda	Oslanja se na stečena znanja.	Mogu biti previše uopšteni ili

Tehnika	Prednosti	Nedostaci
		ograničeni.
Paralelni dizajn – nezavisan rad manjih grupa dizajnera radi iznalaženja različitih rešenja	Mogućnost izbora najbolje ideje i najboljeg rešenja iz skupa ideja i rešenja.	Složena organizacija za okupljanje dizajnerskih timova.
Specifikacija zahteva		
Mapiranje zadataka/funkcija – uspostavljanje i prikazivanje odnosa između zadataka i funkcionalnih zahteva.	Izbor funkcija (kompromis, dodavanje ili ukidanje) koje su relevantne za određene zadatke.	Opravdavanje nepotrebnih funkcija kroz uključivanje nepotrebnih zadataka.
Kategorizacija zahteva – određivanje vrste zahteva.	Grupisanje zahteva u kategorije radi lakšeg procesa dizajna.	Možda će biti teško odlučiti u koju kategoriju pripada zahtev korisnika.
Prioritizacija – određivanje prioriteta zahteva shodno vremenu i resursima.	Osigurava ulaganje resursa u najvažnije aspekte sistema.	Loše upravljanje može dovesti do razočarenja korisnika.
Podešavanje kriterijuma - odnosi se na potrebu da kriterijumi pomognu u odlučivanju da li su zahtevi korisnika ispunjeni.	Način da se utvrdi da li je razvijeni sistem zadovoljio zahteve korisnika.	Nije lako definisati odgovarajuće kriterijume. Opsežno testiranje postignuća može biti resursno intenzivno.

11.4. Prilog br. 3. Međusobni uticaj zahteva iz klasifikacione šeme PKI

	1. Poslovno-organizacioni zahtevi	2. Zahtevi za komponentama i servisima PKI	3. Bezbednosni zahtevi	4.Softversko-hardverski zahtevi	5. Zahtevi za podršku funkcio- nisanju PKI	6. Zahtevi za PKI interoperabilnošću
1. Poslovno-organizacioni zahtevi	-	2.2.Zahtevi za sertifikatima 2.4.Zahtevi za registracionim autoritetom 2.6.Zahtevi za servisima korisnika	3.1.Opšti bezbednosni zahtevi	4.1. Softverski zahtevi 4.2. Hardverski zahtevi	5. Zahtevi za podršku funkcionisanju PKI	6.3.Zahtevi za domensku interoperabilnost
2. Zahtevi za komponentama i servisima PKI	1.1.Poslovni zahtevi	-	3.1.Opšti bezbednosni zahtevi 3.2.Posebni bezbednosni zahtevi 3.3.Zahtevi za kriptografijom	4.1. Softverski zahtevi 4.2. Hardverski zahtevi	5.2.Zahtevi za podršku u funk-cionisanju softvera i hardvera 5.3.Zahtevi za tehničko održavanje 5.5.Zahtevi za podršku u toku funkcionisanja sistema 5.7.Zahtevi za podrškom u ovladavanju PKI sistemom 5.8.Zahtevi za podrškom korisnicima	6.1. Zahtevi za interoperabilnosti aplikacija i hardvera 6.2. Zahtevi za interoperabilnost PKI komponenti

	1. Poslovno-organizacioni zahtevi	2. Zahtevi za komponentama i servisima PKI	3. Bezbednosni zahtevi	4.Softversko-hardverski zahtevi	5. Zahtevi za podršku funkcio- nisanju PKI	6. Zahtevi za PKI interoperabilnošću
					servisa	
3. Bezbednosni zahtevi	1. Poslovno-organizacioni zahtevi	2. Zahtevi za komponentama i servisima PKI	-	4.1. Softverski zahtevi 4.2. Hardverski zahtevi	5.4.Zahtevi za podrškom pre isporuke sistema 5.5.Zahtevi za podršku u toku funkcionisanja sistema 5.7.Zahtevi za podrškom u ovladavanju PKI sistemom zahteve za podršku korisnicima servisa 5.8.Zahtevi za podrškom korisnicima servisa	6.1. Zahtevi za interoperabilnosti aplikacija i hardvera 6.2. Zahtevi za interoperabilnost PKI komponenti 6.3.Zahtevi za domensku interoperabilnost
4.Softversko-hardverski zahtevi	1.1.7.Zahtevi za ekonomičnosti 1.1.2.Zahtevi za unapređenje poslovanja	2.1.Opšti zahtevi za komponentama i servisima 2.3.Zahtevi za sertifikacionim telom	3.3.Zahtevi za kriptografijom	-	5.2.Zahtevi za podršku u funkcionisanju softvera i hardver 5.3.Zahtevi za tehničko održavanje	6.1. Zahtevi za interoperabilnosti aplikacija i hardvera

	1. Poslovno-organizacioni zahtevi	2. Zahtevi za komponentama i servisima PKI	3. Bezbednosni zahtevi	4.Softversko-hardverski zahtevi	5. Zahtevi za podršku funkcio- nisanju PKI	6. Zahtevi za PKI interoperabilnošću
	1.1.3.Zahtevi za unapređenje bezbednosti 1.1.5.Zahtevi za edukacijom 1.1.8.Zahtevi za zainteresovanim stranama	2.6.Zahtevi za servisima korisnika			5.5.Zahtevi za podršku u toku funkcionisanja sistema	
5. Zahtevi za podršku funkcionisanju PKI	1.1.2.Zahtevi za unapređenje poslovanja 1.1.6.Zahtevi za marketingom 1.1.7.Zahtevi za ekonomičnosti 1.1.8.Zahtevi za zainteresovanim stranama 1.2.2.Zahtevi za organizacijom rada	2. Zahtevi za komponentama i servisima PKI	3.1.Opšti bezbednosni zahtevi	4.1. Softverski zahtevi 4.2. Hardverski zahtevi	-	6.1. Zahtevi za interoperabilnosti aplikacija i hardvera
6. Zahtevi za PKI	1.1.5.Zahtevi za	2.3.Zahtevi za	3.1.Opšti bezbednosni	4.1.1. Opšti softverski	5.2.Zahtevi za podršku	-

	1. Poslovno-organizacioni zahtevi	2. Zahtevi za komponentama i servisima PKI	3. Bezbednosni zahtevi	4.Softversko-hardverski zahtevi	5. Zahtevi za podršku funkcio- nisanju PKI	6. Zahtevi za PKI interoperabilnošću
interoperabilnošću	edukacijom 1.1.6.Zahtevi za marketingom 1.2.1.Zahtevi za pripremu uvođenja PKI 1.2.3.Zahtevi za regulatorna dokumenta	sertifikacionim telom 2.4.Zahtevi za registracionim autoritetom 2.5.Zahtevi za statusnim servisima i direktorijumom 2.6.Zahtevi za servisima korisnika	zahtevi 3.2.Posebni bezbednosni zahtevi 3.3.Zahtevi za kriptografijom	zahtevi za PKI 4.2.4. Zahtevi za mrežnu opremu 4.2.2. Zahtevi za serverskom opremom 4.2.3. Zahtevi za kripto opremom	u funkcionisanju softvera i hardv 5.3.Zahtevi za tehničko održavanje 5.5.Zahtevi za podršku u toku funkcionisanja sistema	

11.5. Prilog br. 4. Matrice poređenja parova alternativa u odnosu na kriterijum

Matrica poređenja alternativa prema kriterijumu sveobuhvatnost:

Sveobuhvatnost	IEEE 830	Somme-rville	Lamsw-eerde	Odeh	FOCUS-TBD	ISO/IEC 9126	FURPS	PKI MO i VS	PKI klasi fikacija
IEEE 830	1,00	2	2	2	0,20	3	3	0,5	0,33
Sommerville	0,50	1	0,5	0,5	0,14	2	2	0,33	0,25
Lamsweerde	0,50	2,00	1	1	0,17	3	3	0,5	0,33
Odeh	0,50	2,00	1,00	1	0,17	3	3	0,5	0,33
FOCUS-TBD	5,00	7,00	6,00	6,00	1	7	7	1	0,5
ISO/IEC 9126	0,33	0,50	0,33	0,33	0,14	1	1	0,25	0,2
FURPS	0,33	0,50	0,33	0,33	0,14	1	1	0,25	0,2
PKI MO i VS	2,00	3,00	2,00	2,00	1,00	4	4	1	0,5
PKI klasifikacija	3,00	4,00	3,00	3,00	2,00	5	5	2	1

Matrica poređenja alternativa prema kriterijumu sistematičnost:

Sistematicnost	IEEE 830	Somme-rville	Lamsw-eerde	Odeh	FOCUS-TBD	ISO/IEC 9126	FURPS	PKI MO i VS	PKI klasi fikacija
IEEE 830	1,00	0,5	0,5	3	0,20	0,5	1	0,25	0,2
Sommerville	2,00	1	1	3	0,33	1	2	0,33	0,25
Lamsweerde	2,00	1,00	1	2	0,33	0,5	2	0,33	0,25
Odeh	0,33	0,33	0,50	1	0,17	0,33	0,5	0,2	0,17
FOCUS-TBD	5,00	3,00	3,00	6,00	1	3	4	2	1
ISO/IEC 9126	2,00	1,00	2,00	3,00	0,33	1	2	0,5	0,33
FURPS	1,00	0,50	0,50	2,00	0,25	0,5	1	0,33	0,25
PKI MO i VS	4,00	3,00	3,00	5,00	0,50	2	3	1	0,5
PKI klasifikacija	5,00	4,00	4,00	6,00	1,00	3	4	2	1

Matrica poređenja alternativa prema kriterijumu jednostavnost:

Jednostavnost	IEEE 830	Somme-rville	Lamsw-eerde	Odeh	FOCUS-TBD	ISO/IEC 9126	FURPS	PKI MO i VS	PKI klasi fikacija
IEEE 830	1,00	7	2	6	2,00	3	3	1	2
Sommerville	0,14	1	0,25	0,5	0,14	0,17	0,17	0,17	0,2
Lamsweerde	0,50	4,00	1	0,33	0,5	1	1	0,5	1
Odeh	0,17	2,00	3,00	1	0,2	0,25	0,25	0,2	0,25
FOCUS-TBD	0,50	7,00	2,00	5,00	1	2	2	1	0,5
ISO/IEC 9126	0,33	6,00	1,00	4,00	0,50	1	1	0,5	1
FURPS	0,33	6,00	1,00	4,00	0,50	1	1	0,5	1
PKI MO i VS	1,00	6,00	2,00	5,00	1,00	2	2	1	2
PKI klasifikacija	0,50	5,00	1,00	4,00	2,00	1	1	0,5	1

Matrica poređenja alternativa prema kriterijumu primenjivost:

Primenjivost	IEEE 830	Somme-rville	Lamsw-eerde	Odeh	FOCUS-TBD	ISO/IEC 9126	FURPS	PKI MO i VS	PKI klasi fikacija
IEEE 830	1,00	0,33	0,25	0,5	0,25	1	1	0,33	0,25
Sommerville	3,00	1	0,5	2	0,5	3	3	1	0,5
Lamsweerde	4,00	2,00	1	3	1	3	3	2	1
Odeh	2,00	0,50	0,33	1	0,33	2	2	0,5	0,33
FOCUS-TBD	4,00	2,00	1,00	3,00	1	3	3	1	1
ISO/IEC 9126	1,00	0,33	0,33	0,50	0,33	1	1	0,5	0,33
FURPS	1,00	0,33	0,33	0,50	0,33	1	1	0,5	0,33
PKI MO i VS	3,00	1,00	0,50	2,00	1,00	2	2	1	0,5
PKI klasifikacija	4,00	2,00	1,00	3,00	1,00	3	3	2	1

Matrica poređenja alternativa prema kriterijumu univerzalnost:

Univerzalnost	IEEE 830	Somme-rville	Lamsw-eerde	Odeh	FOCUS-TBD	ISO/IEC 9126	FURPS	PKI MO i VS	PKI klasi fikacija
IEEE 830	1,00	0,33	0,33	0,33	0,25	0,25	0,5	5	0,33
Sommerville	3,00	1	1	1	0,5	0,5	3	7	1
Lamsweerde	3,00	1,00	1	1	1	0,5	2	6	1
Odeh	3,00	1,00	1,00	1	0,5	0,5	2	7	1
FOCUS-TBD	4,00	2,00	1,00	2,00	1	1	3	9	2
ISO/IEC 9126	4,00	2,00	2,00	2,00	1,00	1	3	9	2
FURPS	2,00	0,33	0,50	0,50	0,33	0,33	1	5	0,5
PKI MO i VS	0,20	0,14	0,17	0,14	0,11	0,11	0,2	1	0,14
PKI klasifikacija	3,00	1,00	1,00	1,00	0,50	0,5	2	7	1

Matrica poređenja alternativa prema kriterijumu jasnoća:

Jasnoca	IEEE 830	Somme-rville	Lamsw-eerde	Odeh	FOCUS-TBD	ISO/IEC 9126	FURPS	PKI MO i VS	PKI klasi fikacija
IEEE 830	1,00	2	0,33	3	0,25	0,25	0,2	0,2	0,14
Sommerville	0,50	1	0,17	2	0,2	0,2	0,17	0,17	0,125
Lamsweerde	3,00	6,00	1	5	0,5	0,5	0,33	0,33	0,25
Odeh	0,33	0,50	0,20	1	0,17	0,17	0,14	0,14	0,125
FOCUS-TBD	4,00	5,00	2,00	6,00	1	1	0,5	0,5	0,33
ISO/IEC 9126	4,00	5,00	2,00	6,00	1,00	1	0,5	0,5	0,33
FURPS	5,00	6,00	3,00	7,00	2,00	2	1	1	0,5
PKI MO i VS	5,00	6,00	3,00	7,00	2,00	2	1	1	0,5
PKI klasifikacija	7,00	8,00	4,00	8,00	3,00	3	2	2	1

11.6. Prilog br. 5. Analiza ispunjenosti karakteristika dobrih zahteva

	Karakteristike dobrih zahteva koje zahtev neispunjava										
Zahtevi	Kom	Kor	Izv	Isk	Ned	Pro	Dos	Raz	Jas	Nez	Neo
Eksportovati podatke o osobama iz RA aplikacije prema utvrđenoj strukturi za eksterni informacioni sistem.	x	x	x		x	x					
Provera saglasnosti primljenih podataka sa podacima na kartici koji se obavlja pomoću aplikacije Kontrola kvaliteta.	x	x			x						
Provera integriteta podataka nosioca dokumenta i davanje odobrenja za dalje procesiranje.	x	x		x	x	x					
Aplet treba da sadrži niz logičkih blokova podataka, kao što su fiksni podaci, biometrijski podaci, promenjivi podaci i kripto podaci.	x					x					
Izraditi aplikaciju za kreiranje i validaciju elektronskog potpisa i šifrovanje bilo koje vrste elektronskih dokumenata i foldera.							x			x	
Omogućiti upravljanje i izdavanje više list*ov*a opozvanih sertifikata.	x	x			x	x	x			x	
Sertifikaciono telo kreira profile sertifikata za različite entiteta.	x				x	x		x			
Omogućiti generisanje para ključeva u sistemu na zahtev za izdavanjem sertifikata.	x				x	x					
Sertifikate krajnjeg korisnika opoz*i*vati u okviru jedne transakcije.		x	x	x							
Omogućiti automatizovano publikovanje CRL na definisanu lokaciju.	x	x	x	x			x			x	
Omogućiti automatsko importovanje zahteva za generisanje elektronskog sertifikata za potrebe servisa.				x	x	x			x		

	Karakteristike dobrih zahteva koje zahtev neispunjava										
Zahtevi	Kom	Kor	Izv	Isk	Ned	Pro	Dos	Raz	Jas	Nez	Neo
Generisani elektronski sertifikat dostaviti korisniku.	x				x						
Generisati kriptografske ključeve dovoljne snage (3027 bita) za zaštitu elektronskog dokumenta.	x	x			x	x		x			
Izraditi funkciju za odobravanje korisničkog zahteva, a koja inicira izdavanje sertifikata.	x				x	x					
Mora se omogućiti funkciju pretrage i generisanje izveštaja o zahtevima korisnika, sertifikatima korisnika i životnom veku zahteva i sertifikata.	x	x	x		x			x	x		
Omogućiti upravljanje privilegovanom korisnicima preko aplikacija za upravljanje privilegijama.		x									
Kreirati aplikaciju za elektronsko popisivanje dokumenata koja uzima u obzir vremenski žig.		x	x			x					x
Aplikacija za verifikaciju elektronskog potpisa treba da proveri elektronski potpis i obavest korisnika o statusu potpisa.	x										
Obezbediti zaštićeni prenos podataka između komponenti sistema preko LSS-a.		x		x		x			x		
Kreirati aplikaciju za šifrovanje i dešifrovanje na strani korisnika.	x	x					x			x	
	14	12	5	5	11	11	4	3	3	4	1

Kom – Kompatibilan; Kor – Korektnost; Izv – Izvodljivost; Isk – Iskoristivost; Ned – Nedvosmislenost; Pro – Proverljivost; Dos – Doslednost; Raz – Razumljivost; Jas – Jasan; Nez – Nezavisan; Neo – Neophodnost.

11.7. Prilog br. 6. Pitanja za procenu ispunjenosti indikatora za ocenu kvaliteta zahteva

a) Pitanja za kompletnost:

- Da li je zahtev opisan što je moguće potpunije?
- Da li u opisivanju zahteva nedostaju neke oblasti koje se odnose na: funkcionalnost, perfomanse, interfejs, okruženje, obuku, operativnost i bezbednost?
- Da li su izričito navedene sve pretpostavke?
- Da li zahtev navodi šta je potrebno, a ne kako da se realizuje?
- Da li je zahtev potrebno dodatno doraditi ili pojasniti?
- Da li je svaki identifikovani zahtev zapravo jedan zahtev, a ne skup zahteva?

b) Pitanja pitanja za korektnost:

- Da li je zahtev tako opisan da se može implementirati tražena funkcionalnost?
- Da li zahtev ispunjava sve ili deo stvarnih potreba?
- Da li je zahtev tačna razrada zahteva višeg nivoa?
- Da li su tačne brojčane vrednosti u zahtevu?
- Da li je svaki tekstualni zahtev gramatički tačan?

c) Pitanja za izvodljiv:

- Da li se zahtev može realizovati s obzirom na postojeću hardversku ili softversku tehnologiju?
- Da li se svaki zahtev može realizovati s obzirom na budžet?
- Da li se svaki zahtev može realizovati s obzirom na raspored projekta?
- Da li se svaki zahtev može realizovati s obzirom na ograničenja osoblja (npr., dovoljno osoblja, stručnost i iskustvo)?

d) Pitanja za iskoristivost:

- Da li je zahtev neophodan za uspeh aplikacije ili komponente?
- Da li je zahtev zaista obavezan?
- Da li je zahtev zaista potreban nekima od zainteresovanih strana, korisnika ili organizacija?
- Da li zahtev ima nepotrebna ograničenja (npr. u arhitekturi, dizajnu, implementaciji, testiranju i ostalim tehnološkim odlukama)?

e) Pitanja za nedvosmislenost:

- Da li je svaki zahtev jasan i precizan?
- Da li je značenje svakog zahteva objektivno, a ne subjektivno?
- Da li je svaki zahtev koncizan (tj. bez nepotrebnih i nebitnih informacija)?
- Da li svaki zahtev ima samo jedno tumačenje koje je očigledno?
- Da li će tumačenje svakog zahteva biti isto za one koji su napisali zahtev i za druge koji će tumačiti specifikaciju zahteva?
- Da li svaki zahtev koristi konkretne izraze?

6. Pitanja za proverljiv:

- Da li se sistem nakon implementacije zahteva može testirati, demonstrirati, pregledati ili analizirati kako bi se pokazalo da je zahtev zadovoljen?
- Da li se mogu navesti kriterijumi za verifikaciju?
- Da li su zahtevi precizno navedeni kako bi se olakšala specifikacija kriterijuma i zahteva za uspešno testiranja?
- Da li je specifikacija zahteva takva da ne koristi neproverljive termine kao što su: fleksibilan, lagan, dovoljan, bezbedan, adekvatan, koristan, upotrebljiv, po potrebi, odgovarajući, laki, mali, veliki, maksimalan, minimalan?

11.8. Prilog br. 7. Ocena ispunjenosti karakteristika dobrih zahteva

		Ocena ispunjenosti karakteristike dobrih zahteva					
Zahtevi	Evaluator	Kom	Kor	Izv	Isk	Ned	Pro
Eksportovati podatke o osobama iz CA aplikacije prema utvrđenoj strukturi za eksterni informacioni sistem.	I	30	40	30	60	30	20
	II	20	20	20	40	10	20
	III	25	50	25	55	20	35
Provera saglasnosti primljenih podataka sa podacima na kartici koji se obavlja pomoću aplikacije Kontrola kvaliteta.	I	40	50	80	60	80	80
	II	20	70	60	85	90	75
	III	30	65	90	70	90	90
Provera integriteta podataka nosioca dokumenta i davanje odobrenja za dalje procesiranje.	I	10	20	80	55	80	40
	II	10	35	90	70	80	50
	III	15	50	100	30	70	55
Aplet treba da sadrži niz logičkih blokova podataka, kao što su fiksni podaci, biometrijski podaci, promenjivi podaci i kripto podaci.	I	50	100	80	80	40	40
	II	30	95	90	55	40	30
	III	40	90	90	85	30	55
Izraditi aplikaciju za kreiranje i validaciju elektronskog potpisa u PKCS7 formatu i šifrovanje sa simetričnim AES algoritmom bilo koje vrste elektronskih dokumenata i foldera.	I	90	90	75	90	100	80
	II	85	100	90	100	90	75
	III	100	100	80	100	90	90
Omogućiti upravljanje i izdavanje više list*ov*a opozvanih sertifikata.	I	70	70	60	30	30	65
	II	85	75	70	40	60	80
	III	70	60	70	35	55	70
Sertifikaciono telo kreira profile sertifikata za različite entiteta.	I	30	80	65	60	30	60
	II	60	80	50	55	45	55
	III	40	90	80	80	40	40

		Ocena ispunjenosti karakteristike dobrih zahteva					
Zahtevi	Evaluator	Kom	Kor	Izv	Isk	Ned	Pro
Omogućiti generisanje para ključeva u sistemu na zahtev za izdavanjem sertifikata.	I	60	70	80	80	80	80
	II	85	95	85	75	60	70
	III	70	90	100	90	80	70
Sertifikate krajnjeg korisnika opozivati u okviru jedne transakcije.	I	100	70	70	40	100	100
	II	95	55	70	20	90	95
	III	100	60	60	30	100	100
Omogućiti automatizovano publikovanje CRL na definisanu lokaciju.	I	85	40	30	10	70	100
	II	95	50	10	30	80	90
	III	75	30	20	50	100	100
Omogućiti automatsko importovanje zahteva za generisanje elektronskog sertifikata za potrebe servisa.	I	90	90	40	30	20	80
	II	100	100	35	20	50	95
	III	100	100	60	35	80	90
Generisani elektronski sertifikat dostaviti korisniku.	I	70	80	70	70	30	100
	II	85	95	50	90	40	100
	III	95	100	55	75	55	100
Generisati kriptografske ključeve dovoljne snage (3027 bita) za zaštitu elektronskog dokumenta.	I	80	30	30	80	50	90
	II	100	10	55	65	55	95
	III	100	50	20	90	30	95
Izraditi funkciju za odobravanje korisničkog zahteva, a koja inicira izdavanje sertifikata.	I	70	80	80	70	20	60
	II	85	60	95	70	55	80
	III	85	70	100	90	30	85
Mora se omogućiti funkciju pretrage i generisanje izveštaja o zahtevima korisnika, sertifikatima korisnika i životnom veku zahteva i sertifikata.	I	50	50	40	90	40	80
	II	75	30	60	100	75	90

		Ocena ispunjenosti karakteristike dobrih zahteva					
Zahtevi	Evaluator	Kom	Kor	Izv	Isk	Ned	Pro
	III	60	35	30	100	55	90
Omogućiti upravljanje privilegovanom korisnicima preko aplikacija za upravljanje privilegijama.	I	80	50	70	90	80	100
	II	65	30	90	90	90	90
	III	90	40	90	100	100	90
Kreirati aplikaciju za elektronsko popisivanje dokumenata koja uzima u obzir vremenski žig.	I	90	75	20	70	95	50
	II	85	90	30	65	100	70
	III	100	85	10	65	100	75
Aplikacija za verifikaciju elektronskog potpisa treba da proveri elektronski potpis i obavest korisnika o statusu potpisa.	I	90	90	80	90	90	95
	II	70	95	90	90	100	95
	III	80	95	75	100	95	100
Obezbediti zaštićeni prenos podataka između komponenti sistema preko LSS-a.	I	70	30	40	30	80	30
	II	80	35	55	20	100	40
	III	95	45	75	30	90	40
Kreirati aplikaciju za šifrovanje i dešifrovanje na strani korisnika.	I	65	90	85	70	80	70
	II	50	75	70	95	85	90
	III	70	80	65	100	90	90
Sertifikaciono telo treba da ima komponente koje mu omogućuje neprekidan rad.	I	55	60	80	90	30	50
	II	35	70	90	100	60	70
	III	40	70	90	100	20	50
Komponenta sertifikata tela omogućuje proširivanje strukture sertifikacionog tela sa novim sertifikacionim telima.	I	35	20	100	80	50	90
	II	45	25	95	85	55	95
	III	55	30	70	90	70	100
Realizaciju projekta poveriti firmi koja ima iskustva u razvoju softvera za PKI, ima reference u	I	95	80	80	90	90	100

		Ocena ispunjenosti karakteristike dobrih zahteva					
Zahtevi	Evaluator	Kom	Kor	Izv	Isk	Ned	Pro
razvoju softvera, barem jednu u razvoju softvera za PKI, kadar koji nije osuđivan i sertifikat za rad sa tajnim podacima.	II	90	95	100	95	100	95
	III	100	95	100	60	100	95
Aplikacija za potpisivanje dokumenata sa identifikacionim dokumentom treba da omogući autentikaciju korisnika i aktiviranje ključa za potpis, koristeći šestocifreni PIN kod.	I	70	70	90	85	70	60
	II	60	85	85	70	85	50
	III	70	85	85	90	85	55
Hardverski kriptografski modul treba da ispunjava standarde bezbednosti koji su trenutno aktuelni u svetu.	I	45	80	90	95	30	80
	II	30	90	80	90	45	90
	III	35	85	80	100	15	90
Hardverski kriptografski modul treba da omogući rad sa više slotova i različitim dužinama ključeva.	I	55	70	75	80	65	100
	II	25	75	80	95	90	100
	III	40	75	95	95	70	100
Primeniti Rivest–Shamir–Adleman (RSA) kriptografski algoritam dužine ključa 2048 bita i heš funkciju SHA256 bita za elektronsko potpisivanje dokumenata.	I	95	100	100	70	100	95
	II	100	100	100	95	100	90
	III	100	95	100	100	100	100
Obezbediti korisničku podršku za sve aplikacije i servise 24 sata, 7 dana u nedelji, 356 dana godišnje.	I	85	70	40	90	45	80
	II	95	65	60	100	60	90
	III	95	80	30	90	20	90
Obezbediti sigurnu komunikaciju između registracionog autoriteta i sertifikacionog tela.	I	55	85	85	80	30	50
	II	80	100	85	85	15	40
	III	70	60	70	100	40	30
Sva polja korisničkog interfejsa koja se unose moraju imati internu kontrolu unetog sadržaja.	I	40	80	85	100	50	95
	II	35	65	90	95	60	100
	III	30	90	95	95	30	100

11.9. Prilog br. 8. Funkcije članice za indikatore

Indikatori vrednosti za korektnost i izračunavanje parametara

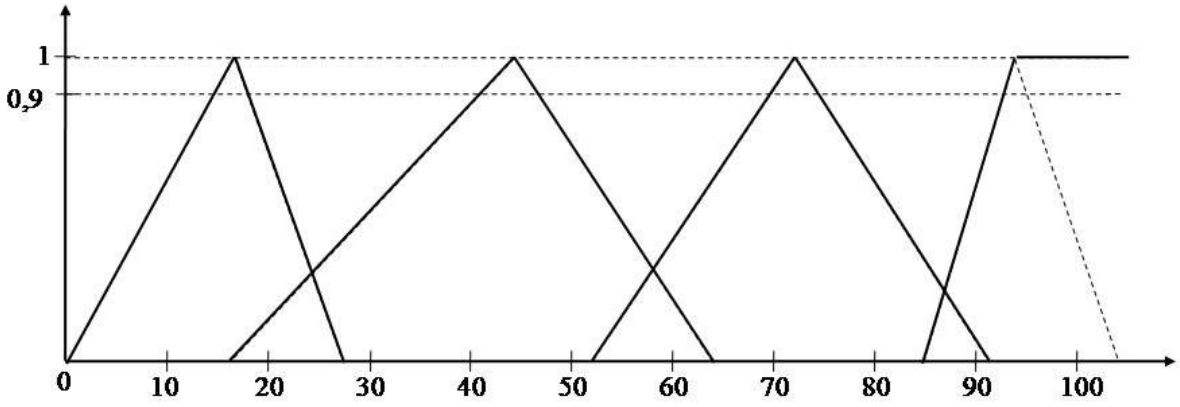
Vrednost	Normalizacija	Klasteri (y_i)	$diff_i$ (v_{i+2}-v_i)	Vrednost sličnosti (S_m)
10	0	y_1	0,111111	0
20	0,111111	y_1	0	1
20	0,111111	y_1	0	1
...				
30	0,222222	y_1	1	1
30	0,222222	y_1	0,420184	0,420184
35	0,277777	y_2	1	1
35	0,277777	y_2	1	1
...				
60	0,555555	y_2	0	1
60	0,555555	y_2	0,055555	0,420184
65	0,611111	y_3	0	1
65	0,611111	y_3	0	1
...				
85	0,833333	y_3	0	1
85	0,833333	y_3	0,055555	0,420184
90	0,888888	y_4	0	1
90	0,888888	y_4	0	1
...				
100	1	y_4	0	1
100	1	y_4	0	1

Osnovni parametri za izračunavanje funkcije članice korektnost

Standardna devijacija (σ_S)	Konstanta (C)	Centar Klastera 1 (b_1)	Centar Klastera 2 (b_2)	Centar Klastera 3 (b_3)	Centar Klastera 4 (b_4)
0,023953	4	0,1666	0,4305	0,7274	0,9423

Dobijeni rezultati za konstrukciju funkcije pripadnosti

Klasteri	a_i	b_i	c_i	d_i	v_{Li}	v_{Ri}
Klaster 1 (y_1)	0	0,1666	0,26248	0,236067	0,14544	0,17169
Klaster 2 (y_2)	0,16706	0,4305	0,64614	0,584301	0,40416	0,45206
Klaster 3 (y_3)	0,52681	0,7274	0,91007	0,870211	0,70734	0,74566
Klaster 4 (y_4)	0,85011	0,9423	1,04175	-	0,9423	0,9423



Funkcija članica za indikator kvaliteta korektnost

Indikatori vrednosti za izvodljivost i izračunavanje parametara

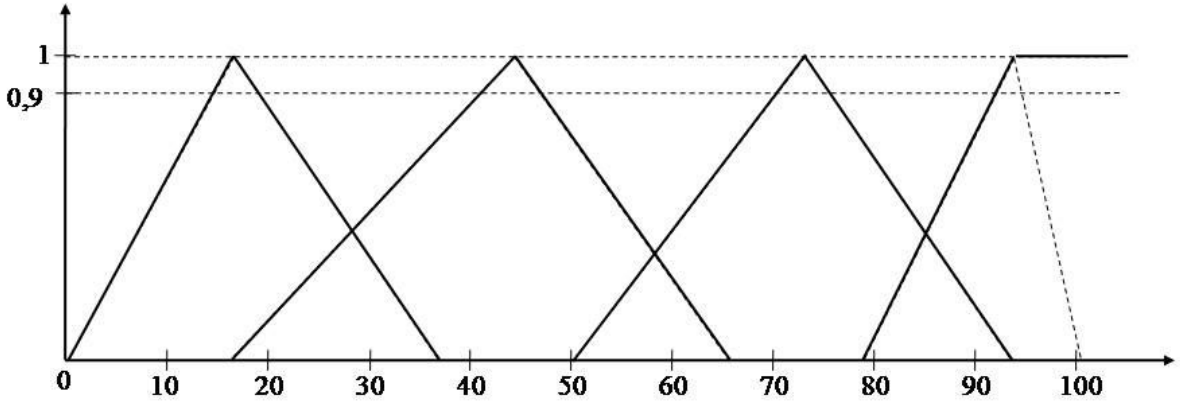
Vrednost	Normalizacija	Klasteri (y_i)	$diff_i$ (v_{i+2}-v_i)	Vrednost sličnosti (S_m)
10	0	y_1	0,111111	0
20	0,111111	y_1	0	1
20	0,111111	y_1	0	1
...				
30	0,222222	y_1	0	1
30	0,222222	y_1	0,055555	0,481215
35	0,277777	y_2	0	1
35	0,277777	y_2	0,055555	0,481215
...				
60	0,555555	y_2	0	1
60	0,555555	y_2	0,055555	0,481215
65	0,611111	y_3	0	1
65	0,611111	y_3	0	1
...				
85	0,833333	y_3	0	1
85	0,833333	y_3	0,055555	0,481215
90	0,888888	y_4	0	1
90	0,888888	y_4	0	1
...				
100	1	y_4	0	1
100	1	y_4	0	1

Osnovni parametri za izračunavanje funkcije članice izvodljivost

Standardna devijacija (σ_S)	Konstanta (C)	Centar Klastera 1 (b_1)	Centar Klastera 2 (b_2)	Centar Klastera 3 (b_3)	Centar Klastera 4 (b_4)
0,026722	4	0,1717	0,4444	0,7264	0,9401

Dobijeni rezultati za konstrukciju funkcije izvodljivost

Klasteri	a_i	b_i	c_i	d_i	v_{Li}	v_{Ri}
Klaster 1 (y_1)	0	0,1717	0,37615	0,288530	0,15453	0,19214
Klaster 2 (y_2)	0,17171	0,4444	0,65862	0,582769	0,41713	0,46582
Klaster 3 (y_3)	0,50408	0,7264	0,93243	0,851502	0,70425	0,74709
Klaster 4 (y_4)	0,79412	0,9401	1,00839	-	0,9401	0,9401



Funkcija članica za indikator kvaliteta izvodljivost

Indikatori vrednosti za iskoristivost i izračunavanje parametara

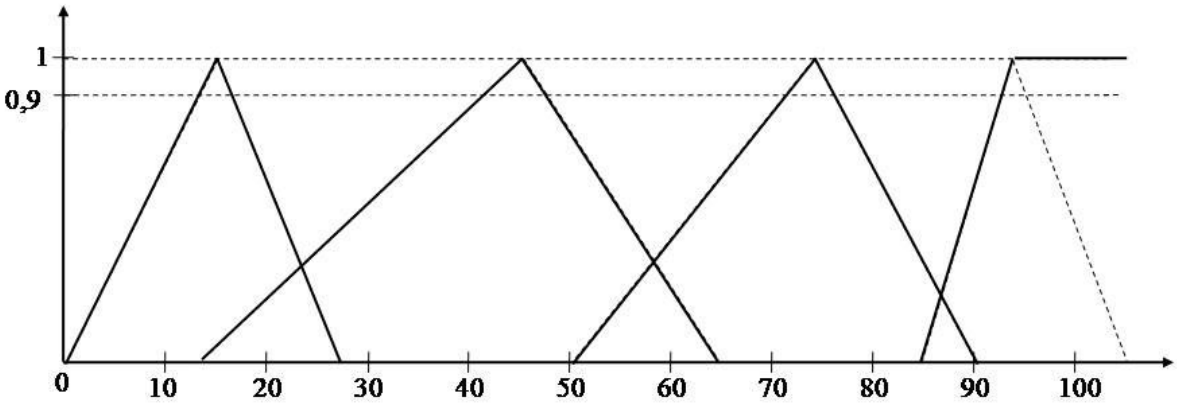
Vrednost	Normalizacija	Klasteri (y_i)	$diff_i$ (v_{i+2}-v_i)	Vrednost sličnosti (S_m)
10	0	y_1	0	1
10	0	y_1	0,111111	0
20	0,111111	y_1	0	1
...				
30	0,222222	y_1	0	1
30	0,222222	y_1	0,055555	0,452676
35	0,277777	y_2	0,055555	0,452676
40	0,333333	y_2	0	1
...				
60	0,555555	y_2	0	1
60	0,555555	y_2	0,055555	0,452676
65	0,611111	y_3	0	1
65	0,611111	y_3	0,055555	0,452676
...				
85	0,833333	y_3	0	1
85	0,833333	y_3	0,055555	0,452676
90	0,888888	y_4	0	1
90	0,888888	y_4	0	1
...				
100	1	y_4	0	1
100	1	y_4	0	1

Osnovni parametri za izračunavanje funkcije članice iskoristivost

Standardna devijacija (σ_S)	Konstanta (C)	Centar Klastera 1 (b_1)	Centar Klastera 2 (b_2)	Centar Klastera 3 (b_3)	Centar Klastera 4 (b_4)
0,025375	4	0,1495	0,4583	0,7444	0,9358

Dobijeni rezultati za konstrukciju funkcije iskoristivost

Klasteri	a_i	b_i	c_i	d_i	v_{Li}	v_{Ri}
Klaster 1 (y_1)	0	0,1495	0,28230	0,238152	0,13464	0,16287
Klaster 2 (y_2)	0,12844	0,4583	0,63596	0,578934	0,42531	0,47606
Klaster 3 (y_3)	0,50083	0,7444	0,90685	0,869650	0,72004	0,76064
Klaster 4 (y_4)	0,85001	0,9358	1,05301	-	0,9358	0,9358



Funkcija članica za indikator kvaliteta iskoristivost

Indikatori vrednosti za nedvosmislenost i izračunavanje parametara

Vrednost	Normalizacija	Klasteri (y_i)	diff$_i$ (v_{i+2}-v_i)	Vrednost sličnosti (S_m)
10	0	y_1	0,055555	0,452676
15	0,055555	y_1	0	1
25	0,055555	y_1	0,055555	0,452676
...				
30	0,222222	y_1	0	1
30	0,222222	y_1	0,111111	0
40	0,333333	y_2	0	1
40	0,333333	y_2	0	1
...				
60	0,555555	y_2	0	1
60	0,555555	y_2	0,055555	0,452676
65	0,611111	y_3	0,055555	0,452676
70	0,666666	y_3	0	1
...				
85	0,833333	y_3	0	1

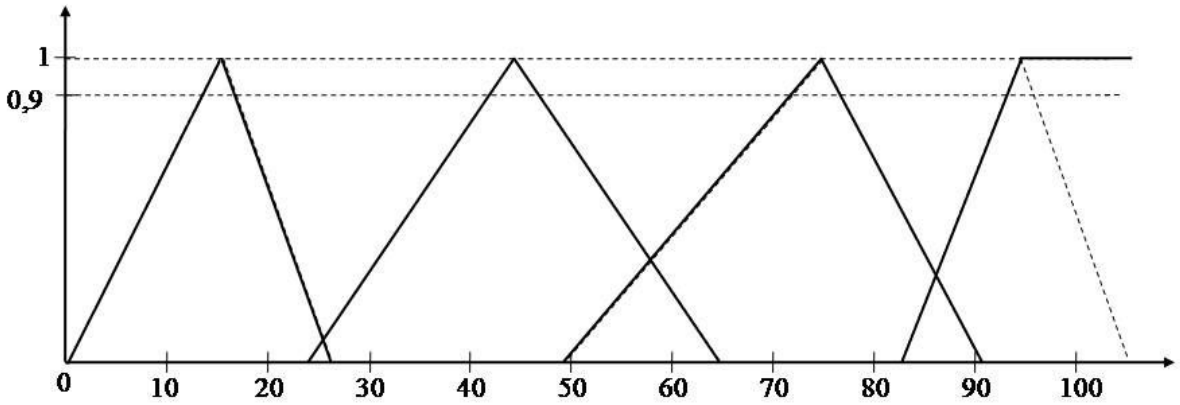
85	0,833333	y_3	0,055555	0,452676
90	0,888888	y_4	0	1
90	0,888888	y_4	0	1
...				
100	1	y_4	0	1
100	1	y_4	0	1

Osnovni parametri za izračunavanje funkcije članice nedvosmislenost

Standardna devijacija (σ_S)	Konstanta (C)	Centar Klastera 1 (b_1)	Centar Klastera 2 (b_2)	Centar Klastera 3 (b_3)	Centar Klastera 4 (b_4)
0,025375	4	0,1637	0,4467	0,7472	0,9506

Dobijeni rezultati za konstrukciju funkcije nedvosmislenost

Klasteri	a_i	b_i	c_i	d_i	v_{Li}	v_{Ri}
Klaster 1 (y_1)	0	0,1637	0,27058	0,259956	0,14733	0,17438
Klaster 2 (y_2)	0,23952	0,4467	0,64553	0,580195	0,42598	0,46658
Klaster 3 (y_3)	0,49853	0,7472	0,90455	0,865655	0,72233	0,76293
Klaster 4 (y_4)	0,83783	0,9506	1,04084	-	0,9506	0,9506



Funkcija članica za indikator kvaliteta nedvosmislenost

Indikatori vrednosti za proverljivost i izračunavanje parametara

Vrednost	Normalizacija	Klasteri (y_i)	$diff_i$ (v_{i+2}-v_i)	Vrednost sličnosti (S_m)
20	0,111111	y_1	0	1
20	0,111111	y_1	0,111111	0
30	0,222222	y_1	0	1
...				
30	0,222222	y_1	0	1
30	0,222222	y_1	0,055555	0,433268
35	0,277777	y_2	0,055555	0,433268
40	0,333333	y_2	0	1

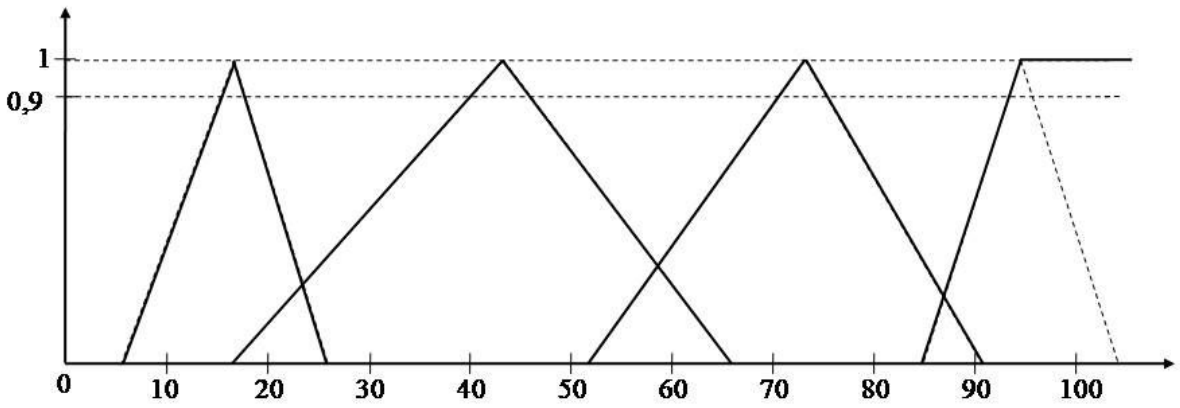
...				
60	0,555555	y_2	0	1
60	0,555555	y_2	0,055555	0,433268
65	0,611111	y_3	0,055555	0,433268
70	0,666666	y_3	0	1
...				
80	0,777777	y_3	0,055555	0,433268
85	0,833333	y_3	0,055555	0,433268
90	0,888888	y_4	0	1
90	0,888888	y_4	0	1
...				
100	1	y_4	0	1
100	1	y_4	0	1

Osnovni parametri za izračunavanje funkcije članice proverljivost

Standardna devijacija (σ_S)	Konstanta (C)	Centar Klastera 1 (b_1)	Centar Klastera 2 (b_2)	Centar Klastera 3 (b_3)	Centar Klastera 4 (b_4)
0,024506	4	0,1777	0,4305	0,7305	0,9444

Dobijeni rezultati za konstrukciju funkcije proverljivost

Klasteri	a_i	b_i	c_i	d_i	v_{Li}	v_{Ri}
Klaster 1 (y_1)	0,06014	0,1777	0,25620	0,237617	0,16603	0,18564
Klaster 2 (y_2)	0,17777	0,4305	0,65111	0,583907	0,40522	0,45256
Klaster 3 (y_3)	0,51979	0,7305	0,90455	0,869225	0,70942	0,74864
Klaster 4 (y_4)	0,84641	0,9444	1,04247	-	0,9444	0,9444



Funkcija članica za indikator kvaliteta proverljivost

Biografija autora

Biografija autora

Lični podaci

Datum rođenja: 17.06.1971. godine

Mesto rođenja: Apatin, Apatin, Republika Srbija

Mesto prebivališta: Beograd (Novi Beograd)

e-mail: radomir.prodanovic@vs.rs

Obrazovanje

- Radomir Prodanović je osnovnu školu završio u Srbu, Republika Hrvatska, a gimnaziju usmerenja matematičko-fizičko-računarskog u Bihaću, odličnim uspehom.
- Vojnotehničku akademiju Kopnene vojske, smer informatike završio je 1995. godine u Beogradu sa ocenom 7,91 u redovnom roku. Diplomirao je na projektovanju informacionih sistema ocenom 10,00.
- Postdiplomske magistarske studije, smer Elektronsko poslovanje završio je 2008. godine na Fakultetu organizacionih nauka, Univerzitet u Beogradu. Magistrirao je sa temom „Zaštita elektronskih dokumenata u elektronskom poslovanju“ sa ocenom 10,00.
- Doktorske studije upisao je na Elektronskom fakultetu, Univerzitet Niš, 2016/17, studijski program elektrotehnika i računarstvo (modul računarska tehnika).

Radno angažovanje

- Radio je na programerskim i organizacionim poslovima, projektovanju i implementaciji aplikacija za potrebe službe;
- na uvođenju višenamenskih softverskih paketa u operativnu upotrebu;
- na razvoju i implementaciji računarske mreže komandovanja Komande RV i PVO;
- vodio je projekat uvođenja digitalno potpisane razmene elektronskih dokumenata;
- učestvovao je u projektu uvođenja Sertifikacionog tela MO i VS i sistema za personalizaciju u operativnu upotrebu;
- angažovan je u radu radnih grupa iz oblasti elektronskog poslovanja i informacione bezbednosti;
- aktivno je učestvovao u izradi pravne regulative iz oblasti elektronske identifikacije, elektronskog dokumenta i usluga od poverenja u elektronskom poslovanju Republike Srbije.

Pored redovnih poslova učesnik je naučno – stručnih skupova i konferencija i bavi se naučno – istraživačkim radom iz oblasti informacione bezbednosti, inženjeringa zahteva, bežičnih senzorskih mreža, infrastrukture javnih ključeva.

Porodica

Oženjen Marinom i ima ćerku Lanu.

Izjave autora

IZJAVA O AUTORSTVU

Izjavljujem da je doktorska disertacija, pod naslovom

UNAPREĐENJE PROCESA DEFINISANJA ZAHTEVA ZA INFRASTRUKTURU JAVNIH KLJUČEVA

koja je odbranjena na Elektronskom fakultetu Univerziteta u Nišu:

- rezultat sopstvenog istraživačkog rada;
- da ovu disertaciju, ni u celini, niti u delovima, nisam prijavljivao na drugim fakultetima, niti univerzitetima;
- da nisam povredio autorska prava, niti zloupotrebio intelektualnu svojinu drugih lica.

Dozvoljavam da se objave moji lični podaci, koji su u vezi sa autorstvom i dobijanjem akademskog zvanja doktora nauka, kao što su ime i prezime, godina i mesto rođenja i datum odbrane rada, i to u katalogu Biblioteke, Digitalnom repozitorijumu Univerziteta u Nišu, kao i u publikacijama Univerziteta u Nišu.

U Nišu, 21.12.2022.g

Potpis autora disertacije:

(Radomir I. Prodanović)

IZJAVA O ISTOVETNOSTI ELEKTRONSKOG I ŠTAMPANOG OBLIKA DOKTORSKE DISERTACIJE

Naslov disertacije: **UNAPREĐENJE PROCESA DEFINISANJA ZAHTEVA ZA INFRASTRUKTURU JAVNIH KLJUČEVA**

Izjavljujem da je elektronski oblik moje doktorske disertacije, koju sam predao za unošenje u **Digitalni repozitorijum Univerziteta u Nišu,** istovetan štampanom obliku.

U Nišu, 21.12.2022.g

Potpis autora disertacije:

(Radomir I. Prodanović)

IZJAVA O KORIŠĆENJU

Ovlašćujem Univerzitetsku biblioteku „Nikola Tesla“ da u Digitalni repozitorijum Univerziteta u Nišu unese moju doktorsku disertaciju, pod naslovom:

UNAPREĐENJE PROCESA DEFINISANJA ZAHTEVA ZA INFRASTRUKTURU JAVNIH KLJUČEVA

Disertaciju sa svim prilozima predao sam u elektronskom obliku, pogodnom za trajno arhiviranje.

Moju doktorsku disertaciju, unetu u Digitalni repozitorijum Univerziteta u Nišu, mogu koristiti svi koji poštuju odredbe sadržane u odabranom tipu licence Kreativne zajednice (Creative Commons), za koju sam se odlučio.

1. Autorstvo **(CC BY)**
2. Autorstvo – nekomercijalno **(CC BY-NC)**
3. Autorstvo – nekomercijalno – bez prerade **(CC BY-NC-ND)**
4. Autorstvo – nekomercijalno – deliti pod istim uslovima **(CC BY-NC-SA)**
5. Autorstvo – bez prerade **(CC BY-ND)**
6. Autorstvo – deliti pod istim uslovima **(CC BY-SA)**

U Nišu, 22.12.2022.g

Potpis autora disertacije:

(Radomir I. Prodanović)