Projekt e-Građani

Nacionalni identifikacijski i autentifikacijski sustav (NIAS)

Kriteriji za određivanje razine osiguranja kvalitete autentifikacije

Verzija 1.2

Sadržaj

Povijest promjena

Verzija	Datum	Opis	Autori
0.1.	24.04.2013	Nacrt - inicijalna verzija	Fina
0.2.	15.05.2013	Izmjene: Poglavlje 3.2.2. točka 5. Dopuna: Poglavlje 3.1.4. Dopuna: Poglavlje 3.2.3 Dopuna: Poglavlje 4. Dopuna: Poglavlje 5.	Fina
0.2.1	22.05.2013	Priprema za inicijalni sastanak s dionicima	MUeH
1.0	11.07.2013	Usuglašena verzija	Fina
1.0.1	29.08.2013	Dopuna: Poglavlje 4	Fina
1.1	06.09.2013	Službeno objavljeno uz Program razvoja elektroničkih usluga	MUeH
1.1.1	06.12.2013	Dopune u poglavljima 1. Uvod i poglavlju 5. Način provođenja procjene razine sigurnosti (STORK smjernice)	Fina
1.2	06.12.2013	Prihvaćene dopune, te ispravljen sadržaj tablice 8. Rezime za ocjenu faze el. autentifikacije (A) – za RC umjesto ID1,… ID4 treba stajati RC1,… RC4	MUeH

1. Uvod

U ovom dokumentu su definirani kriteriji za određivanje razine osiguranja kvalitete autentifikacije korisnika u okviru Nacionalnog identifikacijskog i autentifikacijskog sustava (NIAS), kao središnjoj komponenti projekta e-Građani, za potrebe sigurnog pristupa elektroničkim javnim uslugama u umreženoj upravi.

Ovi kriteriji predstavljaju temeljnu odrednicu koja utječe na donošenje ocjene o razini sigurnosti pojedine vjerodajnice radi njenog uključivanja u sustav NIAS.

Definirani kriteriji su podloga i informacija svim izdavateljima vjerodajnica prilikom ocjene i rangiranja vlastitih vjerodajnica. Jednako tako, podloga su i informacija pružateljima usluga za odabir odgovarajuće razine sigurnosti vjerodajnice kojom se može pristupati njihovoj elektroničkoj usluzi, odnosno, podloga je za ocjenu stupnja rizika prihvatljivog za elektroničku uslugu.

Osnovni zadatak NIAS-a je sigurna i pouzdana autentifikacija korisnika koji putem odgovarajuće vjerodajnice pristupaju javnim elektroničkim uslugama. Rad sustava se temelji na upravljanju atributima elektroničkih identiteta (eID/e-identitetima). Pri tome se razmjenjuju samo nužni atributi koji su elektroničkoj usluzi dovoljni za jednoznačnu identifikaciju korisnika. Jedinstveni identifikator za uspostavu eID korisnika u Republici Hrvatskoj je OIB. NIAS svim vlasnicima vjerodajnica omogućuje sigurno korištenje elektroničkih usluga koje su spojene s NIAS-om. Istovremeno, pružatelje elektroničkih usluga oslobađa od poslova izdavanja vjerodajnica i upravljanja identitetima korisnika.

NIAS je koncipiran na načelima EU projekta STORK (**S**ecure iden**T**ity acr**O**ss bo**R**ders lin**K**ed) kako bi se, uvažavanjem već postojećih praksi i prihvaćenih standarda, u trenutku elektroničkog povezivanja sa članicama EU taj proces izveo na što jednostavniji način. Jedna od preporuka STORK-a je model i način određivanja razine sigurnosti vjerodajnice koja se koristi u svrhu dokazivanja elektroničkog identiteta.

Sadržaj ovog dokumenta je usklađen s važećim pravnim aktima Republike Hrvatske i EU.

2. Opis razina osiguranja kvalitete autentifikacije

Ovaj model ima za cilj omogućiti građanima i tvrtkama svih članica EU, pristup na elektroničke javne usluge uz predočenje svoje nacionalne vjerodajnice (izdane od ili u ime državnih tijela zemlje članice) bez obzira u kojoj zemlji članici se fizički nalaze. Model definira četiri razine osiguranja kvalitete autentifikacije koje su prikazane u Tablici 1.

Tablica 1: ***Razine osiguranja kvalitete autentifikacije***

RAZINA OSIGURANJA KVALITETE AUTENTIFIKACIJE	OPIS
1	Nikakva ili najmanja sigurnost
2	Niska sigurnost
3	Znatna sigurnost
4	Visoka sigurnost

Ove razine slične su onima u IDABC izvještaju o autentifikacijskim razinama i prilično su sukladne dokumentu Okvir za osiguranje slobode i identiteta.

Četiri razine dovoljne su za različite poslovne potrebe upravljanja rizicima te ne predstavljaju preveliki zahtjev za upravljanje sustavom. Ove razine u skladu su i s mogućom štetom koja može nastati u slučaju lažnog predstavljanja.

Razina 1 je najniža razina osiguranja, koja jamči najnižu razinu sigurnosti ili ne jamči nikakvu sigurnost. Vjerodajnice se prihvaćaju bez bilo kakve provjere. Ako se koristi adresa elektroničke pošte, jedina provjera je ispravnost adrese. Ova razina je odgovarajuća kad su posljedice od lažnog predstavljanja vrlo male ili nikakve. Prikladna je za usluge koje primjenjuju najmanji skup zaštitnih mjera ili ih ne primjenjuju.

Razina 2 određuje razinu korištenu u uslugama kod kojih su štetne posljedice od lažnog predstavljanja male. Provjeru i potvrđivanje identiteta te izdavanje vjerodajnice mora obavljati tijelo koje ima odgovarajući ugovor s mjerodavnim državnim tijelom. Na ovoj razini se u postupku provjere i potvrđivanje identiteta ne zahtijeva fizička prisutnost podnositelja zahtjeva za izdavanje vjerodajnice. Vjerodajnica se mora dostaviti točno podnositelju zahtjeva i sa zajamčenom sigurnošću. Prilikom korištenja vjerodajnice u autentifikaciji moraju se primijeniti dovoljno robusni protokoli autentifikacije.

Razina 3 određuje razinu korištenu u uslugama kod kojih su štetne posljedice od lažnog predstavljanja znatne. Provjera i potvrđivanje identiteta obavlja se metodama koje nedvosmisleno i s visokom sigurnošću identificiraju podnositelja zahtjeva za izdavanje vjerodajnice. Izdavatelje vjerodajnica nadzire, odnosno akreditira mjerodavno državno tijelo. Vjerodajnice ove razine su certifikati čiji se ključevi čuvaju u sigurnom softverskom

spremniku (u daljnjem tekstu: soft certifikat), a mogu biti i certifikati čiji se ključevi čuvaju u sigurnom hardverskom spremniku (u daljnjem tekstu: hard certifikati). Postupci korištenja vjerodajnice prilikom udaljene autentifikacije su robusni.

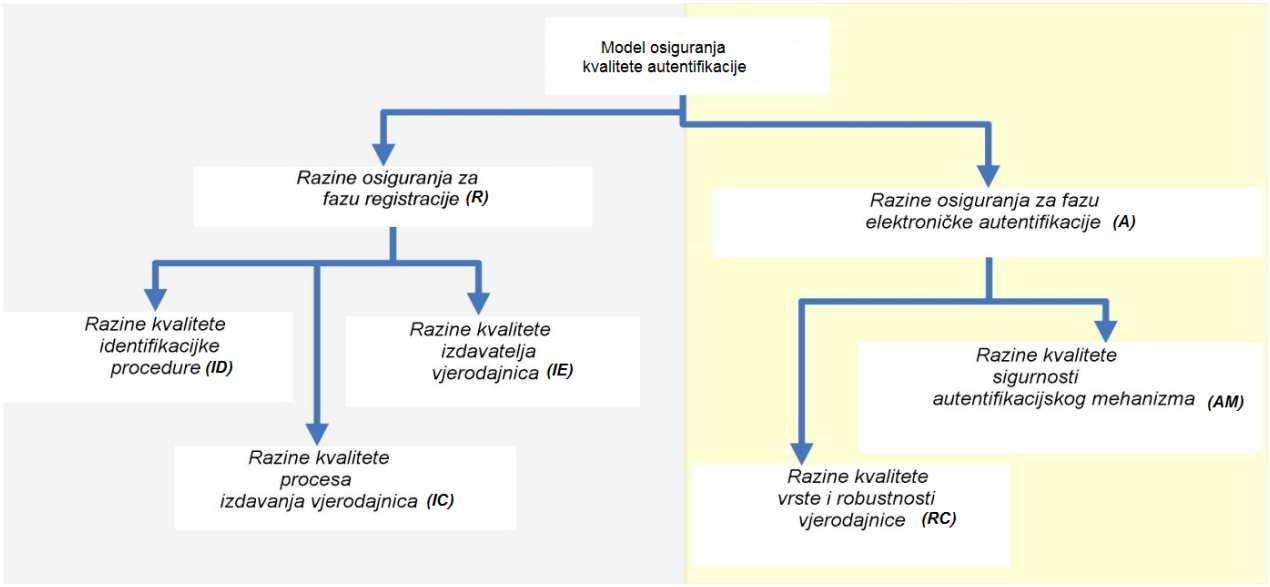
Razina 4 je najviša razina osiguranja koju koriste usluge kod kojih bi lažno predstavljanje imalo visoke štetne posljedice. Postupak registracije zahtjeva barem jednu provjeru i potvrđivanje identiteta uz fizičku prisutnost podnositelja zahtjeva (npr. prilikom podnošenja zahtjeva za izdavanje vjerodajnice ili prilikom njenog preuzimanja). Alternativno, u slučaju on-line zahtjeva, identitet podnositelja zahtjeva se može ustanoviti korištenjem kvalificiranog e-potpisa, a u skladu s odredbama Zakona o elektroničkom potpisu RH. Certifikati su kvalificirani hard certifikati u skladu s direktivom 1999/93/EC. Postupci korištenja vjerodajnice prilikom udaljene autentifikacije su najrobusniji.

3. Zahtjevi razina osiguranja kvalitete autentifikacije

Svaku razinu osiguranja kvalitete autentifikacije određuje skup zahtjeva na bitne čimbenike procesa autentifikacije. Svaki zahtjev definira funkcionalna i tehnička svojstva koja moraju biti zadovoljena unutar određene razine.

Organizacijski čimbenici koji se odnose na fazu registracije nalaze se na lijevoj strani Slike 1., a tehnički čimbenici koji se odnose na fazu elektroničke autentifikacije nalaze se na desnoj strani Slike 1.

Zahtjevi na čimbenike elektroničkog identiteta su organizirani hijerarhijski. Zahtjevi razina osiguranja kvalitete autentifikacije sastoje se od zahtjeva za fazu registracije (off-line ili on-line) i zahtjeva za on-line fazu elektroničke autentifikacije. Zahtjevi svake od ove dvije faze su kombinacija zahtjeva više čimbenika bitnih za određenu fazu.



Slika 1: ***Čimbenici koji utječu na razinu osiguranja kvalitete autentifikacije***

Svaka razina osiguranja kvalitete autentifikacije predstavljena je skupom organizacijskih (ID, IC i IE) i tehničkih (RC i AM) čimbenika te njihovih pojedinačnih razina kvalitete. *Najniža razina jednog od čimbenika određuje konačnu razinu osiguranja kvalitete autentifikacije.*

Ovaj model i pristup primjenjuje se za sve registracijske i autentifikacijske procese pojedine vjerodajnice. Rezultat primjene ovog modela je konačna ocjena razine osiguranja kvalitete autentifikacije vjerodajnice.

3.1 Faza registracije (R)

3.1.1 Kvaliteta procedure identifikacije (ID)

Prije izdavanje vjerodajnice, podnositelj zahtjeva za izdavanje vjerodajnice se mora identificirati. Razina kvalitete ovog procesa ovisi o tri čimbenika.

1. ***FIZIČKA PRISUTNOST PODNOSITELJA ZAHTJEVA TIJEKOM IDENTIFIKACIJE***

   a. Identifikacija podnositelja zahtjeva ne iziskuje fizičku prisutnost uopće.

   b. Identifikacija podnositelja zahtjeva iziskuje fizičku prisutnost tijekom registracije. Takav postupak se mora izvesti najmanje jednom (ne mora biti uvjet prilikom obnavljanja vjerodajnice).

   c. Identifikacija podnositelja zahtjeva iziskuje fizičku prisutnost kada mu se isporučuje certifikat (npr. podnositelj se može registrirati on-line, ali mora osobno doći prilikom preuzimanja certifikata). Osobni dolazak se mora dogoditi najmanje jednom (ne mora biti uvjet prilikom obnavljanja vjerodajnice).

2. ***KVALITETA PODATAKA O IDENTITETU PODNOSITELJA***

   a. Dostavljanje jednog relevantnog podatka o podnositelju kojeg ne zna nužno samo podnositelj zahtjeva (npr. ime i prezime, datum rođenja). Proces ne mora nužno rezultirati jedinstvenom identifikacijom.

   b. Dostavljanje više relevantnih podataka o podnositelju koje ne zna nužno samo podnositelj (npr. ime i prezime, datum rođenja, adresa). Proces mora rezultirati jedinstvenom identifikacijom.

   c. Dostavljanje podataka koje sadrži barem jedan jedinstveni podatak za kojeg se pretpostavlja da ga zna samo podnositelj (npr. OIB, ili neki drugi osobni identifikator, broj putovnice) i koji može biti provjeren u nekom od službenih registara. Ovaj proces uvijek rezultira jedinstvenom identifikacijom.

3. ***PROVJERA PODATAKA O IDENTITETU KOJE JE DOSTAVIO PODNOSITELJ***

   a. Provjera je ograničena na verifikaciju e-mail adrese, ukoliko je ovaj podatak dostavljen. U suprotnom, druga vrsta provjere ne postoji.

   b. Provjera dokaza se izvodi višestrukim provjerama dostavljenih podataka o identitetu korištenjem registara službenih izdavatelja identiteta ili registara neutralnih i pouzdanih izvora (npr. banke, osiguratelji ili državna tijela).

   c. Provjera traži uporabu nekvalificiranog digitalnog potpisa pri dostavljanju podataka.

   d. Provjera traži fizički uvid u službene dokumente (npr. osobna iskaznica, putovnica, vozačka dozvola s fotografijom i/ili potpisom).

e. Provjera traži uporabu kvalificiranog elektroničkog potpisa pri dostavljanju podataka, koji je verificiran od strane Certificiranog Pružatelja Usluge (CSP – *Certificate Service Provider*) prije izdavanja tokena/vjerodajnice.

Tablica 2: ***Ocjena razine kvalitete procesa identifikacije (ID)***

TRAŽI SE ZA OCJENU RAZINE KVALITETE PROCESA IDENTIFIKACIJE (ID)	Rezultat
Fizička prisutnost: ne traži se (tip 1.a). On- line registracija	**ID1**
Kvaliteta podataka: najmanje tipa 2.a	
Provjera podataka: najmanje tipa 3.a	
Fizičko prisutnost: ne traži se (tip 1.a)	**ID2**
Kvaliteta podataka: najmanje tip 2.b	
Provjera podataka: tip 3.b	
Fizička prisutnost: traži se, najmanje tip 1.b	**ID3**
Kvaliteta podataka: najmanje tip 2.b	
Provjera podataka: najmanje tip 3.c	
Fizička prisutnost: ne traži se (npr. tip 1.a). Registracija je on-line.	**ID3**
Kvaliteta podataka: tip 2.c	
Provjera podataka: najmanje tip 3.d	
Fizička prisutnost: traži se npr. najmanje tip 1.b	**ID4**
Kvaliteta podataka: tip 2.c	
Provjera podataka: najmanje tipa 3.d	

3.1.2 Kvaliteta procesa izdavanja vjerodajnice (IC)

Drugi čimbenik u fazi registracije odnosi se na proces u kojem se izdaje token ili vjerodajnica. Kvaliteta izdavanja tokena ili vjerodajnice ovisi o kanalu isporuke (npr. e-mail ili poštom) i o tome je li token isporučen kao cjelina (odjednom) ili u dijelovima koji se kombiniraju naknadno.

Što je viša razina kvalitete izdavanja vjerodajnice, to je čvršća veza između izdane vjerodajnice i stvarnog identiteta podnositelja. Najviša razina prilikom izdavanja vjerodajnice dostiže se fizičkom prisutnošću podnositelja u trenutku izdavanja. Važno je istaknuti da podnositelj mora pri tome proći i najvišu razinu u procesu identifikacije. To zahtijeva da se identitet podnositelja provjeri putem službenog identifikacijskog dokumenta ili na lokaciji izdavanja ili prilikom isporuke na definiranoj adresi.

Minimalni uvjeti za svaku razinu su navedeni u Tablici 3.

Tablica 3: ***Ocjena razina kvalitete izdavanja vjerodajnice (IC)***

TRAŽI SE ZA OCJENU RAZINE KVALITETE IZDAVANJA VJERODAJNICE (IC)	Rezultat
Vjerodajnica se dobije bez ikakve forme provjere (verifikacije).	**IC1**
Vjerodajnica se dobije putem jednostavnije (*light-weight*) kvalitete verifikacije identiteta podnositelja vjerodajnice (npr. ime i/ili adresa). Primjeri: • Korisničko ime i lozinka se izdaju putem dva odvojena kanala, od kojih je jedan obavezno pošta (ne e-mail) poslana na adresu podnositelja navedenu u službenom registru. • Vjerodajnicu podnositelj osobno preuzima po registraciji. Preuzimanje se odvija korištenjem linka poslanog na e-mail adresu koju je dostavio podnositelj prilikom registracije. U tom slučaju, dostupnost linka mora biti vremenski ograničena (npr. 24 sata nakon registracije).	**IC2**
Vjerodajnica se dobije putem srednje razine kvalitete verifikacije identiteta podnositelja vjerodajnice (npr. ime i/ili adresa). Primjeri: • Vjerodajnica se šalje preporučenom pošiljkom na fizičku adresu podnositelja iz nekog od službenih registara. • Vjerodajnica se preuzima putem interneta nakon što je zahtjev za dokazivanjem identiteta potpisan kvalificiranim potpisom (prema uvjetima Zakona o elektroničkom potpisu) i verificiran od strane CSP-a. Odmah nakon verifikacije, CSP generira vjerodajnicu i učitava ju u podnositeljev preglednik. • Vjerodajnicu osobno preuzima podnositelj nakon što je unio tajni kod koji mu je fizički uručen u procesu registracije izvedenom sukladno najmanje razini 3 za proces registracije.	**IC3**
Vjerodajnica se dobije putem čvrste provjere podnositeljevog identiteta.	**IC4**

Primjeri: • Vjerodajnica se osobno uručuje podnositelju nakon provjere identiteta. • Vjerodajnica se šalje podnositelju i aktivira nakon provjere njegovog identiteta (npr. putem fizičke registracije.)	

3.1.3 Kvaliteta izdavatelja vjerodajnice (IE)

Izdavatelj koji izdaje uobičajene (tradicionalne) identifikacijske dokumente (npr. putovnice, osobne iskaznice) obično su državna tijela, dok izdavatelji elektroničkih autentifikacijskih sredstava mogu biti i državna tijela i treća strana. Ulogu certifikacijskog tijela (CA – *Certification Authority*) i izdavatelja identiteta ima obično isti izdavatelj kojeg nazivamo davatelj usluge certificiranja (CSP – *Certification Service Provider*). Samo kvalificirani izdavatelji mogu ponuditi najveću razinu sigurnosti.

Nekvalificirane izdavatelje dijelimo na one koji ne primjenjuju mehanizme koji su odobreni, nadzirani ili akreditirani od strane države i one koji ih primjenjuju, ali ne traže njihov nadzor, odobrenje ili akreditaciju od države (npr. banke).

Kvalificirana tijela ispunjavanju uvjete iz Aneksa II EU Direktive 1999/93/EC (5), dopušteno im je izdavanje kvalificiranih certifikata (Aneks I ista direktiva, poglavlje II – D2.2(2)). Drugi važan dokument je *Policy requirements for CA issuing public key certificates* (ETSI TS 102 042). Taj dokument je važan za svaku PKI instalaciju u Europi i obuhvaća sve aspekte procesa registracije usklađenu s razinama kvalitete sigurnosti navedenim u ovom modelu.

Treba imati u vidu da neki od spomenutih zahtjeva u navedenim direktivama opisuju obveze koje moraju biti ispunjene kad, npr. CSP verificira identitet podnositelja ili kad generira identifikacijski token. Dolazi do preklapanja između zahtjeva za CSP kod certificiranja (prema zahtjevima Direktive) i zahtjeva iz ovog modelu. Npr. u obvezi (d) u Aneksu II Direktive 1999/93/EC stoji da „CA mora verificirati, na odgovarajući način, sukladno nacionalnom zakonu, identitet i ako je to primjenjivo, bilo koje specifično obilježje osobe kojoj se certifikat izdaje“. Ta obveza se preklapa sa zahtjevom u procesu registracije (ID) po ovom modelu. Stoga se oba zahtjeva odnose na najvišu razinu sigurnosti. U suprotnome, ukoliko je proces registracije pri četvrtoj razini obavljen od nekvalificiranog izdavatelja, nije moguće doseći najvišu (četvrtu) razinu prema ovom modelu jer takav izdavatelj pripada razini sigurnosti tri.

Drugi čimbenik, kojeg treba uzeti u obzir, je postojanje ili odsutnost strategije da se poštuju načela čuvanja zapisa iz procedure registracije. Zapisi i dokumenti prikupljeni u procesu registracije omogućavaju, na primjer, da se provede istraga u slučaju zlouporabe. Poštivanje načela čuvanja takvih zapisa i dokumenata jedan je od zahtjeva sadržanih u EU Direktive 1999/93/EC. U stavci I Aneksa II stoji da „bilježenje svih relevantnih informacija koje se tiču kvalificiranog certifikata na određeno razdoblje, naročito u svrhu pružanja dokaza o certificiranju za potrebe legalnog procesuiranja. Takvo bilježenje i čuvanje može biti i elektroničko“. Izdavatelji vjerodajnica koji djeluju u skladu s Direktivom stoga i zadovoljavaju uvjete čuvanja dokaza pa time i ostvaruju najvišu razinu sigurnosti. Mora se, ipak, odrediti značenje „određenog razdoblja“. Značenje može biti određeno na nivou primjene ili države. U Hrvatskoj, period čuvanja dokaza je minimalno 10 godina, za kvalificirane certifikate, po Zakonu o elektroničkom potpisu i pripadajućim aktima.

Izdavatelji koji imaju mehanizme čuvanja dokaza, ali ne djeluju u skladu s Direktivom ne mogu osigurati razinu sigurnosti veću od razine 3.

Tablica 4: ***Ocjena razine kvalitete izdavatelja vjerodajnice (IE)***

TRAŽI SE ZA OCJENU RAZINE KVALITETE IZDAVATELJA VJERODAJNICE (IE)	Rezultat
Nema sporazuma sa državom/državnim tijelom.	**IE1**
Sporazum sa državom/državnim tijelom postoji.	**IE2**
Nadzor od strane države/državnog tijela postoji.	**IE3**
Kvalificiran izdavatelj prema Aneksu II Direktive 1999/93/EC.	**IE4**

3.1.4 Rezime ocjene za fazu registracije (R)

Rezime ocjene za fazu registracije se donosi na temelju dobivenih ocjena svakog od čimbenika u fazi registracije, prema matrici prikazanoj u Tablici 5.

Tablica 5: ***Rezime za ocjenu faze registracije (R)***

	R1	R2	R3	R4
ID	ID1	ID2	ID3	ID4
IC	IC1	IC2	IC3	IC4
IE	IE1	IE2	IE3	IE4

3.2 Faza elektroničke autentifikacije (A)

U ovoj fazi, provjerava se valjanost i autentičnost vjerodajnice kojom se predstavlja korisnik (npr. korisničko ime/lozinka, certifikat, itd.). Kvaliteta ove faze ovisi o čimbenicima kao što su vrsta i robusnost vjerodajnice, protokol za udaljenu autentifikaciju i mehanizam korištenih za obavještavanje korisnika o uspješnosti udaljene autentifikacije.

3.2.1 Vrsta i robusnost vjerodajnice (RC)

Ovaj čimbenik omogućava dokazivanje posjedovanja vjerodajnice. U toj segmentu se razlikuju sljedeće navedene vrste.

Korisničko ime/lozinka ili PIN – Niz znakova za koje se očekuje da ih vlasnik upamti i čuva u tajnosti. Njega koriste e-usluge koje dozvoljavaju pristup uz nižu razinu sigurnosti. Korisničko ime je najčešće javno i može biti odabrano od strane korisnika ili dodijeljeno od strane izdavatelja. Kako je korisničko ime javno, ne utječe na razinu sigurnosti autentifikacije. Lozinka ili PIN moraju biti tajni i kao takvi utječu na razinu sigurnosti autentifikacije, ovisno o tome jesu li korisniku dodijeljeni automatski ili su odabrani od strane korisnika.

Lista lozinki – Osobni soft token (lista na papiru) koju vlasnik posjeduje. Lista sadržava PIN kodove često u kombinaciji sa statičkom lozinkom ili PIN-om unutar autentifikacijskog sustava.

Uređaj za generiranje jednokratnih lozinki (*one time password* – OTP) – Osobni uređaj koji generira jednokratne lozinke koje vrijede samo za jednu autentifikacijsku sjednicu. U određenim slučajevima, OTP se generira kao vremenski žig korištenjem kriptografskog algoritma koji kombinira trenutno vrijeme i tajni kod pohranjen u uređaju. U drugim slučajevima, dodijeljeni čitač kombinira simetrični ključ pohranjen na osobnom uređaju (npr. kartici) s jedinstvenim podatkom za taj trenutak („*nonce*“ podatak. “*Nonce*“ podatak može biti trenutno vrijeme, na čitaču generirani broj ili ako uređaj omogućava unos, upit generiran od strane validatora koji zahtjeva odgovor. Generirani OTP je obično prikazan na zaslonu uređaja te udaljeno dostavljen servisu (ručnim upisom, automatskim slanjem na servis, slanjem putem SMS-a, itd.).

Soft certifikat – Kriptografski ključ koji je obično pohranjen na disk, USB *stick* ili neki drugi uređaj. Autentifikacija se obavlja omogućavanjem posjedovanja i kontrolom ključa. Obično je kriptiran ključem koji se kreira iz lozinke koju zna samo korisnik. Stoga je nužno da vlasnik zna lozinku za aktivaciju certifikata.

Kvalificirani soft certifikat – Njegove tehničke odlike su obuhvaćene u Aneksu I EU Direktive 1999/93/EC. Njegova robusnost je više odlika načina njegovog izdavanja i pravnog učinka. Pod ovu definiciju uključujemo i certifikate koje izdaju državna tijela, a koji su izdani po identičnom procesu kao kod izdavanja kvalificiranog certifikata (npr. normalizirani certifikat izdan po procesu za kvalificirane certifikate).

Hard certifikat – Pametna kartica ili sličan uređaj na koji je pohranjen kriptografski ključ. Autentifikacija se izvodi dokazivanjem da vlasnik posjeduje uređaj i da je na uređaju pohranjeni ključ pod njegovom kontrolom.

Kvalificirani hard certifikat ili njegov ekvivalent – Njegove tehničke odlike su sadržane u Aneksu I EU Direktive 1999/93/EC. Uključuje i hard certifikate koje državno tijelo pojedine države izdaje pod istim uvjetima i istim procesima kao što se izdaje i kvalificirani certifikat.

Poseban vid kvalitete bitan za vjerodajnice je njihova zastarjelost, odnosno koliko često izdavatelj obnavlja listu opozvanih certifikata. Izdavatelji bi trebali objaviti učestalost objavljivanja liste opozvanih certifikata u svojim općim pravilima. Kvaliteta zastarjelosti vjerodajnica je vezana uz kvalitetu izdavatelja i stoga je obuhvaćena i Aneksom 2 EU Direktive 1999/93/EC.

Tablica 6: ***Ocjena razine kvalitete vrste i robusnosti vjerodajnice (RC)***

TRAŽI SE ZA OCJENU RAZINE KVALITETE VRSTE I ROBUSNOSTI VJERODAJNICE (RC)	Rezultat
Zaporka ili PIN, izabrani od strane podnositelja ili automatski generirani, ali NE udovoljavaju smjernicama za izdavanje visoko sigurne zaporke ili PIN-a (npr. nedovoljna duljina znakova, jednoličnost znakova, korištena za više vjerodajnica, itd.) i stoga osjetljiva na napade.	**RC1**
Zaporka ili PIN, izabrani od strane podnositelja ili automatski generirani, ali udovoljavaju smjernicama za izdavanje visoko sigurne zaporke ili PIN-a (npr. dovoljna duljina znakova, nejednoličnost znakova, jedinstvenost korištenja za pojedinu vjerodajnicu).	**RC2**
Soft certifikat ili uređaj za OTP.	**RC3**
Kvalificirani soft certifikat prema Aneksu I Direktive 1999/93/EC.	**RC3**
Hard certifikat.	**RC3**
Kvalificirani hard certifikat prema Aneksu I Direktive 1999/93/EC.	**RC4**

3.2.2 Sigurnost autentifikacijskog mehanizma (AM)

Sigurnost autentifikacijskog mehanizma procjenjuje se u odnosu na najozbiljnije prijetnje u autentifikaciji: krađe identiteta (npr. dohvat osobnih podataka iz različitih izvora/opreme kao npr. servera koji su bez odgovarajućeg nadzora, javnih sumnjivih e-stranica, pretraživanjem po službenim registrima, internet pretraživanjem svih dostupnih izvora, društvenih mreža i sl.).

U ovom aspektu sigurnosti ocjenjuje se rizik direktnog napada u procesu udaljene autentifikacije. To se može dogoditi na neki od sljedećih načina:

1. **Pogađanje** – Jednostavan napad gdje napadač pogađa lozinku/PIN za autentifikaciju. Lako je izvediv kod onih lozinki/PIN-ova koji su jednostavne strukture i predvidivi.
2. **Prisluškivanje –** Napad praćenjem poruke koja putuje komunikacijskim kanalom tijekom procesa autentifikacije. Poruke se obično koriste za izvođenje nekih od „off-line“ analiza kojima se pokreće napad npr. prisluškivač općenito napada da bi došao do autentifikacijskog tokena čijim korištenjem se napadač pretvara da je druga osoba.
3. **Otmica –** Napad kojim se preuzima već postojeća sjednica i kradu osjetljivi podaci.
4. **Ponavljanje –** Napad u kojem napadač ponovo šalje ili odugovlači sa slanjem poruke koju je trenutak ranije presreo s namjerom da dođe do osjetljivih informacija.
5. **„Čovjek-u-sredini“ –** Oblik aktivnog prisluškivanja u kojem se napadač smjesti između dvije strane koje komuniciraju čineći da se vjeruje da se komunikacija među njima odvija direktno i sigurno. Napadač se smjesti u komunikacijski kanal između dvije strane koje komuniciraju, presreće podatke te ih mijenja, pa je cijela komunikacija pod kontrolom napadača. Napadač mora biti sposoban prihvatiti, odnosno presresti sve poruke i odaslati nove pretvarajući se da je uvijek jedna od strana u komunikaciji.

Postoji direktna veza između razine sigurnosti autentifikacijskog protokola i složenosti kod spomenutih napada. Sofisticiranost napada i obrane uzajamno napreduju. Dokazivost sigurnosti može biti delikatna. Može se odnositi na složenost autentifikacijskog mehanizma koja je u uporabi dulje vrijeme bez uspješno izvedenog napada. S druge strane, mora se imati na umu da je neke vrste napada (npr. otmica ili „čovjek-u-sredini“) teško otkriti. Stoga, kad se govori o sigurnosti mehanizama za autentifikaciju, misli se na sigurnost u odnosu na postojeću tehnologiju i ugrađene mehanizme kontrole koji su prepoznati u obrani navedenih napada. Tako je npr. poznato da kreiranje lozinke od barem 8 alfanumeričkih znakova ima veći stupanj složenosti u napadu pogađanjem.

Pri određivanju sigurnosti autentifikacijskog mehanizma, potrebno je imati u vidu Evaluaciju razina sigurnosti (engl. *Evaluation Assurance Level*) u opisanih sedam razina EAL1 - EAL7 u dokumentu „*The Common Criteria for Information Technology Security Evaluation*“ (skraćeno *Common Criteria* ili CC).

Tablica 7. sumira zahtjeve za sigurnost autentifikacijskih mehanizama.

Tablica 7: ***Ocjena razine sigurnosti autentifikacijskog mehanizma (AM)***

TRAŽI SE ZA OCJENU SIGURNOSTI AUTENTIFIKACIJSKOG MEHANIZMA (AM)	Rezultat
AM koji nude malu ili nikakvu zaštitu u odnosu na spomenute napade.	**AM1**
AM koji nude neku vrstu zaštite u odnosu na spomenute napade.	**AM2**
Sigurnosni mehanizmi koji nude zaštitu u odnosu na većinu spomenutih napada.	**AM3**
Prepoznati sigurnosni mehanizmi koji nude zaštitu u odnosu na sve spomenute napade usporedive sa EAL4+ ili više prema CC.	**AM4**

3.2.3 Rezime ocjene za fazu elektroničke autentifikacije (A)

Rezime ocjene za fazu elektroničke autentifikacije donosi se na temelju dobivenih ocjena svakog od čimbenika u fazi elektroničke autentifikacije, prema matrici prikazanoj u Tablici 8.

Tablica 8: ***Rezime za ocjenu faze elektroničke autentifikacije (A)***

	A1	A2	A3	A4
RC	RC1	RC2	RC3	RC4
AM	AM1-3	AM1-3	AM1-3	AM4

4. Potrebna dokumentacija pri procjeni razine sigurnosti vjerodajnice

Za provođenje procjene razine sigurnosti određene vjerodajnice, potrebno je zatražiti od izdavatelja vjerodajnice odgovarajuću dokumentaciju koja opisuje aspekte svih čimbenika navedenih u ovom dokumentu.

Dodatno se može, ovisno o specifičnostima za pojedinu vjerodajnicu, zatražiti i dostavljanje dodatne dokumentacije kao što je:

- Protokol registracije korisnika i provjere njegovog identiteta;
- Protokol izdavanja vjerodajnice;
- Sporazum/ugovor s državnim tijelima koji regulira izdavanje vjerodajnice;
- Procjena rizika;
- Dokaz o provedenom nadzoru i rezultatima provedenog nadzora (vrijedi za izdavatelje koji provode unutarnji ili vanjski nadzor);
- Opća pravila davanja usluga certificiranja (samo za davatelje usluga certificiranja);
- Pravilnik o postupcima certificiranja (javno objavljena verzija, ukoliko postoji);
- Potvrda o usklađenosti sa standardima iz područja izdavanja vjerodajnica od neovisnog tijela (ukoliko postoji);
- Dokumentacija prema D5.8.2d Security Principles and Best Practices; 11 - Appendix: ISO/IEC 2700x usage
- i dr.

5. Način provođenja procjene razine sigurnosti vjerodajnice

Ocjena razine sigurnosti vjerodajnice se donosi na temelju prethodno dobivenih ocjena za fazu registracije i fazu elektroničke autentifikacije. Model na temelju kojeg se donosi ukupna ocjena baziran je na matrici mogućih kombinacija ocjena za obje faze koja je prikazana u Tablici 9.

Tablica 9: ***Matrica kombinacija ocjena svih čimbenika koji utječu na ukupnu ocjenu razine sigurnosti***

		FAZA AUTENTIFIKACIJE			
		A1	**A2**	**A3**	**A4**
FAZA REGISTRACIJE	**R1**	RAZINA 1	RAZINA 1	RAZINA 1	RAZINA 1
	R2	RAZINA 1	RAZINA 2	RAZINA 2	RAZINA 2
	R3	RAZINA 1	RAZINA 2	RAZINA 3	RAZINA 3
	R4	RAZINA 1	RAZINA 2	RAZINA 3	RAZINA 4

Razina sigurnosti vjerodajnice se ocjenjuje kroz audit na temelju inicijalno dostavljene dokumentacije izdavatelja vjerodajnice te dokumentacije koja se može naknadno zatražiti na uvid. Tijekom provođenja audita, moguće je dodatno zatražiti određena pojašnjenja koja trebaju biti dokumentirana i ovjerena od strane nadležne(ih) osobe(a) izdavatelja vjerodajnice.

Auditom se ocjenjuju svi čimbenici u fazi registracije i fazi autentifikacije. Pri evaluaciji određenih čimbenika, sukladno preporuci STORK-a, koristi se najbolja praksa u domeni sigurnosnih funkcionalnosti preporučenih od različitih organizacija koje definiraju i/ili preporučuju standarde sigurnosti, organizacija koje razvijaju različite tehnološke platforme i organizacija koje razvijaju infrastrukturne sustave za sigurnost.

Audit se provodi temeljem STORK-ovih smjernica, Protokola rada NIAS-a, Kriterija za određivanje razine osiguranja kvalitete autentifikacije u okviru NIAS-a, normi ISO 19011:2011 i ISO/IEC 2700X. Audit tim sačinjava najmanje jedan predstavnik Fine koji ima završen tečaj za internog auditora za ISO 27001 (ili za Lead auditora ISO 27001) i najmanje jedan predstavnik Ministarstva uprave. Dodatno se mogu angažirati stručnjaci za pojedina područja audita po zahtjevu člana tima.

Rezultat audita se iskazuje u dokumentu Mišljenje NIAS audit tima o razini osiguranja kvalitete autentifikacije za predmetnu vjerodajnicu. Ovaj dokument izrađuje audit tim, a

prihvaća se potpisom svih članova audit tima. Mišljenje se daje na verifikaciju Ministarstvu uprave Republike Hrvatske, Upravi za e-Hrvatsku, koje donosi konačnu Odluku o prihvaćanju i ocjeni predmetne vjerodajnice u okviru NIAS-a.

Sukladno preporukama STORK-a, audit se provodi svake dvije godine.