Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva

Nacrti norma

Isporuka 5

Verzija 2.2

Zagreb, 2009.

Izradili:

Dr.sc. Zoran Bohaček
Prof. dr.sc. Krešimir Fertalj
Prof.dr.sc. Nikola Hadjina
Prof.dr.sc. Damir Kalpić
Prof.dr.sc. Mario Kovač
Dr.sc. Ivan Magdalenić
Prof.dr.sc. Zoran Skočir
Ranko Smokvina, dipl.oec.
Doc.dr.sc. Boris Vrdoljak

Voditelj Projekta:

Prof.dr.sc. Damir Kalpić

Odgovorna osoba:

Dekan Fakulteta elektrotehnike
i računarstva

Prof.dr.sc. Vedran Mornar

Dozvola uporabe:

Sadržaj:

0. Uvod

Temeljem pregleda stanja u području normiranja e-Poslovanja u elaboratu **Studija normizacije u e-Poslovanju**, te po načelima evaluacije norma navedenima u **Metodološkom priručniku za evaluaciju**, izdvojene su odabrane norme navedene uz plan njihova uvođenja u Republici Hrvatskoj prema materijalu **Plan izrade nacrta norma i popratne dokumentacije**. Korištene kratice navedene su već u **Studiji normizacije u e-Poslovanju**, **Metodološkom priručniku za evaluaciju** i **Obrazovnim materijalima**, te se nije smatralo potrebnim ponavljati ih jer su objašnjene u kontekstu prvog javljanja, a mnoge od njih nemaju globalni značaj. U ovom su elaboratu nešto detaljnije opisane norme koje zavrjeđuju pozornost, odnosno koje se mogu preporučiti na daljnji postupak tehničkim odborima za normizaciju. Pokrivena područja su e-Potpis i e-Identitet, Web servisi, norme za definiranje strukture i semantike. Posebna pažnja je posvećena uređajima i normama za poslovanje s pametnim karticama. Kao ogledni primjer *de facto* norme za e-Račun navodi se primjer u praksi prihvaćenog HUB obrasca.

1. Sigurnosne norme za e-Poslovanje

Sustav za elektroničko poslovanje mora zadovoljiti četiri važna zahtjeva na informacijsku sigurnost u procesu razmjene, obrade i skladištenja poruka:

- **Privatnost i povjerljivost**; informacija mora biti zaštićena od pristupa neovlaštenih strana
- **Integritet**; poruke se ne smiju neovlašteno mijenjati
- **Autentifikacija**; pošiljalac i primatelj poruka se moraju jednoznačno identificirati
- **Neporecivost**; nepobitan dokaz odašiljanja i prijema poruka

Da bi se ti zahtjevi ispunili, kao i zahtjevi na interoperabilnost heterogenih i distribuiranih sustava, koriste se sigurnosni mehanizmi te mehanizmi za interoperbilnost kroz upotrebu međunarodnih priznatih norma i specifikacija koji se mogu grupirati u četiri glavna područja:

1. **Elektronički potpisi (DS - *Digital Signature*)**
2. **Sigurni i interoperabilni WEB servisi (WSS- *Web Services Security* & WS-I-*Security*)**
3. **ebXML *Messaging Services* (ebMS)**
4. **Elektronički identitet (e-Identitet)**

U nastavku su dani prijedlozi primjene norma i specifikacija od međunarodno priznatih grupa (ISO, OASIS, W3C, ITEF, CEN/ISSS, ETSI i dr.) za sva navedena područja.

1.1. Elektronički potpis (e-Potpis)

Normizacija u području elektroničkog potpisa za EU krenula je donošenjem direktive **1999/93/EC** (http://portal.etsi.org/esi/Documents/e-sign-directive.pdf) Europske komisije. Namjera je ove direktive da se omogući korištenje elektroničkih potpisa te da se doprinese njegovoj zakonskoj prepoznatljivosti. Ona uspostavlja zakonski radni okvir za upotrebu i uspostavu elektroničkog potpisa te za usluge certificiranja kako bi se osiguralo ispravno funkcioniranje internog tržišta EU-a. Kako bi se osigurali postavljeni ciljevi za njegovo korištenje te kako bi se osigurala interoperabilnost između raznih vrsta implementacije elektroničkog potpisa donesen je skup norma i specifikacija od strane normizacijskih tijela CEN i ETSI unutar Europske inicijative EESSI (*European Electronic Signature Standardisation Initiative*), a na osnovi zahtjeva Direktive i mandata Europske komisije. Ova normizacija treba stvoriti opće prihvaćeni stupanj povjerenja i sigurnosti u uspostavi elektroničkih usluga kakvo je i e-Poslovanje.

Elektronički potpisi se kreiraju i verificiraju upotrebom kriptografije, grane primijenjene matematike, kroz transformaciju poruka u nerazumljivu (*unintelligible*) formu te povratno u razumljivu (*intelligible*) formu. Elektronički potpisi se kreiraju provođenjem određenih operacija nad informacijom tako da drugi mogu potvrditi da je nositelj tajne izvršio te operacije te da se potpisana informacija nije naknadno mijenjala. U sustavima sa simetričnim ključevima pošiljatelj i primatelj informacije moraju vjerovati osobnim tajnama koje posjeduju. U sustavima sa primjenom javnih ključeva nositelj privatnog (tajnog) ključa potpisuje informaciju, dok svatko tko posjeduje pripadni javni ključ može potvrditi da je elektronički potpis valjan (izdan od osobe koja se deklarira da je potpisala i poslala pripadnu informaciju). Važno svojstvo u ovom slučaju primjene javnog ključa je da se posjedovanjem javnog ključa ne može izračunati pripadni privatni ključ.

CEN i ETSI unutar EESSI inicijative trebaju pokriti sve aspekte operativnosti elektroničkih potpisa kao što su: proces upravljanja digitalnim certifikatima, proces generiranja potpisa, proces validacije i verifikacije potpisa te dodatnih povjerljivih procesa kao što su usluge vremenskog označavanja (*Time stamping*).

Potpuno je jasno da se zahtjev za PKI (*Public Key Infrastructure*) infrastrukturom kao i zahtjev za razvojem tržišta elektroničkog potpisa ne može zakonski zahtijevati. Ipak Direktiva je neophodan radni instrument koji treba osigurati platformu povjerenja u kontekstu elektroničkih potpisa, a samim time treba doprinijeti poticaju razvoja sigurnog e-Poslovanja. Sve veća pojava *e-Government* aplikacija koje koriste PKI zasnovane kartice identiteta za članove EU-a podiže potrebu za korištenje elektroničkih potpisa, bilo naprednih ili kvalificiranih.

1.1.1. Inicijative i preporuke u normizaciji

U okviru ovih inicijativa navedene su radne grupe, konzorciji i povjerenstva osnovana od međunarodno priznatih organizacija koje su izradile preporuke i specifikacije kojih se trebamo pridržavati kod uvođenja i primjene elektroničkih potpisa, a koje preporučamo kao rezultat najbolje prakse.

1.1.1.1. CEN Information Society Standardization System *(CEN/ISSS)*

CEN/ISSS *Workshop on Electronic Signature* (WS/E-*Sign*) radi pod nadležnošću *Comité Européen de Normalisation* (CEN), Europsko povjerenstvo za normizaciju. CEN/ISSS je odgovoran za dio programa EESSI (*Electronic Exchange of Social Security Information*) koji se odnosi na norme kvalitete i funkcionalnosti za kreiranje i verifikaciju elektroničkih potpisa kao i na norme za kvalitetu i funkcionalnost dobavljača usluga certificiranja (CSP - *Certification Service Providers*). Brze promjene u informacijskoj i komunikacijskoj tehnologiji (ICT) uvele se potrebu za korištenje radionica (*Workshop*), pored tradicionalnih CEN tehničkih povjerenstava, koje su otvorene za sve zainteresirane strane. One rade na principu konsenzusa i proizvode specifikacije (prethodnica norme), smjernice i ostale korisne materijale. Isporuke tih radionica publiciraju se od strane CEN-a kao CEN *Workshop Agreements* (CWAs).

U EESSI radnom okviru CEN/ISSS-u i ETSI/SEC-u (*European Telecommunications Standards Institute - Electronic Signature and Infrastructure*) je povjeren rad na tom programu elektroničkih potpisa. Glavni element u definiranju radnog programa su izvješća od strane tima eksperata koji čine preporuke za uspostavu norma u području elektroničkih potpisa.

Neke od predloženih radnih sporazuma (CWA) mogu se naći *on-line* na adresi ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/ . Specifikacije koje preporučamo u ovom području su:

- **CWA 14355**: *Guidelines for the implementation of Secure Signature-Creation Devices* (ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14355-00-2004-Mar.pdf) . Svrha ove specifikacije je definiranje smjernica za implementaciju SSCD (*Secure Signature Creation Device*) uređaja na specifičnim platformama (kao što su pametne kartice, osobna računala, PDA uređaji, mobilni telefoni) i specifičnim okolinama (kao što su terminali ili zaštićena okolina). Ovaj CWA dokument je namijenjen kako za upotrebu pravnim tako i tehničkim ekspertima u području elektroničkih potpisa, a isto tako i projektantima sustava i proizvoda u tom području.

- **CWA 14169**: *Secure signature-creation devices* "EAL 4+" (http://www.standardsdirect.org/standards/standards4/StandardsCatalogue24_view_24789.html). Ovaj dokument definira zahtjeve za SSCD prema Aneksu III direktive 1999/93/EC (Direktiva). Cilj ove norme je standardizirati zahtjeve za SSCD-ove kako bi se osigurala njihova usklađenost sa EU direktivom kao i njihova međusobna interoperabilnost. Ovi zahtjevi trebaju biti što više neovisni od tehnologije. Na osnovi ovog pristupa ovaj dokument nastoji pokriti što više mogućih implementacija različitih SSCD-ova, a prema postojećem tehnološkom stanju.

- **CWA 14365**: *Guide on the use of Electronic Signature* (ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14365-01-2004-Mar.pdf). Svrha ovog dokumenta je osiguranje smjernica za upotrebu elektroničkih potpisa. Dok je fokus bio na "kvalificiranim elektroničkim potpisima" kako je specificirano u Članku 5.1 Direktive, popratni efekt je bio da zahtjevi za primjenu običnog elektroničkog potpisa nisu dovoljno razrađeni. Svrha je ovog dokumenta da opiše zakonske i tehničke aspekte elektroničkog potpisa kako bi se proširilo područje scenarija e-Poslovanja, posebno korištenjem tehnologija s velikom primjenom, te podiglo povjerenje bez ostvarenja jakih zahtjeva koji su određeni člankom 5.1 Direktive. CWA dokument je namijenjen kako za upotrebu pravnim tako i tehničkim ekspertima u području elektroničkih potpisa, a isto tako i projektantima sustava i proizvoda u tom području. Ovaj dokument se sastoji od dva dokumenta:
    - Zakonski i tehnički aspekti
    - Zaštitni profile (PP - *Protection Profile*) za *Software Signature-Creation Devices*
- **CWA 14167-1:** *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signature* (ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14167-01-2003-Jun.pdf). Svrha ovog dokumenta je da opiše zahtjeve na sigurnost za povjerljive sustave koji upravljaju elektroničkim potpisima. Isto tako namjena ovog dokumenta je da definira sveopće zahtjeve na sigurnost sustava s obzirom na specifične zahtjeve sigurnosti za kriptografske module. Ovaj dokument postavlja funkcionalne zahtjeve za CSP (*Certificate Service Provider*) dobavljače kako bi provodili svoju zadaću, te formulira opće sigurnosne zahtjeve i pretpostavke. Pretpostavlja se da TWS (*Trustworthy System*) sustavi koji su certificirani na sukladnost s ovim dokumentom mogu biti usvojeni od strane CSP-a kako bi se smanjio napor u uspostavi sustava koji trebaju zadovoljiti Direktivu 1999/93/EC. Ova procedura omogućava maksimalnu fleksibilnost za gospodarstvo u razvoju sustava koji moraju zadovoljiti zahtjeve koji su naznačeni u *Annex* II ove Direktive.
- **CWA 14167-2:** *Cryptographic Module for CSP Signing Operations - Protection Profile* (ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14167-02-2004-May.pdf). Ovaj dokument se koristi od strane EU komisije prema proceduri koja je označena u članku 9 Direktive 1999/93/EC, a odnosi se na zajednički radni okvir unutar EU za područje elektroničkog potpisa. Ovaj dokument je pripremljen kao *Protection Profile* (PP) i slijedi pravila i formate ISO 15408 norme poznate kao *Common Criteria*.
- **CWA 14167-3:** *Cryptographic Module for CSP Key Generation Services - Protection Profile*

(http://www.neytendastofa.is/lisalib/getfile.aspx?itemid=956). Ovaj dokument je pripremljen kao *Protection Profile* (PP) koji slijedi pravila i formate koji su dani normom ISO 15408. Ovaj PP još nije vrednovan.

- **CWA 14168:** *Secure Signature-Creation Devices*-"EAL 4" (http://www.google.hr/search?hl=hr&q=CWA+14168&btnG=Tra%C5%BEi&meta=). Ovaj dokument specificira sigurnosne zahtjeve na SSCD što se smatra TOE (*Target of Evaluation*) prema ISO 15408 normi. Oni su formulirani kao PP prema istoimenoj normi. Ovi zahtjevi su obvezatni za uspostavu elektroničkog potpisa, a prema članku 5.1 EU Direktive. Dakle korištenje ovakvih SSCD-ova treba biti jasno i vidljivo. PP je sastavni dio ovog dokumenta kao *Annex* A. Ovaj dokument se koristi za utvrđivanje sukladnosti SSCD-a sa zakonskom regulativom u zemljama članicama EU-a. Ovaj dokument se također koristi u slučajevima kada se SSCD sastoji od više komponenata.

- **CWA 14170:** *Security Requirements for Signature Creation Applications* (ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14170-00-2004-May.pdf). Ovaj dokument :

    - osigurava model za stvaranje uvjeta za e-Potpis (*Signature Creation Environment*) te model za aplikacije koje kreiraju elektronički potpis (*Signature Creation Applications*)

    - specificira sveukupne zahtjeve koji se primjenjuju kroz sve funkcije koje su identificirane u funkcionalnom modelu

    - specificira sigurnosne zahtjeve za svaku od funkcija koje su identificirane u aplikaciji (*Signature Creation Application*) izuzev uređaja za kreiranje potpisa (*Signature Creation Device*)

  Svrha *Signature Creation Application* je da isporuči korisniku ili nekoj drugoj aplikaciji formu koja je specificirana od korisnika, napredni ili gdje je moguće kvalificirani elektronički potpis koji je povezan s potpisanim dokumentom kao potpisanim podatkovnim objektom.

- **CWA 14171:** *General Guidelines for Electronic Signature Verification* (ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14171-00-2004-May.pdf). Ovaj dokument identificira one podatke koje treba dohvatiti i pohraniti kako bi se kasnije mogli koristiti za rješavanje sporova između potpisnika i onoga koji verificira potpis. Ovaj dokument također identificira sigurnosne zahtjeve različitih elemenata koji čine sustav za verifikaciju potpisa. U interesu korisnika i povjerenja u e-Poslovanje verifikacija potpisa mora biti lagana i ne teža od verifikacije ručnog potpisa. Ona treba smanjiti vjerojatnost ljudske pogreške te treba biti dostupna većini korisnika. Ovaj dokument daje preporuke za korištenje sučelja kao i smjernice za organizacijske mjere kako

bi se postiglo ovo povjerenje i sigurnosni zahtjevi za različite elemente sustava za verifikaciju potpisa.

- **CWA 14172-1**: EESSI *Conformity Assessment Guidance: Part* 1 - *General* (http://www.google.hr/search?hl=hr&q=iso+14172-1&btnG=Tra%C5%BEi&meta=). Svrha ovog dokumenta je da se osiguraju smjernice za usklađenu primjenu norma za servise, procese, sustave i proizvode za e-Potpis. Dokument je namijenjen CSP dobavljačima, proizvođačima, operaterima, nezavisnim tijelima, procjeniteljima, laboratorijima za vrednovanje i testiranje koji su svi uključeni u procjenu usklađenosti prema EESSI isporukama. Ovaj dokument predstavlja logičku podlogu za smjernice za ocjenu usklađenosti koja se odnosi na servise, procese, sustave i proizvode koji su adresirani slijedećim EESSI, opće prihvaćenim, normama koje se odnose na e-Potpis:
    - **CWA 14167-1** *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements*;
    - **CWA 14167-2** *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations with Backup - Protection Profile* (CMCSOB-PP)
    - **CWA 14167-3** *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Module for CSP Key Generation Services - Protection Profile* (CMCKG-PP);
    - **CWA 14167-4** *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4*: *Cryptographic Module for CSP Signing Operations — Protection Profile* (CMCSO-PP)
    - **CWA 14169** *Secure Signature-Creation Devices* "EAL 4+";
    - **CWA 14170** *Security Requirements for Signature Creation Applications*;
    - **CWA 14171** *General Guidelines for Electronic Signature Verification*;
    - **CWA *14365*-2** *Protection Profile - Software Signature-Creation Device* SCDev-PP;
    - **ETSI TS 101 456** *Policy requirements for certification authorities issuing qualified certificates*;
    - **ETSI TS 102 023** *Policy requirements for time-stamping authorities*;
    - **ETSI TS 102 042** *Policy requirements for certification authorities issuing public key certificates*.
- **CWA 14172-2:** EESSI *Conformity Assessment Guidance: Part 2 - Certification Authority services and processes* (http://www.google.hr/search?hl=hr&q=iso+14172-2&btnG=Tra%C5%BEi&meta=). Ovaj dokument daje smjernice za procjenu

usklađenosti Certifikacijskih tijela (CA - *Certificate Authority*) prema slijedećim normama:

- **ETSI TS 101 456** "*Policy requirements for certification authorities issuing qualified certificates*" (http://pda.etsi.org/exchangefolder/ts_101456v010403p.pdf) ;
- **ETSI TS 102 042** "*Policy requirements for certification authorities issuing public key certificates*" (http://pda.etsi.org/exchangefolder/ts_102042v010304p.pdf).

Ovaj dokument je namijenjen nezavisnim tijelima i njihovim procjeniteljima.

- **CWA 14172-3:** EESSI *Conformity Assessment Guidance: Part 3 - Trustworthy systems managing certificates for electronic signature* (http://www.google.hr/search?hl=hr&q=iso+14172-3&btnG=Tra%C5%BEi&meta=). Ovaj dokument daje smjernice za procjenu usklađenosti povjerljivih sustava (TS) prema normi: **CWA 14167-1** "*Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements*".

  Dokument je namijenjen za korištenje od strane IT revizora kao i proizvođača i dobavljača povjerljivih sustava (TWS) i dobavljača CSP usluga certificiranja.

- **CWA 14172-4:** EESSI *Conformity Assessment Guidance: Part 4 - Signature creation applications and general guidelines for electronic signature verification* (ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14172-04-2004-Mar.pdf). Ovaj dokument daje smjernice za ocjenu usklađenosti proizvoda, sustava i aplikacija prema specifikacijama: **CWA 14170** "*Security Requirements for Signature Creation Applications*" i **CWA 14171** "*General Guidelines for Electronic Signature Verification*". Ovaj dokument je namijenjen za upotrebu od strane proizvođača i operatera.

- **CWA 14172-5:** EESSI *Conformity Assessment Guidance: Part 5 - Secure signature creation devices* (http://www.google.hr/search?hl=hr&q=iso+14172-5&btnG=Tra%C5%BEi&meta=). Ovaj dokument daje smjernice za procjenu usklađenosti SSCD-a (Secure Signature Creation Devices) prema specifikaciji **CWA 14169** "*Secure Electronic Signature Devices, version* EAL4+". Ova publikacija specificira vodič, koji osigurava odgovarajućim tijelima i njihovim vrednovateljima i procjeniteljima rad na konzistentan i pouzdan način, a time omogućuje njihovo opće prihvaćeno odobrenje na nacionalnoj i međunarodnoj osnovi. Ova publikacija stoga predstavlja osnovu za prepoznavanje nacionalnih sustava u cilju provođenja e-Poslovanja.

*1.1.1.2. ETSI (***European Telecommunication Standards Institute***)*

ETSI SEC je odgovoran za ETSI *Electronic Signatures and Infrastructures* (EESSI program) unutar ETSI-a. ESI (*Electronic Signatures and Infrastructures*) radna grupa od ETSI SEC je odgovorna za izvođenje tog programa. Posao se odrađuje u zajednici sa CEN/ISSS unutar ITCSB/EESSI radnog programa. ETSI je neprofitna organizacija

čija je misija da proizvodi telekomunikacijske norme koje će se koristiti u EU i šire kroz duže vrijeme. ETSI ima 912 članova iz 54 zemlje unutar i izvan Europe te okuplja administraciju, mrežne operatere, dobavljače usluga, proizvođače opreme, istraživačka tijela i korisnike. Zadatci slijede program koji je predložen od EESSI i podupiru implementaciju Europske direktive 1999/93/EC za elektronički potpis, a prema dogovorenoj podjeli posla između ETSI-a i CEN-a. Na osnovu tog posla izrađene su norme i specifikacije koje preporučamo u okviru ovog područja:

- **ETSI TR 102 038** TC- *Security - Electronic Signature and Infrastructure* (ESI). XML *Format for Signature Policies.* **(**http://pda.etsi.org/exchangefolder/tr_102038v010101p.pdf. Dokument prezentira XML format za politiku potpisa koji može zaprimiti informaciju o sigurnosnoj politici kako je specificirano sa ETSI TS 101 733 specifikacijama.

- **ETSI TS 101 903** XML *Advanced Electronic Signatures* (XadES). (http://pda.etsi.org/exchangefolder/ts_101903v010302p.pdf). Ovaj dokument definira XML formate za napredni elektronički potpis koji treba biti valjan za duži period te koji je sukladan sa 1999/93/EC direktivom. On sadrži također korisne informacije kao što je dokaz o valjanosti u slučajevima kada potpisnik ili ovjeritelj (verifikator) poriče valjanost potpisa. Ovaj dokument je zasnovan na kriptografiji upotrebom javnog ključa koja je podržana s certifikatima javnog ključa.

- **ETSI TS 101 861** *Time Stamping Profile.* (http://pda.etsi.org/exchangefolder/ts_101861v010301p.pdf) . Vremensko označavanje je kritično za elektronički potpis kako bi se znalo da li je elektronički potpis dodan za vrijeme perioda valjanosti odgovarajućeg digitalnog certifikata. *Time Stamp* protokol je definiran od strane IETF-a. Ovaj dokument ograničava broj opcija kroz uspostavu dodatnih ograničenja. Ovaj profil je zasnovan na TSP (*Time Stamp Protocol*) protokolu. On definira što mora klijent TSP-a podržati te što mora podržati poslužitelj kod primjene TSP-a.

- **ETSI TS 101 733** *Electronic signature formats*. (http://pda.etsi.org/exchangefolder/ts_101733v010704p.pdf). Ovaj dokument definira elektronički potpis koji treba biti valjan za duži period vremena. To uključuje dokaz valjanosti potpisa čak i u slučajevima kada potpisnik ili strana koja izvodi njegovu verifikaciju poriče njegovu valjanost. Isto tako ovaj dokument specificira korištenje povjerljivih usluga (servisa) (npr. *Time Stamping Authorities*) kao i podataka koje treba arhivirati (npr.vezne (*cross*) certifikate te liste za opoziv certifikata) kako bi se održao zahtjev za dugotrajniju valjanost elektroničkog potpisa (arhiviranje potpisa). Elektronički potpis koji je definiran ovim dokumentom može se koristiti za rješavanje spora između potpisnika i verifikatora potpisa, što se može dogoditi znatno kasnije od njegove upotrebe. Ovaj dokument koristi politiku potpisa (*Signature Policy*), koju referencira potpisnik, kao osnovu za valjanost elektroničkog

potpisa. Ovaj dokument je zasnovan na kriptografiji upotrebom javnog ključa koja je podržana s certifikatima javnog ključa.

- **ETSI TS 101 456** *Policy Requirements for Certification Authorities Issuing Qualified Certificates.* (http://webapp.etsi.org/action/PU/20070515/ts_101456v010403p.pdf). Ovaj dokument specificira zahtjeve na politiku koja se odnosi na certifikacijsko tijelo (CA) koje izdaje kvalificirane certifikate, a koji su u skladu sa direktivom 1999/93/EC. Ova specifikacija definira zahtjeve koji se odnose na operativni rad i upravljanje certifikacijskog tijela (CA) koje izdaje kvalificirane certifikate kako bi svi nositelji certifikata, svi subjekti koji su certificirani od CA te treće strane koje se pouzdaju (pouzdajuće strane) u te certifikate imali povjerenje u primjenjivost certifikata kao podrške za izradu elektroničkih potpisa.

- **ETSI TS 102 042** "*Policy requirements for certification authorities issuing public key certificates*" (http://webapp.etsi.org/action/PU/20071211/ts_102042v010304p.pdf) . Ovaj dokument uključuje opcije koje podržavaju istu razinu kvalitete od strane certifikacijskog tijela (CA) koje izdaje kvalificirane certifikate, ali "normalizirano" za širu primjenjivost i lako usklađenje sa drugim sličnim specifikacijama i normama iz drugih izvora i institucija. Kroz ovu harmonizaciju, razina kvalitete koja je postavljena od strane Direktive za elektronički potpis može se puno šire prihvatiti i prepoznati i bez primjene kvalificiranih certifikata.

- **ETSI TS 102 280** - X.509 V.3 *Certificate Profile for Certificates Issued to Natural Persosns* (http://pda.etsi.org/exchangefolder/ts_102280v010101p.pdf). Ovaj dokument definira opći profil za ITU-T *Recommendation* X.509 certifikate koji se izdaju za stvarne osobe. Pokrivenost ovog dokumenta odnosi se na osiguranje profila certifikata koji će omogućiti interoperabilnost certifikata koji su izdani za potrebe kvalificiranih elektroničkih potpisa, za autentifikaciju od točke do točke te za autentifikaciju podataka. Ovaj profil ovisi o Internet normama RFC 3280 i RFC 3739 za generičko formiranje ITU-T *Recomendation* X.509, te ovisi o normi ETSI TS 101 862 kako bi definirao implementaciju zahtjeva koji su određeni direktivom 1999/93/EC (Aneksima I i II) .

- **ETSI TS 101 862** *Qualified Certificate Profile* (http://pda.etsi.org/exchangefolder/ts_101862v010303p.pdf). Ovaj dokument definira profil za kvalificirane certifikate koji su zasnovani na tehničkoj definiciji koja je dana u RFC 3739, a koji se može koristiti od strane izdavatelja kvalificiranih certifikata koji su sukladni sa Aneksima I i II direktive 1999/93/EC. Ovaj profil kvalificiranog certifikata kao i IETF kvalificirani certifikat adresiraju kvalificirane certifikate na malo različit način. Dok IETF profil koristi kvalificirani certifikat unutar univerzalnog konteksta neovisno o lokalnim zakonskim zahtjevima, ovaj profil koristi

termin kvalificiranih certifikata eksplicitno kako je opisano u direktivi 1999/93/EC za elektronički potpis.

*1.1.1.3. IETF/RFC (***Internet Engineering Task Force/Request for Comment***)*

Zadatak je ovih specifikacija definirati na tehničkoj razini digitalne certifikate, protokole u realizaciji PKI infrastrukture i elektroničkih potpisa na Internetu. U okviru toga donesene su slijedeće specifikacije (*Request for Comments,* RFC):

- **RFC 3280** *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. (http://www.faqs.org/ftp/rfc/pdf/rfc3280.txt.pdf). Ovaj dokument profilira X.509 V3 certifikate i *Certificate Revocation List* (CRL) za korištenje na Internetu. Dan je pregled rješenja i modela kao uvod. X.509 V3 je detaljno opisan zajedno s dodatnim informacijama koje se odnose na format i semantiku Internetskih imena formi. X.509 V2 CRL format je detaljno opisan zajedno s potrebnim definicijama ekstenzija. Opisan je i algoritam za validaciju X.509 certifikacijskog puta.

- **RFC 3739** *Internet X.509 Public Key Infrastructure: Qualified Certificates Profile* (http://www.ietf.org/rfc/rfc3739.txt). Ovaj dokument formira profil certifikata koji je temeljen na RFC 3280, kao certifikat identiteta koji se izdaje stvarnoj osobi. Profil definira specifične konvencije koje su kvalificirane unutar zakonskog okvira koji se naziva Kvalificirani certifikat. Ipak, profil ne definira nikakav zakonski zahtjev za Kvalificirane certifikate.

- **RFC 2256** *A Summary of the X.500(96) User Schema for use with LDAPv3*. (http://www.ietf.org/rfc/rfc2256.txt). Ovaj dokument opisuje pristupni protokol za direktorije (imenike) koji omogućuje pristup za čitanje i ažuriranje. Pristup za ažuriranje zahtjeva sigurnu autentifikaciju, ali ovaj dokument ne propisuje implementaciju bilo kojeg autentifikacijskog mehanizma.

- **RFC 2251** *Lightweight Directory Access Protocol (v3)* (http://www.faqs.org/ftp/rfc/pdf/rfc2251.txt.pdf). Ovaj dokument opisuje pristupni protokol za direktorije (imenike) koji omogućuje pristup za čitanje i ažuriranje. Pristup za ažuriranje zahtjeva sigurnu autentifikaciju, ali ovaj dokument ne propisuje implementaciju bilo kojeg autentifikacijskog mehanizma. Interes za korištenje X.500 tehnologije za korištenje direktorija na Internetu je doveo do potrebe reduciranja napora i koštanja za implementaciju tog "teškog" protokola, što je dovelo do razvoja ovog LDAP protokola koji je detaljno opisan u ovom dokumentu.

1.1.1.4. RSA Laboratories - Public Key Crypto Standards *(PKCS)*

Zbog potrebe tehničke realizacije PKI infrastrukture koja je zasnovana na primjeni RSA algoritma asimetrične enkripcije primjenom javnog ključa donesene su slijedeće PKCS (*Public Key Cryptography Standards*) norme od strane RSA Laboratories.

- **PKCS 1** *RSA Encryption Standard*. (ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf). Ovaj dokument daje preporuke za implementaciju kriptografije primjenom javnog ključa zasnovane na RSA algoritmu što pokriva slijedeće aspekte:
    - Kriptografske procedure
    - Sheme enkripcije
    - Sheme digitalnog potpisa s dodatkom
    - ASN.1 sintaksu koja reprezentira ključeve te identifikaciju shema.

  Ove preporuke se mogu primijeniti unutar računalno komunikacijskih sustava s vrlo velikom fleksibilnošću. Aplikacijske norme koje se zasnivaju na ovim preporukama mogu uključiti i dodatna ograničenja.

- **PKCS 5** *Password-based Cryptography Standard*. (ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-5v2/pkcs5v2_1.pdf). Ovaj dokument osigurava preporuke za implementaciju kriptografije koja je zasnovana na lozinkama što pokriva slijedeće aspekte:
    - Funkcije za izvođenje ključeva
    - Sheme enkripcije
    - Sheme autentifikacije poruka
    - ASN.1 sintaksu za identifikaciju shema

- **PKCS 7** *Cryptographic Message Syntax Standard* . (ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-7.doc). Ova norma opisuje opću sintaksu za podatke na koje se može primijeniti kriptografija, kao što su digitalni potpis i digitalna ovojnica. Ova sintaksa dozvoljava rekurziju, tako da primjerice jedna ovojnica može postojati unutar druge, ili da neka strana može potpisati prethodno omotane digitalne podatke. Sintaksa također dozvoljava proizvoljne atribute, kao što je vrijeme potpisivanja, koji su autentificirani sa sadržajem poruke, osigurava i druge atribute kao što su supotpisi, potpisi na već potpisane podatke i poruke.

- **PKCS 9** *Selected Attribute Types* (ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-9-v2/pkcs-9.pdf). Ova norma definira dvije nove pomoćne klase objekata **pkcsEntity** i **naturalPerson** kao i vrste selektiranih atributa za upotrebu ovih

klasa. Norma također definira neke vrste atributa koji su povezani s korištenjem norma PKCS 7 za elektronički potpis poruka, PKCS 10 za potpisane zahtjeve za certifikatima, PKCS 12 za osobnu razmjenu informacija i PKCS 15 za kriptografske *token*e.

- **PKCS 10** *Certification Request Syntax* (ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-10/pkcs-10v1_7.pdf). Ovaj dokument opisuje sintaksu za zahtjeve za izdavanje digitalnih certifikata. Zahtjev za certifikatom se sastoji od jedinstvenog imena, javnog ključa, te opcionalno od skupa atributa, a sve zajedno je potpisano od entiteta koji je zahtijevao certifikaciju. Taj zahtjev se šalje u certifikacijsko tijelo (*certificate authority,* CA) koje transformira ovaj zahtjev u X.509 certifikat javnog ključa.

- **PKCS 11** *Cryptographic Card Interface Standard* (ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf) . Ova norma specificira aplikacijsko programsko sučelje (API) koje se naziva "Cryptoki" prema uređajima koji drže kriptografsku informaciju i provode kriptografske funkcije. Cryptoki dolazi od "*crypto-key*" i predstavlja kraticu od "*cryptographic token interface*". Cryptoki slijedi jednostavno objektno rješenje, postavlja ciljeve neovisno od tehnologije, te prezentira aplikacijama opći logički pogled na uređaj koji se naziva kriptografski *token* (npr. pametna kartica).

- **PKCS 15** *Cryptographic Token Information Syntax Standard* (ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-15/pkcs-15v1_1.pdf). Kriptografski tokeni kao što su *Integrated Circuit Cards* (IC *cards*, pametne kartice) su izvorno sigurne platforme, idealne za osiguranje sigurnosnih funkcija aplikacijama. One mogu obraditi autentifikaciju, digitalne certifikate, elektroničko potpisivanje, autorizaciju, kriptografske ključeve i dr. Cilj je ove norme da kroz definiranje sintakse :

    - Omogući interoperabilnost između komponenti koje se obrađuju na različitim platformama (neutralnost u odnosu na platforme)

    - Omogući aplikacijama da koriste prednosti produkata i komponenti od strane više proizvođača (neutralnost u odnosu na ponuđače)

    - Omogući korištenje napretka u tehnologiji bez prepisivanja aplikacijskog softvera (aplikacijska neutralnost) i

    - Održava konzistentnost s postojećim relevantnim normama kada vršimo proširenja koja su nužna i praktična.

1.1.1.5. IETF/W3C (Internet Engineering Task Force/World Wide Web Consortium*) - RFC*

IETF XML *Digital Signature* radna grupa je združena grupa od strane IETF-a i W3C XML *Signature* radne grupe. Njihove specifikacije su:

- ECDSA *with* XML-*Signature Syntax*. (**ITEF** *draft*). Ovaj dokument specificira kako koristiti ECDSA (*Elliptic Curve Digital Signature Algorithm*) zajedno sa (ITEF/W3C) XML potpisom.Ovaj mehanizam osigurava integritet, autentifikaciju poruke, i/ili usluge autentifikacije potpisnika za podatke bilo koje vrste, bilo da su smješteni unutar XML-a koji uključuje potpis ili su uključeni kroz referencu.

- *Digital Signature for Internet Open Trading Protocol (IOTP)*. **ITEF RFC 2802** (http://www.faqs.org/ftp/rfc/pdf/rfc2802.txt.pdf)**.** Cilj ovog dokumenta je da predloži sintaksu i procedure za izračunavanje i verifikaciju elektroničkog potpisa koji se primjenjuje na poruke prema IOTP protokolu, čime se osigurava: (1) autentifikacija IOTP transakcija, (2) osiguravaju se načini čime se štiti da poruka ne bude probijena (*tamperproof*), ili se omogućava detekcija njenog probijanja, (3) opisuje se skup algoritama za izradu sažetka (*digest*) i algoritama za potpis, od kojih je barem jedan obvezatan za ostvarenje interoperabilnosti, (4) jednostavna integracija sa IOTP specifikacijama, (5) osigurava se jednostavan potpis s minimalnom redundancijom i (6) dozvoljava se potpisanom dijelu poruke da bude proslijeđen drugom sudioniku u razmjeni poruka koji koristi drugi algoritam za potpis.

- *Digest values for DOM (DOMHASH)*. **IETF RFC 2803** (http://www.faqs.org/ftp/rfc/pdf/rfc2803.txt.pdf) . Ovaj dokument jasno definira sažetak XML objekata bez obzira na varijacije izvornog niza znakova XML-a. Ova definicija se koristi za XML elektronički potpis kao i za učinkovitu replikaciju XML objekata. Postoje barem dva scenarija za korištenje DOMHASH-a. Jedan je osnova za elektronički potpis XML-a. DOMHASH osigurava konkretnu definiciju izračunavanja sažetka. Drugi scenarij se koristi za sinkronizaciju dvije DOMHASH strukture.

1.1.1.6. IETF/W3C XML Signature and *XML* Key Management

Misija ove radne grupe je da razvije specifikacije za XML aplikacijski protokol koji treba omogućiti klijentu dobivanje ključnih informacija (vrijednosti, certifikat, upravljanje povjerljivim podatcima) od web servisa.

Ključne W3C specifikacije koje preporučamo su:

- XML-*Signature Syntax and Processing*. (http://www.w3.org/TR/2000/CR-xmldsig-core-20001031/). Ovaj dokument specificira pravila obrade i sintaksu XML elektroničkog potpisa. XML potpis osigurava integritet,

autentifikaciju poruke, i/ili autentifikacijske servise za potpisnika za podatke bilo koje vrste, bez obzira da li su smješteni unutar XML-a koji uključuje potpis ili bilo gdje drugdje.

- XML-*Signature* X*Path Filter*.(http://www.w3.org/TR/2002/REC-xmldsig-filter2-20021108/). XML *Signature* (XML-DSig) norma preporuča standardne načine za specificiranje sadržaja informacije koja treba biti digitalno potpisana te za prezentaciju proizvedenog digitalnog potpisa u XML-u. Neke aplikacije zahtijevaju specificiranje podskupa danog XML dokumenta kao informaciju koju treba potpisati. Ova specifikacija zadovoljava te zahtjeve uz pomoć X*Path* transformacije. Ipak, ovu je transformaciju teško učinkovito provesti uz postojeću tehnologiju. Ova specifikacija definira novu XML Signature transformaciju kako bi se omogućilo učinkovita implementacija podjele dokumenta na njegove dijelove koje bi trebalo potpisati.

- *Canonical* XML (http://www.w3.org/TR/xml-c14n). Svaki XML dokument je dio skupa dokumenta koji su logički ekvivalent unutar konteksta primjene, koji međutim variraju u fizičkoj prezentaciji koja se zasniva na sintaksnim promjenama koje su dozvoljene od XML-a kao i imenovanju prostora (*NameSpaces*) u XML-u. Ova specifikacija opisuje metodu za generiranje fizičke prezentacije, kanoničkog oblika XML dokumenta, koja vodi računa o dozvoljenim izmjenama. S izuzetkom nekih neuobičajenih slučajeva, ako dva dokumenta imaju isti kanonički oblik, tada su ta dva dokumenta logički ekvivalentni unutar danog konteksta primjene (aplikacije). Treba napomenuti da ipak dva dokumenta mogu imati različite kanoničke oblike, a da su još uvijek ekvivalenta u danom kontekstu koji se zasniva na aplikacijski specifičnim pravilima ekvivalencije za koje opća XML specifikacija ne odgovara.

- XML-*Signature Requirements* (http://www.w3.org/TR/1999/xmldsig-requirements-990623). Ovaj dokument propisuje principe dizajna, opsega i zahtjeva na specifikaciju za XML elektronički potpis. On uključuje zahtjeve koji se odnose na sintaksu potpisa, model podataka, kriptografsku obradu te vanjske zahtjeve i koordinaciju.

- XML *Key Management Specification* (XKMS) (http://www.w3.org/TR/2001/NOTE-xkms-20010330/). Ovaj dokument specificira protokole za distribuciju i registraciju javnih ključeva, što je pogodno za korištenje zajedno sa predloženom normom za XML Signature (XML-SIG) koja je razvijena od *World Wide Web Consortium* (W3C) i ITEF-a i prethodno usvojenom normom za enkripciju - XML *encryption*. XKMS sastoji se od dva dijela -- XML *Key Management Specification* (X-KISS) i XML *Key Registration Services Specification* (X-KRSS).

- XML *Key Management Requirements* (http://www.w3.org/2001/XKMS/Drafts/xkms-req.html) Ovaj dokument prikazuje principe projektiranja, opseg i zahtjeve na specifikaciju za XML *Key*

Management kao i na povjerljive implementacije upravljanja ključevima na serveru. On uključuje zahtjeve koji se odnose na sintaksu, obradu i sigurnost upravljanja ključevima kao i na koordinaciju s drugim aktivnostima u normizaciji.

- SOAP *Security Extensions: Digital Signature.* (http://www.w3.org/TR/2001/NOTE-SOAP-dsig-20010206/) Ovaj dokument specificira pravila sintakse i obrade ulaza u SOAP (*Simple Object Access Protocol*) zaglavlje kako bi se mogla prenijeti informacija elektroničkog potpisa unutar SOAP 1.1 ovojnice.

- *Digital Signature Label Architecture.*(http://www.w3.org/TR/WD-DSIG-label-arch). Ovaj dokument prikazuje arhitekturu i logičku podlogu dizajna koji stoji iza *Digital Sig's Digital Signature Labe*l specifikacija. Ukupni cilj je upotrijebiti elektronički potpisane oznake kako bi se dobile autentične potvrde o samostalnim dokumentima ili o očitovanju o agregiranim objektima. Tri osnovna elementa, elektronički potpisi, potvrde i očitovanja se pojedinačno analiziraju u pogledu njihovog dizajna, operacija, formata podataka i strategiji distribucije. Ovi elementi se mogu skupiti danas unutar PICS (*Platform for Internet Content Selection*) oznaka, kako bi se dobila potpisana potvrda o informacijskom resursu, ili kroz potpis očitovanja, formirajući potvrde za nekoliko resursa.

*1.1.1.7. ISO (***International Organization for Standardization***)*

U ovom području elektroničkog potpisa postoji nekoliko važnih norma koje preporučamo:

- **ISO 9796-2** *Digital signature schemas giving message recovery.* ISO 9796-2 specificira tri sheme digitalnog potpisa koje omogućavaju oporavak poruke, od kojih su dvije determinističke, a jedna je slučajna. Sigurnost sve tri sheme je zasnovana na teškoći faktorizacije velikih brojeva. Sve tri sheme mogu osigurati potpuni ili djelomični oporavak poruke. Metoda za proizvodnju ključa za sve tri sheme potpisa je specificirana u ovom dokumentu. Korisnicima ove norme se, gdje god je moguće, preporuča usvajanje drugog mehanizma (*Digital signature scheme* 2). Ipak, u uvjetima gdje je generiranje slučajnih varijabli nemoguće preporuča se *Digital signature scheme* 3. *Digital signature scheme* 1 upotrebljava se samo u onim slučajevima gdje se zahtijeva kompatibilnost sa sustavima koji su implementirali prvo izdanje ove norme. *Digital signature scheme* 1 je kompatibilna samo sa sustavima koji su upotrijebili sažetak (*hash*) najmanje dužine od 160 bita.

- **ISO 9797-2** *Message Authentication Codes.* Ova norma specificira tri MAC algoritma koji koriste tajni ključ i *hash*-funkciju sa n-bitnim rezultatom kako bi izračunali m-bitni MAC. Ovi se mehanizmi koriste i kao mehanizmi za zaštitu integriteta kako bi verificirali da nije bilo neovlaštene izmjene podataka. Isto tako koriste se i za autentifikaciju pošiljaoca poruke koji

raspolaže tajnim ključem. Jakost ovih mehanizama ovisi o dužini i tajnosti ključa, dužini sažetka (*hash*) koji se dobije korištenjem *hash*-funkcije, jakosti *hash*-funkcije, dužinom MAC-a te o specifičnom mehanizmu. U ovoj normi specificirana su tri mehanizma koji se zasnivaju na dediciranim *hash*-funkcijama koje su specificirane u normi ISO 10118-3. Prvi mehanizam koji je specificiran je MDx-MAC. On poziva cijelu *hash*-funkciju jednom, ali radi male izmjene na funkciji zaokruživanja dodaje ključ aditivnoj konstanti u funkciji zaokruživanja. Drugi mehanizam u ovoj normi je poznat kao HMAC. On poziva cijelu *hash*-funkciju dva puta. Treći mehanizam je varijanta MDx-MAC koji uzima kao ulaz kratki (najviše 256 bitova) niz. On nudi bolje performanse za aplikacije koje rade samo s kratkim ulaznim nizovima. Ova norma se može primijeniti za sigurnosne servise bilo koje sigurnosne arhitekture, procese ili aplikacije.

- **ISO 10118-2** *Hash-functions.* Ovaj dio norme specificira *hash*-funkcije koje koriste algoritme za n-bit blok enkripciju. Stoga su one pogodne za okolinu u kojoj su ti algoritmi već implementirani. Specificirane su četiri *hash*-funkcije. Prva osigurava sažetak (*hash*) dužine manje ili jednake *n,* gdje je *n* dužina bloka algoritma koji se koristi. Druga osigurava sažetak dužine koja je manja ili jednaka 2*n*; a treća osigurava sažetak dužine jednak 2*n*; četvrta osigurava sažetak dužine 3*n*. Sve četiri funkcije zadovoljavaju opći model koji je specificiran u ISO 10118-1 normi.

- **ISO 11770** *Key Management.* ISO 11770-1 dokument definira opći model upravljanja ključevima i to neovisno o pojedinom kriptografskom algoritmu u upotrebi. On identificira ciljeve upravljanja ključevima, osnovne koncepte te usluge za upravljanje ključevima. ISO 11770-2 opisuje tri okoline za uspostavu ključeva: *Point-to Point, Key Distribution Centre* (KDC) te *Key Translation Centre* (KTC). Ovaj dokument ujedno i postavlja zahtjeve na sadržaje poruka koje nose podatke o ključevima ili su neophodne za postavljanje uvjeta pod kojima se podatci o ključevima trebaju uspostaviti. ISO 11770-3 definira mehanizme upravljanja ključevima koji su temeljeni na asimetričnim kriptografskim tehnikama. ISO 11770-4 definira mehanizme za uspostavu ključeva koji su temeljeni na slaboj tajni, tj. tajnama koje se uobičajeno pamte od ljudi, koje su prema tome izabrane iz relativno malog skupa mogućnosti.

- **ISO 13888** *Non-repudiation.* Cilj servisa neporecivosti je generiranje, prikupljanje, održavanje, raspoloživost i verifikacija dokaza koji se koriste u cilju rješavanja sporova poricanja poduzetih ili ne poduzetih akcija. Različiti dijelovi ove norme osiguravaju mehanizme neporecivosti za slijedeće faze: generiranje dokaza, prijenos, uskladištenje, dohvat i verifikaciju. Ovi mehanizmi se tada primjenjuju na specifične servise neporecivosti kao što su: neporecivost izvora, neporecivost isporuke (prijema), neporecivost pokretanja i neporecivost prijenosa. Mehanizmi neporecivosti osiguravaju protokole za izmjenu specifičnih *token*a neporecivosti za svaki pojedinačni servis

neporecivosti. Neporecivi *token* sastoji se od sigurnosnih ovojnica, i/ili elektroničkih potpisa i proizvoljno od dodatnih podataka.

- **ISO 14888** *Digital signature with appendix.* Postoje dvije vrste mehanizama za elektronički potpis:

    - Kada proces verifikacije treba poruke kao dio ulaznih podataka, mehanizmi se zovu "mehanizam potpisa s dodatkom". *Hash*-funkcija se koristi u izračunavanju dodatka.

    - Kada proces verifikacije otkriva sve ili samo dio poruke tada se mehanizam naziva "mehanizam potpisa koji oporavlja poruku". *Hash*-funkcija se također koristi u generiranju i verifikaciji ovih potpisa.

  ISO 14888-1 specificira opće principe i zahtjeve za elektroničke potpise sa dodatkom. ISO 14888-2 adresira elektroničke potpise temeljene na faktorizaciji cijelih brojeva, a ISO 14888-3 opisuje elektroničke potpise temeljene na diskretnim logaritmima.

- **ISO 15946** *Cryptographic techniques based on elliptic curves*. Ova norma specificira tehnike kriptografije upotrebom javnog ključa koje su zasnovane na eliptičkoj krivulji. Ova norma se sastoji od pet dijelova te uključuje tehnike za uspostavu ključeva za simetričnu enkripciju kao i mehanizme elektroničkog potpisa. Ovaj dokument opisuje matematičku podlogu kao i specifične tehnike neophodne za implementaciju mehanizama koji su temeljeni na eliptičkim krivuljama definiranim na konačnim poljima ili na uparivanju na eliptičkim krivuljama.

- **ISO/TS 15000-2:*2004*** *Electronic business eXtensible Markup Language (ebXML) -- Part 2: Message service specification (ebMS).* Ova norma ukazuje na zahtjeve koji se postavljaju na ebXML *Message Service Handler* za potrebe razmjene poruka za e-Poslovanje. Ona definira neutralnu metodu komunikacijskog protokola za razmjenu elektroničkih poslovnih poruka te specificira učahurivanje (*encapsulation*) koje podržavaju pouzdanu i sigurnu isporuku poslovnih informacija. Norma uključuje fleksibilne tehnike enkapsulacije, što omogućuje poruke koje su neovisne od tereta, neovisne od komunikacijskog protokola te prihvaćaju bilo koju vrstu formata. Ova raznovrsnost omogućava prihvat postojećih sustava za e-Poslovanje koji koriste tradicionalne sintakse (npr. UN/EDIFACT, ASCX12, ili HL7) da koriste ebXML infrastrukturu zajedno s korisnicima nadolazećih tehnologija. U normi su uključeni primjeri koji koriste ove specifikacije sa HTTP (RFC2616) i SMTP (RFC2821) protokolima. Ova norma je s aspekta sigurnosti detaljnije opisana u poglavlju 2.3 ebXML *Messaging Services* (ebXML - *Security Module*)

- **ISO 7498-2:1989** *Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture.*

Ova norma daje opći prikaz sigurnosnih servisa i pripadnih sigurnosnih mehanizama koji se osiguravaju Referentnim modelom, te poziciju u Referentnom modelu na kojoj se osiguravaju pripadni servisi i mehanizmi. Isto tako norma proširuje polje njene primjene na područje sigurne komunikacije između otvorenih sustava. Dodatci na postojeće koncepte i principe ne mijenjaju postojeće stanje nego ih proširuju. Ona nije vezana na specifičnu implementaciju niti je osnova za procjenu usklađenosti sa stvarnom implementacijom.

- **ISO/IEC 10181-4**: 1998 *Information technology -- Security techniques -- Hash-functions -- Part 4: Hash-functions using modular arithmetic.* Ovaj dio norme ISO 10118 specificira dvije *hash*-funkcije koje koriste modularnu aritmetiku. Ove *hash*-funkcije, za koje se smatra da su otporne na koliziju, sažimaju poruke proizvoljnih dužina u sažetak (*hash code*) čija je dužina određena dužinom prostog (prim) broja koji se koristi u funkciji redukcije. Na taj način se sažetak lako prilagođava prema ulaznoj dužini od strane bilo kog mehanizma (npr. algoritam digitalnog potpisa, shema identifikacije i dr.).

- **ISO 9594-8** *Information technology — Open Systems Interconnection — The Directory: Public key and attribute certificate frameworks*. Ova norma definira radni okvir za certifikate koji su zasnovani na javnim ključevima. Ona uključuje specifikaciju podatkovnih objekata koji predstavljaju same certifikate, a isto tako i izjave o opozivu izdanih certifikata kojima se više ne može vjerovati. Ova norma definira neke kritične komponente PKI infrastrukture, a ne PKI infrastrukturu u cjelini. Ipak ove specifikacije daju podlogu za izgradnju i korištenje svih raspoloživih svojstava koje pruža PKI infrastruktura.

- **ISO 19785-1** *Information technology / Common Biometric Exchange Formats Framework - Part 1: Data element specification* (http://webstore.iec.ch/preview/info_isoiec19785-1%7Bed1.0%7Den.pdf). *Common Biometric Exchange Formats Framework* (CBEFF) doprinosi interoperabilnosti biometrijskih aplikacija. Osnovna svrha CBEFF-a je definirati apstraktne podatkovne elemente, podatkovne elemente sa skupom definiranih apstraktnih vrijednosti, te njihovom semantikom. Ova CBEFF struktura sastoji se od tri dijela: standardno biometrijsko zaglavlje (SBH), biometrijski blok podataka (BDB) i blok sigurnosti (SB). Ovaj dokument upravo definira takove podatkovne elemente.

- **ISO 19794-2** *Information technology -- Biometric data interchange formats -- Part 2: Finger minutiae data* (http://webstore.iec.ch/preview/info_isoiec19794-2%7Bed1.0%7Den.pdf). U cilju implementacije interoperabilnosti biometrijskih sustava za prepoznavanje ova norma postavlja format razmjene ključnih podataka koji se uzimaju za otisak prsta, kao i podataka potrebnih za uređaje za prepoznavanje otiska prsta. Ova norma specificira ekstrakciju ključnih podataka od uzetog otiska. Definirana su dvije vrste formata podataka, jedan za opće uskladištenje i

transport, i drugi za kartične sustave. Kartični format ima standardnu i kompaktnu varijantu.

1.1.1.8. OASIS Digital Signature Services

OASIS tehnička komisija (TC) razvija tehnike i specifikacije koje trebaju poduprijeti obradu elektroničkih potpisa. To uključuje definiranje sučelja za zahtjev web servisima da proizvedu ili verificiraju elektronički potpis za dani komad podataka, kao i tehnike za dokaz ispravnosti kreiranja elektroničkog potpisa unutar perioda valjanosti privatnog ključa. TC isporuke uključuju: (1) XML protokol za kreiranje i verifikaciju elektroničkog potpisa i vremenskih oznaka *(time stamps*); (2) uvezivanje elemenata protokola iz (1) u SOAP, HTTP i TLS sigurnost. (3) skup profila za primjenu navedenih protokola na specifično aplikacijsko područje. Radovi ove komisije uključuju postojeće norme elektroničkog potpisa kao što su: IETF/W3C XML Signature, IETF *Cryptographic Message Syntax* (RFC 2630); ETSI XML *Advanced Electronic Signature* (XAdES TS 101 733), IETF *Time Stamp Protocol* (RFC 3161)). U nastavku su dane specifikacije koje se odnose na servise elektroničkog potpisa:

- OASIS *Access Control* TC (XACML)(www.oasis-open.org/committees/download.php/2406/oasis-xacml-1.0.pdf). Ova specifikacija definira XML shemu za jezik proširene politike kontrole pristupa. XACML definira tri krovne razine elemenata politike pristupa: <*Rule*> , <*Policy*> i <*PolicySet*>. XML je prirodni izbor za opći jezik sigurnosne politike zbog lakoće njegove sintakse i semantike te zbog velike podrške koju ima na svim većim platformama i alatima.

- OASIS *Rights Language TC (XrML).* (http://www.xrml.org/get_XrML.asp). XrML je jezik za specifikaciju prava. XrML je temeljen na XML-u te koristi gramatiku za specifikaciju prava i uvjeta kako bi upravljao pristupom digitalnim sadržajima i servisima. XML Signature i XML Encryption se koriste za autentifikaciju i zaštitu izraza koji definiraju pravila pristupa. Ta pravila se mogu sigurno dodjeljivati pojedincima ili grupama korisnika. Jezik može osigurati i povjerenje kako bi se održao integritet prava i uvjeta.

- OASIS *Security Services* TC (SAML)(http://www.oasis-open.org/specs/#samlv2.0) . Ova specifikacija predstavlja XML radni okvir za razmjenu autentifikacje, korištenje prava te atributnih informacija. Kao što samo ime kaže SAML (*Security Assertion Markup Language*) dozvoljava poslovnim entitetima formiranje potvrda koje se odnose na identitet, atribute i prava subjekata (koji je najčešće ljudsko biće-korisnik) prema drugim entitetima, kao što je partnerska tvrtka ili neka aplikacija. Federativan način upravljanja identitetima je danas dominantan. Federativni pristup se odnosi na uspostavu svih ili nekih poslovnih sporazuma, kriptografskog povjerenja, korisničkih identifikatora ili atributa preko sigurnosnih domena kako bi se omogućila djelotvorna interakcija između poslovnih domena.

- OASIS *Web Services Security* TC (WSSTC)(http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss) . Skup *Web Services Security* specifikacija uključuje: *Web Services Security*: SOAP *Message Security* 1.0 (WS-*Security* 2004), *Web Services Security Username Token profile* 1.0, *Web Services Security* X.509 *Certificate Token Profile* te dvije relevantne XML *Scheme*. WSSTC tehnička komisija također kreira dodatne profile zaloga (*token*) koji se koriste sa jezgrom SOAP *Message Security* 1.0 specifikacije, što uključuje *Web Services Security*: SAML *Token Profile* koji je sada u naprednoj fazi pripreme. Ove specifikacije bit će detaljnije obrađene u posebnom poglavlju "Sigurni WEB servisi".

1.2. Sigurni i interoperabilni Web servisi

XML sigurnosne norme, norme za sigurnost Web servisa, norme za sigurnosnu interoperabilnost, uz navedene norme za e-Potpis, predstavljaju osnovu za sigurnost e-Poslovanja. Ove norme omogućuju autentifikaciju, povjerljivost i integritet u realizaciji SOAP (*Simple Object Access Protocol*) komunikacije koja se koristi kao osnovna komunikacijske infrastrukture (osnovni protokol) u realizaciji e-Poslovanja, a sama ne posjeduje zahtijevane sigurnosne sposobnosti.

1.2.1. XML sigurnosne norme

XML omogućava razvoj i realizaciju e-Poslovanja kroz upotrebu Web servisa. Stoga je nužno osigurati sigurnost korištenja XML-a kroz normizaciju u kojoj su najvažnije norme: XML *Signature*, XML *Encryption* i SAML. XML Signature specifikacija osigurava integritet podataka i autentičnost (kako poruke tako i potpisnika), a uključena je u XML format. XML *Encryption* specifikacija osigurava povjerljivost (tajnost) podataka korištenjem enkripcijskih algoritama, koja je također uvezana u XML format. SAML omogućava da partnerske aplikacije dijele informacije vezane na korisničku autentifikaciju i autorizaciju. To je u biti *single sign-on* (SSO) specifikacija koju nude svi veći ponuđači proizvoda za e-Poslovanje. Korištenjem SAML specifikacije omogućeno je i uključenje tih podataka, za autentifikaciju i autorizaciju, u XML format, čime se postiže interoperabilan SSO.

1.2.1.1. XML Signature *(XML potpis)*

XML-*Signature Syntax and Processing* specifikacija je razvijena i publicirana od strane IETF-a i W3C-a u cilju uspostave XML usklađene sintakse koja se koristi za predstavljanje elektroničkih potpisa WEB resursa i dijelova protokolarnih poruka (sve što se referencira sa *Uniform Resource Identifier* (URI) te procedura za izračunavanje i verifikaciju takvih potpisa. Ove norme i specifikacije su detaljno opisane u poglavlju e-Potpis.

1.2.1.2. XML Encryption

XML enkripcija je metoda pomoću koje se XML sadržaj transformira na takav način da je vidljiv (dostupan) samo za određenog primatelja, a nevidljiv za sve ostale. Postoje mnoge primjene ove specifikacije čime se podiže značaj XML-a na Internetu i WEB-u uključujući i zaštitu informacija u obradi transakcija plaćanja, osobnih podataka i dr. Specifikacija opisuje kako kriptirati XML dokumente uključujući i pojedinačne elemente. XML *Encryption Syntax and Processing* specifikacija proizvedena od W3C XML *Encryption Working Group* s ciljem da uspostavi proces enkripcije/dekripcije digitalnih sadržaja (uključujući XML dokumente kao i njihove dijelove) te sintaksu, kako bi se reprezentirao (1) kriptirani sadržaj i (2) informacija koja omogućava određenom primatelju da dekriptira primljeni sadržaj. XML *Encryption* specifikacija specificira proces kriptiranja podataka te predstavljanja njegovog rezultata u XML-u. Podatci koji se kriptiraju mogu biti proizvoljnog oblika, uključujući i XML dokumente, XML elemente ili XML sadržaj elemenata. Rezultat kriptiranja je XML *Encryption* kriptirani podatkovni element koji sadrži (preko jednog od svojih elemenata djece) ili identificira (preko URI reference) kriptirane podatke. Kad kriptiramo XML element ili sadržaj elementa kriptirani podatci (*EncryptedData element*) zamjenjuju element odnosno sadržaj u kriptiranoj verziji XML dokumenta. Kada kriptiramo proizvoljne podatke (uključujući sve XML dokumente) *EncryptedData* element može postati korijen (*root*) novog XML dokumenta ili postaje element-dijete u aplikacijski izabranom XML dokumentu. Ova specifikacija implementira svojstva koja su navedena u dokumentu XML *Encryption Requirements* koji popisuje principe dizajna, opseg, i zahtjeve za XML enkripciju. Ovaj dokument uključuje zahtjeve koji se odnose na sintaksu kriptiranja, model podataka, format, kriptografsku obradu te vanjske zahtjeve i potrebnu koordinaciju.

Dokumenti koji se referenciraju kroz ovu specifikaciju su:

- XML *Encryption Syntax and Processing* (http://www.w3.org/TR/xmlenc-core/)
- XML *Encryption Requirements* (http://www.w3.org/TR/xml-encryption-req)
- W3C XML *Encryption Working Group* (http://www.w3.org/Encryption/2001/)
- W3C XML *Encryption Working Group Charter* (http://www.w3.org/Encryption/2001/01/xmlenc-charter.html)
- JSR 106: XML *Digital Encryption* APIs (http://jcp.org/en/jsr/detail?id=106)
- XML *and Encryption* (http://xml.coverpages.org/xmlAndEncryption.html)

1.2.1.3. Security Assertion Markup Language *(SAML)*

Security Assertion Markup Language (SAML) verzija 2.0 publicirana je kao OASIS norma. SAML je radni okvir temeljen na XML-u koji omogućava razmjenu

autentifikacijske informacije, prava i atributa. Kao što i samo ime kaže SAML omogućava poslovnim entitetima da izrađuju svoje vlastite potvrde (tvrdnje) koje se odnose na identitet, atribute i prava entiteta (entitet je najčešće korisnik) za druge entitete kao što su partnerske tvrtke ili aplikacije u tim tvrtkama. SAML norma vezana je na glavne norme za WEB servise uključujući XML, SOAP, *Transport Layer Security* (TLS), XML *Signature* i XML *Encryption*. SAML definira radni okvir za razmjenu sigurnosnih informacija između poslovnih partnera na Internetu. SAML verzija 2.0 omogućuje sigurnu razmjenu autentifikacijske informacije, atributa i autorizacije između nejednakih (različitih) sigurnosnih domena, čime je omogućena WEB *single-sign on* (SSO) prijava te sigurnost poslovnih transakcija neovisno od postojećih tehnoloških rješenja i ponuđača. Kroz definiciju standardnih mehanizama za komunikaciju sigurnosnih informacija i identiteta između poslovnih partnera, SAML formira federativne identitete i transakcije između poslovnih domena koje to omogućuju.

Ova norma bazirana je na slijedećim referencama i dokumentaciji:

- *Security Assertion Markup Language* (SAML) V2.0- *Technical Overview* (http://xml.coverpages.org/SAML-TechOverviewV20-Draft7874.pdf)
- *Security Assertion Markup Language* (SAML) V2.0, OASIS *Standard* (http://xml.coverpages.org/ni2005-03-14-a.html)
- *Security Assertion Markup Language* (SAML) V1.0 (http://xml.coverpages.org/ni2002-11-12-b.html)
- *Security Assertion Markup Language* (SAML) (http://xml.coverpages.org/saml.html)
- *Liberty Identity Web Services Framework* (ID-WSF) *Supports* SAML *Version* 2.0 (http://xml.coverpages.org/ni2005-02-11-b.html).

1.2.2. Sigurni Web servisi (WS-*Security*)

WSS (WS-*Security, Web Services Security*) je komunikacijski protokol koji osigurava sigurnost primjene Web servisa. Ovaj protokol je publiciran od strane OASIS normizacijskog tijela kao WS-*Security* norma 1.1. Izvorno je protokol razvijen od IBM-a, Microsoft-a i VeriSign-a.

Protokol sadrži specifikacije kako očuvati integritet i povjerljivost poruka u izvršavanju Web servisa. WSS protokol uključuje detalje u korištenju SAML (*Security Assertion Markup Language*) jezika, Kerberosa (sustav za autentifikaciju i autorizaciju) te digitalnih certifikata kao što su X.509 certifikati koji se koriste u primjeni PKI infrastrukture.

WSS opisuje kako pripojiti elektronički potpis i zaglavlja enkripcije na SOAP (*Simple Object Access Protocol*). Ujedno protokol prikazuje kako pripojiti sigurnosne tokene,

uključujući binarni sigurnosni zalog (*token*) kao što je X.509 certifikat i Kerberos karte, na poruke u izvršavanju Web servisa.

WSS protokol uključuje svoje sigurnosne mogućnosti u zaglavlje SOAP poruke. Budući da radi na aplikacijskoj razini osigurana je sigurnost s kraja na kraj (*end-to end-security*).

WS-*Security* normu 1.1 čine sljedeći dokumenti i specifikacije:

- SOAP *Message Security 1.1* (http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf). Ova specifikacija opisuje poboljšanje SOAP poruka kroz zaštitu integriteta poruka te kroz autentifikaciju korištenjem jedne poruke. Ovi mehanizmi mogu se upotrijebiti na širokom spektru sigurnosnih modela i tehnologija kriptiranja. Pored toga ova specifikacija sadrži opće mehanizme za prihvat sigurnosnih *token*a od strane poruka. Ne zahtjeva se specifični oblik sigurnosnog *token*a. Specifikacija je dizajnirana tako da može podržati višestruke formate sigurnosnih *token*a. Na primjer klijent može osigurati jedan format *token*a za dokaz identiteta, a isto tako može osigurati drugi format kako bi dokazao da posjeduje specifičnu poslovnu certifikaciju. Pored toga ovaj dokument opisuje kako kodirati binarne sigurnosne *token*e, definira radni okvir za XML temeljene *token*e te opisuje kako uključiti ključeve za enkripciju. Isto tako uključuje mehanizme proširenja koji se mogu upotrijebiti za daljnji opis svojstava *token*a koji su uključeni s porukama. Ova specifikacija je fleksibilna i dizajnirana tako da se može koristiti kao osnova za osiguranje Web servisa unutar različitih sigurnosnih modela uključujući PKI, Kerberos i SSL. Posebno, ova specifikacija podržava višestruke sigurnosne *token*e, višestruke domene povjerenja, višestruke formate elektroničkih potpisa kao i više vrsta tehnologija kriptiranja. Specifikacija sadrži tri glavna mehanizma, mogućnost slanja sigurnosnih *token*a kao dio poruke, integritet poruke te povjerljivost (tajnost) poruke. Ovi mehanizmi ne pružaju potpuno sigurnosno rješenje za Web servise nego daju blokove za građenje koji se mogu koristiti s drugim proširenjima Web servisa i specifičnim protokolima na višim aplikativnim razinama kako bi omogućili realizaciju različitih sigurnosnih modela i sigurnosnih tehnologija. Ovi mehanizmi se mogu koristiti potpuno odvojeno (npr. dostava sigurnosnih *token*a) ili na potpuno uvezan način (npr. potpisivanje i kriptiranje poruka, osiguranja puta *token*a zajedno sa ključevima za potpisivanje i enkripciju).

- *Username Token Profile* 1.1 (http://www.oasis-open.org/committees/download.php/16782/wss-v1.1-spec-os-UsernameTokenProfile.pdf). Ovaj dokument opisuje kako koristiti *UsernameToken* sa WSS *core* specifikacijama. On opisuje kako korisnik Web servisa dostavlja *UsernameToken* kao način identifikacije korištenjem "korisničkog imena" i proizvoljnog korištenja lozinke (ili dijeljenje tajne ili nekog ekvivalenta lozinke) kako bi se korisnik autentificirao kod dobavljača Web servisa.

- X.509 *Token profile* 1.1 (http://www.oasis-open.org/committees/download.php/16785/wss-v1.1-spec-os-x509TokenProfile.pdf). Ovaj dokument opisuje kako koristiti X.509 certifikate sa WSS uslugama: SOAP *Message Security* specifikacijom (WS-*Security*). X.509 certifikat specificira vezu između javnog ključa i skupa atributa (najmanje), ime subjekta, ime tko je izdao certifikat, serijski broj i period valjanosti certifikata. Ova veza može bit predmetom opoziva uz pomoć mehanizma za objavu što uključuje publiciranje CRL (*Certificate Revocation List*) liste opoziva certifikata, OCSP (*Online Certificate Status Protocol*) *token*a ili mehanizama koji su izvan X.509 okvira, kao što je XKMS (XML *Key Management Specification*). X.509 može se koristiti za validaciju javnog ključa koji se koristi za autentifikaciju SOAP poruka ili za identifikaciju javnog ključa sa SOAP porukom koja je bila kriptirana.

- *SAML Token profile 1.1* (http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf). Ovaj dokument opisuje kako upotrijebiti *Security Assertion Markup Language* (SAML) V1.1 i V2.0 potvrde sa *Web Services Security* (WSS): SOAP *Message Security* V 1.1 specifikacijom. Ova specifikacija opisuje upotrebu SAML potvrda kao sigurnosnih tokena kroz *<wsse: Security>* zaglavlje koje je definirano sa WSS: SOAP *Message Security* specifikacijom. Cilj ove specifikacije je definiranje upotrebe SAML potvrda u kontekstu WSS: SOAP *Message Security* uključujući potrebu sigurnosti SOAP poruka te razmjene SOAP poruka. Da bi se postigao ovaj cilj, ovaj profil opisuje kako se:

    - SAML poruke prenose i referenciraju iz *<wsse: Security>* zaglavlja

    - SAML poruke koriste sa XML potpisom kako bi objedinili subjekte i izjave o potvrdama (tj. dokaza o pravima) na SOAP poruci.

- Ova specifikacija proširuje model obrade procesno neovisnih tokena koji su definirani WSS: SOAP *Message Security* specifikacijom. Kada primatelj obrađuje *<wsse: Security>* zaglavlje koje sadrži referencu na SAML potvrdu, on odabire, na temelju svoje politike, potpise i izjave koje će on obraditi. Pretpostavlja se da politika odabira prijemnog potpisa smije ležati na semantičkom označavanju *<wsse:SecurityTokenReference>* elementa koji se pojavljuju u *<ds:KeyInfo>* elementima unutar potpisa. Također se pretpostavlja da će potvrde koje su odabrane za validaciju i obradu uključivati i one koje se referenciraju iz *<ds:KeyInfo>* i *<ds:SignedInfo>* elemenata selektiranog potpisa. Kao dio svoje validacije i obrade odabranih potvrda primatelj mora uspostaviti odnos između subjekata i potvrda (dokaza o pravima) SAML naredbi (od referencirajućih SAML potvrda) i entiteta koji osiguravaju dokaz koji zadovoljava metodu potvrđivanja koja je definirana za naredbe (tj. atestirajući entitet). U specifikaciji su definirane dvije metode za uspostavu ovih odnosa koje se moraju implementirati kroz primjenu ove specifikacije.

- *Kerberos Token Profile* 1.1 (http://www.oasis-open.org/committees/download.php/16788/wss-v1.1-spec-os-KerberosTokenProfile.pdf). Ova specifikacija opisuje upotrebu Kerberos (Kerb) tokena u odnosu na WSS: SOAP *Message Security* specifikaciju (WSS). Posebno, ovaj dokument definira kako kodirati Kerberos karte te kako ih spojiti na SOAP poruke. Jednako tako ova specifikacija opisuje kako dodati potpise i enkripciju na SOAP poruke, a u skladu sa WSS: SOAP *Message Security* specifikacijom koja koristi i referencira Kerberos tokene. Zbog interoperabilnosti, te zbog nekih sigurnosnih razloga, specifikacija je ograničena na korištenje AP-REQ paketa (karta usluge i autentifikator) kako je definirano Kerberosom i Kerberos *token*om. Time je omogućena usluga autentifikacije karte sa postojećom Kerberos implementacijom.

- *Rights Expression Language* (REL) *Token profile* 1.1 (http://www.oasis-open.org/committees/download.php/16687/oasis-wss-rel-token-profile-1.1.pdf). Ovaj dokument opisuje kako upotrijebiti ISO/IEC 21000-5 *Rights Expressions* sa WSS specifikacijom. WSS: SOAP *Message Security* (WS-*Security*) specifikacija predlaže standardni skup SOAP proširenja koja se mogu koristiti kod izgradnje sigurnih WEB servisa kako bi se implementirala sigurnost poruka kroz očuvanje integriteta i tajnosti poruka.

- SOAP *with Attachments* (SwA) *profile* 1.1 (http://www.oasis-open.org/committees/download.php/16672/wss-v1.1-spec-os-SwAProfile.pdf). Ovaj dokument opisuje kako upotrijebiti *Web Services Security*: SOAP *Message Security* normu (WSS-*Security*) sa SOAP *Messages with Attachments* (SwA). Detaljnije rečeno, ova specifikacija opisuje kako korisnik Web servisa može osigurati SOAP dodatke koristeći SOAP *Message Security* normu za očuvanje integriteta, tajnosti i autentičnosti izvora dodatka, te kako primatelj može obraditi takvu poruku. U širokom području gospodarstva od automobilske industrije, osiguranja, financija, medicine, maloprodaje i dr. zahtjeva se da aplikacijski podatci budu zaštićeni od izvora do krajnjih korisnika. Dok su neki od tih podataka u XML obliku, velika većina nije. Kako bi se osigurali sigurni Web servisi i rješenja i u tim slučajevima potrebna je interoperabilna norma za sigurnost s kraja na kraj *(end-to-end*) kako za XML tako i za ne XML podatke. Provođenje SwA sigurnosti pomaže u interoperabilnosti između tvrtki i partnera u e-Poslovanju koristeći dodatke koji prenose ne-XML podatke koji nisu nužno povezani na XML teret (*payload*). Mnoge grane gospodarstva kao osiguravajuća društva zahtijevaju izmjenu dokumenta u slobodnom formatu koji je povezan sa porukama Web servisa. Stoga je ova SwA specifikacija neobična važna. Pored toga ovom specifikacijom je omogućeno da se dio sadržaja, koji je dio SOAP tijela, može se prenijeti kao dodatak, kako bi se smanjio utjecaj na veličinu i obradu XML poruke, a kako bi se osigurala sigurnost dodatka koji preuzima dio tog sadržaja.

1.2.3. Interoperabilni sigurni WEB servisi (WS-I *Basic Security Profile* 1.0)

WS-I (*Web Services-Interoperability*) organizacija publicirala je dokument WS-I *Basic Security Profile* 1.0 (http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html) koji je temeljen na nevlasničkim specifikacijama za Web servise zajedno sa pojašnjenjima i dopunama tih specifikacija koje promoviraju interoperabilnost. WS-I *Basic Security Profile* radna grupa razvila je interoperabilni profil koji je povezan sa sigurnošću transporta, sigurnošću razmjena SOAP poruka te ostalim osnovnim profilima koji su orijentirani na sigurnost Web servisa. Usklađenost s ovim specifikacijama se definira kao poštivanje skupa zahtjeva koji su definirani za specifični cilj unutar opsega određenog profila. Ovi zahtjevi definiraju kriterije za usklađenost s profilima. Oni se tipično odnose na postojeće specifikacije i sjedinjena usklađenja, proširenja, interpretacije i pojašnjenja kako bi se poboljšala interoperabilnost. Svi zahtjevi u ovom dokumentu se smatraju normativnim pa se i specifikacije koje se u njemu referenciraju također smatraju normativnim. Ciljevi usklađenosti (npr. SECURE_ENVELOPE, SECURE_MESSAGE, SENDER, RECEIVER, SECURITY_HEADER, ENCRYPTED_KEY, SIGNATURE, SECURITY_TOKEN) identificiraju zahtjeve koji se primjenjuju na podatkovne stavke (npr, SOAP poruke, WSDL opis, UDDI *registry data*) ili na sudionike u komunikaciji (npr. SOAP *processor*, krajnji korisnik). To omogućava definiranje usklađenosti za različite kontekste primjene, kako bi se osigurala nedvosmislena interpretacija primjene zahtjeva kao i testiranje usklađenosti podatkovnih stavaka (npr. SOAP poruka, WSDL opisa) i ponašanja različitih sudionika u izvođenju Web servisa (npr. klijenti, servisi) .

1.3. ebXML *Messaging Services* (ebMS - *Security Module*)

ebXML (*Electronic Business using eXtensible Markup Language*) je modularni skup specifikacija koji omogućava tvrtkama bilo koje veličine na bilo kojem geografskom području vođenje poslovanja uz upotrebu Interneta. Korištenjem ebXML-a tvrtke imaju na raspolaganju standardnu metodu za razmjenu poslovnih poruka, provođenje trgovinskih odnosa, komunikaciju podataka na zajedničkoj osnovi kao i definiranje i registraciju poslovnih procesa. Usluge razmjene ovih poruka dane su kroz dvije verzije ebMS specifikacije:

- ebXML *Messaging Services* V: 2.0
- ebXML *Messaging Services* V: 3.0

koje su opisane u nastavku.

1.3.1. ebXML *Messaging Services* V: 2.0

ebXML *Messaging Service* norma V: 2.0 (http://www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0.pdf) osigurava sigurnu metodu razmjene elektroničkih poslovnih transakcija kroz korištenje Interneta. Ova specifikacija proširuje postojeće stanje sigurne i pouzdane razmjene podataka za potrebe izvođenja e-Poslovanja, naročito za EDI preko Interneta i za poslovno kvalitetne Web servise. Sa naglaskom na B2B sigurnost, pouzdanost i proširljivost,

ova specifikacija premošćuje postojeće EDI sustave sa pojavom infrastrukture i tehnologije koja je zasnovana na Web servisima, interaktivnim uzorcima i XML dokumentima - koji su relevantni i atraktivni za sljedeću generaciju B2B načina rada. Stoga ova specifikacija igra važnu ulogu u tranziciji e-Poslovanja od lokalnih privatnih mreža na Internet. Štoviše ova specifikacija definira fleksibilan sustav formiranja ovojnica čime je omogućeno da poruke mogu sadržavati teret bilo kojeg formata.

Ova specifikacija pokriva sljedeće ključne funkcionalnosti:

- Specifikaciju za pakiranje poruka - opis kako pakirati ebXML poruke i njihove pripadne dijelove u oblik koji se može slati korištenjem komunikacijskog protokola kakav je HTTP ili SMTP

- Proširenja za ebXML SOAP ovojnicu - specifikaciju strukture i sastav informacija za servisiranje i obradu ebXML poruka

- Obrada grešaka - opis kako ebXML *Message Service* izvještava o greškama koje detektira prema ebXML *Message Service Handler* (MSH)

- Sigurnost - osigurava specifikacije za sigurnosnu semantiku ebXML poruka

- *SyncReply* - ukazuje slijedećem MSH-u da li treba ili ne sinkrono vratiti odgovor

Jedan od glavnih modula ove specifikacije je svakako Modul sigurnosti (*Security Module*) koji je posebno razrađen. U tom svom dijelu specifikacija opisuje skup profila, ili kombinacije selektiranih sigurnosnih kontrola, koje su odabrane na ključnim rizicima zasnovanim na opće raspoloživim tehnologijama. Svaki od specificiranih profila uključuje opis rizika koji nisu njime pokriveni. Arhitektura ovih profila je uspostavljena u namjeri da osigura sigurnosne servise potrebne za e-Poslovanje. Ovi profili ili njihova kombinacija podržavaju specifične sigurnosne politike za ebXML korisničku zajednicu. Osnovni servisi koji su zadovoljeni ovim profilima odnose se na integritet, tajnost, autentifikaciju, autorizaciju, digitalno potpisivanje u odašiljanju i prijemu te vremensko označavanje.

Za ovu specifikaciju pojam potpisane poruke znači svaku poruku koja sadrži Signaturni element (*Signature Element*) koji pripada XML Signature (XMLDSIG) imenovanom prostoru (specifikaciji), a koji je prisutan kao dijete SOAP zaglavlja.

Implementatori ove norme moraju znati da postoji ranjivost, iako se koristi XML Digital Signature, kako bi se zaštitio integritet i izvor ebXML poruka. Značaj ove ranjivosti ovisi o okolini implementacije i transportu koji se koristi za razmjenu ebXML poruka. Ta ranjivost je prisutna budući je ebXML razmjena poruka integracija XML-a i MIME tehnologije. Uvijek kada se koriste više tehnologija rezultat su dodatni sigurnosni problemi koje treba adresirati. U ovom slučaju MIME se koristi kao okvir za pakiranje poruka koje sadrže SOAP ovojnicu (Envelope) i bilo

koji kontejner tereta (*payload*). Različiti elementi SOAP ovojnice referenciraju terete koji se identificiraju kroz MIME mehanizme. Pored toga različite oznake su duplicirane u SOAP i MIME okruženju. Pored toga MIME zaglavlja nisu zaštićena kroz primjenu XML digitalnog potpisa što može dovesti do DoS (Denial of Service) napada. Zbog svega navedenog potrebno je ozbiljno razmotriti i smanjiti postojeću ranjivost ovog sustava za razmjenu poruka.

1.3.2. ebXML *Messaging Services* V.3.0

Gore navedena svojstva odnose se na EbXML MS V.2.0. U cilju što veće interoperabilnosti i što širem korištenju postojećih norma i specifikacija donesena je nova verzija ebXMl *Message Services* V: 3.0 : *Part* 1, *Core Features* (http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/ebms_core-3.0-spec.pdf). Njezin drugi dio (*Advanced Features*) je u izradi. Ova specifikacija definira povezivanje na opće prihvaćenu tehnologiju Web servisa na koje dograđuje, primjenom konstrukcija ovojnica, rješenja za sigurnost razmjene poslovnih informacija različitih oblika i formata. Tako da se i tradicionalni EDI formati mogu prenositi putem ebMS-a. Ova specifikacija definira funkcije, protokole i ovojnice koje rade iznad SOAP (SOAP 1.1 i SOAP *with Attachments*) protokola. Povezivanje na niže protokole kao što su HTTP i SMTP leži na standardnom povezivanju SOAP protokola koji postoji, a ebMS samo specificira neke komplementarne zahtjeve. Ova verzija ebMS specifikacije koristi već postojeću SOAP specifikaciju za obradu QoS (*Quality of Service*) u području pouzdanosti i sigurnosti, u ebMS kontekstu. Glavni izbor u dizajnu ove specifikacija je specifikacija za MSH (*Message Service Handler*) i njegovih pridruženih pravila za korištenje sigurnosnih norma za Web servise, koje su prethodno dane. Ova verzija ebMS-a je bitno sukladnija od prethodne verzije ebMS-a (verzija 2.0) s modelom obrade SOAP protokola i prikladnija je za korištenje *Web Service Security* (WS-*Security*) norma i specifikacija kroz definirana SOAP proširenja.

Sukladnost implementacije ebMS 3 s posljednjom verzijom WS-I profila vrlo je značajno svojstvo ove specifikacije. U pogledu očuvanja sigurnosti ova specifikacija koristi u potpunosti normu *Web Services Security* (WS-*Security*) V1.0 ili V1.1. Kako je prethodno navedeno WS-*Security* koristi tri mehanizma za sigurnost poruka: mogućnost slanja sigurnosnih *token*a kao dijela ebMS poruke, integritet i tajnost poruke.

Sigurnosni elementi koji pripadaju WSS-u (WS-*Security*) prisutni su kao dijete SOAP zaglavlja prema usvojenoj specifikaciji za norme WSS-a. Ova specifikacija ocrtava korištenje *Web Services Security* X.509 *Certificate Token Profile*-a ili korištenje WSS *Username Token Profile*-a. Implementacija MSH može koristiti jedan od gore navedenih *token*a.

Potpisivanje ebMS poruka definirano je kroz WSS. Podrška za X.509 *Certificate Token Profile* je obavezna kako bi se poruka mogla potpisati. Za enkripciju ebMS poruka također se zahtjeva korištenje X.509 *Certificate Token Profile*-a.

U ograničenim uvjetima, gdje nije moguća primjena X.509 *Certificate Token Profile*-a za autentifikaciju, dozvoljava se primjena WSS *Username Token Profile*-a.

1.4. e-Identitet

Uvođenje e-Identiteta je nužnost za ostvarenje svih prethodnih funkcija sigurnosti za e-Poslovanje. Bez jasno definiranog identiteta u sustavu e-Poslovanja nemoguće je provesti odgovorno i povjerljivo poslovanje. U cilju ostvarenja globalizacije osim sigurnosti nužan je i zahtjev interoperabilnosti stoga je normizacija u ovom području nužna i neizbježna. Osnovni koncept na kojem se zasnivaju sve poslovne transakcije je identifikacija, autentifikacija i elektronički potpis (**IAS** - *Identification, Authentication, Signature*). Ova normizacija zasniva se direktivama Europske unije i to:

- **1999/93/EC (**http://portal.etsi.org/esi/Documents/e-sign-directive.pdf**)** za elektronički potpis i
- **95/46/EC (**http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf**)** za zaštitu osobnih podataka na *token*ima za elektronički identitet.

Realizacija e-Identiteta provodi se kroz korištenje *token*a za elektronički identitet koji su danas najčešće, prema preporuci EU, ICC (*Integrated Circuit Card*) kartice. Najčešće se koriste pametne kartice (*smart card*). Jedan takav primjer je i preporuka EU za uvođenje ECC (*European Citizenship Card*) kartica koja treba postati sve europska kartica za elektronički identitet. S tim u vezi formirano je nekoliko radnih grupa i odbora (Provoo *Group*, CEN/TC 224 (WG 15, WG16 i WG17) , ICAO - *International Civil Aero Organisation*, JTC1/SC17,SC37), koje donose preporuke na kojima se zasniva i ova normizacija koja je dana u nastavku, i to prema tijelima koja su njihovi donosioci.

1.4.1. ISO (*International Organization for Standardization*)

Norme koje su ovdje specificirane odnose se na identifikacijske kartice realizirane kao ICC kartice koje su specificirane u poglavlju 3.2 ovog dokumenta. Preostale norme koje ovdje nisu navedene, a odnose se na pametne kartice, nalaze se također u poglavlju 3.2 (pametne kartice) ovog dokumenta.

- **ISO 24727- (1-3)** *Identification cards - Integrated circuit card programming interfaces.* Ova norma je skup programskih sučelja za vezu ICC kartica i vanjskih aplikacija kako bi se uključili generički servisi za upotrebu u različitim sektorima primjene. Organizacija i operacije ICC kartica sukladni su s ISO 7816-4 normom. Ova norma je relevantna za ICC aplikacije za koje se zahtjeva interoperabilnost između različitih aplikacijskih domena. Norma definira sučelja tako da su nezavisne implementacije međusobno interoperabilne. Ona se sastoji od tri dijela:

    - Part 1: Architecture
    - Part 2: Generic card interface
    - Part 3: Application interface

- **ISO 19794-(1-8)** *Information Technology -- Biometric data interchange formats.*
  To je skup norma koje definiraju razmjenu biometrijskih podataka vlasnika ICC kartice i vanjskih aplikacija. Sastoji se od više dijelova ovisno o vrsti biometrijskih podataka koji su vezani za identitet osoba:

    - *Part 1: Framework*
    - *Part 2: Finger minutiae data*
    - *Part 3: Finger pattern spectral data*
    - *Part 4: Finger image data*
    - *Part 5: Face image data*
    - *Part 6: Iris image data*
    - *Part 7: Signature/sign behavioral data*
    - *Part 8: Finger pattern skeletal data*

- **ISO 9594-8** *Information technology — Open Systems Interconnection — The Directory: Public key and attribute certificate frameworks* (opisano u poglavlju 1.1 (e-Potpis) ovog dokumenta)
- **ISO 7816 (1-9)** *Identification Cards - Integrated Circuit Card(s) with contacts.* (opisano u poglavlju 3.2 (pametne kartice) ovog dokumenta)
- **ISO 7816 - 13** *Identification cards − Integrated circuit cards − Part 13: Commands for application management in multi-application environment* (opisano u poglavlju 3.2 (pametne kartice) ovog dokumenta)

- **ISO 7816 -15** *Identification Cards - Integrated Circuit Card(s) with contacts : Cryptographic information application* (opisano u poglavlju 3.2 ovog dokumenta)
- **ISO 14443-(1-4)** *Identification cards — Contactless integrated circuit cards - Proximity cards.* Ova norma definira korištenje ICC kartica za identifikaciju kroz blisko, bez kontaktno čitanje, a koristi standardni format, ID-1 definiran u normi ISO 7810. Ova norma se sastoji od četiri dijela i opisuje dvije vrste kartica: A i B. Glavna razlika između ove dvije vrste kartica je metoda modulacije, shema kodiranja (*Part* 2) te procedure protokola inicijalizacije (*Part* 3). Obje vrste kartica koriste isti transmisijski protokol koji je opisan u *Part* 4. Dijelovi norme su:

    - *Part 1: Physical characteristics*
    - *Part 2: Radio frequency power and signal interface*
    - *Part 3: Initialization and anticollision*
    - *Part 4: Transmission protocol*

- **ISO 15693 - (1-4)** *Identification Cards - Contactless integrated circuit cards - Vicinity cards.* Ova norma se odnosi na korištenje bez kontaktnih ICC kartica koje se mogu čitati s veće udaljenosti nego "*proximity*" kartice. Kartice se mogu pričvrstiti na torbe, vrijedne predmete, novčanike i druge predmete. Norma specificira fizičke karakteristike kartice, sučelja te protokole za inicijalizaciju, transmisiju i antikoliziju. Dijelovi norme su:

    - *Part 1: Physical characteristics*
    - *Part 2: Air interface and initialization*
    - *Part 3: Anticollision and transmission protocols*
    - *Part 4: Extended command set and security features*

- **ISO 15946** *Cryptographic techniques based on elliptic curves*. (definirano i opisano u poglavlju 1.1 (e-Potpis) ovog dokumenta)

1.4.2. CEN/TC 224 - CEN/*Technical Committee* 224

CEN (*European Commission for Standardisation*) je osnovala tehničko povjerenstvo CEN/TC 224 za harmonizaciju različitih e-Identiteta za građane EU sa zadatkom donošenja specifikacija koje će definirati:

- Kartice i pripadna sučelja
- Biometričke formate
- Osobnu identifikaciju što uključuje autentifikaciju i povjerljivost
- Elektronički potpis

- Minimalni skup podatkovnih elementa za interoperabilnost
- Upravljanje životnim ciklusom kartica

Ove specifikacije moraju biti zasnovane na postojećim normama i direktivama EU. U okviru tog povjerenstva osnovane su radne grupe:

- WG 15 ECC - *European Citizen Card*
- WG 16 *Application Interface for smart cards used as Secure Signature Creation Device* (SSCD)
- WG 17 *Protection profiles in the context of* SSCD .

U okviru radne grupe WG 15 ECC - *European Citizen Card* donesene su tehničke norme i specifikacije koje definiraju servise i mehanizme koje treba usvojiti kako bi se osigurala svojstva produkata koji zadovoljavaju funkcionalne zahtjeve (IAS servise), zahtjeve na korištenje tih produkata te njihovu integraciju u različitim okolinama. Ove norme osiguravaju izvjesnu razinu nužne interopearbilnosti u korištenju e-Identiteta (eID tokena). Stoga se ova interoperabilnost postiže kroz otvorene norme koje predstavljaju centralni element za interoperabilan eID sustav upravljanja. *European Citizen Card* (ECC) nije niti fizička kartica niti specifična kartična aplikacija ili skup aplikacija, nego definicija logičkih grupa podataka i servisa koji se mogu osigurati za bilo koju karticu (eID *token*) koju izdaje Vlada za svoj vlastiti aplikacijski kontekst, npr, eID *token* za potrebe javne administracije i dr. ECC specifikacije sastoje se od četiri dijela koji su dani u nastavku:

- **CEN/TS 15480-1** *Identification card systems - European Citizen Card - Part 1: Physical, electrical and transport protocol characteristic* (http://www.evs.ee/Checkout/tabid/36/screen/freedownload/productid/165215/doclang/en/preview/1/CEN_TS_15480_1;2007_en_preview.aspx). Ova tehnička specifikacija definira zahtjeve za ECC kartice. ECC je pametna kartica koja je izdana od strane Vlade, nacionalne ili lokalne, a nosi podatke kako bi se osigurali sljedeći servisi:
    - Verifikacija identiteta
    - Dokument za putovanje unutar EU
    - Omogućiti logički pristup sustavima e-*Government* ili servisima lokalne administracije

  Ovi zahtjevi se koriste kako bi se:
    - Definirale plastične kartice sa svojstvima fizičke i logičke sigurnosti
    - Specificirala električna sučelja i transportni protokoli za ECC
    - Osigurao osnovni skup identifikacijskih i autentifikacijskih elementa koji su vidljivi na površini kartice.

  Ova norma se referencira na specifikacije za pametne kartice kao što su ISO 7810, ISO 7816 i ISO 14443. Isto tako ona slijedi ICAO (*International Civil*

Aero Organization) preporuke za MRTD (*Machine Readable Travel Document*) u ID-1 formatu. Ne postoje ograničenja na korištenje sučelja za kartice (kontaktno, bez kontaktno ili dualno).

- **CEN/TS 15480-2** *Identification Card systems - European Citizen Card - Part2 : Logical data structure and card services* (http://www.evs.ee/Checkout/tabid/36/screen/freedownload/productid/165216/doclang/en/preview/1/CEN_TS_15480_2;2007_en_preview.aspx. Ovaj dio ECC normizacije definira kartične servise koji su obvezatni za građane EU, te proširenja koja su opcionalna. Ova tehnička specifikacija definira logičke karakteristike i sigurnosna svojstva sučelja kartica/sustav za ECC kartice. ECC kartica je pametna kartica sa servisima za identifikaciju, autentifikaciju i elektroničko potpisivanje IAS (*Identification, Authentication, Signature*) . IAS servisi su uglavnom zasnovani na procedurama za javne ključeve, tj. na RSA operacijama, iako je moguće koristiti kriptografiju javnih ključeva primjenom eliptičkih krivulja, što može biti određena prednost. U specifikaciji su navedeni ovi servisi, struktura podataka i pristup tim podatcima te je definiran skup naredbi koji to omogućava. Definicije servisa i komandi nisu ograničeni na specifičnu tehnologiju sučelja. Ipak pojedina vrsta sučelja,bez kontaktno sučelje, može imati specijalni tretman u postizanju dodatne sigurnosti u odnosu na kontaktno sučelje. Kako bi se osigurala interoprabilnost, IAS servisi su sukladni s normama CWA 14890-1 i CWA 14890-2 koje su navedene u nastavku.

- **CEN/TS 15480-3** *Identification card systems - European Citizen Card - Part 3: ECC Interoperability using API Interface* (*draft*). Ova norma će definirati interoperabilni model koji će osigurati IAS servise koji će biti usklađeni s tehničkim zahtjevima, kako bi se osigurala interoperabilnost različitih implementacija ECC kartica. Ovaj model će biti razvijen tako da slijedi iz CEN/TS 15480-2 norme, a osigurava dodatne tehničke specifikacije za posredničku (*middleware*) arhitekturu koja je zasnovana na ISO 24727 normi. API osigurava klijentskoj aplikaciji IAS servise koji su podržani od ECC-a. ECC *middleware* provjerava funkcionalnost podržanu od kartice čitajući određene sadržaji na kartici, čime se određuje upotrebna vrijednost eID *token*a (kartice). *Middleware* sa kartice komunicira sa klijentskom aplikacijom bez obzira na primijenjeno kartično sučelje. Ova norma još nije usvojena.

- **CEN/TS 15480-4** *Identification card systems -European Citizen Card - Part 4 Recommendations for ECC Issuance, operation and use* (*draft*). Ova norma će predložiti procedure izdavanja i upotrebe kartica uključujući i registraciju građana. Ova norma ujedno će identificirati skup standardnih upotreba (profila) ECC kartica (nacionalni ID, kartice za e-Vlada, e-Poslovanje, i dr.). Svaki od ovih profila sadrži jednu ili više aplikacija. Za svaki od ovih slučajeva korištenja (profila) norma će specificirati zahtjeve iz CEN/TS 15480-1 i CEN/TS 15480-2 normi, sučelja i transportne protokole te načine rada za svaki pojedinačni slučaj korištenja. Minimalni skup funkcija koje treba zadovoljiti su IAS servisi. Između tih profila najvažniji su :

- **Profil 1 - ID** *card* koji opisuje karticu koja se koristi kao dokument za identifikaciju
- **Profil 2 - ESIGN-K** koja se koristi za aplikaciju elektroničkog potpisa (ESIGN) te opcije za dodatnu funkcionalnost za elektronički potpis
- Pored gore navedenih profila moguće je dodavati proizvoljne profile kroz WG 15 grupu, budući da ova norma sadrži obrasce za formiranje novih profila. Svaka zemlja EU-a može dodavati i svoje specifične profile za vlastite potrebe.

Ova norma još nije usvojena.

Radna grupa **WG 16** *Application Interface for smart cards used as Secure Signature Creation Device (SSCD)* donosi slijedeće specifikacije:

- **CWA 14890-1** *Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements*. (ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14890-01-2004-Mar.pdf). Ovaj dokument opisuje normizaciju i rješenja za pametne kartice kao specijalnog uređaja za kreiranje elektroničkog potpisa (SSCD - *Secure Signature Creation Device*). Ključna stvar u ovom dokumentu je kako omogućiti interoperabilnost, tako da pametne kartice različitih proizvođača mogu komunicirati s različitim aplikacijama koje generiraju elektroničke potpise. Ova specifikacija je podjednako prikladna za pametne kartice koje podržavaju datotečno usmjerene aplikacije kao i objektno usmjerene aplikacije (Java apleti). Specifikacija se zasniva na EU direktivi za elektronički potpis (1999/93/EC) te na svim normama za elektronički potpis koje su proistekle iz te direktive.

- **CWA 14890-2** *Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services* (ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14890-02-2004-May.pdf). Ovaj dokument sadrži specifikacije za dodatne servise, koji se ne zahtijevaju za generiranje elektroničkih potpisa. Ipak, ovi servisi se često koriste u kontekstu aplikacija za elektronički potpis. Ovi servisi se zasnivaju na istoj tehnologiji koja je raspoloživa i za uređaje za elektroničke potpise. To uključuje dekripciju upotrebom ključa, autentifikaciju nositelja kartice ili servera, verifikaciju potpisa kao i pripadne informacije kriptografskog tokena. Ove definicije su usklađene s normom ISO 7816-4 koja je opisana u poglavlju 3.2 (pametne kartice).

Radna grupa **WG 17** *Protection profiles in the context of* SSCD donosi slijedeće specifikacije:

- **CWA 14169** *Secure Signature-Creation Devices* "EAL 4+. Nova norma donijet će poboljšanje i unapređenje postojeće norme CWA 14169 koja je opisana u poglavlju 1.1 (e-Potpis) ovog dokumenta, a odnosi se na primjenu pametnih kartica za generiranje elektroničkih potpisa. (u izradi).

1.4.3. CEN Information Society Standardization System *(CEN/ISSS)*

- **CWA 14171-00** *General guidelines for electronic signature verification* (definirano i opisano u poglavlju 1.1 (e-Potpis) ovog dokumenta)

1.4.4. *ETSI* (*European Telecommunication Standards Institute*)

Sve dolje navedene norme opisane su u poglavlju 1.1 (e-Potpis) ovog dokumenta.

- **ETSI QCP 101 456** *Policy Requirements for Certification Authorities Issuing Qualified Certificates*
- **ETSI TS 101 733** *Electronic Signature Format*
- **ETSI TS 101 862** *Qualified Certificate Profile*
- **ETSI TS 102 042** *Policy requirements for certification authorities issuing public key certificates*
- **ETSI TS 102 280** - X.509 V.3 *Certificate Profile for Certificates Issued to Natural Persons*

1.4.5. RSA *Laboratories - Public Key Crypto Standards* (PKCS)

Sve dolje navedene norme opisane su u poglavlju 1.1 (e-Potpis) ovog dokumenta.

- **PKCS 1** RSA *Encryption Standard*.
- **PKCS 5** *Password-based Cryptography Standard*
- **PKCS 7** *Cryptographic Message Syntax Standard*
- **PKCS 9** *Selected Attribute Types*
- **PKCS 10** *Certification Request Syntax*
- **PKCS 11** *Cryptographic Card Interface Standard*
- **PKCS 15** *Cryptographic Token Information Syntax Standard*

1.4.6. IETF/RFC (Internet Engineering Task Force/Request for Comment)

Sve dolje navedene norme opisane su u poglavlju 1.1 (e-Potpis) ovog dokumenta.

- **RFC 2256** *A Summary of the* X.500(96) *User Schema for use with* LDAPv3

- **RFC 2251** *Lightweight Directory Access Protocol* (v3)
- **RFC 3280** *Internet* X.509 *Public Key Infrastructure Certificate and Certificate Revocation List* (CRL) *Profile*
- **RFC 3739** *Internet* X.509 *Public Key Infrastructure: Qualified Certificates Profile*

2. Norme za definiranje strukture i semantike u e-Poslovanju

2.1. ISO/TS 15000-5: *Core Components Technical Specification*

http://www.unece.org/cefact/ebxml/CCTS_V2-01_Final.pdf

CCTS je namijenjen za definiranje semantičkog značenja poslovnih dokumenta i njihovih sastavnih elemenata na način da definira poslovne pojmove kao samostalne komponente činim grupiranjem nastaju cjeloviti poslovni dokumenti. U specifikaciji je opisana metodologija za razvoj zajedničkog skupa semantičkih građevnih blokova koji prezentiraju općenite tipove poslovnih podataka koji se danas koriste. CCTS koncept definira novu paradigmu u dizajniranju i implementaciji ponovno iskoristivih, sintaksno neutralnih informacijskih građevnih blokova.

Razvoj na CCTS je započet u sklopu ebXML inicijative, a nastavljen je pod okriljem UN/CEFACT. CCTS je prihvaćen kao ISO norma 2005. godine pod nazivom ISO/TS 15000-5:2005. CCTS - skraćeno *Core Components* (CC) je razvijena i održava se u UN/CEFACT-u. UN/CEFACT na temelju CC norme dva puta godišnje objavljuje i ažurira biblioteku ključnih podatkovnih komponenti - CC *library* (CCL) koja nosi oznaku CCL + godina + A ili B tako da trenutno najsvježija verzija biblioteke (stanje studeni 2008.) nosi oznaku CCL08A.

Koncepte definiranja i izgradnje poslovnih dokumenta prihvatile su vodeće međunarodne norme u domeni elektroničkog poslovanja.

Prva norma koja se temelji na CCTS-u je *Universal Business Language* (UBL) koja je u trenutnoj verziji 2.0. Podatkovne komponente koje se koriste za izgradnju UBL dokumenata su u početku preuzete iz biblioteke CCL, a kasnije je razvoj krenuo odvojeno. Danas je situacija takva da CCL ima nekoliko puta više definiranih komponenti od UBL-a. Razlog ovog odstupanja moguće je naći u činjenici da CCL pokriva puno veće područje nego li je to slučaj kod UBL-a.

GS1 XML razvoj poruka je baziran na *Global Data Dictionary* (GDD) (www.gs1.org/productssolutions/ecom/xml/overview/). GDD je repozitorij u kojem se nalaze podatkovne komponenti koje se koriste za izgradnju GS1 XML norme i koje su razvijene prema CCTS-u i poslovni termini i njihova reprezentacija u GS1 XML-u i ostalim ciljnim normama. GS1 *Core Components* su predane kao unos UN/CEFACT-u.

CEN *Workshop Agreement* (CWA) dokumenti koji se odnose na opis poslovnih zahtjeva (*Business requirements specifications*) također su izgrađeni koristeći koncepte CCTS-a. Komponente koje su koriste za izgradnju informacijskih modela prikazanih u CWA dokumentima još nisu sastavni dio CCL biblioteke.

Open Applications Group Integration Specification (OAGIS) norma je jedna od prvih međunarodnih norma koje se temelje na XML-u i čija namjena je semantički i sintaksno definirati poslovne dokumente. Od 2006. godine strateško opredjeljenje OAGIS-a je da se sve nove verzije temelje na CCTS-u. Sve verzije 9.x i nadalje se temelje na CCTS-u.

UNeDOCs je zajednički projekt *United Nations Economic Commission for Europe* (UNECE) i SITPRO Ltd. UNeDOCs dokumenti u papirnatom i elektroničkom obliku se temelje na zajedničkom podatkovnom modelu iz kojeg se isti podaci mogu koristiti u različitim dokumentima. Podatkovni model UNeDOCs-a se temelji na CCTS/ISO 15000 *Part* 5 reviziji iz 2004 UNTDED/ISO 7372.

Implementacija CCTS specifikacije u vodećim međunarodnim normama ukazuje da se radi o dugovječnoj normi koja služi kao temelj za izgradnju poslovnih dokumenata.

Iz tog razloga se predlaže da se ISO/TS 15000-5: *Core Components Technical Specification* prihvati kao hrvatska norma u Hrvatskom zavodu za norme.

2.2. OASIS *Universal Business Language* 2.0

http://docs.oasis-open.org/ubl/os-UBL-2.0/

OASIS UBL je nastao u OASIS-u odmah nakon što je završena i objavljena ebXML norma CCTS. Verzija 2.0 UBL-a je nastala 2006. godine i definira 31 tip poslovnih dokumenata. U verziji 2.0 UBL je pored proširenog skupa obuhvaćenih poslovnih procesa uveo i nekoliko tehnoloških novosti kao što su: korištenje CCTS norme i CCL biblioteke kao i izdvajanje svih šifarnika iz samih XML shema pa je tu funkciju provjere sadržaja poruke preuzeo Schematron. UBL norma od svoje verzije 2.0 omogućuje izgradnju vlastitih podskupova

UBL norma predstavlja dobru podlogu za izgradnju dokumenta koji se razmjenjuju u postupku naručivanja. Za potrebe korištenja UBL-a u Republici Hrvatskoj potrebno je izgraditi vlastiti podskup od postojećih elemenata UBL-a i proširiti ih sa specifičnim hrvatskim potrebama.

2.3. OAGIS

http://www.oagi.org/

OAGIS je norma pod nadzorom *Open Applications Group Inc.* (OAGi). OAGi je organiziran za promociju interoperabilnosti poslovnih procesa za vanjske i unutrašnje poslovne procese i za stvaranje jedne ili više specifikacija koji će pomoći organizacijama u postizanju povezivanja i integracije vanjskih i unutrašnjih poslovnih procesa poduzeća.

OAGIS norma je jedna od prvih međunarodnih norma koje se temelje na XML-u i čija namjena je semantički i sintaksno definirati poslovne dokumente. Strateško opredjeljenje OAGIS-a je da se od verzije 9.X pa nadalje norma temelji na CCTS-u.

OAGIS pruža definiciju poslovnih poruka u formi nazvanoj *Business Object Documents* (BOD) i daje primjere korištenja BOD-ova kroz definiranje poslovnih scenarija. Poslovni scenariji identificiraju poslovne aplikacije i komponente koje se integriraju i koje BOD-ove pritom koriste. U verziji 9.0. definirano je 434 BOD-ova. Norma OAGIS se već koristi u Republici Hrvatskoj u svrhu integracije poslovnih procesa.

2.4. CWA (CEN *Workshop Agreement*)

Svi CWA dokumenti dostupni su na:

http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/cen+workshop+agreements/cwa_listing.asp

- CWA 15666 BRS - *Cross industry e-Tendering process* (http://www.cen.eu/cenorm/sectors/sectors/isss/cen+workshop+agreements/cwa1566620071.pdf)
  e-Natjecanje (e-*Tendering*) predstavlja prvi korak u procesu e-Nabave i podrazumijeva odvijanje procesa natjecanja elektroničkim putem. U dokumentu CEN CWA 15666 *Business requirements specification - Cross industry e-Tendering process* prikazani su glavni procesi otvorenih i selektivnih natječaja za naručivanje radova, roba i usluga kakvi se uobičajeno primjenjuju u javnoj nabavi.

- CWA 15667 BRS - *Cross industry catalogue process* (http://www.cen.eu/cenorm/sectors/sectors/isss/cen+workshop+agreements/cwa1566720071.pdf)
  CEN CWA 15667 dokument opisuje poslovne procese koji se koriste za ponudu roba ili usluga od strane dobavljača potencijalnom kupcu te razmjenu osnovnih informacija potrebnih za naručivanje tih roba i usluga. Pored opisa poslovnih procesa i transakcija CEN CWA 15667 specifikacija poslovnih zahtjeva (*Business requirements specification*) opisuje i strukturu informacija u elektroničkom katalogu koje se mogu potencijalnom kupcu slati u cijelosti ili po dijelovima i koje mogu biti osnovicom za naručivanje roba i usluga definiranih u tim katalozima, odnosno služiti kao podloga za e-Naručivanje. Korisnici kataloga mogu podatke zatražiti ad-hoc ili se mogu pretplatiti na dijelove kataloga. Pored osnovnog CEN CWA 15667 dokumenta područje kataloga pokrivaju i sljedeći CEN CWA dokumenti:

  - CEN CWA 15045 *Multilingual Catalogue strategies for eCommerce and eBusiness*, 2004. [2.09]

  - CEN CWA 15294 *Terminology for Product Classification*, 2005. [2.10]

  - CEN CWA 15295 *References and Data Models for Classification*, 2005. [2.11]

- CEN CWA 15566-1 *Product Description and Classification - Part 1: New Property Library*, 2006. [2.12]

- CEN CWA 15566-2 *Product Description and Classification - Part 2: Product Classes with sets of properties*, 2006. [2.13]

- CEN CWA 15566-3 *Product Description and Classification - Part 3: Results of development in harmonization of product classification*, 2006. [2.14]

Napomena: Oznake tipa [2.09], [2.10]... odnose se na podatke iz Tablice 10 u poglavlju 8 (Rezime preporuka za norme u procesima) **Studije normizacije u e-Poslovanju**.

- CWA 15668 BRS - *Cross industry invoicing process* (http://www.cen.eu/CENORM/sectors/sectors/isss/cen+workshop+agreements/cwa1566820071.pdf)
  CEN CWA 15668 *Business requirements specification - Cross industry invoicing process* iz ožujka 2007. godine je u cjelini temeljen na UN/CEFACT dokumentu *Business requirements specification* (BRS), *Cross Industry Invoicing Process, revision 1.1, release*: R.06A iz veljače 2006. godine. U CEN CWA 15668 dokumentu prikazano je mjesto procesa fakturiranja u poslovnom procesu *Order to cash* (sa stanovišta prodavatelja) i *Purchase to payment* (sa stanovišta kupca). Fakturiranje kao proces obuhvaća dva procesa: tradicionalno fakturiranje i samofakturiranje (ili samoizdavanje računa - *self-billing*), a događa se nakon obavljanja glavnih procesa: pribavljanja osnovnih informacija, naručivanja, vremenskog terminiranja i isporuke, a prije glavnog procesa: plaćanje. **Na temelju gore iznesenog potrebno je u Republici Hrvatskoj prihvatiti CEN CWA 15668 dokument kao temelj za opis poslovnog procesa fakturiranja.** Pored osnovnog CEN CWA 15668 dokumenta područje elektroničkog računa pokrivaju i sljedeći CEN CWA dokumenti:

  - CWA 15574 - *Commission Recommendation 1994/820/EC October 1994, proposed revision with the requirements of Directive* 2001/115/EC, *present day e-Commerce practices and revised definition of EDI Electronic Data Interchange*

  - CWA 15575 - *The list of invoice content details identified in the directive 2001/115/EC expressed as UN/CEFACT Core Components*

  - CEN CWA 15576 *Recommendation to allow coded identifiers as an alternative to the current unstructured clear text identifications*, 2006

  - CEN CWA 15577 *A standardised set of codes with definitions to replace plain text clauses in eInvoice messages for VAT exemptions*, 2006.

- CWA 15578 *Survey of VAT Data Element usage in the Member States and the use of codes for VAT Exemptions*
- CWA 15579 - *E-invoices and digital signatures. This version was published in 2007 and supersedes the 2006 one*
- CWA 15580 - *Storage of Electronic Invoices*
- CWA 15581 - *Guidelines for eInvoicing Service Providers*
- CWA 15582 - *eInvoice Reference Model for EU VAT purposes specification*

- CWA 15669 BRS - *Cross industry ordering process* (dijelovi 1 do 4)
  CWA 15669 sadrži specifikaciju poslovnih zahtjeva u procesu naručivanja, informacijski model narudžbe, informacijski model promjene narudžbe i informacijski model odgovora na narudžbu.
  - *Part 1: Global ordering process model definition*

    (http://www.cen.eu/CENORM/sectors/sectors/isss/cen+workshop+agreements/cwa15669120071.pdf)
  - *Part 2: Order transaction*

    http://www.cen.eu/cenorm/sectors/sectors/isss/cen+workshop+agreements/cwa15669220071.pdf)
  - *Part 3: Order change transaction*

    (http://www.cen.eu/cenorm/sectors/sectors/isss/cen+workshop+agreements/cwa15669320071.pdf)
  - *Part 4: Order response transaction*

    http://www.cen.eu/cenorm/sectors/sectors/isss/cen+workshop+agreements/cwa15669420071.pdf)

CWA 15671 BRS - *Cross industry scheduling process*
(http://www.cen.eu/cenorm/businessdomains/sectors/isss/cen+workshop+agreements/cwa1567120071.pdf)
U CEN CWA 15671 dokumentu opisani su sustavi vremenskog terminiranja koji se mogu primijeniti u različitim vrstama i granama e-Poslovanja i to vremensko terminiranje isporuke od strane kupca (*Customer controlled supply*) i vremensko terminiranje isporuke od strane prodavatelja (*Supplier controlled supply*) koje se još naziva i VMI (*Vendor Managed Inventory*).

3. Uređaji za sigurnosnu podršku sustava e-poslovanja

Sustavi e-Poslovanja zahtijevaju visoke razine zaštite kako podataka tako i procedura izvođenja određenih koraka u postupku. Kao što je objašnjeno u poglavlju 1, zahtjevi za privatnost, povjerljivost, integritet, autentifikaciju, autorizaciju, neporecivost kao i još neki zahtjevi zasnivaju se na uporabi normiranih ili opće priznatih kriptografskih algoritama.

Norme i preporuke navedene i opisane u poglavlju o sigurnosti koriste kriptografske algoritme za zaštitu podataka koje možemo u najosnovnijem obliku podijeliti u grupe simetričnih i asimetričnih algoritama. Simetrični algoritmi pružaju jednostavniji način kriptiranja i računalno su manje zahtjevni od asimetričnih ali imaju osnovni nedostatak da i pošiljatelj i primatelj poruke moraju imati potpuno identičan kriptografski ključ kako bi bili u mogućnosti razmjenjivati poruke. Upravo ta karakteristika čini ove algoritme neadekvatnim za mnoge gore navedene zahtjeve. Za razliku od njih asimetrični algoritmi definiraju skupove privatnih i javnih ključeva kojima je omogućeno kriptiranje i dekriptiranje podataka uz očuvanje privatnosti ključeva za generiranje poruka čime se ostvaruju navedeni zahtjevi. Nažalost, asimetrični algoritmi znatno su kompleksniji i računalno zahtjevniji od simetričnih te nisu efikasni za kriptiranje velike količine podataka.

Sljedeća grupa algoritama koja predstavlja osnovu ranije opisanih norma i preporuka su algoritmi vezani za izvedbu infrastrukture javnih ključeva (PKI), certifikata te ostalih pripadnih algoritama. Takve infrastrukture i algoritmi su potpora odnosno preduvjeti za korištenje kriptografskih algoritama za zaštitu podataka i u osnovnim funkcionalnostima se brinu o načinu generiranja, distribucije, zaštite i korištenja kriptografskih ključeva.

Sigurnost svih ranije navedenih algoritama u većini slučajeva može se usredotočiti na najvažniju kariku koja je način generiranja, zaštita i dozvoljena uporaba pojedinih kriptografskih ključeva u sustavu.

S obzirom da je način generiranja, zaštita od neovlaštene uporabe te pravilno korištenje kriptografskih ključeva osnova sigurnosti poslovnih sustava mnoge inicijative, preporuke i norme stvorene su kako bi se definirala okolina koja omogućuje siguran rad takvih sustava.

3.1. Sklopovski sigurnosni moduli (HSM)

U općenitom razmatranju može se definirati da kriptografski ključevi koji se koriste unutar nezaštićene računalne okoline omogućuju relativno jednostavan način za kompromitaciju cjelokupne sigurnosti sustava. Na isti se način općenito smatra da sigurnost pojedinog kriptografskog algoritma nije vezana za poznavanje algoritma (velika većina kriptografskih algoritama javno je specificirana upravo zbog tog njihovog svojstva da poznavanje algoritma ni na koji način ne omogućuje sigurnosni proboj, već naprotiv, osigurava sigurnost kroz višestruke teorijske potvrde). Iz

navedenoga može se zaključiti kako je jedni preostali dio sustava koji uistinu treba štititi u stvari dio gdje se pohranjuju i koriste kriptografski ključevi.

Razmatranjima i projektiranjima arhitektura računalnih sustava namijenjenih sigurnoj razmjeni podataka može se definirati da je zaštita kriptografskih ključeva moguća jedino korištenjem posebnih uređaja koji mogu osigurati sigurnost. Takvi uređaji općenito na tržištu dolaze pod kraticom HSM (*Hardware Security Module* - sklopovski sigurnosni modul). Uporaba HSM nužna je za ostvarenje sigurnosnih zahtjeva navedenih ranije.

Primarne funkcije HSM-a su generiranje kriptografskih ključeva na siguran način, pohrana ključeva te izvođenje osjetljivih dijelova kriptografskih algoritama. Sigurnost HSM-a ostvarena je kroz više slojeva fizičke, sklopovske, algoritamske i logičke zaštite. Napredni sklopovski sigurnosni moduli imaju ugrađene funkcije uništenja čuvanih podataka a ponekad i samouništenja modula u slučaju pokušaja proboja.

3.1.1. Preporučene norme i specifikacije za HSM

Sklopovski sigurnosni moduli namijenjeni velikim sustavima najčešće dolaze u obliku (manjeg ili većeg) sklopovskog modula koji je pridružen serveru sustava koji poruke obrađuje ili može čak i neovisno obrađivati poruke koje dolaze preko mreže. Ovakve module nalazimo u svim sustavima plaćanja, PKI sustavima, sustavima za uspostavu sigurnih komunikacijskih linija te je jedna od preporuka da se u budućoj arhitekturi sustava e-Plaćanja predvidi sklopovska zaštita korištenjem HSM-a. Sami uređaji često su certificirani prema nekim opće prihvaćenim sigurnosnim razinama pa tako kod HSM-a često nalazimo podatke o FIPS PUB 140-2 razini zaštite.

3.1.1.1. Federal Information Processing Standard, Publication 140-2

National Institute of Standards and Technology je ustanova u USA koja je definirala normu FIPS (*Federal Information Processing Standard***)** u svojoj publikaciji pod brojem 140-2 kojom se definiraju neke osnovne karakteristike i način validacije kriptografskih modula (ili HSM-ova navedenih ranije). Ova norma može se pronaći na adresi

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Pored ostalih detalja, u ovoj normi definiraju se četiri osnovne sigurnosne razine koje neki kriptografski modul može zadovoljavati. Najniža razina sigurnosti je predstavljena razinom 1 (*Level* 1) dok je najviša razina predstavljena razinom 4 (*Level* 4). **Ovu normu preporučujemo pri definiranju sustava e-Plaćanja.**

Na tržištu se pored naziva HSM ili kriptografski moduli, uređaji za podršku sigurnosnim algoritmima referenciraju i pod nazivom SSCD (*Secure Signature-Creation Devices*) (pogledaj poglavlje 2.1.1. i ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/).

Iako HSM koji su pridijeljeni serverima imaju veliku važnost jer rješavaju probleme velikih sustava, posebna rješenja potrebna su za uporabu na izvoru podataka/transakcije tj. kod pokretanja neke radnje od strane osobe. Kao što je ranije navedeno bez obzira na kompleksnost algoritma sigurnost sustava temelji se primarno na sigurnosti kriptografskih ključeva. U tom smislu javlja se problem generiranja, pohrane i korištenja kriptografskih ključeva koji su povezani s radnjama od strane neke osobe (npr. autorizacija plaćanja, potpisivanje dokumenta,...). U svrhu omogućavanja obavljanja i takvih aktivnosti bez kompromitiranja sigurnosti sustava u današnje vrijeme osobni HSM uglavnom su izvedeni u arhitekturi sigurnih mikroračunalnih sustava umetnutih u neki korisniku prihvatljiv medij za prijenos koji je najčešće plastična kartica. Na taj način dobije se minijaturni HSM koji se često naziva i pametna kartica zbog svojih karakteristika da može izvoditi jedan ili više kriptografskih algoritama, na siguran način generirati i pohranjivati kriptografske ključeve te predstavljati bitan dio ukupnog sigurnog sustava.

Kako je korištenje pametnih kartica jedan od preduvjeta sigurnog načina funkcioniranja sustava e-Poslovanja u nastavku su navedene neke norme koje se preporučuju pri definiciji i normizaciji e-Poslovanja.

3.2. Pametne kartice

3.2.1. Preporučene norme i specifikacije za pametne kartice

3.2.1.1. ISO/IEC 7810 Identification cards -- Physical characteristics

Upotreba raznih vrsta kartica proizašla je iz potrebe da se određene informacije važne za obavljanje neke usluge ili poslovnog procesa pohrane na medij koji je nekoj osobi stalno na raspolaganju. U početku su kartice imale otisnute, utisnute ili izbočene osnovne podatke o vlasniku kartice, poput imena, prezimena, identifikacijskog ili nekog drugog broja (broj bankovnog računa, broj kreditne/debitne kartice i sl.). Osoba na taj način ne mora pamtiti kompleksne brojeve, a u sustav se uvela dodatna razina zaštite. Posjedovanje kartice uz eventualnu identifikaciju nekim osobnim dokumentom značajno uvećava faktor sigurnosti da stvarni vlasnik želi obaviti neku akciju.

Ova norma je jedna u nizu norma koja opisuje fizičke karakteristike identifikacijskih kartica i to tipove ID-1, ID-2, ID-3 i ID-000. Kartice proizvedene prema ovoj normi osiguravaju mogućnost uporabe u različitim oblicima sustava i uređaja za obradu kartica.

Sama norma i detalji oko ove norme mogu se pronaći na

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31432

3.2.1.2. ISO/IEC 7811 Identification cards -- Recording technique

Kod određenih tipova kartica na pozadinu kartice stavlja se magnetska traka na koju se zapisuju željeni osobni podaci te podaci vezani uz usluge koje su tom karticom omogućene. Kartica s magnetskom trakom provlači se kroz čitač magnetske trake te se podaci direktno unose u računalni sustav bez potrebe ručnog unošenja/prepisivanja. Tehnologija magnetskog zapisa ne zahtijeva postojanje izvora napajanja na samoj kartici, što je dobra karakteristika ovakvih kartica. Iako je sustav magnetske trake na karticama uveden davno, on još uvijek održava svoju veliku prisutnost i upotrebljivost prvenstveno zbog izuzetno široke baze terminala koji mogu obrađivati podatke s takvih kartica te zbog veoma niske cijene same tehnologije magnetske trake. Međutim, mora se napomenuti da je ovaj sustav inherentno nedovoljno siguran za brojne primjene koje se uvode u današnje vrijeme.

Ova norma sastoji se od devet dijelova (7811-1 do 7811-9) i opisuje načine zapisivanja podataka i to *embossing* (istisnuta slova), opis i kodiranje na magnetsku traku na poleđini kao i neke specifikacije same magnetske trake.

3.2.1.3. *ISO/IEC 7816* Identification cards -- Integrated circuit cards

Ova norma se sastoji od 15 dijelova:

- *7816-1: Physical characteristics*
- *7816-2: Cards with contacts — Dimensions and location of the contacts*
- *7816-3: Cards with contacts — Electrical interface and transmission protocols*
- *7816-4: Organization, security and commands for interchange*
- *7816-5: Registration of application providers*
- *7816-6: Interindustry data elements for interchange*
- *7816-7: Interindustry commands for Structured Card Query Language (SCQL)*
- *7816-8: Commands for security operations*
- *7816-9: Commands for card management*
- *7816-10: Electronic signals and answer to reset for synchronous cards*
- *7816-11 Personal verification through biometric methods*
- *7816-12 Cards with contacts -- USB electrical interface and operating procedures*

- *7816-13: Commands for application management in multi-application environment*

- *7816-15: Cryptographic information application*

Ova norma jedna je od ključnih norma za pametne kartice jer se u njoj navode najvažnije karakteristike koje kartica u nekom sustavu mora posjedovati kako bi se omogućilo njeno korištenje na pravilan način. Naročito je važno što svi proizvođači pametnih kartica koriste ovu normu pri specifikaciji proizvoda a također je zanimljiva i povezanost nekih dijelova ove norme s drugim normama i specifikacijama (poput *Global Platform* specifikacije http://www.globalplatform.org/).

Neke od norma navedenih u nastavku namijenjene su samo za određene podskupove pametnih kartica. U tom smislu potrebno je definirati neke osnovne podjele kartica jer su one bitne i za definicije zahtjeva nad aplikacijama te sigurnosnih zahtjeva.

3.2.2. Podjela prema tehnologiji: magnetske, memorijske i procesorske kartice

3.2.2.1. Magnetske kartice

Kao što je već rečeno (vidi normu ISO 7811) određeni tipovi kartica na pozadini imaju magnetsku traku na koju se zapisuju željeni osobni podaci te podaci vezani uz usluge koje su tom karticom omogućene. Ovaj tip kartica je potpuno pasivan (nema mogućnosti nikakve obrade ili zaštite podataka) te se smatra inherentno nedovoljno siguran za brojne primjene koje se uvode u današnje vrijeme.

3.2.2.2. Memorijske kartice

Razvoj mikroračunalnih i memorijskih sustava rezultirao je u stvaranju kartica koje funkciju pamćenja određenih podataka ostvaruju izvedbom memorijskih modula ugrađenih u plastičnu karticu. Memoriji se pristupa preko nekoliko metalnih izvoda ostvarenih na površini plastične kartice (definiranim prema ranije navedenoj normi ISO 7816). Umetanjem kartice u posebno prilagođen uređaj za čitanje uspostavljaju se veze između memorije na kartici i računalnog sustava koji tada može pristupati memorijskim lokacijama. Funkcioniranje ovih kartica zahtjeva dovođenje napajanja na memorijski modul kartice. Za ovo se također koriste kontakti izvedeni na površini kartice. Značajna prednost memorijskih kartica u odnosu na magnetske jest u tome što se unutar memorijskog modula mogu definirati prava pristupa i manipulacije podacima, što značajno podiže razinu sigurnosti sustava, a time i spektar primjenjivosti kartica i aplikacija koje se njima služe. No kako su i memorijske kartice pasivan element u sustavu, moguće je ugroziti zaštitu podataka a time i sigurnost sustava koji takve kartice koriste. Također se mora napomenuti da memorijske kartice ne nude mogućnost izvedbe nekih kriptografskih algoritama te se zbog nedostatka te funkcionalnosti ne mogu koristiti u mnogim naprednim primjenama.

3.2.2.3. Procesorske kartice

Procesorske kartice na sebi imaju ugrađen mikroračunalni modul. Mikroračunalni modul u načelu se sastoji od jednostavnog procesora, pripadajuće memorije i dodatnih sklopova za ostvarenje nekih drugih ključnih algoritama ako za njih ima potrebe. Pristup procesoru i računalnom sustavu na kartici izvodi se na isti način kao i kod memorijskih kartica preko kontakata izvedenih na površini plastične kartice. Uvođenje aktivne komponente (procesora) u kartice doveo je do značajnog skoka u razini zaštite podataka te u mogućnosti izvođenja nekih veoma važnih kriptografskih algoritama u okviru zaštićene okoline na samoj kartici. Kartice s ugrađenim procesorom mogu se nazivati pametne kartice jer mogu samostalno obrađivati podatke na temelju unaprijed pohranjenog programa na kartici ili na temelju programa koji se na karticu pohranjuje naknadno. Današnje procesorske kartice često imaju ugrađen operacijski sustav koji upravlja procesima na samoj kartici.

3.2.3. Podjela prema načinu uspostavljanja komunikacije za memorijske i procesorske kartice

3.2.3.1. Kontaktno sučelje

U prethodnom poglavlju opisane su memorijske i procesorske kartice čije je osnovno sučelje za komunikaciju izvedeno kao grupa od nekoliko kontakata izvedenih na površini plastične kartice. Umetanjem kartice u odgovarajuće čitače u kojima se nalazi pripadajući kontakt dovodi se napajanje potrebno za rad takvih kartica te se ostvaruju fizičke veze prema podatkovnim i upravljačkim linijama potrebnim za komunikaciju. Kontaktna sučelja prvo su se počela koristiti u bankarstvu i telekomunikacijama.

Prva i najvažnija prednost kontaktnog sučelja u odnosu na kasnije opisano beskontaktno jest u tome da je moguće jednostavnije kontrolirati je li započeta transakcija provedena u cijelosti. Naime, prekidanjem veze između kartice i sustava moguće je prekinuti transakciju koja je u tijeku, te se u mnogim primjenama koriste čitači koji onemogućuju vađenje kartice iz čitača za vrijeme dok traje izvođenje transakcije. Pored toga, zbog fizičkog kontakta prednost je u relativno visokoj sigurnosti od neovlaštenog čitanja podataka koji se prenose između kartice i čitača. Dodatna prednost kontaktnog sučelja je i relativno niska cijena čitača jer su oni u upotrebi već preko desetak godina i proizvode se u milijunima primjeraka od strane brojnih proizvođača. Nedostatak ovog sučelja jest fizička osjetljivost kontakata na kartici kao i cijelog čitača na namjerna ili nenamjerna oštećenja (vandalizam, atmosferski utjecaji, voda,…), ograničenja na broj umetanja, relativno spora obrada velikog broja kartica u kratkom vremenu zbog potrebe fizičkog umetanja kartice u čitač, potreba za pravilnim umetanjem i sl. Treba naglasiti također da su troškovi održavanja kontaktnih sustava znatno viši od troškova održavanja beskontaktnih sustava.

3.2.3.2. Beskontaktno sučelje

Memorijske i procesorske kartice u novije vrijeme nude i mogućnost izvedbe s beskontaktnim sučeljem. Kod ovakvog sučelja u tijelo plastične kartice umeće se antena s pripadnim sklopovljem. Sve ovo povezuje se s memorijskim ili procesorskim modulom i zatvara u tijelo kartice. Približavanjem kartice elektromagnetskom polju koje emitira čitač, na kartici se inducira potreban napon za funkcioniranje te se preko RF komunikacije aktivira izvođenje potrebnih operacija i prijenos podataka. Određeni tipovi beskontaktnog sučelja omogućavaju obavljanje transakcija približavanjem kartice na udaljenost približno 1 m od čitača. Drugi tipovi sučelja omogućuju obavljanje transakcije na udaljenosti od samo nekoliko centimetara od čitača. S obzirom na to da se u polju čitača može istovremeno nalaziti nekoliko kartica, većina protokola omogućuje detekciju više kartica u polju te obavljanje transakcije bez kolizije između pojedinih kartica. Osnovna prednost kartica s beskontaktnim sučeljem očituje se u mogućnosti obavljanja transakcije bez potrebe da se kartica fizički umetne u čitač, što omogućuje veliku brzinu obrade jednostavnih transakcija. Ovo se posebno koristi kod sustava javnog prijevoza, kontrole pristupa i sl. Dodatna prednost ovog sučelja je i relativno velika neosjetljivost na mogućnosti oštećenja jer niti kod kartice niti kod čitača ne postoje posebno osjetljiva područja zato što su i kartica i čitač potpuno zatvoreni uređaji. Ova sučelja su zato pogodna za javna mjesta i primjene u raznim okolinama. Nedostatak beskontaktnog sučelja jest u mogućnosti izlaska kartice iz polja čitača tijekom obavljanja transakcije te u mogućnosti preslušavanja komunikacije od treće strane, što može ugroziti sigurnost sustava. Nedostatak ovog sustava je i u današnjoj cijeni čitača, koja je znatno viša od cijene kontaktnog. Međutim, očekuje se da će porastom tržišta cijena beskontaktnih čitača i kartica znatno pasti, dok su već sada troškovi održavanja beskontaktnih sustava znatno manji od troškova održavanja kontaktnih.

3.2.4. ISO/IEC 14443 *Identification cards - Contactless integrated circuit cards - Proximity cards*

Ova norma koja se sastoji od nekoliko dijelova definira tehničke parametre te protokole za antikoliziju i prijenos podataka kod kartica/uređaja koje koriste beskontaktno sučelje. Kartice izvedene prema ovoj normi mogu se još podijeliti prema tipu (A ili B) jer tijekom usuglašavanja norme nije postignuto jedinstvo dva tipa sustava u primjeni. Danas postoje milioni kartica koje rade prema ovoj normi i koje se koriste u velikoj količini u sustavima plaćanja (npr. javni prijevoz, MIFARE, AMEX Blue,...).

Ova norma definira kartice koje s čitačem komuniciraju na malim udaljenostima, tj. potrebna je volja i akcija korisnika da bi se obavila transakcija. Ova norma aktivno se koristi i pri kreiranju novih biometrijskih osobnih dokumenata (npr. putovnica, osobna) te je njena primjena i provođenja važno za sve buduće aplikacije koje imaju potrebu za identificiranjem korisnika.

3.2.5. ISO/IEC 15693 *Identification cards - Contactless integrated circuit cards - Vicinity cards*

Za razliku od ISO 14443 ova norma definira kartice koje mogu komunicirati s čitačem na većim udaljenostima (do 1,5m). Ova norma koristi se u mnogim primjenama gdje je potrebno evidentirati prisutnost ili očitati proizvode na udaljenost.

3.2.6. Kartice s više sučelja

Za određene primjene danas se na tržištu nude i kartice koje imaju izvedena oba sučelja: kontaktno i beskontaktno čime s omogućuje korištenje najboljih strana oba rješenja. Takve kartice nazivaju se kartice s dvostrukim sučeljem (*dual interface*) no postoje i rješenja da se u istoj kartici nalaze i dva neovisna sklopa od kojih jedan komunicira preko kontaktnog sučelja a drugi preko beskontaktnog.

U zadnje vrijeme postoje i kartice sa tri sučelja koje su prvenstveno predviđene za povezivanje kartica preko dodatnog USB sučelja na računalni sustav. USB sučelje definirano je unutar norme ISO 7816.

U nastavku slijedi pregled još nekih norma i preporuka značajnih za izvedbu projekta

3.2.7. EMV preporuka

EMV je skraćenica nastala od naziva triju institucija: *Europay*, *Mastercard* i VISA. Te su institucije inicijalno donijele ovu preporuku. Svrha EMV preporuke je uspostavljanje interoperabilnosti između pametnih kartica (kontaktno sučelje, ISO 7816) i POS terminala koji prihvaćaju takve kartice u cilju sigurnog izvođenja kreditnih i debitnih transakcija. EMV preporuka definira međudjelovanje na fizičkoj, električnoj, podatkovnoj i aplikacijskoj razini između pametnih kartica te terminala koji te kartice prihvaćaju. EMV preporuka omogućuje visoku sigurnost izvođenja financijskih transakcija na globalnoj razini. Sigurnost izvođenja transakcija zasniva se na korištenju kriptografskih algoritama tijekom obrade. Osnovni način identifikacije vlasnika realizira se za sada još uvijek starim rješenjem, PIN-om, no predviđa se da će u budućnosti prevladavati rješenje temeljeno na biometrijskim senzorima.

S obzirom da EMV nije međunarodna norma, primjena ove preporuke stimulira se indirektno kroz promjenu politike odgovornosti za štete nastale zlouporabom. Naime, ako dođe do zlouporabe u sustavu, EMV ne preuzima odgovornost za štetu ako sudionici nisu koristili opremu i procedure opisane EMV preporukom.

Uvođenje EMV preporuka dovelo je do značajnog porasta zahtjeva za infrastrukturom koja koristi pametne kartice od strane banaka. U tom smislu svaki budući sustav koji koristi kartice namijenjene i bankovnim transakcijama vjerojatno će biti podložan EMV preporukama.

Detalji se mogu pronaći na:

http://www.emvco.com/

3.2.8. Global Platform

Global Platform je međunarodna organizacija s predstavnicima mnogih industrijskih segmenata koja definira niz svjetski prihvaćenih i primjenjivanih specifikacija za pametne kartice i sustave koji koriste pametne kartice. Značenje *Global Platform* pristupa je vidljivo u velikim sustavima koji žele biti neovisni o dobavljaču tehnologije, državnim sustavima identifikacijskih dokumenata, sustavima sa velikim brojem usluga koje moraju biti interoperabilne i sl.

Detalji se mogu pronaći na:

http://www.globalplatform.org/

3.2.9. *Mifare/Felica*/NFC

U današnje vrijeme u svijetu su veoma prisutne neke tehnologije za beskontaktne pametne kartice. *Mifare* je tehnologija iza koje se nalazi *Philips* i koja se koristi u mnogim javnim sustavima, a naročito u sustavima javnog prijevoza. *Felica* je slična tehnologija firme *Sony* i veoma je prisutna u državama Dalekog istoka. Ove dvije firme zajednički su sudjelovale u formiranju nove norme ISO 18092 koja ima cilj na tržištu ojačati prisutnost beskontaktnih tehnologija kroz kompatibilnost s oba prethodna sustava te kroz uvođenje dodatnih funkcionalnosti.

Detalji se mogu pronaći na:

http://www.nfc-forum.org/home

ISO/IEC 18092: *Near Field Communication Interface and Protocol-1*,

ISO/IEC 21481: *Near Field Communication Interface and Protocol-2*

Ove dvije norme definiraju NFC (*Near Field Communication*) specifikacije.

3.3. Svrha pametnih kartica u sustavima vezanim za e-Ugovore i e-Račune

Ranije navedene tehnologije predstavljaju jednu od ključnih tehnoloških podloga za korištenje PKI infrastrukture u sigurnosnim sustavima. Naime, uporaba kriptografskih ključeva izvan sigurne okoline kompromitira cjelokupnu arhitekturu sigurnosnog sustava. Ako neki od npr. tajnih ključeva napusti sigurnu okolinu i makar i na najmanji način postane dostupan osobama koje nisu njegovi vlasnici tada cijeli protokol osiguranja vjerodostojnosti postaje ništavan.

U tom smislu pametne kartice omogućuju da tajni ključ nikada ne napušta sigurnu okolinu i nemoguće ga je pročitati, a njegovo korištenje omogućeno je samo unutar sigurne aplikacije koja se izvodi na samoj kartici. Na taj način osigurano je funkcioniranje kriptografskih algoritama, a u isto vrijeme i tajnost pojedinih ključeva.

4. HUB standard

4.1. Tekst standarda

HRVATSKA UDRUGA BANAKA

CROATIAN BANKING ASSOCIATION

Sukladno Ugovoru o osnivanju HUB-a i Poslovniku Odbora za platni promet te temeljem zaključaka Radne skupine za e-račun

Odbor za platni promet HUB-a

prihvaća Standard

formata e-HUB obrasca

(1) POVOD

Usvajanjem Strategije razvitka elektroničkog poslovanja u RH za razdoblje od 2007-2010 od strane Vlade RH formiran je Tehnički odbor i šira radna skupina za

e-račun. Na sastanku šire radne skupine održanom 11.12.2007. godine u prostorima FINE, šira radna skupina dogovorila je da će se pri HUB-u oformiti uža radna skupina tj. radna skupina bankara koja će se pozabaviti prvenstveno petim dijelom e-računa, odnosno e-plaćanjem. Jedna od zadaća uže radne skupine je prema HUB1 obrascu izraditi e-HUB obrazac, odnosno odrediti standard, uputu i xml format za isti. Standard će biti javno objavljen na e-portalu i HUB-ovim web stranicama i dostupan za slobodnu upotrebu svim zainteresiranim korisnicima. Standard će se razvijati, mijenjati i nadopunjavati u skladu sa zakonskim promjenama i zahtjevima tržišta. Radi potrebe poslovanja i zahtjeva klijenata već sada je potrebno razviti i dinamički xml. Njegova struktura biti će objavljena na isti način.

(2) OPĆE ODREDBE

Ovim standardom uređuju se oblik, sadržaj i upotreba elektronskog naloga za plaćanje u domaćem platnom prometu, kao petog dijela e-računa - **e-HUB obrasca.**

Navedeni obrazac namijenjen je sudionicima platnog prometa koji su svoje poslovanje dogovorili i proveli kroz e-poslovanje, e-računom, te pružateljima navedene usluge. Iz tog razloga napravljen je standard u XML formatu. Osim XML formata prilažemo i opis svakog pojedinog atributa aplikacijske sheme te izgled obrasca e-HUB nakon ispisa na zaslonu ili štampaču.

E-HUB obrazac mora sadržavati sve potrebne podatke za plaćanje sukladno Zakonima i Podzakonskim aktima koji su na snazi, te će se po potrebi mijenjati i/ili nadopunjavati. Očekujući donošenje Uredbi Vlade o jedinstvenom katalogu i rječniku javne nabave javlja se mogućnost da će pojedine nazive atributa trebati mijenjati.

Razvitkom e-poslovanja u RH kao i pristupanjem RH u EU postoji mogućnost proširenja namjene i upotrebe e-HUB obrasca što će se regulirati dopunom standarda i upute. Predviđajući neke od mogućih izmjena pojedini atributi su već definirani ovim standardom i uputom, iako su u ovom času možda i nepotrebni. Postupak za promjene i dopune ovog standarda i upute može se pokrenuti odlukom Tehničkog odbora, šire ili uže radne skupine za e-račun.

Navedeni obrazac biti će objavljen, te time dostupan za upotrebu, nakon njegovog prihvaćanja od strane šire radne skupine za e-račun i Odbora za platni promet HUB-a. Datum početka primjene dogovoriti će se naknadno.

HUB neće izdavati posebna odobrenja za korištenje navedenog obrasca već je on dostupan svim bankama i drugim korisnicama temeljem objave na e-portalu i

HUB-ovim web stranicama.

Ovaj standard ne uređuje troškove i naknade za izvršenje e-naloga za plaćanje.

(3)XML STANDARD

Prilog XML standard sastavni je dio ovog standarda i upute.

(4) IZGLED OBRASCA NA ZASLONU ILI ŠTAMPAČU

Prilog Obrazac e-HUB sastavni je dio ovog standarda i upute.

(5) NAZIVI I OPIS ATRIBUTA APLIKACIJSKE SHEME

Prilog Opis atributa u aplikacijskoj shemi sastavni je dio ovog standarda i upute.

U Zagrebu, dana 13 studenog 2008.

Predsjednica Odbora	Direktor GIU Hrvatska
za platni promet HUB-a:	udruga banaka:
Vesna Ćebetarević, v.r.	dr Zoran Bohaček, v.r.

4.2. Obrazac e-HUB

Obrazac e-HUB

Transakcija hitnost ___ kanal izvršenja ___ oznaka valute HRK

iznos _____ datum valute _____

Platitelj naziv tvrtke ili ime i prezime _____

adresa *ulica* _____ *kućni broj* _____

mjesto _____ *poštanski broj* _____

država HR Republika Hrvatska

broj računa (IBAN) HR ___ ___ _____ _____

model i poziv na broj zaduženja *model* ___ *poziv na broj* _____

Ovjera platitelja

_____ _____

Primatelj naziv tvrtke ili ime i prezime _____

adresa *ulica* _____ *kućni broj* _____

mjesto _____ *poštanski broj* _____

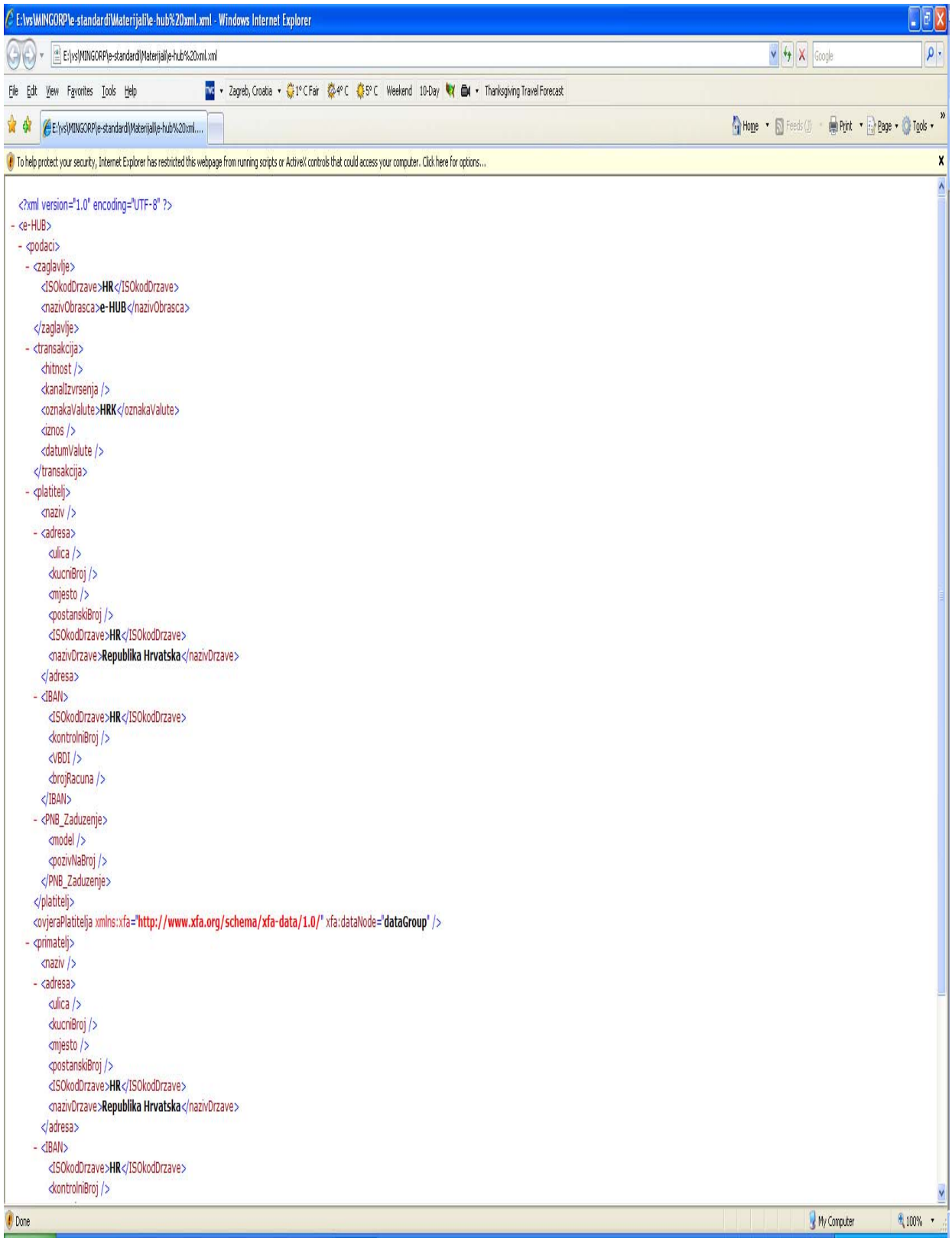
država HR Republika Hrvatska

broj računa (IBAN) HR ___ ___ _____ _____

model i poziv na broj odobrenja *model* ___ *poziv na broj* _____

opis plaćanja _____

4.3. XML primjer



5. Zaključak

Predložene su sigurnosne norme za e-Potpis, e-Identitet, sigurnost Web servisa i sigurnost razmjene elektroničkih poruka. Opisane su i preporučene norme za definiranje strukture i semantike u e-Poslovanju. Opisani su uređaji za sigurnosnu podršku e-Poslovanju. Radi se o sklopovlju i o pametnim karticama kao neophodnom preduvjetu masovnosti e-Poslovanja. Kao primjer *de-facto* prihvaćene norme pokazan je dokument kojim se prihvaća „Standard formata e-HUB obrasca“, tj. obrasca za e-Račun Hrvatske udruge banaka. Ovom normom uređen je oblik, sadržaj i upotreba elektronskog naloga za plaćanje u domaćem platnom prometu, kao petog dijela e-računa - e-HUB obrasca**.**

6. Reference

Reference su navedene uz opise pojedinih norma.