

Digiallkirjastamine. Nõudmised digiallkirjale, standardid

Erika Matsak, PhD

1

Definitsioonid

Valdo Praust:

- *Sõnumi (faili) digitaalsignatuuriks (digital signature) nimetatakse sellest sõnumist (failist) arvutatud krüptoräsi, mis on šifreeritud digitaalsignatuuri looja privaatvõtmega.*
- *Digiallkirjaks (pikema nimetusega – digitaalalkirjaks) nimetatakse selliseid digisignatuure, mis vastavad teatud õigusakti(de) tingimustele. Digiallkirjaga tingimustele vastavate digisignatuuridega varustatud digidokumendid on nimetatud õigusaktide kohaselt tavaliselt samasuguse õigusliku staatusega, kui omakäelise allkirjaga varustatud paberdokumendid.*

http://www.ra.ee/public/Digiarhiiv/da_autentsus.pdf

2

Digiallkirja vajadus ja omadused

- Autentimine kaitseb suhtlevaid osapooli selle eest, et sekkub keegi kolmas. Samuti tagab teksti terviklikkuse.
 - Keegi kolmas (vastane) võib saata Bobile kirja Alice nimel
 - Keegi kolmas (vastane) võib kirja üle võtta ja muuta selle sisu
- On olemas võimalikud probleemid, mis võivad esile tulla ka kahe suhtleja vahel. Olgu, et John saadab krüpteeritud teksti Mary-le.
 - Mary saab võltsida sõnumi ning väita, et see on tulnud Johnilt.
 - John võib väita, et ta pole üldse seda kirja saatnud, kuna Mary saab ju seda ise võltsida
- Situatsioonis, kus osapooled ei usalda üksteist on väga oluline digiallkiri. Digiallkirjal peavad olema järgmised omadused
 - Peab olema võimalus kontrollida autorit, allkirjastamise kuupäeva ja kellaega
 - Peab olema võimalus autentida teksti digiallkirjastamise ajal
 - Digiallkiri peab olema kontrollitav kolmanda osapoollega vaidluste reguleerimiseks

3

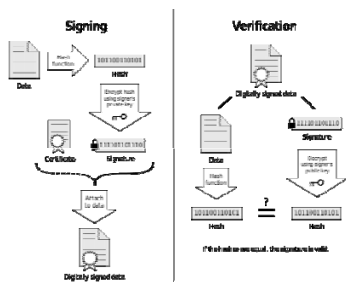
Nõudmised digiallkirjale

- Digiallkiri peab olema bitijada, mis sõltub allkirjastatud tekstist
- Digiallkiri peab sisaldama mingit unikaalset isikliku infot, selleks, et vältida võltsimist
- Digiallkirja moodustamine peab olema suhteliselt lihtne
- Peab olema arvutuslikult võimatu võltsida digiallkirja sel teel, et moodustatakse uus tekst olemasolevale digiallkirjale ning samuti sel teel, et moodustakse vale digiallkiri olemasolevale tekstile.
- Digiallkiri peab olema kompaktne ning mitte võtma palju mälu.

4

Digiallkirja skeem

- Digiallkirjastamine koosneb tavaliselt kolmest algoritmist:
- Privaatvõtme genereerimise algoritm, mis genereerib suvalise privaavõtme kõikidest võimalikest privaavõtmetest. Sama algoritm väljastab ka avaliku võtme.
- Allkirjastamise algoritm, mis lähtudes avatekstist ja privaavõttest moodustab digitaalse allkirja.
- Digiallkirja kontrollimise algoritm, mis lähtudes tekstist, digiallkirjast ning avalikust võtmest aktsepteerib või lükkab tagasi autentimise.



5

Digiallkirja liigid

- Otsene digiallkiri
 - Osalevad ainult kaks poolt: saatja ja saaja. Digiallkiri saab olla moodustatud terve avateksti šifreerimisega või hash-koodi šifreerimisega privaavõtme abil. Konfidentsiaalsus tagatakse sellega, et pärast eelnimetatud sammu šifreeritakse tekst koos allkirjaga avaliku võtmega (kui tegu on asümmeetrilise algoritmiga) või ühise salajase võtmega (sümmeetrilise algoritmi puhul).
- Arbiitriga digiallkiri
 - Iga digiallkirjastatud tekst saadetakse kõigepealt arbiitrile A, kes kontrollib, kas antud allkiri on õige. Selle järgi pannakse kuupäev ja kellaeg ning edastatakse tekst isikule Y märkusega, et digiallkiri on kontrollitud.

6

Digiallkirjaga seotud liigendamised

- Rajatud sümmeetrilistele algoritmidele
- Rajatud asümmeetrilistele algoritmidele

- Otsene, kahe inimese vaheline digiallkirjastamine. Kolmas osapool on võimalik.
- Kohustusliku kolmanda osapoolega, ehk "arbiitriga"

- Avateksti digiallkirjastamine
- Hash-koodi allkirjastamine

7

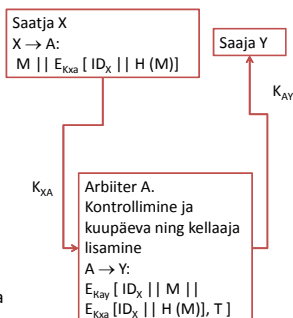
Otsene, kahe inimese vaheline digiallkiri

- Kaks etappi: digiallkirjastamine ning teksti ja allkirja krüpteerimine koos
- Vaidluste tekkimisel peab kolmas osapool saama kinnitada allkirja
- Kui digiallkiri oli antud avatekstile, siis peab saaja säilitama avateksti (et seda kasutada ning vajadusel esitada kolmandale osapoolele) ja sellele lisatud digiallkirja (kolmanda osapoole jaoks)
- Kui digiallkiri oli antud šifreeritud tekstile, siis peab saaja hoidma nii šifreerimata teksti (et seda kasutada) kui ka šifreeritud teksti (et vaidluste tekkimisel pöörduda kolmanda osapoole poole). Või peab hoidma algoritmi salastatud võtit, mille abil saab kolmas osapool kontrollida digiallkirja õigsust (sümmeetrilise algoritmi puhul).
- Kui tegu on sümmeetrilise algoritmiga, siis turvalisus sõltub sellest, kui hästi oli hoitud salajane võti. On võimalik väita, et võti on varustatud ja digiallkiri on võltsitud.

8

Digiallkiri kohustusliku kolmanda osapoolega, ehk "arbiitriga". Sümmeetriline algoritm.

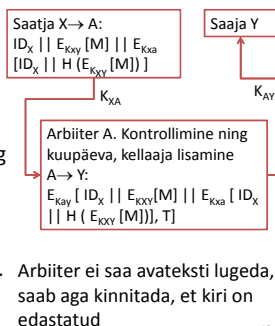
- X ei saa tagantjäreli väita, et ta pole oma kirja saanud.
- Nii saatja kui saaja peavad saama arbiitrit usaldada.
- X moodustab teksti M ning arvutab selle hash-koodi $H(M)$
- Digiallkiri moodustatakse X identifikaatorist (ID) ning hash-koodist $h=H(M)$. Seda kõike krüpteeritakse koos tekstiga võtme K_{XA} abil.
- A saab $E_{K_{XA}} [ID_X || H(M)]$, dekrüpteerib selle ning kontrollib hash-koodi. Seejärel A krüpteerib ID, esialgse sõnumi ja hetkel oleva kellaaja võtmega K_{AY} .



9

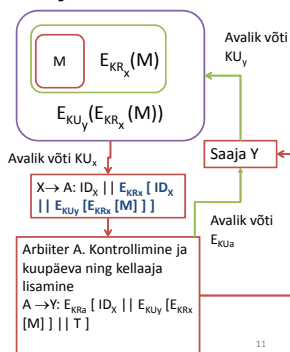
Konfidentsiaalsus arbiitriga sümmeetrilise digiallkirjastamise korral

- X edastab A-le enda ID, teksti, mis on šifreeritud võtmega K_{XY} ning allkirja.
- Allkiri koosneb ID-st ning hash-koodist, mis on šifreeritud võtmega K_{XA} .
- A dešifreerib digiallkirja ning kontrollib hash-koodi.
- A edastab Y-le kõik, mis on saadud X-lt pluss paneb kellaaja (ajatempel) šifreerides kõik võtmega K_{AY}



Konfidentsiaalsus arbiitriga asümmeetrilise digiallkirjastamise korral

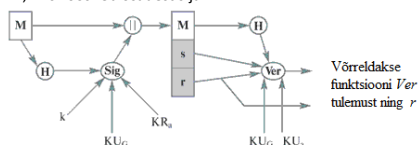
- X šifreerib teksti M kaks korda, kõigepealt privaativõtmega KR_x , seejärel avaliku võtmega KU_y , mis on saadud isikult Y käest. Sellele lisatakse X-i ID ning šifreeritakse uuesti privaativõtmega KR_x .
- Arbiiter dekrüpteerib saadud krüptogrammi avaliku võtmega ning kontrollib X-i ID-d. Teine pool on tema jaoks salastatud. Kontrollime annab garantii, et paar (avalik võti ; privaativõti) on õige.
- Järgnevalt šifreerib Arbiiter kõike enda avaliku võtmega ning edastab Y-le



Digiallkirjastamise standardi DSS põhimõtted

- DSS (Digital Signature Standard), DSA (Digital Signature Algorithm) kasutab tugevat Hash-funktsiooni (SHA). Väljatöötatud NIST ja NSA poolt ning võetud USA standardiks.
- Digiallkirja (Sig) sisendiks on hash-kood ning juhuslik arv k , mis moodustatakse just selle allkirja jaoks
- Digiallkirjastamise funktsioon sõltub samuti allkirjastaja privaativõtmest KR_s ning globaalsest avalikust võtmest KU_G , mis on oma loomusest avaliketest parameetritest moodustatud hulk.
- Tulemuseks on digiallkiri, mis koosneb osadest s ja r .

Verifitseerimiseks arvutatakse samuti hash-kood tekstist M ning võetakse sisendiks s ja r .



Võrreldakse funktsiooni Ver tulemust ning r

Funktsioon Ver sõltub samuti globaalsest avalikust võtmest KU_G ning saatja avalikust võtmest KU_s .

Digiallkirjastamise algoritm DSA

- Algoritm baseerub diskreetsete logaritmidest arvutuse keerukusele ning ElGamal ja Schnorr-i poolt esitatud skeemidele. (http://en.wikipedia.org/wiki/Schnorr_signature ning http://en.wikipedia.org/wiki/ElGamal_signature_scheme)
- Kasutatakse kolme parameetrit, mis on avalikud ning millest moodustatakse globaalne avalik võti:
 - 160 bitine algarv q , ehk $2^{159} < q < 2^{160}$.
 - Algarv p , mille pikkus on vahemikus 512-1024 bitti, mis peab olema selline, et arv $(p-1)$ oleks jagatav arvuga q , ehk $2^{L-1} < p < 2^L$, kus $512 < L < 1024$ ning $(p-1)/q$ on täisarv.
 - Arv $g = h^{(p-1)/q} \bmod p$, kus h on täisarv arvude 1 ja $(p-1)$ vahel
- Nende arvude põhjal moodustatakse avalik võti ning neid arve kasutatakse privaativõtme genereerimisel

13

Digiallkirjastamise algoritm DSA

- Privaativõti x peab olema täisarv arvude 1 ja $(q-1)$ vahel ning peab olema valitud juhuslikult või pseudojuhuslikult
- Avalikku võtit arvutatakse lähtudes privaativõtmest $y = g^x \bmod p$.
- Valitakse arv k , mis on juhuslik või pseudojuhuslik arv arvude 0 ja q vahel. Arv k on unikaalne iga allkirja jaoks.
- Digiallkirjastamise protsessis arvutatakse kaks arvu s ja r :

$$r = (g^k \bmod p) \bmod q$$

$$s = [k^{-1} (H(M) + xr)] \bmod q$$
 Digiallkiri = (r, s)

14

Digiallkirjastamise algoritm DSA

- Digiallkirja verifitseerimisel arvutatakse arv v , lähtudes avalikest parameetritest, hash-koodist ning avalikust võtmest. Seda arvu v võrreldakse arvuga r .

$$w = s^{-1} \bmod q$$

$$u_1 = [H(M)w] \bmod q$$

$$u_2 = rw \bmod q$$

$$v = [(g^{u_1} y^{u_2}) \bmod p] \bmod q$$
 Digiallkiri on korrektne kui $v = r$.

15

Ülesanne. Näidata, et $v=r$

Selleks, et saaksime sellist võrdust tõestada, paneme mõned tähtsad momendid kirja:

- Mooduli aritmeetikast:

$$a^n \bmod x = (a \bmod x)^n$$

$$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$$

- Kuna $w = s^{-1} \bmod q$, siis $(ws) \bmod q = 1$.

Järelikult:

$$((H(M) + xr)w) \bmod q =$$

$$= (((H(M) + xr) \bmod q) (w \bmod q)) \bmod q =$$

$$= (((ks) \bmod q) (w \bmod q)) \bmod q =$$

$$= (kws) \bmod q = (k \bmod q) ((ws) \bmod q) \bmod q = k \bmod q$$

Kuna $0 < k < q$, siis $k \bmod q = k$.

16

Muud digiallkirjastamise algoritmid

- RSA algoritmile toetuvad skeemid
- Elliptiliste kõverate (elliptic curve) algoritm.
 $y^2 = x^3 + ax + b \pmod{p}$
- ElGamal skeem (millele toetub DSA), variatsioonid Schnorr ning Pointcheval-Stern digiallkirja algoritmides
- Rabin'i algoritm. Tugineb raskustele, mis tekivad seoses arvu esitamisega kahe suure algarvu korrutisena. $N = p \times q$. Seejuures $p = 3 \bmod 8$ ja $q = 7 \bmod 8$. Arvu p kasutatakse privaatvõtme juures, milleks on paar (N, k) ja $k = 1/2 (1/4 * (p-1) * (q-1) + 1)$; $0 \leq b < n$. Funktsioon $E_{n,b}(x)$, kus $0 \leq x < n$ on defineeritud kui $E_{n,b}(x) = x(x+b) \bmod n$. Paar (n, b) on avalik võti.
<http://publications.csail.mit.edu/lcs/pubs/pdf/MIT-LCS-TR-212.pdf>
- BLS (Boneh-Lynn-Shacham) skeem. Antud digiallkirjale σ ning avalikule võtmele g^* , vastab verifitseerimine $e(\sigma, g^*) = e(H(m), g^*)$.
- Undeniable signature (David Chaum ja Hans van Antwerpen) Valitakse inimene, kes tohib allkirja kontrollida.
- Aggregate signature (N allkirja, N kasutajat, N dokumenti)

17

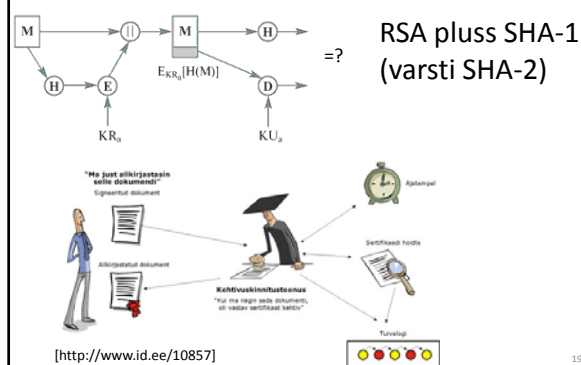
Privaatvõtme hoidmine

- Vastane, kes on varastanud privaatvõtme, saab anda teise inimese allkirja.
- Hoidmine arvutis on ohtlik.
 - Smart-kaardid
 - mälupulk
 - Touch-Memory
- Parim viis on hoida Smart-kaardil, kuna see on kaitstud ka PIN parooliga. Selline lahendus võimaldab topelt autentimist. Kaardi abil kirjutatakse alla dokument ning selle hash-koodi kontrollitakse samuti Smart-kaardis. Privaatvõtit ei kopeerita kusagile. Kopeerimine Smart-kaardilt on samuti keerulisem, kui teistelt andmekandjatelt. Privaatvõtme ning selle hoidmise eest vastutab omanik.



18

Eestis kasutatav digiallkiri



Avaliku võti ja sertifikaadid

- Avalikku võtit on vajalik seostada isikuga (isikuandmetega). Nimetatud seostamiseks kasutatakse sertifikaate. Sertifikaat on digidokument, mis on allkirjutatud sertifitseerimise osutaja poolt. Sisaldab isikuandmeid, avalikku võtit, sertifitseerimiskeskuse andmeid, kehtivusaega. Avaliku võtme asemel – sertifikaat.
- "ID-kaartide väljastamisel väljastatakse igale kasutajale kaks sertifikaati, millest üks on seotud digiallkirjastamisega. Sertifikaati võib tavaliselt võrrelda isiku allkirjanäidisega - see on avalik ja selle abil saavad kõik kontrollida, kas isiku antud allkiri on tõepoolest ehne. Sertifikaadis on kirjas ka isikuandmed, nimi ja isikukood.
- Kõik sertifikaadid on erinevad ja vastavad konkreetsete isikute isiklikele võtmetele. Sertifikaadi abil saab kontrollida digitaalalkirju: kui sertifikaat ja allkiri omavahel matemaatiliselt klappivad, võib väita, et allkirja on andnud see isik, kes on sertifikaadis kirjas."
[http://www.id.ee/10857]

20

Isikusertifikaadid (digitaalset allkirjastamist võimaldavad sertifikaadid)

Tähis	OID	Sisu
cn	2.5.4.3	common name (sertifikaadi üldnimi)
Givenname	2.5.4.42	Eesnimi
sn	2.5.4.4	Perekonna nimi
serialnumber	2.5.4.5	Isikukood
usercertificate:binary	2.5.4.36	Sertifikaat DER kodeeringus
objectclass	2.5.4.0	top
objectclass	2.5.4.0	person
objectclass	2.5.4.0	organizationalPerson
objectclass	2.5.4.0	inetOrgPerson

Näidisparing: Otsing isikukoodi järgi
 ldap://ldap.sk.ee:389/c=EE?sub?(cn=*,36603150241)

http://www.sk.ee/files/kataloogiteenuse_tehniline_juhend.pdf

21

Kui turvaline?

- Krüptoalgoritmidel on oma eluiga. See, mis täna pole murdav, ei pruugi olla samuti murdmatu homme. Asümmeetrilised algoritmid toetuvad polünoomiaalsele keerukusele selles osas, mis on arvutatav. (Seda, mida pole võimalik arvutada polünoomiaalses ajas, loetakse n-ö praktilises elus mitte arvutatavaks).
- Ühe eesmärgi saavutamiseks on võimalik kasutada ekvivalentseid algoritme. Kas leitakse diskreetsele logaritmile alternatiivne arvutusmeetod?
- Enamike algoritmide puhul on turvalisus säilinud viis kuni mõnikümmend aastat. Kahjuks ei saa alati prognoosida (kuigi mingil määral on see võimalik), millal algoritm ei ole enam turvaline.
- On vaja õigeaegselt asendada ühed algoritmid teistega.

http://www.ra.ee/public/Digiarhiiv/da_autentsus.pdf

25

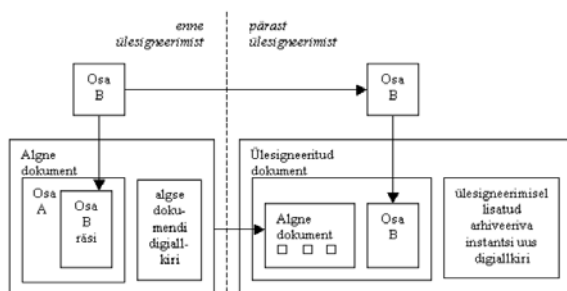
Ülesigneerimine

- Situatsioonis, kui vana algoritmi puhul allkirjastatud dokumendi turvalisus on küsitav, on vaja seda dokumenti üle signeerida (selleks ajaks peab olema uus algoritm väljatöötatud.).
- Kuna selleks ajaks on suurem osa dokumentidest juba arhiivis, siis ülesigneerimisega tegeleb vastav instants või vastava instantsi töötaja.
- Kui dokumentide allkirjastamisel oli kasutatud hash-funktsioone, siis tuleb asju ümber arvutada ka uute hash-funktsioonidega (sest ka need "aeguvad").
- Uus allkiri peab kaitsma eelmise dokumendi kogu sisu, sh varem antud digiallkirju. Vanu digiallkirju peab olema võimalik vajadusel verifitseerida.

http://www.ra.ee/public/Digiarhiiv/da_autentsus.pdf

26

Kaheosalise dokumendi võimaliku ülesigneerimise näide



http://www.ra.ee/public/Digiarhiiv/da_autentsus.pdf

27

Balti digisigi standardid

[Urmo Keskel]

- **DigiDoc**
 - De fakto digitaalallkirja standard Eestis
 - Kasutusel 2002 aastast, antud allkirju ca 5 miljonit
 - XML konteiner
 - Allkirja formaat on XAdES-X-L profiil
- **eDoc**
 - Kasutusel Lätis aastast 2006
 - ZIP konteiner, baseerub OpenXML standardil
 - Allkirja formaat baseerub XAdES-el
- **BDOC on Balti WPKI foorumi raames välja töötatud uus digitaalallkirjastatud failiformaat, mis on mõeldud asendada DigiDoc ja eDoc failiformaate.**

Loe lähemalt:

www.id.ee/public/ID_arendajate_seminar_Urmo_Keskel.ppt

ning <http://wpki.eu/wiki/upload/4/4f/BDoc-1.02.pdf>

28
