

Uurimisprojekt „Digiallkirja formaadile BDOC ülemineku hinnang“

Urve Venesaar, Marianne Kallaste,
Merle Küttim, Enn Õunapuu

29.10.2014



TALLINNA TEHNIKAÜLIKOOLI
MAJANDUSTEADUSKOND

Määrangud

Valdo Praust:

- *Sõnumi (faili) digitaalsignatuuriks (digital signature) nimetatakse sellest sõnumist (failist) arvutatud krüptoräsi, mis on šifreeritud digitaalsignatuuri looja privaativõtmega.*
- *Digiallkirjaks (pikema nimetusega – digitaalallkirjaks) 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.*



Digiallkirja vajadus ja omadused

Autentimine kaitseb suhtlevaid osapooli selle eest, et sekkub keegi kolmas. Samuti tagab teksti terviklikkuse.

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.

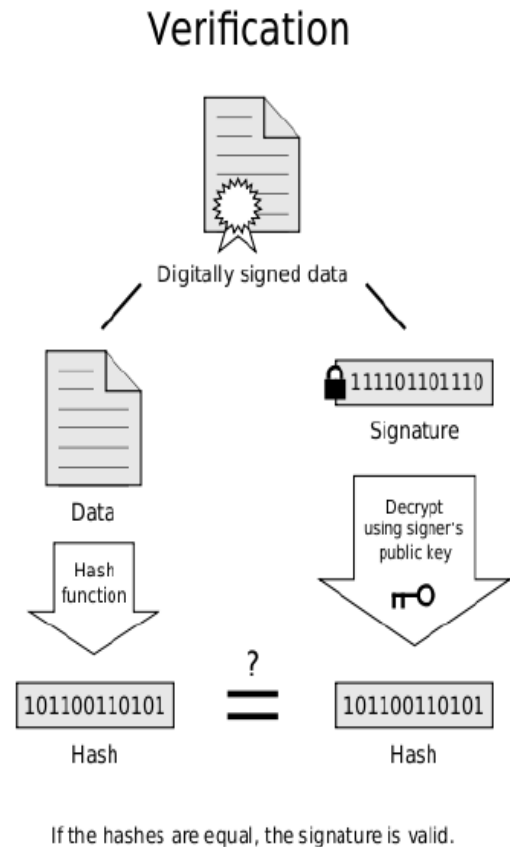
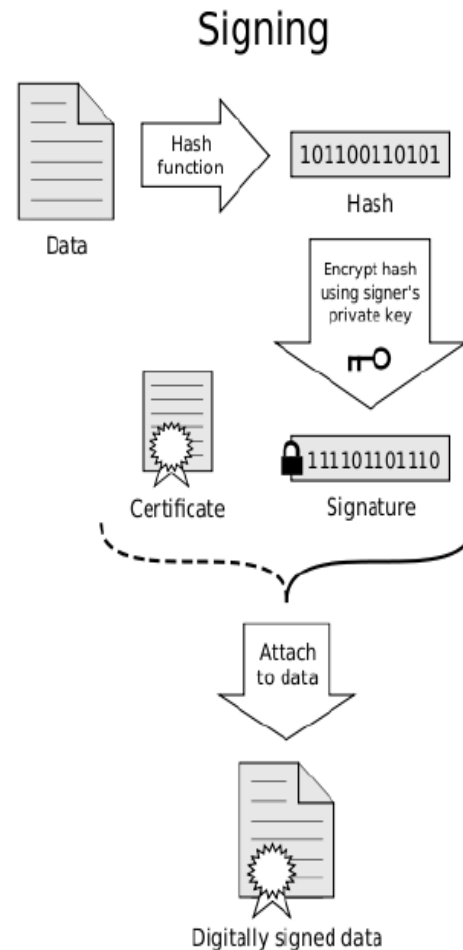
Digiallkirjal peavad olema järgmised omadused:

- Peab olema võimalus kontrollida autorit, allkirjastamise kuupäeva ja kellaaega
- Peab olema võimalus autentida teksti digiallkirjastamise ajal
- Digiallkiri peab olema kontrollitav kolmanda osapoolega vaidluste reguleerimiseks



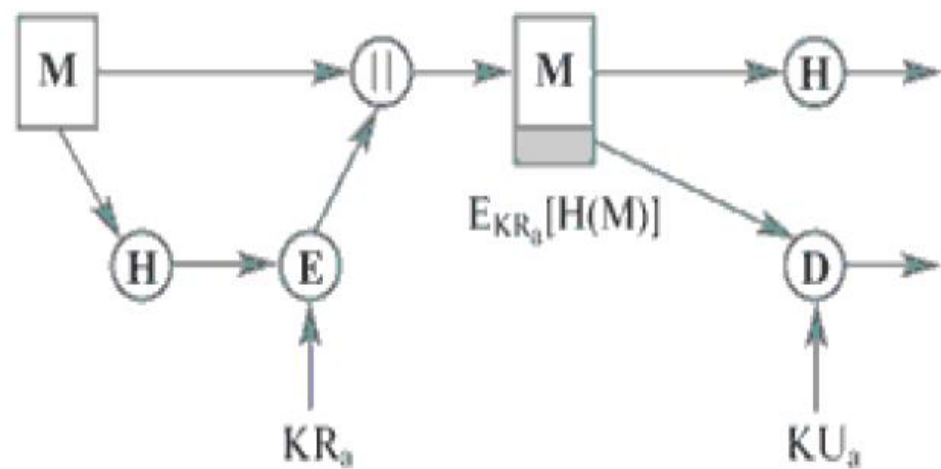
Digiallkirja skeem

- Digiallkirjastamine koosneb tavaliselt kolmest algoritmist:
- Privaatvõtme genereerimise algoritm, mis genereerib suvalise privaatvõtme kõikidest võimalikest privaatvõtmetest. Sama algoritm väljastab ka avaliku võtme.
- Allkirjastamise algoritm, mis lähtudes avatekstist ja privaatvõtmest moodustab digitaalse allkirja.



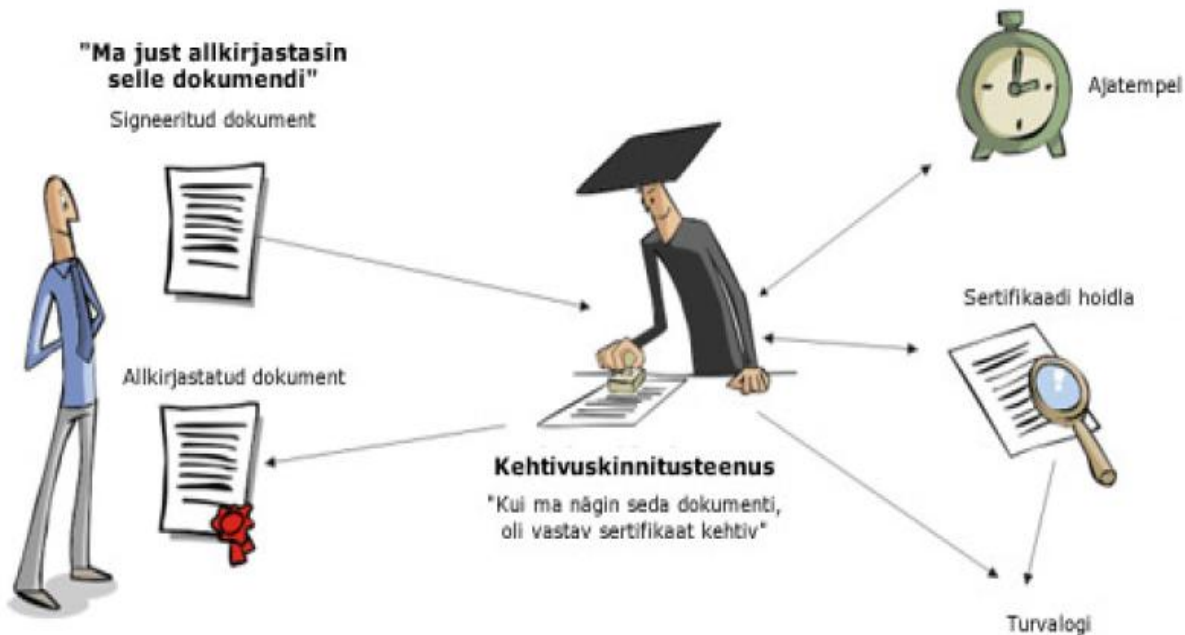
- Digiallkirja kontrollimise algoritm, mis lähtudes tekstist, digiallkirjast ning avalikust võtmest aktsepteerib või lükkab tagasi autentimise.

Eestis kasutatav digiallkiri



=?

RSA pluss SHA-1
(varsti SHA-2)



Avalik võti ja sertifikaadid

- Avalikku võtit on vajalik seostada isikuga (isikuandmetega). Nimetatud seostamiseks kasutatakse sertifikaate. Sertifikaat on digidokument, mis on allkirjutatud sertifitseerimisteenuse 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 tavaelus võrrelda isiku allkirjanäidisega - see on avalik ja selle abil saavad kõik kontrollida, kas isiku antud allkiri on tõepoolest ehtne. Sertifikaadis on kirjas ka isikuandmed, nimi ja isikukood.*
- *Kõik sertifikaadid on erinevad ja vastavad konkreetsete isikute isiklikele võtmetele. Sertifikaadi abil saab kontrollida digitaalallkirju: kui sertifikaat ja allkiri omavahel matemaatiliselt klappivad, võib väita, et allkirja on andnud see isik, kes on sertifikaadis kirjas.”*



Ajatempel

“Ajatempel on digitaalne tõend, mis võimaldab objektiivselt kindlaks teha mingi digitaalse andmekogumi loomise aega. “

“Cybernetica AS-s loodud ajatemplitehnoloogia seob jooksvalt välja antavad ajatemplid krüptograafiliselt kõigi varasemate ajatemplitega. Uusimad ajatemplid avaldatakse perioodiliselt avalikes teabekanalites, seetõttu muutub ajatemplite võltsimine - tagantjärele välja andmine või väljaantud ajatemplite modifitseerimine - võimatuks (isegi teenuse osutajale).”



Algoritmi turvalisuse eluiga

Krüptoalgoritmidel on oma eluiga. See, mis täna pole murtav, ei pruugi olla samuti murdmatu homme. Asümmeetrilised algoritmid toetuvad polünomiaalsele keerukusele selles osas, mis on arvutatav. (Seda, mida pole võimalik arvutada polünomiaalses 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.



Uuringu eesmärk

- Hinnata digitaalalkirja formaadivahetuse eeltingimusi ja majanduslikku mõju ning allkirjade arhiveerimise meetodeid ja nende kasutusvõimalusi



Lähteülesanne

- Kui palju on käibel allkirjastamisvahendeid, mis ei toeta uuemaid krüptomeetodeid
- Teenuste uuenduste elutsükkel
- Autentimiste ja allkirjade käive teenustes
- Soovituslik ajakava allkirja formaadi vahetuseks
- Allkirjaformaadi vahetuse majanduslik mõju
- Kriitiline teenuste hulk enne vana formaadi väljalülitamist
- Arhiveerimise võimalused
- Soovitused arhiveerimisliigi valikul



Valim

- Intervjuud 13 suurema e-teenuste pakkuja, ettevõtte ja riigiasutusega (Sertifitseerimiskeskus, QuardTime, SignWise, Rahvusarhiiv, E-notar, E-tervis, Ida-Tallinna Keskhaigla, Saku vallavalitsus, Amphora, Swedbank, SEB, EMT, Eesti Energia)
- Ankeetküsitlus väikese- ja keskmise suurusega ettevõtte (49), riigiasutuse (55) ning eraisikuga (60). Kokku 164 vastanut



Järeldused intervjuudest

- Suuretevõtetes ja riigiasutustes teati vähe formaadivahetuse detailidest
- Väljendati muret dokumendihaldussüsteemide muutmise osas
- Dokumentide säilitamine on organiseerimata
- Vähene teadlikkus archiveerimisest



Ankeetküsitlus

- digitaalalkirjastamise maht, viisid ja kogemused;
- senised digidoc uuendused;
- digitaalalkirjastatud dokumentide säilitamise maht ja viisid;
- teadlikkus digitaalalkirja vormingu muutusest, sellega kaasnev kulu, vajadus abi järele



Valim: asutuste suurus

Töötajate arv	Eraettevõtted		Riigiasutused	
	N	%	N	%
1-9	30	61,2	14	25,5
10-49	17	34,7	20	36,4
50-249	2	4,1	14	25,5
250-1000			4	7,3
NA			3	5,5
Kokku	49	100,0	55	100,0



Valim: ettevõtete tegevusvaldkond

Eraettevõtted	N	%
Põllumajandus, metsamajandus ja kalapüük	2	4,1
Info ja side	3	6,1
Finants- ja kindlustustegevus	2	4,1
Kinnisvaraalane tegevus	1	2,0
Tervishoid ja sotsiaalhoolekanne	1	2,0
Muud teenindavad tegevused	10	20,4
Töötlev tööstus	7	14,3
Energiaga varustamine	1	2,0
Ehitus	5	10,2
Hulgi- ja jaekaubandus	11	22,4
Veondus ja laondus	2	4,1
Majutus ja toitlustus	4	8,2
Kokku	49	100,0

Valim: riigiasutuste tegevusvaldkond

Riigiasutused	N	%
Kutse-, teadus- ja tehnikaalane tegevus	1	1,8
Haldus- ja abitegevused	1	1,8
Avalik haldus ja riigikaitse; kohustuslik sotsiaalkindlustus	26	47,3
Haridus	18	32,7
Tervishoid ja sotsiaalhoolekanne	5	9,1
Kunst, meelelahutus, vaba aeg	2	3,6
NA	2	3,6
Kokku	55	100,0

Valim: eraisikud

Vanus	N	%
19-25	6	10,0
26-35	16	26,7
36-45	10	16,7
46-55	7	11,7
56-65	9	15,0
66-79	12	20,0
Sugu		
Mees	26	43,3
Naine	34	56,7
Haridus		
Keskharidus või madalam	24	40,0
Kutseharidus	2	3,3
Kõrgharidus (bakalaureus)	14	23,3
Kõrgharidus (magister, diplom)	17	28,3
Kõrgharidus (doktor)	3	5,0

Ankeetküsitluse tulemused



Digitaalalkirjastamine

- Eraettevõtted väljastavad ja võtavad vastu keskmiselt 1-10, riigiasutused 11-1000 dokumenti kuus
- 16% ettevõtetest ja 13% riigiasutustest on vahetanud digitaalalkirju rahvusvaheliselt
- Väga väike osa asutustest on kokku puutunud teiste digitaalalkirja formaatidega (2%)
- Positiivne – lihtne, turvaline, kiire, odav, mugav
- Probleemid - tehnilised (dokument ei avane, ei ole loetav, ID kaart pole loetav, probleemid erinevates keskkondades, nt Mozilla), tarkvara muudatused, pikaajaline hoidmine, allkirjade vahetamine välismaaga



Digitaalalkirjastamine

- Kolmandik allkirjastab üle 50% dokumentidest digitaalselt
- Väga väike osa eraisikutest on kokku puutunud mõne teise digitaalalkirja formaadiga (2%)
- Mobiil-ID on kasutusel vähe (15%), 43% mobiil-ID kasutajatest annab sellega üle 50% digitaalalkirju
- Positiivne – mugav, kiire, lihtne, kindel, turvaline
- Probleemid - sertifikaatide aegumine, tehnilised probleemid, dokument 'kaob', dokumendi maht ei võimalda e-postiga saata, dubleerimise vajadus paberil, digitaalalkirja levik, nt suhtlemisel teiste riikidega



Tarkvara uuendused

- Ettevõtetes ja riigiasutustes on digidic tarkvara uuendused seganud igapäevatööd vähe (8% ja 10%)
- Riigiasutused on aktiivsemad tarkvara uuendajad, ettevõtted uuendasid tarkvara enim 11-50 päeva tagasi, riigiasutused ka 1-10 päeva tagasi



Arhiveerimine

- Ettevõtetel on 1-50, riigiasutustel 51-100 säilitamist vajavat dokumenti
- Pikaajalist säilitamist vajavaid dokumente on ettevõtetel 1-10, riigiasutustel 11-50
 - on ka riigiasutusi, kus 51-10 000 sellist dokumenti



Arhiveerimine

- Digitaalalkirjastatud dokumente hoitakse kombinatsioonina mitmest variandist
- Ettevõtete puhul enim arvuti kõvakettal erinevates kaustades, riigiasutuste puhul dokumendihaldussüsteemis
- Dokumente säilitatakse enamuses asutuse siseselt, sest enamik ettevõtteid (98%) ja riigiasutusi (96%) ei osta dokumentide säilitamise teenust sisse



Arhiveerimine

- Erasisikutes üle poole (58%) säilitab digitaalalkirjastatud dokumente, enim arvuti kõvakettal, aga ka e-kirjadena
- Säilitamist vajavaid dokumente on ca kolmandikul erasisikutel 1-10, ca kümnendikul on neid 11-50
- Viiendik vastanutest on mõnd juba varasemalt digitaalalkirjastatud dokumenti uuesti kasutanud



Allkirjaformaadi vahetus

- Enamik ettevõtteid (94%) ja riigiasutusi (78%) ei olnud digitaalallkirja vormingu muutusest teadlikud
- Ettevõtetest 2% ja riigiasutustest 4% olid formaadi vahetuseks valmistunud
- Enamik ettevõtteid (78%) ei planeeri muudatusi infosüsteemides ja dokumendi-haldussüsteemis ette, nagu ka ligi pooled riigiasutustest (49%)



Allkirjaformaadi vahetus

- Suur osa ettevõteteid ja riigiasutusi ei osanud hinnata aega ega rahalisi ressursse
- Aega hinnati keskmiselt 1-2 kuni 6 kuud,
- Ressursivajadust hinnati ettevõtetes 1000-2000 EURi ja riigiasutustes kuni 30 000
- Ettevõtted ja riigiasutused vajavad juhendmaterjale, infotelefoni ja koolitust



Järeldused ankeetküsitlusest

- Riigiasutused vahetavad digitaalallkirjastatud dokumente rohkem kui ettevõtted, neil on rohkem säilitamist vajavaid dokumente, nad on olnud aktiivsemad tarkvara uuendajad
- Eraisikud on aktiivsed digitaalallkirja kasutajad ja neile on oluline dokumentide säilitamine
- Riigiasutused olid rohkem formaadi muutustest teadlikud, nad planeerivad muudatusi infosüsteemides rohkem ette
- Riigiasutustes võtavad formaadi muutused rohkem aega ja raha, nad vajavad rohkem digidoc allkirjastamise tuge, ja vahetumat toetust (koolitust)



Uuringu kokkuvõte



TALLINNA TEHNIKAÜLIKOOLI
MAJANDUSTEADUSKOND

Allkirjaformaadi vahetuse eeltingimused

- Vajadus muuta digitaalallkirjastamine turvaliseks ja rahvusvaheliselt kasutatavaks
- Arvesse võtta **teenuste uuenduste elutsükkel**
 - hinnanguliselt mõnest päevast paari aastani, pikem dokumendihaldussüsteemide uuendamisel
- Riigiasutustes on digitaalallkirjade **käive teenustes** suurem kui erasektoris.
 - Tippkoormused on seotud palgapäevadega ja sõltuvuses tegevusvaldkonnast (nt tervishoius haigestumiste periood).



Kriitilised teenused

- Vajalikud teenused enne vana formaadi väljalülitamist rakendustest:
 - Avalik teavitamine
 - Tööjaamade valmiduse tagamine
 - Integratsioon dokumendihaldussüsteemides
 - Testkeskkonna loomine
 - Klientide teavitamine ja juhendamine



Majanduslik mõju

- Lõpptarbijad (eraisikud, VKE) – piirdub uuenduse salvestamisega
- Pangad – 300 000 EUR /pank
- Dokumendihaldussüsteemid – 5 000-20 000 EUR
- Tervishoid – 30 000 /süsteemi kohta
- Registrate jt asutuste isehitatud süsteemid - 30 000 /süsteemi kohta



Ettepanekud formaadimuutuseks

- Erinevate sihtrühmade teadlikkuse tõstmine
- Luua testkeskkond ja muutuste tehniline kirjeldus
- Tagada muutuste integreerimine dokumendihaldussüsteemidesse
- Üleminekuperioodil tagada allkirjaformaatide paralleelne kasutusvõimalus
- Riik poolt on tagatud digitaalallkirjastamise süsteemi usaldusväärsus, nt seniste digitaalallkirjade verifitseerimise funktsionaalsus



Dokumentide säilitamise probleemid

- Digitaalalkirjastatud dokumente hoitakse asutustes ja ettevõtetes süstematiseerimata
- Arhiveerimise vajaduse teadlikkus ettevõtete, asutuste ja eraisikute hulgas on madal
- Arhiveerimisvõimalused on kõige halvemini e-teenustega kaetud



Arhiveerimise vajalikkus

- Arhiveerimise lahenduse leidmine on vastutusrikas, nõuab kõrge usalduse ja turvalisusega säilitamissüsteemi loomist
- Teadlikkuse tõstmine ja lahenduse leidmine digitaalalkirjastatud dokumentide arhiveerimiseks on lähemas tulevikus hädavajalik.
- Dokumendi elutsüklit tuleks vaadelda ja juhtida kui tervikut ja olla varakult valmis dokumendi süsteemseks arhiveerimiseks.

Arhiveerimise väljakutsed

- Arhiveeritud digitaalselt allkirjastatud dokumendi funktsioonid:
 - Allkirja andva isiku tuvastamine
 - Allkirjastatava dokumendi terviklikkuse tagamine
 - Allkirja andmise mitte tunnustamise vältimine (non-repudiation)



Digiarhiivile esitatavad nõuded

- Tõestama, et arhiveeritud andmeobjekte ei ole aja jooksul muudetud ja on täpselt sellisel kujul nagu nad algselt salvestati
- Tõestama arhiveeritud andmeobjektide salvestamise aega
- Kaitsma arhiveeritud andmeobjekte väga pika aja jooksul, mis ületab avatud võtme sertifikaatide ja ajatemplite eluaja piire ja kohanema ka olukorraga, kus kasutatud algoritmide turvalisus on juba murtud.



Nõude saavutamine

Elektroonsed dokumendid säilitatakse algses vormis kui:

- Salvestatud andmed ja sisu on **kättesaadav ja kasutatav igal aja momendil ka tulevikus**
- Need säilitused peegeldavad **tegelikke algseid andmeid ja vormi**
- Nende **allikas, loomise aeg, koht ja andmete saatja ja vastuvõtja on vaieldamatult tõestatavad**

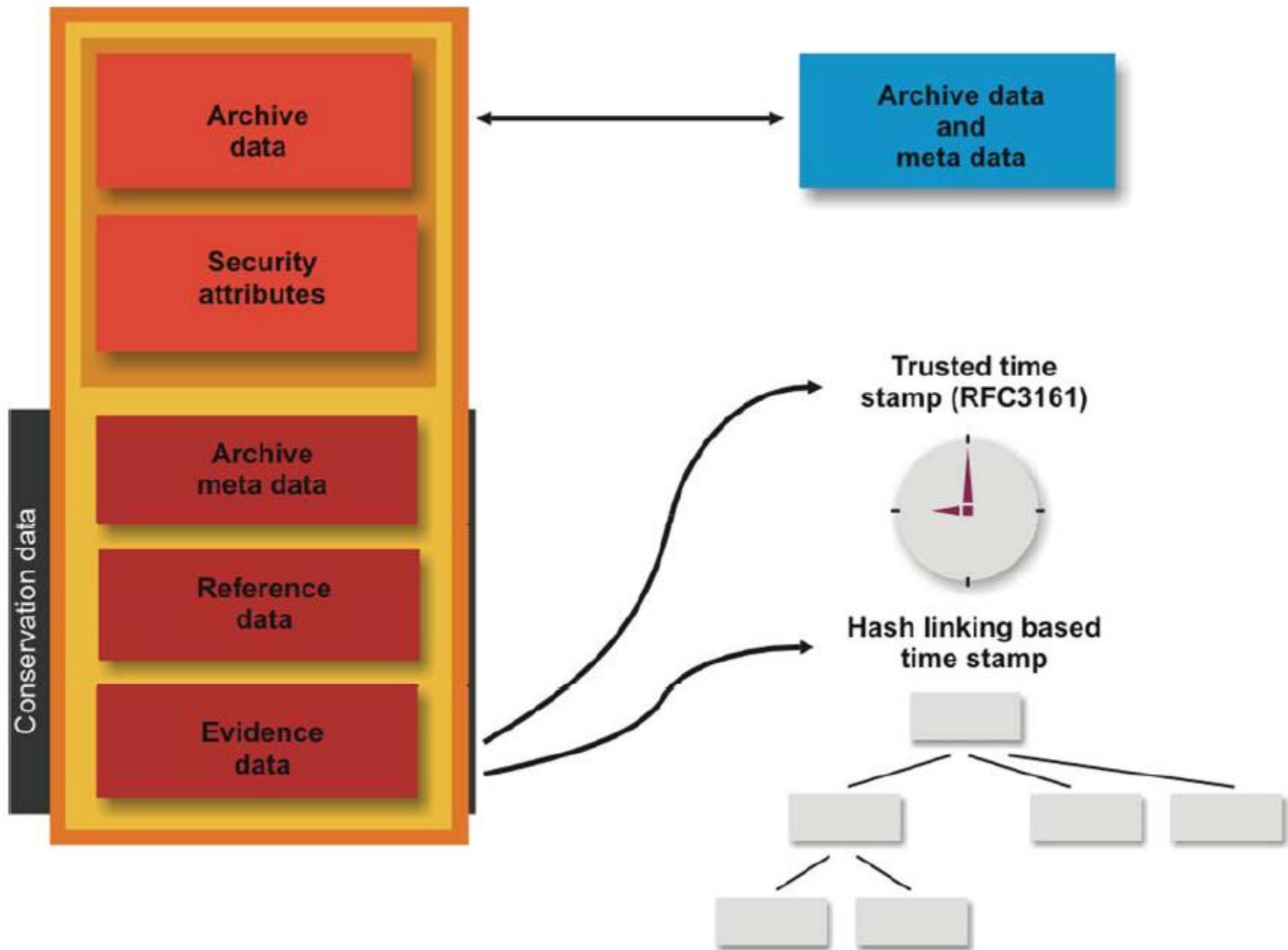


Kuidas tehniliselt saavutada?

Kasutatavad tehnoloogiad ja protseduurid peavad tagama:

- et andmete ja sisu terviklikkuse garantii oleks tõestatav (modifitseerimise, muutmise ja muutumise vältimine),
- et oleks säilitatud ka kaasnevad andmed ja vahendid (metadata, digitaalallkirjad)
- ka turvaatribuutide kehtivus peab olema tagatud





Trusted Archive Service

Arhiveerimise võimalused

- Praegu pakutakse alljärgnevaid lahendusi arhiveerimiseks:
 - Dokumentide ümberallkirjastamine ja formaatimine arhiivi kandmisel,
 - Vana dokumendi säilitamine algsel kujul, kuid uue ümbriku kasutamine koos autoriseeritud tõestusega
 - Guardtime ajatempli lahendus



Soovitused arhiveerimisliigi valikul

- Teadlikkuse tõstmine ja lahenduse leidmine digitaalalkirjastatud dokumentide arhiveerimiseks
- Lahendada dokumentide arhiveerimine riiklikul tasemel ja pakkuda vastavaid teenuseid sihtgruppidele
- Arhiveerimismeetodi valik peab olema arusaadav ja kergesti kasutatav erinevate sihtrühmade poolt
- Arvestada erinevate ettevõtete ja asutuste mahtude ja vajadustega
- Konfidentsiaalsuse küsimus dokumentide välistesse teenustesse saatmisel



Standardid

The new standard is in two parts:

- ISO 14533-1:2012, *Processes, data elements and documents in commerce, industry and administration – Long term signature profiles – Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)*
- ISO 14533-2:2012, *Processes, data elements and documents in commerce, industry and administration – Long term signature profiles – Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)*



Väljakutse

Kuna andmekandjad, tehnoloogiad ja vormingud pidevalt arenevad on väga raske või isegi võimatu tagada, et ühtegi bitti algdokumendis ei ole muudetud. Seega on paljud väga skeptilised digitaalselt allkirjastatud dokumente on võimalik adekvaatselt archiveerida.



Ameerikas pakutud lahendus

Selle olemus on kolmanda usaldusväärse osapoole kasutamine

Protseduur oleks:

- Usaldatav osapool valmistab ette uuele formaadile ülemineku, kontrollides seejuures ülekantava dokumendi algset terviklikust
- Dokument allkirjastatakse uuesti uues vormingus.
- Usaldusväärne osapool tagab dokumendi ajalise järjepidevuse



Täname tähelepanu eest!



TALLINNA TEHNIKAÜLIKOOLI
MAJANDUSTEADUSKOND