Centar Informacijske Sigurnosti

XML digitalni potpis

srpanj 2011.

CIS-DOC-2011-07-020

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

XML (eng. *Extensible Markup Language*) je vrlo jednostavan, fleksibilan tekstualni format razvijen iz SGML (eng. *Standard Generalized Markup Language*) jezika. SGML je ISO (eng. *International Organization for Standardization*) standard za definiranje *markup* jezika za dokumente. XML je originalno dizajniran zbog izazova koje je donosio veliki porast elektroničkog objavljivanja dokumenata. Također, veliku ulogu ima u razmjeni podataka raznih vrsta na Internetu. Više o XML-u moguće je pročitati u poglavlju 2.

Digitalni potpis je elektronička zamjena za rukom pisani potpis, a služi istoj funkciji. Uz to pruža i potvrdu autentikacije, integriteta, neporecivosti te povjerljivosti izvora i podataka koji se prenose. Važno je napomenuti da digitalni potpis nije kopija ručno pisanog potpisa. U tehničkom smislu, digitalni potpis stvara i provjerava posebna aplikacija koja generira kriptografske poruke. Kao bi digitalni potpis funkcionirao, stvaraju se dva različita ključa. Prvi, zvan javni ključ, kreira digitalni potpis transformacijom podataka u nerazumljiv kod. Drugi, zvan privatni ključ, provjerava digitalni potpis te dešifrira transformiranu poruku u izvorni oblik. Ovaj sustav je siguran dok je privatni ključ zadržan tajnim. Detaljniji opis digitalnih potpisa dan je u poglavlju 3.

XML digitalni potpis je u principu digitalni potpis dizajniran za uporabu u XML transakcijama, a može se koristiti za potpisivanje bilo kojeg tipa podataka. Standard definira shemu za snimanje rezultata operacije digitalnog potpisivanja primijenjene na proizvoljne podatke. Pruža autentikaciju, integritet te podršku za neporecivost podataka koji su potpisani. Više informacija o digitalnim XML potpisima nalaze se u poglavlju 4.

Budući razvoj XML digitalnih potpisa mogao bi doživjeti veliki uspjeh posebno u financijskim i bankarskim uslugama. Manje organizacije se još uvijek suspreže od uvođenja ovakvih tehnologija zbog manjka znanja te želje da se izbjegnu troškovi uvođenja novih tehnologija. Osvrt na budući razvoj digitalnih XML potpisa dan je u poglavlju 5.

2. Što je XML?

XML (eng. *Extensible Markup Language*) je skup pravila za šifriranje dokumenata u obliku prilagođenom za računala. Pravila su definirana u XML specifikaciji inačice 1.0 koju izdaje organizacija W3C (eng. *World Wide Web Consortium*), te nekoliko drugih standarda koji su javno dostupni. W3C je organizacija koja se bavi standardizacijom tehnologija korištenih na Internetu, a više informacija o djelovanju i izdanim standardima nalazi se na poveznici u nastavku.

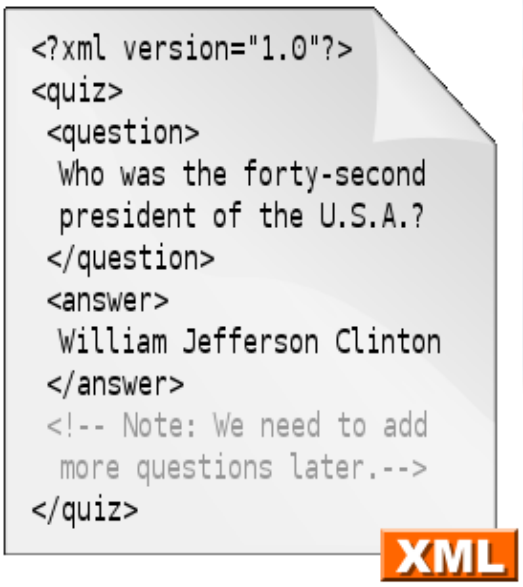
http://www.w3.org/

Cilj XML-a (primjer je dan na Slika 1), kao tekstualnog formata jezika su jednostavnost, općenitost i lakoća uporabe preko Interneta. Iako se dizajn XML-a fokusira na dokumente, često se koristi kao reprezentacija za proizvoljne podatkovne strukture, kao primjerice u web uslugama.

Mnoga API (eng. *application programming interface*) sučelja[1] razvijena su kako bi omogućila programerima obradu XML podataka. Od 2009. godine razvijeno je i stotinu jezika temeljenih na XML-u, uključujući:

- RSS (eng. *Really Simple Syndication*) –skup formata za web polja (eng. *feeds*) korištena za objavljivanje informacija koje se redovito osvježavaju poput unosa na blogu, novosti i sl., u standardiziranom obliku,
- Atom – XML jezik koji se koristi za polja,
- SOAP (eng. *Simple Object Access Protocol*) – specifikacija protokola za izmjenu strukturiranih informacija u implementaciji web usluga u računalnoj mreži,
- XHTML (eng. *eXtensible HyperText Markup Language*) – skupina XML jezika koja proširuje često korišteni jezik za razvoj web stranica, HTML (eng. *Hypertext Markup Language*).

Formati temeljeni na XML-u postali su osnova za mnoge alate kao što su, na primjer, Microsoft Office (Office Open XML), OpenOffice.org (OpenDocument) i Appleov iWork.



Slika 1. Primjer XML dokumenta
Izvor: Wikipedia

[1] API sučelje je skup pravila i specifikacija koja programi mogu slijediti prilikom uspostavljanja međusobne komunikacije.

2.1. Osnovni XML elementi

U nastavku dokumenta predstavljeni su osnovni elementi koji čine jedan XML dokument.

- **Znak**

  Po definiciji, XML dokument je niz znakova (eng. *characters*), a podržan je skoro svaki znak standarda Unicode[2].

- **Procesor i aplikacija**

  Procesor (eng. *processor*) analizira jezik te predaje strukturirane informacije aplikaciji (eng. *application*). Specifikacija definira zahtjeve na to što XML procesor mora i ne mora činiti, ali aplikacija nije uključena u nju.

- ***Markup* i sadržaj**

  Znakovi koji čine jedan XML dokument podijeljeni su u *markup* i sadržaj, a razlikuje ih aplikacija prema nizu jednostavnih sintaksnih pravila. Svi nizovi koji predstavljaju *markup* počinju ili sa znakom „<“ te završavaju znakom „>“ ili počinju znakom „&“ te završavaju s „;“. Svi ostali znakovi predstavljaju sadržaj.

- **Oznaka**

  Oznaka (eng. *tag*) je *markup* konstruktor koji počinje znakom „<“ i završava znakom „>“. Oznake dolaze u tri oblika:

  1. početne oznake (eng. *start-tags*),
  2. završne oznake (eng. *end-tags*),
  3. prazne oznake (eng. *empty-element tags*).

  Primjer navedenih oznaka dan je u nastavku.

```
<section> - početna oznaka
</section> - završna oznaka
<line-break> - prazna oznaka
```

- **Element**

  Logička komponenta dokumenta koji ili počinje s početnom oznakom i završava s odgovarajućom završnom oznakom ili sadrži samo praznu oznaku. Znakovi između početne i završne oznake su sadržaj, a mogu sadržavati i markup ili druge elemente koji se tada nazivaju elementi djeca (eng. *child elements*). Primjer elementa je dan u nastavku.

```
<Greeting>Hello, world.</Greeting>
```

- **Atribut**

  Atribut je markup konstruktor koji sadrži par „ime/vrijednost“, a postoji unutar početne ili prazne oznake. U primjeru koji slijedi element *img* ima dva atributa, *src* i *alt*:

```
<img src="madonna.jpg" alt='Foligno Madonna, by Raphael' />.
```

  Drugi primjer, gdje je ime atributa "*number*" i vrijednost "3", je:

```
 <step number="3">Connect A to B.</step>.
```

- **XML deklaracija**

  XML dokument može početi deklariranjem nekih informacija o samom dokumentu, kao što je prikazano u primjeru u nastavku.

```
<?xml version="1.0" encoding="UTF-8" ?>
```

[2] Unicode je računalni standard za konzistentno kodiranje, predstavljanje i rukovanje tekstom prisutnim u većini svjetskih sustava za pisanje.

2.2. Uporaba i rukovanje pogreškama

XML specifikacija definira XML dokument kao tekst koji je dobro formiran (eng. *well-formated*), tj. zadovoljava listu sintaksnih pravila. Neka od tih pravila su:

- dokument sadrži samo dopuštene Unicode znakove,
- nijedan od posebnih znakova (poput „<“ ili „&“) ne pojavljuje se nigdje osim u markup pravilima,
- početne, završne i prazne oznake moraju biti ispravno postavljene pri čemu niti jedna ne smije nedostajati i nijedna ne smije biti višak,
- u dokumentu može postojati samo jedan „root“ element koji sadrži sve ostale.

Osim što mora biti dobro formiran, XML dokument mora biti i valjan. To znači da sadrži referencu na DTD (eng. *Document Type Definition*) shemu i da su njegovi elementi i atributi deklarirani u DTD-u te slijede gramatička pravila koja shema specificira. DTD je primjer jedne sheme ili gramatike, a od inicijalne objave XML jezika inačice 1.0 razvijene su razne sheme predstavljene u nastavku dokumenta.

- **DTD**

  Najstarija shema za XML jezik, naslijeđena iz jezika SGML, a karakteriziraju ju sljedeće prednosti:

  - sveprisutna podrška jer je uključena u standard XML 1.0,
  - sažeta u usporedbi sa shemama temeljenim na elementima,
  - omogućuje deklaraciju standardnih javnih skupina za objavljivanje znakova te
  - definira tip dokumenta čime se omogućava grupiranje svih ograničenja u jednu skupinu.

  Osim navedenih prednosti, DTD shema ima i neke nedostatke:

  - ne sadrži podršku za novije značajke XML-a,
  - nedostaje ekspresivnosti, tj. određene strukture ne mogu se izraziti s regularnom gramatikom,
  - nedostaje čitljivosti te
  - koristi se sintaksa temeljena na regularnim izrazima preuzetim iz SGML-a.

  Dvije osnovne značajke koje izdvajaju DTD shemu od ostalih su sintaksna podrška za ugradnju DTD-a unutra XML dokumenta i definiranje entiteta (eng. *entities*) koji su proizvoljni fragmenti teksta i/ili *markup* dijelova koje XML procesor umeće u DTD i XML dokument na referencirana mjesta. Opisana shema se još uvijek koristi u mnogim aplikacijama zbog svoje sveprisutnosti.

- **XML Shema**

  Novija shema, koju organizacija W3C opisuje kao nasljednika DTD-a. Često se spominje kao akronim za XSD (eng. *XML Schema Definition*). Koristi bogati sustav podatkovnih tipova i omogućava detaljnija ograničenja logičke strukture XML dokumenta. Također, koristi format temeljen na XML jeziku koji omogućava uporabu XML alata za procesiranje.

- **RELAX NG**

  RELAX NG je inicijalno specificirala organizacija OASIS i sada je također ISO međunarodni standard. Može biti pisana u sintaksi temeljenoj na XML jeziku ili više kompaktnoj sintaksi koja nije temeljena na XML jeziku. Dvije navedene sintakse su izomorfne, a postoje alati koji omogućuju prebacivanje iz jedne u drugu bez gubitka informacija (npr. alat „Trang“[3]). RELAX NG sadrži jednostavnije sučelje za definicije i provjeru od XML Sheme, što ju čini jednostavnijom za uporabu i implementaciju. Također sadrži podršku za uporabu raznih dodataka.

- **Schematron**

  Schematron je jezik za stvaranje tvrdnja (eng. *assertions*) o prisutnosti ili odsutnosti uzoraka (eng. *patterns*) u XML dokumentu, a obično koristi XPath izraze.

[3] Alat Trang omogućuje pretvaranje različitih shema za XML jezik, a sadrži podršku za sljedeće sheme: RELAX NG (XML sintaksa i kompaktna sintaksa), XML 1.0 DTD i XML Schema.

- **ISO DSDL**

  ISO DSDL (eng. *Document Schema Description Languages*) standard donosi opsežan skup malih shema od kojih je svaka usmjerena na poseban problem. Uključuje RELAX NG, Schematron i jezike za definiranje podatkovnih tipova, ograničenja na znakove, proširenja entiteta i prosljeđivanje dijelova dokumenata različitim programima za provjeru. Ipak, još ne sadrži podršku za XML Shemu.

2.3. Prednosti i nedostaci XML-a

Glavne prednosti jezika XML navedene su u nastavku:

- radi se o jednostavnom formatu koji je ljudima lako čitljiv i razumljiv,
- sadrži podršku za Unicode znakove pa je moguće prikazati bilo koju informaciju,
- može prikazati najosnovnije strukture podataka u računarstvu: zapise (eng. *records*), liste (eng. *lists*) i stabla (eng. *trees*),
- njegov format opisuje strukture i imena polja, kao i posebne vrijednosti,
- stroga sintaksa i zahtjevi za obradu čine algoritme za obradu posebno jednostavnim, efikasnim i konzistentnim,
- često se koristi kao format za dokumentiranje pohrane ili obrade podataka,
- temelji se na međunarodnim standardima,
- omogućuje provjeru uporabom shema kao što su XSD i Schematron, što omogućuje efektivno ispitivanje i razvoj programa,
- hijerarhijska struktura je dovoljna za većinu tipova dokumenata,
- očituje se kao obična tekstualna datoteka, što stvara manje ograničenja od drugih formata dokumenata,
- nije ovisan o platformi pa time nije ovisan ni o promjenama u tehnologijama,
- njegov prethodnik, SGML, koristi se još od 1986. godine pa postoji puno iskustva i dostupnih programa,
- potpuno je kompatibilan s aplikacijama poput Jave,
- potpuno prijenosan jezik što znači da se može koristiti od aplikacija na malim uređajima do Interneta,
- sadrži mogućnost proširivanja, što znači da korisnik može sam kreirati svoje oznake ili koristiti oznake koje su već stvorene.
- XML dokumente moguće je jednostavno pretvoriti u bilo koji drugi format.

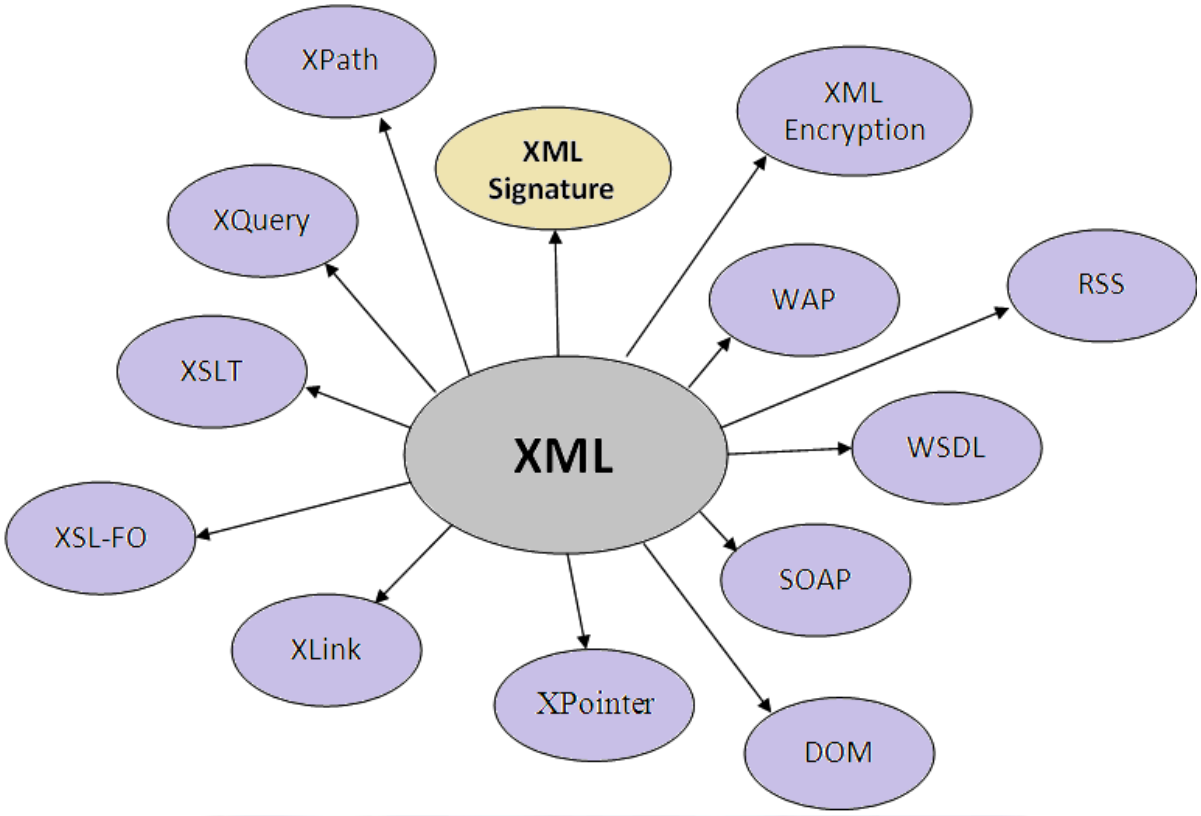
Osnovni nedostaci XML-a dani su u nastavku:

- XML sintaksa je redundantna i jako opširna u usporedbi s binarnom reprezentacijom istih podataka,
- redundantnost može utjecati na efikasnost aplikacije zbog većih zahtjeva na resurse za pohranu, prijenos i obradu podataka,
- ne postoji podrška za unutrašnje podatkovne tipove poput tipova „*integer*“, „*string*“, „*boolean*“ i sl.,
- hijerarhijski model za reprezentaciju je ograničen u usporedbi s relacijskim modelom ili objektno orijentiranim grafom,
- predstavljanje veza preklapajućih čvorova (eng. *overlapping node*) zahtjeva dodatni napor,
- XML imenovanje zadaje probleme pri uporabi i može biti dosta teško za ispravno implementiranje u alatima za obradu (eng. *parser*).
- razvijen je za rukovanje malom količinom informacija,
- dokument lako postaje teško čitljiv ako sadrži veliku količinu informacija pa je potrebno koristiti neke od naprednih alata za uređivanje (kao što je na primjer Microsoft Visual Web Developer),

- XML nije najbolji izbor u slučaju kada se prikazuju neki drugi formati, poput slikovnih datoteka.

2.4. XML proširenja

Iz osnovnog XML jezika razvilo se više proširenja koja obavljaju neku specijaliziranu funkciju. Poznatija proširenja navedena su u nastavku te ih prikazuje Slika 2.



Slika 2. XML specijalizirana proširenja

- **XPath** je jezik koji omogućuje jednostavnije pretraživanje sadržaja u XML dokumentu.
- **XQuery** je upitni jezik za pretraživanje XML dokumenta. On je za XML isto ono što je SQL za relacijske baze podataka.
- **XSLT** je jezik koji omogućuje transformacije XML dokumenata iz jednog formata u drugi (npr. iz XML-a u HTML).
- **XSL-FO** je jezik koji služi za formatiranje izlaznog rezultata XML dokumenta.
- **XML Linking Language** je jezik koji opisuje standardni način stvaranja poveznica u XML dokumentima.
- **XML Pointer Language** je jezik koji opisuje standardni način na koji *hiperlinkovi* pokazuju na određeno mjesto unutar XML dokumenta.
- **XML DOM** (eng. *Document Object Model*) je sučelje koje omogućuje računalnim programima pristup i ažuriranje sadržaja te strukture XML dokumenta.
- **SOAP** je jednostavan protokol zasnovan na XML-u koji omogućuje programima razmjenu podataka u tekstualnom obliku preko HTTP protokola.
- **WSDL** (eng. *Web Services Description Language*) je jezik zasnovan na XML-u koji omogućuje opis web servisa i sučelja za njihovo korištenje.
- **RSS** (eng. *Really Simple Syndication*) je način za distribuciju sadržaja s jednog *weba* na druge pomoću XML-a.

- **WAP** (eng. *Wireless Application Protocol*) je protokol razvijen s namjerom pristupa internetskim sadržajima pomoću prijenosnih uređaja (npr. mobitela, ručnih računala i sl.).
- **XML** Signature definira sintaksu i pravila za kreiranje digitalnog potpisa XML sadržaja.
- **XML** Encryption definira sintaksu i pravila za šifriranje XML sadržaja.

3. Digitalni potpis

Digitalni potpis ili shema digitalnog potpisa je matematička shema za demonstriranje autentikacije digitalne poruke ili dokumenta. Valjan digitalni potpis daje primatelju razlog za vjerovanje da je poruku stvorio poznati pošiljatelj te da nije izmijenjena u prijenosu. Obično se koriste za distribuciju programa, financijske transakcije i u drugim slučajevima gdje je važno detektirati lažiranje ili izmjenu podataka.

Digitalni potpisi obično se koriste za implementaciju elektroničkih potpisa, izraz koji se odnosi na svake elektroničke podatke koji nose svrhu potpisa, ali ne koriste svi elektronički potpisi digitalne potpise. U nekim zemljama, uključujući SAD, Indiju te zemlje članice Europske Unije, elektronički potpisi imaju legalno značenje. Međutim, zakoni o elektroničkim potpisima ne definiraju točno da li su digitalni kriptografski potpisi korišteni, što čini njihov značaj i definiciju zbunjujućim.

Digitalni potpisi uključuju asimetričnu kriptografiju. Za poruku poslanu kroz nesigurni kanal, pravilno implementiran digitalni potpis daje primatelju razlog da vjeruje da poruku šalje pravi pošiljatelj. Može se reći da su digitalni potpisi ekvivalentni tradicionalnim rukom pisanim potpisima u mnogim točkama, ali pravilno implementirane digitalne potpise teže je krivotvoriti od rukom pisanih. Shema digitalnih potpisa je temeljena na kriptografiji te mora biti pravilno implementirana da bi bila efikasna. Također može pružiti ne pobijanje (eng. *non-repudiation*), što znači da izvor poruke ne može poreći da je istu poslao jer ju je potpisao privatnim ključem koji je tajan. Nadalje, neke sheme pružaju vremensko ograničenje za potpise pa, čak i u slučajevima kada je privatni ključ otkriven, potpis više nije valjan. Digitalno potpisane poruke mogu sadržavati bilo što prikazano kao niz bitova, a primjeri uključuju poruke elektroničke pošte, ugovore ili poruke poslane preko nekog kriptografskog protokola.

Digitalni potpisi su jedna od grana kriptografije javnog ključa (eng. *Public-key cryptography*), pa je u nastavku objašnjen njen princip rada.

3.1. Kriptografija javnog ključa

Kriptografija javnog ključa označava kriptografski sustav koji zahtjeva postojanje dva odvojena ključa, jedan za šifriranje čistog teksta (eng. *plaintext*), a drugi za dešifriranje šifriranog teksta (eng. *cyphertext*). Jedan od ključeva se objavljuje javno (javni ključ), dok drugi ostaje tajan (privatni ključ). Ako se objavi ključ za šifriranje, omogućuje se privatna komunikacija javnosti s vlasnikom ključa. Za razliku od toga, ako se objavi ključ za dešifriranje, omogućuje se provjera potpisa dokumenta šifriranog s vlasnikovim privatnim ključem.

Ovaj kriptografski pristup koristi algoritme asimetričnog ključa (eng. *asymmetric key algorithms*). Neki od tih algoritama imaju obilježje tajnog i privatnog ključa, što znači da nijedan ključ ne može biti izveden iz drugog. Zbog toga se javni ključ može koristiti za prijenos poruke u nečitljiv oblik koji mogu dešifrirati samo korisnici koji znaju odgovarajući privatni ključ. Sudionici komunikacije u takvom sustavu moraju kreirati matematički povezane parove ključeva kao što su privatni i javni ključ. Objavom javnog ključa, vlasnik omogućuje svim korisnicima da proizvedu poruke koje samo on može čitati jer samo on ima kopiju privatnog ključa koja je potrebna za dešifriranje. Kada korisnik želi poslati sigurnu poruku kreatoru ključeva, pošiljatelj ju šifrira uporabom primateljeva javnog ključa. Za dešifriranje poruke primatelj tada koristi svoj privatni ključ.

Za razliku od algoritma simetričnog ključa (eng. *symmetric key algorithms*), algoritam javnog ključa ne zahtjeva inicijalnu sigurnu izmjenu jednog ili više ključeva između primatelja i pošiljatelja. Razlog tomu je što on svoju snagu nalazi u činjenici da je izrazito teško odrediti privatni ključ na temelju poznavanja javnog ključa jer su temeljeni na matematičkoj vezi (većinom faktorizaciji[4] ili problemu diskretnih logaritama[5]).

[4] Faktorizacija je razvoj broja u male djelitelje čijim se međusobnim množenjem dobije originalni, polazni broj.

Uporabom ovih algoritama također se omogućuje provjera autentičnosti poruke kreiranjem digitalnog potpisa poruke uporabom privatnog ključa, koji se može provjeriti uporabom javnog ključa.

3.2. Način rada digitalnog potpisa

Shema digitalnog potpisa sadrži tri algoritma:

1. Algoritam za generiranje ključa – odabire privatni ključ slučajno iz skupa mogućih ključeva te daje par privatni/javni ključ.
2. Algoritam za potpisivanje – za danu poruku i privatni ključ generira potpis,
3. Algoritam za provjeru – za danu poruku, javni ključ i potpis prihvaća ili odbija tvrdnju o autentičnosti.

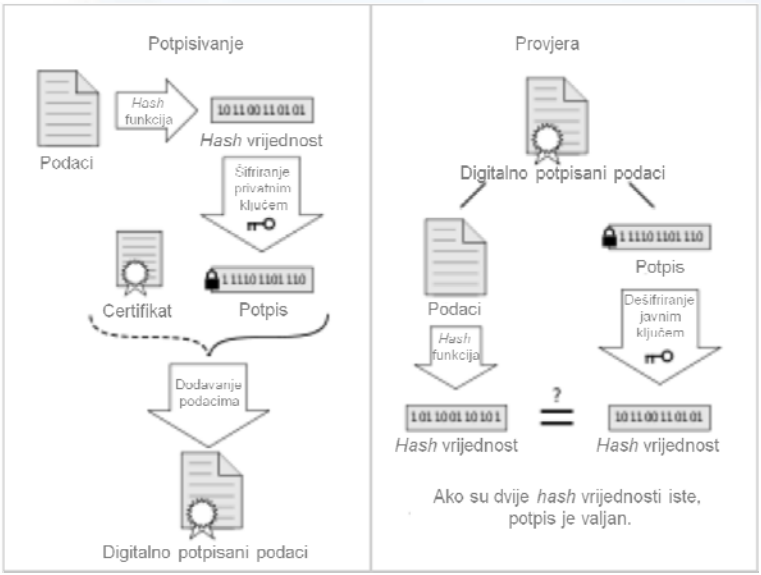
Prilikom rada postoje dva glavna zahtjeva koja se moraju ispuniti. Prvi je da generirani potpis iz fiksne poruke i privatnog ključa treba provjeriti autentičnost poruke koristeći odgovarajući javni ključ. Drugi zahtjev govori da mora biti računalno nemoguće generirati valjani popis osobi koja ne posjeduje odgovarajući privatni ključ.

3.2.1. Potpisivanje podataka i provjera

Postupak potpisivanja podataka (slika 3) obavlja se tako da se prvo odredi *hash* vrijednost uporabom neke od *hash* funkcija. *Hash* funkcija je svaki algoritam ili rutina koja preslikava mali skup podataka u veći skup podataka zvan ključevi. Vrijednosti koje vraća jedna *hash* funkcija zove se *hash* vrijednost ili kod.

Nakon određivanja *hash* vrijednosti podataka za šifriranje, ta vrijednost se šifrira privatnim ključem pošiljatelja čime se dobije potpis poruke. Zajedno s certifikatom, potpis se dodaje inicijalnim podacima te se dobiju digitalno potpisani podaci.

Postupak provjere, prikazan na slici 3, počinje s digitalno potpisanim podacima. Prvi korak je odvajanje potpisa i podataka kako bi se mogla provjeriti njegova valjanost. Znači, podaci i potpis se odvajaju i posebno obrađuju. Na jednoj strani obavlja se obrada podataka koji se propuštaju kroz istu *hash* funkciju kako bi se dobila ista *hash* vrijednost primljenih podataka. Na drugoj strani se obavlja dešifriranje potpisa javnim ključem pošiljatelja kako bi se dobila *hash* vrijednost koju je izračunao i poslao pošiljatelj. Dvije *hash* vrijednosti se zatim uspoređuju te, ukoliko su identične, potpis se proglašava valjanim.



Slika 3. Šifriranje i provjera podataka

[5] Problem disketnih logaritama koristi matematičke strukture zvane grupe, tj. skupinu elemenata i binarnu operaciju.

3.3. Uporaba digitalnog potpisa

Kako su organizacije napustile ručno potpisivanje dokumenata, digitalni potpisi pružaju dodatnu sigurnost za podrijetlo, identitet i status elektroničkih dokumenata, kao i priznanje pristanka i odobrenja potpisnika. Razne organizacije koriste digitalne potpise u svakodnevnim aktivnostima. Organizacija GPO[6] (eng. *Government Printing Office*) u SAD-u objavljuje elektroničku inačicu privatnog i javnog zakona te kongresne račune s digitalnim potpisima. Sveučilišta, uključujući *University of Chicago*, objavljuju elektroničke prijepise s digitalnim potpisima studentima.

Nekoliko osnovnih razloga za uporabu digitalnih potpisa u komunikacijama navedeni su u nastavku.

- **Autentikacija** (eng. *Authentication*)

  Iako poruke često sadrže informacije o pošiljatelju poruke, ti podaci ne moraju biti pouzdani. Digitalni potpis može se koristiti za autentikaciju izvora poruke. Kada je vlasništvo digitalno potpisanog tajnog ključa vezano za određenog korisnika, valjani potpis pokazuje da je poruku poslao upravo taj korisnik. Važnost visoke povjerljivosti u autentikaciji pošiljatelja je posebno važna u financijskom kontekstu. Na primjer, područni ured banke šalje naredbe središnjem uredu zahtijevajući izmjenu u balansu nekog računa. Ako središnji ured nije uvjeren da je takva poruka zaista poslana iz autenticiranog izvor, postupanje po primljenom zahtjevu bila bi velika pogreška.

- **Integritet** (eng. *Integrity*)

  U mnogim scenarijima, pošiljatelj i primatelj poruke mogu imati potrebu za povjerenjem da poruka nije mijenjana tijekom prijenosa. Iako šifriranje skriva sadržaj poruke, moguće je izmijeniti šifriranu poruku bez njenog razumijevanja. Međutim, ako je poruka digitalno potpisana, svaka promjena u poruci nakon potpisivanja rezultirat će neslaganjem potpisa s porukom. Nadalje, ne postoji efikasan način izmijene poruke i njenog potpisa kako bi se proizvela nova poruka s valjanim potpisom jer se takav postupak za sada smatra računalno neisplativim za većinu kriptografskih *hash* funkcija.

- **Neporicanje izvora** (eng. *Non-repudiation of origin*)

  Neporicanje izvora je važan aspekt digitalnih potpisa. Ovom značajkom entitet koji je potpisao neku informaciju ne može kasnije poreći tu radnju. Slično tomu, pristup javnom ključu ne omogućuje trećoj strani da napravi valjani potpis u ime vlasnika javnog ključa.

3.4. Sigurnosni problemi

Sigurnosni stručnjaci Goldwasser, Micali i Rivest opisali su nekoliko modela napada na digitalne potpise:

- napad poznavanjem samo ključa (eng. *key-only attack*) – napadač posjeduje samo javni ključ za provjeru,
- napad poznavanjem poruke (eng. *known message attack*) – napadač posjeduje valjan potpis poruke,
- napad adaptivnim izborom poruke (eng. *adaptive chosen message attack*)– napadač prvo nauči potpise na proizvoljnim porukama po vlastitom izboru.

Rezultati uspješnih napada mogu biti:

- totalni proboj (eng. *total break*) – otkrivanje ključa za potpisivanje,
- univerzalno krivotvorenje (eng. *universal forgery*)– mogućnost lažiranja potpisa za bilo koju poruku,
- selektivno krivotvorenje (eng. *selective forgery*) – potpis poruke po izboru suparniku,
- egzistencijalno krivotvorenje (eng. *existential forgery*) – valjana poruka/potpis koji nisu već znani suparniku.

[6] Organizacija GPO objavljuje i širi službene i autentične vladine objave Kongresu, Vladinim agencijama, Vladinim depozitarnim knjižnicama te američkoj javnosti.

4. XML digitalni potpis

XML potpis (zvan i *XMLDsig*, *XML-DSig*, *XML-Sig*) definira XML sintaksu za digitalne potpise te je specificiran u W3C preporuci „XML *Signature Syntax and Processing*“. Može se koristiti za potpisivanje podataka bilo kojeg tipa (resursa), obično XML dokumenata, ali svi podaci kojima se može pristupiti preko URL[7] (eng. *Uniform Resource Locator*) niza mogu se potpisati. XML potpis ima više oblika s obzirom na način uporabe:

- Odvojeni potpis (eng. *detached signature*) - potpis korišten za potpis resursa izvan XML dokumenta,
- Omotani potpis (eng. *enveloped signature*) – potpis korišten za potpis nekog dijela dokumenta,
- Omotavajući potpis (eng. *enveloping signature*) – potpis sadrži potpisane podatke unutar sebe

Struktura jednog XML potpisa dana je u nastavku, a sastoji se od elementa *Signature*.

```
<Signature>
  <SignedInfo>
    <CanonicalizationMethod />
    <SignatureMethod />
    <Reference>
       <Transforms>
       <DigestMethod>
       <DigestValue>
    </Reference>
    <Reference /> etc.
  </SignedInfo>
  <SignatureValue />
  <KeyInfo />
  <Object />
</Signature>
```

Element *SignedInfo* sadrži ili referencira potpisane podatke i specificira korištene algoritme. Elementi *SignatureMethod* (parametri za generiranje potpisa) i *CanonicalizationMethod* (algoritam za generiranje potpisa) koriste element *SignatureValue* te su uključeni u element *SignedInfo* radi zaštite od izmjene. Jedan ili više elemenata *Reference* specificira resurse koji se potpisuju te transformaciju koja se obavlja na resursu prije potpisivanja. Transformacija može biti XPath izraz koji odabire definiran podskup stabla dokumenta. Element *DigestMethod* definira *hash* algoritam, a *DigestValue* sadrži rezultat primjene tog algoritma na transformirani resurs. Element *SignatureValue* sadrži rezultat potpisivanja kodiran preko algoritma Base64[8]. Element *KeyInfo* opcionalno omogućava potpisniku pružanje ključa za validaciju potpisa, obično u obliku jedno ili više X.509[9] digitalnih certifikata. I na kraju, element *Object* opcionalno sadrži potpisane podatke ako se radi o omotavajućem potpisu.

4.1. XML šifriranje

XML šifriranje (eng. XML *Encryption*) ili *XML-Enc* je standard organizacije W3C pomoću kojeg se XML sadržaj kodira i tako postaje vidljiv (dostupan) samo za određenog primatelja, a nevidljiv za sve ostale. Osim kriptiranja cijelog dokumenta, moguće je zaštititi i pojedinačne dijelove XML dokumenta.

[7] URL niz je niz zakova koji specificira gdje je neki resurs na Internetu dostupan.

[8] Base64 je skupina sličnih shema za šifriranje koja predstavlja binarne podatke u ASCII formatu transformacijom u radix-64 reprezentaciju.

[9] X.509 je ITU-T standard za PKI (eng. *public key infrastructure*), SSO (eng. *single sign-on*) i PMI (eng. *Privilege Management Infrastructure*).

Iako se XML šifriranje može koristiti za šifriranje bilo koje vrste podataka, poznato je pod tim nazivom zbog XML elemenata („*EncryptedData*“ i „*EncryptedKey*“) koji sadrže informacije o šifriranom tekstu, ključu i algoritmima.

Postoje tri pristupa XML šifriranja:

1. **Šifriranje XML dokumenta koristeći samo simetričnu enkripciju** – u jednoj sjednici se koristi samo jedan ključ koji služi za šifriranje i za dešifriranje XML dokumenta. Ključ nije pohranjen sa šifriranim XML-om pa mora biti učitan tokom procesa i zaštićen prilikom pohranjivanja.
2. **Šifriranje XML-a kombiniranjem asimetrične i simetrične enkripcije** – ovaj pristup zahtijeva simetrični ključ za šifriranje podataka i asimetrični ključ za zaštitu simetričnog ključa. Oba ključa za enkripciju podataka spremljeni su u XML dokumentu. Javni asimetrični ključ se koristi za šifriranje ključa sjednice, dok se privatni asimetrični ključ koristi za dešifriranje ključa.
3. **Šifriranje pomoću XML X.509 certifikata** – ovaj pristup koristi X.509 certifikat kao simetrični ključ. X.509 certifikate osiguravaju sigurne treće strane, primjerice VeriSign.

U nastavku teksta dan je primjer šifriranja XML dokumenta.

Originalni dokument je:

```
<PaymentInfo xmlns='http://example.org/paymentv2'>
  <Name>John Smith</Name>
  <CreditCard Limit='5,000' Currency='USD'>
    <Number>4019 2445 0277 5567</Number>
    <Issuer>Example Bank</Issuer>
    <Expiration>04/02</Expiration>
  </CreditCard>
</PaymentInfo>
```

Kod u nastavku prikazuje XML dokument nakon šifriranja. Element *EncryptedData* predstavlja šifrirani element *CreditCard*. Element *EncryptionMethod* opisuje primijenjeni algoritam šifriranja, a to je trostruki DES[10] (eng. *Data Encryption Standard*) u ovom primjeru. Element *KeyInfo* sadrži podatke za preuzimanje ključa dešifriranja, a to je element *KeyName* u ovom primjeru. Element *CipherValue* sadrži šifrirani tekst dobiven šifriranjem elementa *CreditCard*.

```
<PaymentInfo xmlns='http://example.org/paymentv2'>
  <Name>John Smith</Name>
  <EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Element'
     xmlns='http://www.w3.org/2001/04/xmlenc#'>
    <EncryptionMethod
       Algorithm='http://www.w3.org/2001/04/xmlenc#tripledes-cbc'/>
       <KeyInfo xmlns='http://www.w3.org/2000/09/xmldsig#'>
         <KeyName>John Smith</KeyName>
       </KeyInfo>
       <CipherData>
         <CipherValue>ydUNqHkMrD...</CipherValue>
       </CipherData>
  </EncryptedData>
</PaymentInfo>
```

U primjeru 2 se pretpostavlja da pošiljatelj i primatelj imaju zajednički tajni ključ šifriranja. Ako primatelj ima javni i privatni ključ, što je najvjerojatniji slučaj, element *CreditCard* može biti šifriran kao što je prikazano u nastavku. Element *EncryptedData* je isti kao element *EncryptedData* u primjeru 2. Međutim, može se vidjeti da element *KeyInfo* u ovom primjeru sadrži element *EncryptedKey*.

[10] DES je blokovska šifra koja se koristi za dijeljene tajni informacija za šifriranje. Trostruki DES (eng. Triple Data Encryption Algorithm) ili TDEA je blokovska šifra koja primjenjuje DES šifru tri puta za svaki blok podataka.

```
<PaymentInfo xmlns='http://example.org/paymentv2'>
  <Name>John Smith</Name>
  <EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Element'
    xmlns='http://www.w3.org/2001/04/xmlenc#'>
    <EncryptionMethod
      Algorithm='http://www.w3.org/2001/04/xmlenc#tripledes-cbc'/>
    <KeyInfo xmlns='http://www.w3.org/2000/09/xmldsig#'>
      <EncryptedKey xmlns='http://www.w3.org/2001/04/xmlenc#'>
        <EncryptionMethod
          Algorithm='http://www.w3.org/2001/04/xmlenc#rsa-1_5'/>
        <KeyInfo xmlns='http://www.w3.org/2000/09/xmldsig#'>
          <KeyName>Sally Doe</KeyName>
        </KeyInfo>
        <CipherData>
          <CipherValue>yMTEyOTA1M...</CipherValue>
        </CipherData>
      </EncryptedKey>
    </KeyInfo>
    <CipherData>
      <CipherValue>ydUNqHkMrD...</CipherValue>
    </CipherData>
  </EncryptedData>
</PaymentInfo>
```

4.2. Provjera XML digitalnih potpisa

Prilikom provjere XML potpisa, slijedi se procedura zvana „*Core Validation*“, koja se sastoji od dva dijela:

1. **Provjera referenci** (eng. *Reference Validation*) – sažetak svake reference se provjerava preuzimanjem odgovarajućeg resursa i primjenom transformacija i metoda. Rezultat se uspoređuje s vrijednosti *DigestValue*, a ako dođe do neslaganja vrijednosti, provjera je neuspješna.
2. **Provjera potpisa** (eng. *Signature Validation*) – element SignedInfo je serijaliziran kanoničkom metodom definiranom u elementu *CanonicalizationMethod*, ključni podaci se dohvaćaju preko elementa *KeyInfo* te se potpis provjerava uporabom metode specificirane u elementu *SignatureMethod*.

Ova procedura određuje da li je resurse zaista potpisala povjerljiva strana. Međutim, budući da se koriste kanoničke i transformacijske metode, strana koja provjerava mora voditi računa o tome što je doista potpisano te da su sažeci doista sažeci informacije koja je prisutna u originalnim podacima. Drugim riječima, potrebno je osigurati da korišteni algoritmi ne mijenjaju potpisane podatke.

4.3. Prednosti i nedostaci XML digitalnih potpisa

Dobra strana XML digitalnih potpisa je bolja fleksibilnost od digitalnih potpisa kao što su PGP[11] (eng. *Pretty Good Privacy*) i CMS[12] (eng. *Cryptographic Message Syntax*), jer ne radi na binarnim podacima nego na XML informacijskom skupu (eng. XML *Information Set* ili XML *Infoset*). Spomenuti skup je specifikacija organizacije W3C koja opisuje podatkovni model XML dokumenta u obliku skupa informacijskih točaka. Definicije skupa su namijenjene za uporabu u drugim specifikacijama koje se trebaju referirati na informacije u dobro formiranom XML dokumentu.

[11] PGP je računalni program za šifriranje i dešifriranje podataka koji pruža kriptografsku privatnost i autentikaciju u komunikaciji.

[12] CMS je standard za kriptografski zaštićene poruke, a može se koristiti za digitalno potpisivanje, sažetke, autentikaciju ili šifriranje bilo kojeg oblika digitalnih podataka.

Uporabom navedenog informacijskog skupa omogućuje se:

- rad na podskupu podataka,
- postojanje različitih načina za povezivanje potpisa i potpisanih informacija,
- izvođenje transformacija.

Ostale prednosti XML digitalnih potpisa dolaze zbog koncepta zvanog kanonizacija (eng. *canonicalization*) što omogućuje potpisivanje samo važnog dijela te uklanjanje manje važnih podataka poput praznih razmaka i završetka retka.

Kanonizacija se koristi kako bi se izbjegli razni problemi kod XML potpisa te da bi se moglo garantirati da logički jednaki XML dokumenti daju identičan digitalni potpis. Kreiranje XML potpisa je malo složenije od kreiranje običnog digitalnog potpisa jer XML dokument može imati više od jedne legalne reprezentacije. Na primjer, razmak unutar XML elementa nije sintaksno važan pa je <Elem > sintaksno identičan kao i <Elem>. Također, budući da je digitalni potpis kreiran uporabom algoritma asimetričnog ključa, razlika u jednom oktetu podataka uzrokovala bi razliku u digitalnim potpisima. Nadalje, ako se XML dokument prenosi od računala do računala, oznaka za kraj reda CR (eng. *Carriage return*) može se promijeniti u LF (eng. *Line feed*) ili obrnuto. Program koji provjerava XML dokument može kasnije prevesti dokument na različite načine, na primjer dodati višak prostora između atributa. Kanonički XML je vrlo važan kada XML potpis označava udaljeni dokument. Kanonizacija je zapravo transformacija koja se koristi prilikom potpisivanja dokumenta.

Arhitekturu XML potpisa, kao i kanonizaciju, za potpisivanje i šifriranje XML podataka često kritiziraju stručnjaci zbog njihove složenosti, inherentnim zahtjevima za obradom i slabim karakteristikama izvođenja. Provođenje XML kanonizacije uzrokuje prekomjerno kašnjenje koje je preveliko za savladavanje u SOA[13] (eng. *Service-oriented architecture*) aplikacijama.

Također, bez odgovarajuće politike za uporabu XML digitalnih potpisa u SOAP i WS-Security uslugama, može doći do ozbiljnih sigurnosnih problema (opisano u poglavlju 4.4).

4.4. Ranjivosti XML digitalnih potpisa

Nepravilno rukovanje XML digitalnim potpisima može dovesti do pojave sigurnosnih ranjivosti. Jedno od važnih obilježja ovih potpisa je da se potpisani XML elementi, zajedno s potpisom, mogu kopirati iz jednog dokumenta u drugi uz zadržavanje mogućnosti za provjeru potpisa. Navedeno obilježja može se iskoristiti kada više sudionika obrađuje i transformira dokument kroz poslovni proces. Međutim, isto obilježje može se iskoristiti kako bi se neopaženo izmijenio dokument. U slučaju XML-a moguće je provesti jednostavne mjere zaštite od ovakvih napada, ali u slučaju SOAP usluga te mjere zaštite obično nisu moguće zbog strukture poruke i povezanih pravila koje SOAP koristi. Postoji više inačica napada koje se mogu izvesti u ovom slučaju, a u nastavku je prikazan jedan kontekst.

4.4.1. Kontekst jednostavnog pretka

U nekim slučajevima, element mora biti na određenom mjestu u dokumentu, a njegova semantika može biti potpuno izvedena iz njegovog imena, atributa te vrijednosti i imena njegovih predaka. Ovaj slučaj naziva se kontekst jednostavnog pretka, a jedan od primjera takvih elemenata je SOAP *Body*.

Primjer u nastavku prikazuje jednostavnu SOAP poruku.

```
<soap: Envelope …>
   <soap: Body>
     <getQuote Symbol="IBM"/>
   </ soap: Body>
</soap: Envelope …>
```

[13] SOA je fleksibilna skupina principa za dizajn koji se koriste tijekom faza razvoja sustava i integracije u računarstvu.

Poruka sadrži *root* element dokumenta *soap:Envelope*. Unutar njega nalazi se element *soap:Body* koji je dijete elementa *soap:Envelope*, a element *soap:getQuote* je dijete elementa *soap:Body*.

Aplikacija o burzovnoj kotaciji koja primi ovakvu poruku treba vratiti cijenu identificiranu s vrijednošću atributa *qetQuote/@Symbol*. Aplikacija bi trebala moći autenticirati identitet osobe koja šalje takav zahtjev te zaštititi poruku od namjerne ili nenamjerne izmijene tijekom prijenosa. U tom slučaju pružatelj usluge bi objavio sigurnosnu politiku u kojoj opisuje zahtjeve da:

1. Element *soap:Body* mora biti potpisan uporabom WSS[14] (eng. *Web Services Security* ili *WS-Security*) proširenja s XML potpisom.
2. Pridruženi ključ za provjeru potpisa mora biti pružen preko X.509v3 certifikata koji izdaje pouzdana strana.

Primjer u nastavku sadrži poruku koju je pošiljatelj zaštitio uporabom WSS-a i XML potpisa.

```
<soap: Envelope …>
   <soap: Header>
      <wsse: Security>
         <wsse:BinarySecurityToken
           ValueType="…#x509v3"
           EncodingType="…#Base64Binary"
           Wsu:Id="X509Token">
           MIabcdefg0123456789…
         </wsse:BinarySecurityToken>
         <ds:Signature>
            <ds:SignedInfo>
            <ds:CanonicalizationMethod
              Algorithm="…/xml-exc-c14n#"/>
            <ds:SignatureMethod
              Algorithm="…#rsa-sha1"/>
            <ds: Reference URI="#theBody">
            …
            </ds:SignedInfo>
            <ds:SignatureValue>
            …
            <ds:KeyInfo>
               <wsse:SecurityTokenReference>
                  <wsse:Reference URI="#x509Token"/>
               </wsse:SecurityTokenReference>
         </ds:KeyInfo>
         </ds:Signature>
      </wsse: Security>
   </soap: Header>
   <soap: Body wsu:Id="theBody">
     <getQuote Symbol="IBM"/>
   </ soap: Body>
</soap: Envelope …>
```

Primatelj prethodne poruke obrađuje uključeni potpis za provjeru da potpisani element, u ovom slučaju soap:Body, nije bio mijenjan nakon potpisivanja. Primatelj također provjerava da je korisnik koji zahtjeva podatke, identificiran u polju *Subject* X.509v3 certifikata, autoriziran za postavljenje takvog zahtjeva.

U nastavku je primjer izmijenjene inačice poruke u kojoj napadač želi podići prava pristupa.

```
<soap: Envelope …>
   <soap: Header>
      <wsse: Security>
      …
```

[14] WSS je fleksibilan dodatak SOAP-u koji omogućuje primjenu sigurnosti u web uslugama.

```
          <ds:Signature>
             <ds:SignedInfo>
             …
                <ds: Reference URI="#theBody">
             …
             </ds:SignedInfo>
          </ds:Signature>
       </wsse: Security>
       <Wrapper
         soap:mustUnderstand="0"
         soap:role="…/none">
          <soap:Body wsu="theBody">
             <getQoute Symbol="IBM" />
          </soap:Body>
       </Wrapper>
    </soap:Header>
       <soap:Body wsu:Id="newBody">
          <geQoute Symbol="MBI" />
       </soap:Body>
</soap:Envelope>
```

Vidljivo je kako je sada element *soap:Body* dijete elementa *Wrapper* umjesto elementa *soap:Envelope*. Novi element *soap:Body* je dodan na kraj i on je dijete elementa *soap:Envelope* te specificira različitu vrijednost atributa *getQoute/@Symbol*.

U ovom primjeru atribut *soap:mustUnderstand* se koristi da indicira da element *Wrapper* može biti ignoriran. Također, atribut *soap:role* ukazuje da primatelj ne cilja na element *Wrapper*. Međutim, i bez tih atributa, očekivano ponašanje je isto jer primatelj ne treba razumjeti uvedeni element *Wrapper*, a uobičajeno ponašanje u takvom slučaju je ignoriranje elemenata.

Loše implementirane usluge odobrit će ovakav zahtjev jer:

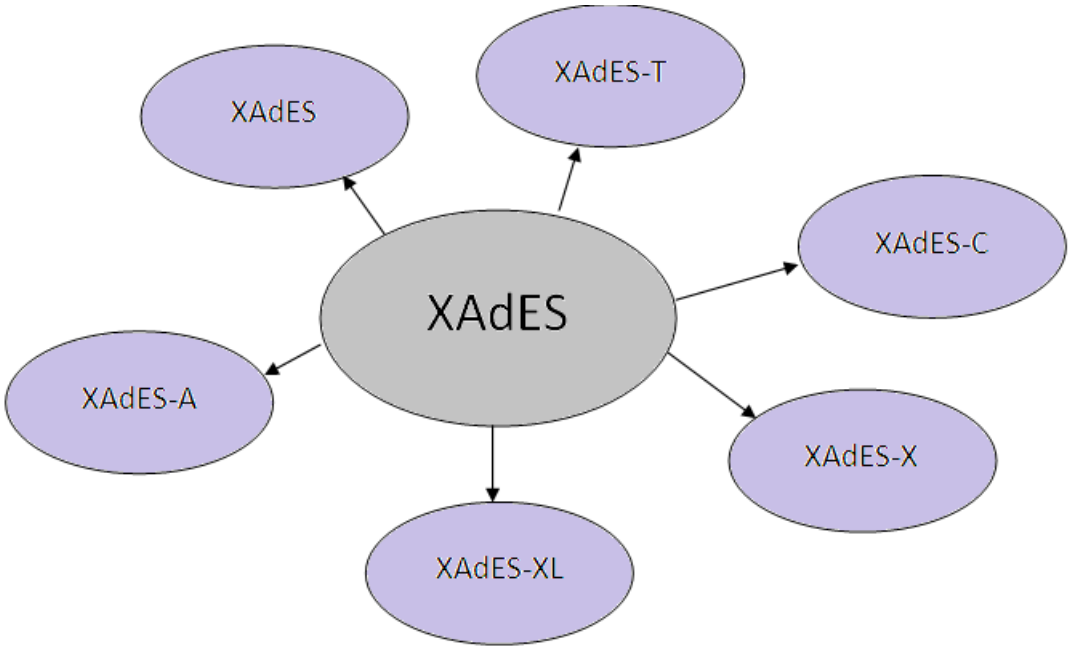
1. poruka sadrži valjani potpis,
2. vrijednost elementa na koji se odnosi potpis je nepromijenjena,
3. referenca koristi mehanizam neovisan o mjestu.

Ovakav pokušaj napada može se spriječiti odgovarajuće specificiranom i uvedenom sigurnosnom politikom. Potrebno je provesti provjeru da je potpisani element *soap:Body* koji će aplikacija obraditi, a ne bilo koji element s istim imenom.

4.5. XAdES proširenje

XAdES (eng. XML *Advanced Electronic Signatures*) je skup proširenja XML digitalnih potpisa, što ga čini pogodnim za napredne elektroničke potpise. Dok je XML digitalni potpis općenit način digitalnog potpisivanja dokumenata, XAdES određuje precizne uvjete korištenja XML potpisa s naprednim elektroničkim potpisom kojeg propisuje EU Direktiva 1999/93/EZ. Jedna važna prednost XAdES-a je da elektronički potpisani dokumenti mogu ostati na snazi dugo vremena, čak i ako su temeljni kriptografski algoritmi otkriveni.

XAdES definira šest profila (oblika) koji se razlikuju prema razini zaštite koju nude, a svaki profil uključuje i proširuje prethodni. XAdES profili su dani u nastavku (slika 4) te kategorizirani u tablici 1.



Slika 4. Podjela XAdES proširenja

- **XAdES** – osnovni oblik naprednog potpisa koji samo zadovoljava zakonske uvjete za napredni potpis.
- **XAdES-T** (*timestamp*) – napredni potpis u kojem je dodano polje *timestamp* za zaštitu od odbijanja.
- **XAdES-C** (*complete*) – napredni potpis u kojem su dodane reference na provjeru podataka (certifikati i lista opozvanih certifikata) potpisanih dokumenata kako bi se omogućila *off-line* verifikacija i provjera u budućnosti (ali ne i pohrana stvarnih podataka).
- **XAdES-X** (*extended*) – napredni potpis u kojem su dodane vremenske oznake na reference koje sadrži XAdES-C kako bi se zaštitilo od mogućih pogrešaka certifikata u lancu u budućnosti.
- **XAdES-XL** (*extended long-term*) – napredni potpis u kojem su dodani stvarni certifikati i lista opozvanih certifikata kako bi se omogućila provjera u budućnosti, čak i ako njihov izvor nije dostupan.
- **XAdES-A** (*archival*) – napredni potpis u kojem je dodana mogućnost periodičnog *timestamping*-a (npr. svake godine) za arhivirane dokumente kako bi se spriječile pogreške uzrokovane slabljenjem potpisa tijekom dugogodišnjeg razdoblja.

	Omogućuje digitalno potpisivanje	**Omogućuje kriptografsku vremensku oznaku**	**Sadrži povučene reference**	**U potpunosti sadrži povučene podatke**	**Omogućava sigurnosnu periodičnu vremensku oznaku**
XAdES	DA	NE	NE	NE	NE
XAdES-T	DA	DA	NE	NE	NE
XAdES-C	DA	DA	DA	NE	NE
XAdES-X	DA	DA	DA	NE	NE
XAdES-XL	DA	DA	DA	DA	NE
XAdES-A	DA	DA	DA	DA	DA

Tablica 1. Rezime XAdES naprednih elektroničkih potpisa

5. Normizacija digitalnih potpisa

Normizacija[15] u području elektroničkog potpisa za EU krenula je donošenjem direktive 1999/93/EC Europske komisije. Poznatija normizacijska tijela koja se bave normizacijom digitalnih XML potpisa u sklopu općenite normizacije digitalnih potpisa su: CEN/ISSS (eng. *CEN Information Society Standardization System*), ETSI (eng. *European Telecommunication Standards Institute*), IETF/RFC (eng. Internet *Engineering Task Force/Request For Comment*) i PKCS (eng. *Public Key Cryptography Standards*). Namjera ove direktive je 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 interoperabilnost između raznih vrsta primjene elektroničkog potpisa donesen je skup normi i specifikacija. Norme i specifikacije donijeli su normizacijska 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.

U okviru ovih inicijativa navedene su radne skupine, konzorciji i povjerenstva osnovana od međunarodno priznatih organizacija koje su izradile preporuke i specifikacije kojih se treba pridržavati kod uvođenja i primjene elektroničkih potpisa. Te skupine su navedene u nastavku dokumenta.

1. **CEN/ISSS (eng. CEN *Information Society Standardization System*)**

   CEN/ISSS WS/E-*Sign* (eng. *Workshop on Electronic Signature*) radi pod nadležnošću Europskog povjerenstva za normizaciju - CEN (eng. *Comité Européen de Normalisation*). CEN/ISSS je odgovoran za dio programa EESSI (eng. *Electronic Exchange of Social Security Information*) koji se odnosi na norme kvalitete i funkcionalnosti za stvaranje i verifikaciju elektroničkih potpisa, kao i na norme za kvalitetu i funkcionalnost dobavljača usluga certificiranja (eng. *Certification Service Providers,* CSP). Radionice se često koriste radi brzih promjena u tehnologijama, a otvorene su za sve zainteresirane sudionike. Rezultati rada radionica objavljuju se kao CWA (eng. CEN *Workshop Agreements*) sporazumi, a neke specifikacije s tog područja su:

   - **CWA 14355** Vodiči za implementaciju sigurnosnih uređaja za kreiranje potpisa (eng. *Guidelines for the implementation of Secure Signature-Creation Devices*),
   - **CWA 14169** Sigurnosni uređaji za kreiranje potpisa “EAL 4+” (eng. *Secure signature-creation devices* "EAL 4+"),
   - **CWA 14365** Vodič za upotrebu elektroničkog potpisa (eng. *Guide on the use of Electronic Signature*),
   - **CWA 14167-1** Sigurnosni zahtjevi za certificate sustava za elektronički potpis (eng. *Security Requirements for System Certificates for Electronic Signature*) te
   - **CWA 14167-3** Kriptografski modul za CSP uređaje za generiranje ključa – profil zaštite (eng. *Cryptographic Module for CSP Key Generation Services - Protection Profile*).

2. **ETSI (eng. *European Telecommunication Standards Institute*)**

   ETSI SEC je odgovoran za EESSI (eng. ETSI *Electronic Signatures and Infrastructures*) program, a radna skupina ESI (eng. *Electronic Signatures and Infrastructures*) je odgovorna za izvođenje tog programa. Posao se odrađuje u zajednici s CEN/ISSS unutar ITCSB/EESSI radnog programa. Zadaci slijede program koji je predložen od EESSI te podupiru primjenu Europske direktive 1999/93/EC za elektronički potpis. Na osnovu tog posla izrađene su norme i specifikacije u okviru ovog područja:

   - **ETSI TR 102 038** TC- TC sigurnosno - elektronički potpis i infrastruktura (ESI) (eng. *Security - Electronic Signature and Infrastructure* (ESI)),
   - **ETSI TS 101 903** Napredni XML elektronički potpisi (eng. XML *Advanced Electronic Signatures*),
   - **ETSI TS 101 861** Profil vremenske oznake (eng. *Time Stamping Profile*),

[15] Normizacija je djelatnost uspostavljanja odredaba za opću i višekratnu uporabu koje se odnose na postojeće ili moguće probleme radi postizanja najboljeg stupnja uređenosti u danome kontekstu.

- **ETSI TS 101 733** Formati elektroničkog potpisa (eng. *Electronic signature formats*) te
- **ETSI TS 102 280** - X.509 V.3 profil certifikata za certifikate izdane osobama (eng. X.509 V.3 *Certificate Profile for Certificates Issued to Natural Persons*).

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

   Zadatak je ovih specifikacija definirati digitalne certifikate na tehničkoj razini te protokole u PKI infrastrukturi i elektroničkim potpisima na Internetu. U okviru toga donesene su sljedeće specifikacije (eng. *Request for Comments,* RFC):

   - **RFC 3280** Infrastrukturni certifikat internetskog X.509 javnog ključa i lista povučenih certifikata (eng. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*),
   - **RFC 3739** Infrastruktura internetskog X.509 javnog ključa (eng. *Internet X.509 Public Key Infrastructure: Qualified Certificates Profile*),
   - **RFC 2251** Trivijalni protokol za pristup direktoriju (eng. *Lightweight Directory Access Protocol*) te
   - **RFC 2256** Sažetak X.500(96) korisničke sheme za upotrebu s LDAPv3 (eng. *A Summary of the X.500(96) User Schema for use with LDAPv3*).

4. **RSA *Laboratories* – PKCS (eng. *Public Key Crypto Standards*)**

   Zbog potrebe tehničkog ostvarivanja PKI infrastrukture koja je zasnovana na primjeni RSA (eng. Rivest, Shamir and Adleman) algoritma asimetrične enkripcije primjenom javnog ključa donesene su sljedeće PKCS (eng. *Public Key Cryptography Standards*) norme:

   - **PKCS 1** RSA enkripcijski standard (eng. *RSA Encryption Standard*),
   - **PKCS 5** Kriptografski standard zasnovan na lozinkama (eng. *Password-based Cryptography Standard*),
   - **PKCS 7** Kriptografski standard za sintaksu poruka (eng. *Cryptographic Message Syntax Standard*),
   - **PKCS 9** Odabrani tipovi atributa (eng. *Selected Attribute Types*) te
   - **PKCS 10** Sintaksa zahtjeva za certifikaciju (eng. *Certification Request Syntax*).

6. Budućnost XML digitalnih potpisa

Uporaba tradicionalnog potpisivanja dokumenata u slučaju sklapanja poslovnih ugovora još uvijek prevladava u svijetu. Razlog tomu je činjenica da je sigurnosni faktor u *online* ugovaraju bio loše zastupljen u prošlosti što je moglo vrlo lako rezultirati prevarama. Ipak, rano su prepoznate prednosti koje donosi *online* komunikacija pa su razvijeni sustavi i procedure za zadovoljavanje zahtjeva autentikacije, integriteta, neporecivosti i povjerljivosti podataka koji se prenose. Osnovni koncept koji se pri tome koristi su digitalni potpisi koji imaju više prednosti nad rukom pisanim potpisima. Digitalni potpis pruža informaciju o tome da li je digitalno potpisana informacija izmijenjena nakon potpisivanja, što tradicionalni potpisi ne omogućavaju. Dodatno, pošiljatelj poruke može uključiti informacije o sebi i svom identitetu šifrirane unutar digitalnog potpisa.

Zahvaljujući razvoju sustava s opisanim obilježjima, koncept *online* komunikacije mogao bi otvoriti vrata novim uslugama i oblicima poslovanja. Takvo poslovanje omogućilo bi brže i jednostavnije poslovanje i sklapanje ugovora uz razne oblike ušteda. Ipak, uvođenje ovih tehnologija u Hrvatskoj vrlo je slabo prihvaćeno i rijetko se provodi. Država ulaže sve više sredstava u napore da se ovakav oblik poslovanja uvede u bankarstvo, financijske transakcije, zdravstvo i dr. Za razliku od toga, manje, privatne firme i dalje preferiraju tradicionalne načine komunikacije, većinom zbog slabog poznavanja i povjerenja u sigurnost novih tehnologija. Također, dosta često organizacije ne žele ulagati u uvođenje novih tehnologija. Zbog toga, budućnost digitalnog potpisa leži ponajprije u Internet bankarstvu te obavljanju drugih bankovnih i financijskih transakcija. Može se očekivati da će jednom digitalni potpis postati osnovni oblik određivanja autentičnosti dokumenata, a treba uzeti u obzir i da je XML digitalni potpis najraširenija vrsta takvih potpisa što mu daje veliku prednost i široke mogućnosti uporabe.

7. Zaključak

Kako je XML postao osnovna komponenta za implementaciju elektroničke poslovne infrastrukture, potrebno je osigurati pouzdanost i sigurnost XML poruka kako bi se oformila osnova poslovnih transakcija. Jedan od ključnih koraka u osiguravanju transakcija je koncept digitalnog potpisa, koji pruža integritet i autentikaciju izvora poslovnog dokumenta ili bilo koje druge poslane poruke. XML digitalni potpis je standard za digitalne potpise koji se bavi problemima i zahtjevima XML-a u operacijama digitalnog potpisivanja te koristi XML sintaksu za dohvaćanje rezultata, što olakšava njegovu uporabu u XML aplikacijama.

Lako je uočiti sve prednosti koje nosi komunikacija uporabom digitalnih potpisa, od raznih vrsta ušteda do pružanja dodatnih informacija o pošiljatelju i osiguravanju poruke, što nije slučaj kod tradicionalnih načina potpisivanja. Ipak, ova tehnologija još je nedovoljno proširena ponajprije zbog slabe edukacije korisnika. Još jednu prepreku uporabi digitalnih potpisa donosi potreba za implementacijom posebnih aplikacija za stvaranje i provjeru potpisa. Naravno, tu su i sigurnosni problemi vezani uz uporabu tih sustava. Treba napomenuti i da svako šifriranje podataka leži na nekom algoritmu te svoju snagu vuče iz toga koliko je taj algoritam teško probiti.

U budućnosti se očekuje širenje opisanih tehnologija zbog njihove jednostavnosti i lakoće uporabe u raznim područjima. Također, veliku prednost donose i dobre karakteristike digitalnog potpisivanja koje mogu donijeti razne pogodnosti organizacijama koje ga koriste.

8. Leksikon pojmova

PKI (Infrastruktura javnih ključeva)

PKI je sustav poslužitelja koji služi kao središnji autoritet koji povezuje javne ključeve s njihovim vlasnicima.

http://searchsecurity.techtarget.com/definition/PKI

DES (DES algoritam šifriranja)

Vrlo popularan kriptografski standard, danas zamijenjen standardom AES. - Vrlo popularan kriptografski standard, danas zamijenjen standardom AES. Tajni ključ za šifriranje podataka sastoji se od 56 bita, što znači da postoji ukupno 2^56 (više od 72,000,000,000,000,000) mogućih kombinacija. Za šifriranje poruke se koristi jedan od ključeva iz velikog broja kandidata. Algoritam je simetričan, što znači da obadvije strane moraju imati tajni ključ kako bi mogli komunicirati.

http://nvl.nist.gov/pub/nistpubs/sp958-lide/250-253.pdf

SOAP (*Simple Object Access Protocol*)

Protokol koji služi za izmjenu strukturiranih informacija web usluga u računalnim mrežama. Za prijenos sadržaja se koristi jezik XML i koristi protokole na aplikacijskom sloju za prijenos podataka.

http://www.w3.org/TR/soap/

URI (*Uniform Resource Identifier*)

URI je niz znakova koji se koristi za identifikaciju imena ili nekog drugog resursa na Internetu. URI sintaksa započinje URI shemom (npr. http, ftp, mailto, sip), nakon čega slijedi dvotočka i niz znakova koji ovisi o odabranoj shemi.

http://searchsoa.techtarget.com/definition/URI

XML (*EXtensible Markup Language*)

XML je kratica za *EXtensible Markup Language*, odnosno jezik za označavanje podataka. Ideja je bila stvoriti jedan jezik koji će biti jednostavno čitljiv i ljudima i računalnim programima. U XML-u se sadržaj uokviruje odgovarajućim oznakama koje ga opisuju i imaju poznato, ili lako shvatljivo značenje.

http://webdesign.about.com/od/xml/a/aa091500a.htm

DTD (*Document Type Definition*)

DTD (eng. *Document Type Definition*) je skup deklaracija označavanja koje određuju vrstu dokumenta za SGML-skup označnih jezika (SGML, XML, HTML). DTD su prethodnica XML shema i imaju sličnu funkciju, a različite mogućnosti.

http://searchsoa.techtarget.com/definition/Document-Type-Definition

XMLDsig (XML digitalni potpis)

XMLDsig (također se nazivaju XML Signature, XML-DSig, XML-Sig) definira XML sintaksu za digitalne potpise, a definira ga W3C preporuka XML *Signature Syntax and Processing* (Sintaksa i obrada XML potpisa).

http://en.wikipedia.org/wiki/XML_Signature

XAdES (Napredni XML elektronički potpisi)

XAdES (eng. XML *Advanced Electronic Signatures*) je skup proširenja XML-DSig preporuka što ga čini pogodnim korištenje u naprednim elektronskim potpisima.

http://en.wikipedia.org/wiki/XAdES

9. Reference

[1] Wikipedia: XML, http://en.wikipedia.org/wiki/Xml, rujan 2011.

[2] Wikipedia: Digital Signature, http://en.wikipedia.org/wiki/Digital_signature, rujan 2011.

[3] Wikipedia: XML Signature, http://en.wikipedia.org/wiki/XML_Signature, rujan 2011.

[4] XML Signature Syntax and Processing, http://www.w3.org/TR/xmldsig-core/, rujan 2011.

[5] IBM Research Report, XML Signature Element Wrapping Attacks and Countermeasures, http://domino.research.ibm.com/library/cyberdig.nsf/papers/73053F26BFE5D1D385257067004CFD80/$File/rc23691.pdf, kolovoz 2005.

[6] Wikipedia: XAdES, http://en.wikipedia.org/wiki/XAdES, rujan 2011.