

ELEKTRONISKO DOKUMENTU DROŠĪBA

Prof. Uldis Sukovskis, CISA

Rīgas Tehniskā universitāte

Tiesiskās reglamentācijas nepieciešamība

- Informācijas tehnoloģijas iespējas
- Privātās dzīves aizsardzība
- Elektroniskā komercija
- Valsts pārvaldes modernizācija
- Eiropas Savienības prasības



Starptautiskās tiesību normas



ES Direktīva 1999/93/EC par Kopienas pamatnostādnēm elektroniskā paraksta jomā
(Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signature)

Apvienoto Nāciju Organizācijas UNCITRAL elektroniskās komercijas parauglikums, 2000.gads
(United Nations Commission on International Trade Law Model Law for Electronic Signatures)

Starptautisko dokumentu galvenās pamatnostādnes

- Datu apmaiņai elektroniskā formā nevar liegt juridisko spēku tikai tāpēc, ka informācija ir elektroniskā formā
- Elektroniskajam dokumentam nevar liegt pierādījuma spēku tiesā tikai tāpēc, ka tas ir elektroniskā formā
- Ja likums prasa rakstisku formu, to var aizstāt ar elektronisko formu, ja ir iespējams pārbaudīt personas identitāti, datu integritāti un konfidencialitāti
- Komunikāciju dalībnieki var vienoties par personas identifikācijas, datu integritātes un konfidencialitātes pārbaudes metodēm uz līguma pamata
- Elektroniskā dokumenta tiesisko spēku nosaka likums vai līgums



Elektronisko dokumentu likums (definīcijas)



elektroniskais dokuments — jebkuri elektroniski radīti, uzglabāti, nosūtīti vai saņemti dati, kas nodrošina iespēju tos izmantot kādas darbības veikšanai, tiesību īstenošanai un aizsardzībai;

elektroniskais paraksts — elektroniski dati, kas pievienoti elektroniskajam dokumentam vai loģiski saistīti ar šo dokumentu, nodrošina elektroniskā dokumenta autentiskumu un apstiprina parakstītāja identitāti;

elektroniskā paraksta radīšanas dati — tikai vienreiz radīti dati, kurus parakstītājs izmanto, lai radītu elektronisko parakstu;

elektroniskā paraksta pārbaudes dati — dati, kurus izmanto, lai pārbaudītu elektronisko parakstu;

Elektronisko dokumentu likums (definīcijas)



drošs elektroniskais paraksts — elektroniskais paraksts, kas atbilst visām šādām prasībām:

- a) tas ir piesaistīts vienīgi parakstītājam,
- b) tas nodrošina parakstītāja personas identifikāciju,
- c) tas ir radīts ar drošiem elektroniskā paraksta radīšanas līdzekļiem, kurus var kontrolēt tikai parakstītājs,
- d) tas ir saistīts ar parakstīto elektronisko dokumentu tā, lai vēlākas izmaiņas šajā dokumentā būtu pamanāmas,
- e) tas ir apliecināts ar kvalificētu sertifikātu;

sertifikāts — elektronisks apliecinājums, kas saista elektroniskā paraksta pārbaudes datus ar parakstītāju un kalpo parakstītāja identitātes noteikšanai;

kvalificēts sertifikāts — sertifikāts, kurš ietver šajā likumā noteikto informāciju un kuru izsniedzis uzticams sertifikācijas pakalpojumu sniedzējs;

laika zīmogs — elektroniski parakstīts apstiprinājums tam, ka elektroniskais dokuments ir noteiktā datumā un laikā iezīmēts pie sertifikācijas pakalpojumu sniedzēja;

Elektroniskā dokumenta juridiskais spēks



- Prasība pēc rakstiskas formas var būt izpildīta ar elektronisko dokumentu
- Elektroniskais dokuments iegūst juridisko spēku, ja tas noformēts atbilstoši likuma prasībām un satur normatīvajos aktos noteiktos rekvizītus
- Elektroniskais dokuments ir uzskatāms par pašrocīgi parakstītu, ja tam ir drošs elektroniskais paraksts
- Ja normatīvie akti nosaka prasības atsevišķa veida papīra dokumentu izstrādāšanai, noformēšanai un glabāšanai, šie paši noteikumi attiecināmi arī uz elektroniskajiem dokumentiem

Dokumentu aprite starp valsts un pašvaldību iestādēm



- Elektronisko dokumentu apritē starp valsts un pašvaldību iestādēm vai starp šīm iestādēm un fiziskajām un juridiskajām personām elektroniskais dokuments uzskatāms par parakstītu, ja tam ir drošs elektroniskais paraksts un laika zīmogs
- Ja pastāv rakstveida vienošanās par elektroniska paraksta izmantošanu, tad laika zīmogu var aizstāt ar elektronisko parakstu.

Elektronisko dokumentu likuma piemērošanas izņēmumi



Elektronisko dokumentu likums nav piemērojams:

- tiesību nodošana uz nekustamo īpašumu, izņemot nomas tiesības
- līgumi, kuri jāapliecina likumā noteiktā kārtībā
- ģimenes tiesības un mantojums
- galvojuma līgumi

Dokumentu aprites noteikumi



MK noteikumi Nr. 473

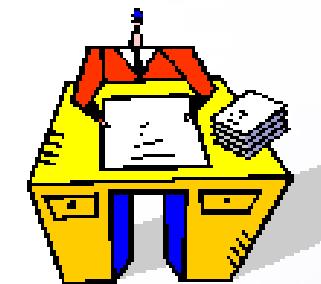
"Elektronisko dokumentu izstrādāšanas, noformēšanas, glabāšanas un aprites kārtība valsts un pašvaldību iestādēs un kārtība, kādā notiek elektronisko dokumentu aprite starp valsts un pašvaldību iestādēm vai starp šīm iestādēm un fiziskajām un juridiskajām personām"

pieņemti 2005.g. 28.jūnijā

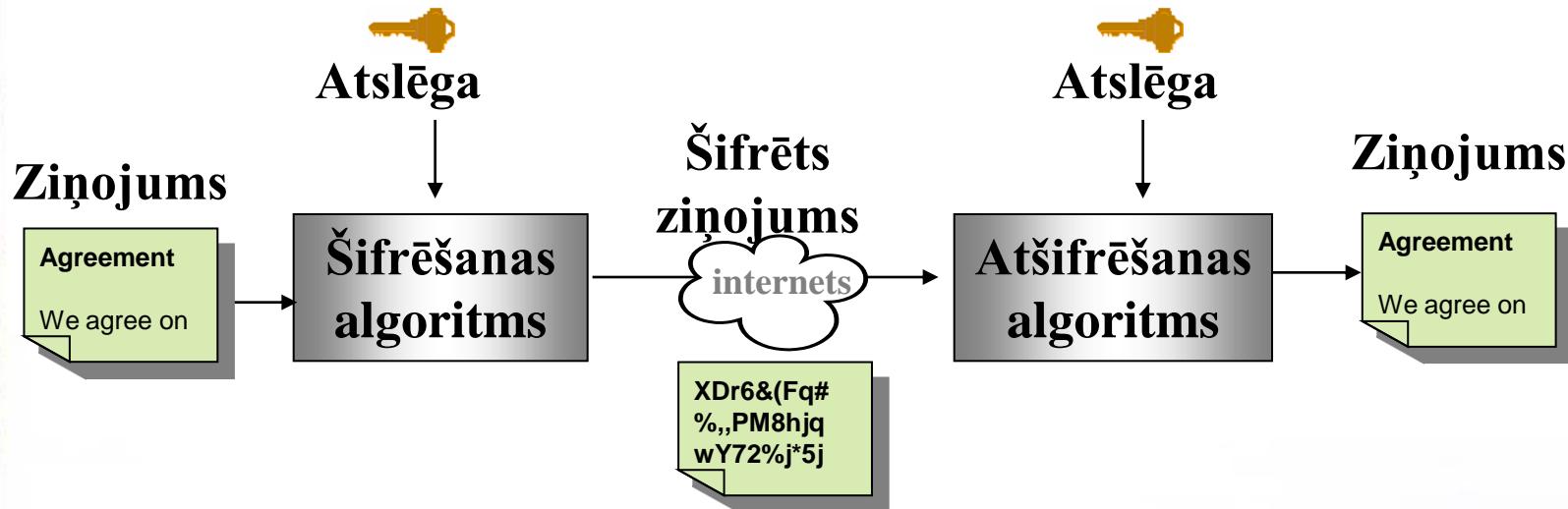
Dokumentu aprites noteikumi (turpinājums)

8. Elektroniskā dokumenta parakstīšanas laiks ir laika zīmoga pievienošanas datums un laiks.
9. Elektroniskā dokumenta izstrādāšanā un noformēšanā lieto kodus saskaņā ar Latvijas nacionālo standartu LVS 8:1992+ A1:1993 "8.bitu kodēto grafisko simbolu kopa Baltijas jūras reģiona valstīm".
10. Elektroniskajam dokumentam izmanto šādus datņu formātus:
 - 10.1. nenoformētam tekstam – TXT;
 - 10.2. noformētam tekstam – RTF, SGML (XML);
 - 10.3. grafiskai informācijai – JPEG, TIFF vai PNG;
 - 10.4. vektoru grafikai – CGM.
11. Papildus šo noteikumu 10.punktā minētajiem datņu formātiem iestāde var izmantot citus datņu formātus, informāciju par to norādot savā mājas lapā internetā vai nododot to atklātībai citā veidā.

Elektroniskais paraksts un laika zīmogs



Simetriskā šifrēšana

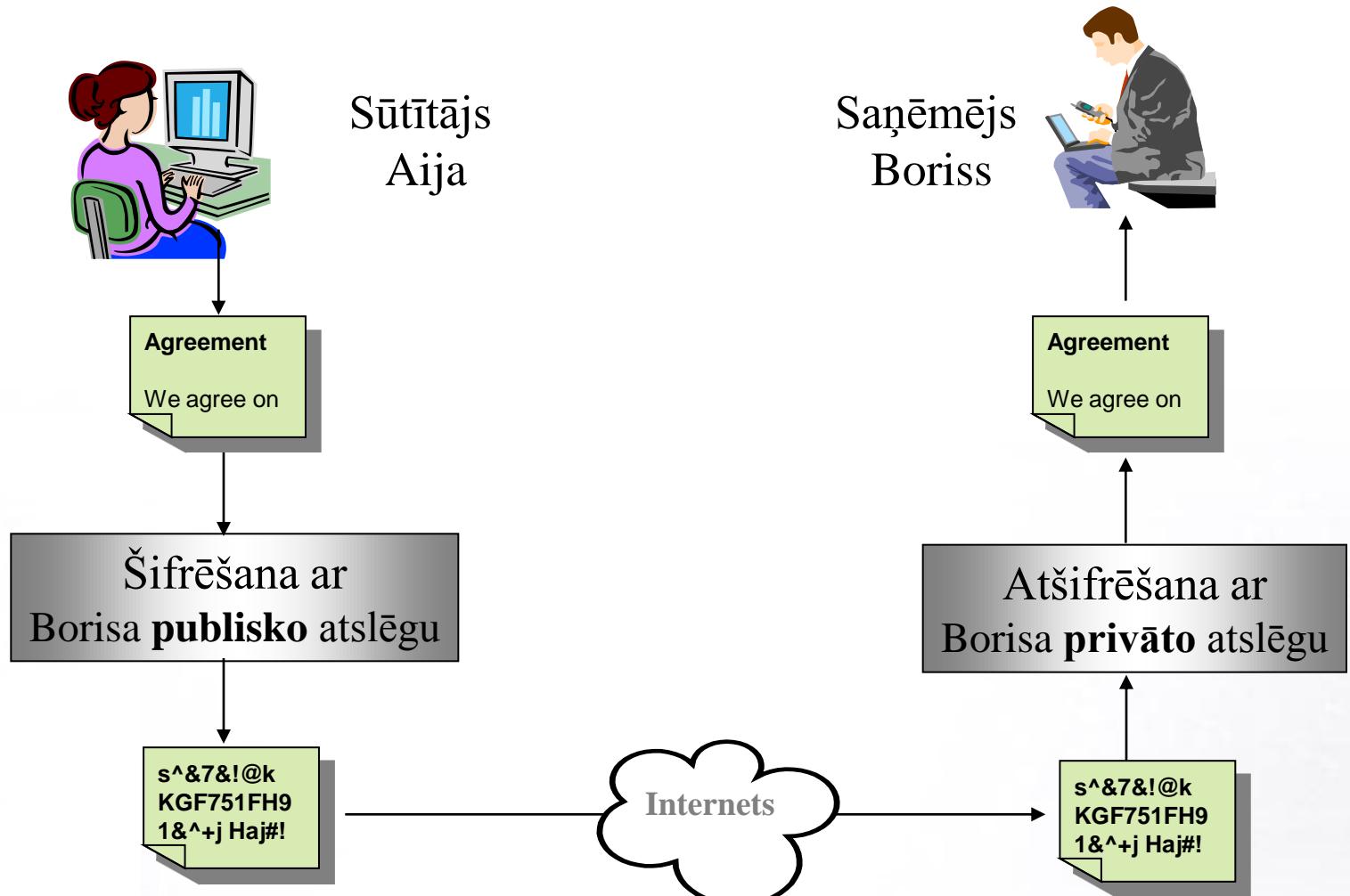


- Šifrēšanai un atšifrēšanai lieto vienu un to pašu atslēgu (*secret key*).
- Visizplatītākais simetriskās šifrēšanas algoritms ir DES (Data Encryption Standard), Triple-DES.
- **Galvenā problēma** - atslēgu pārvaldība.

Asimetriskā šifrēšana

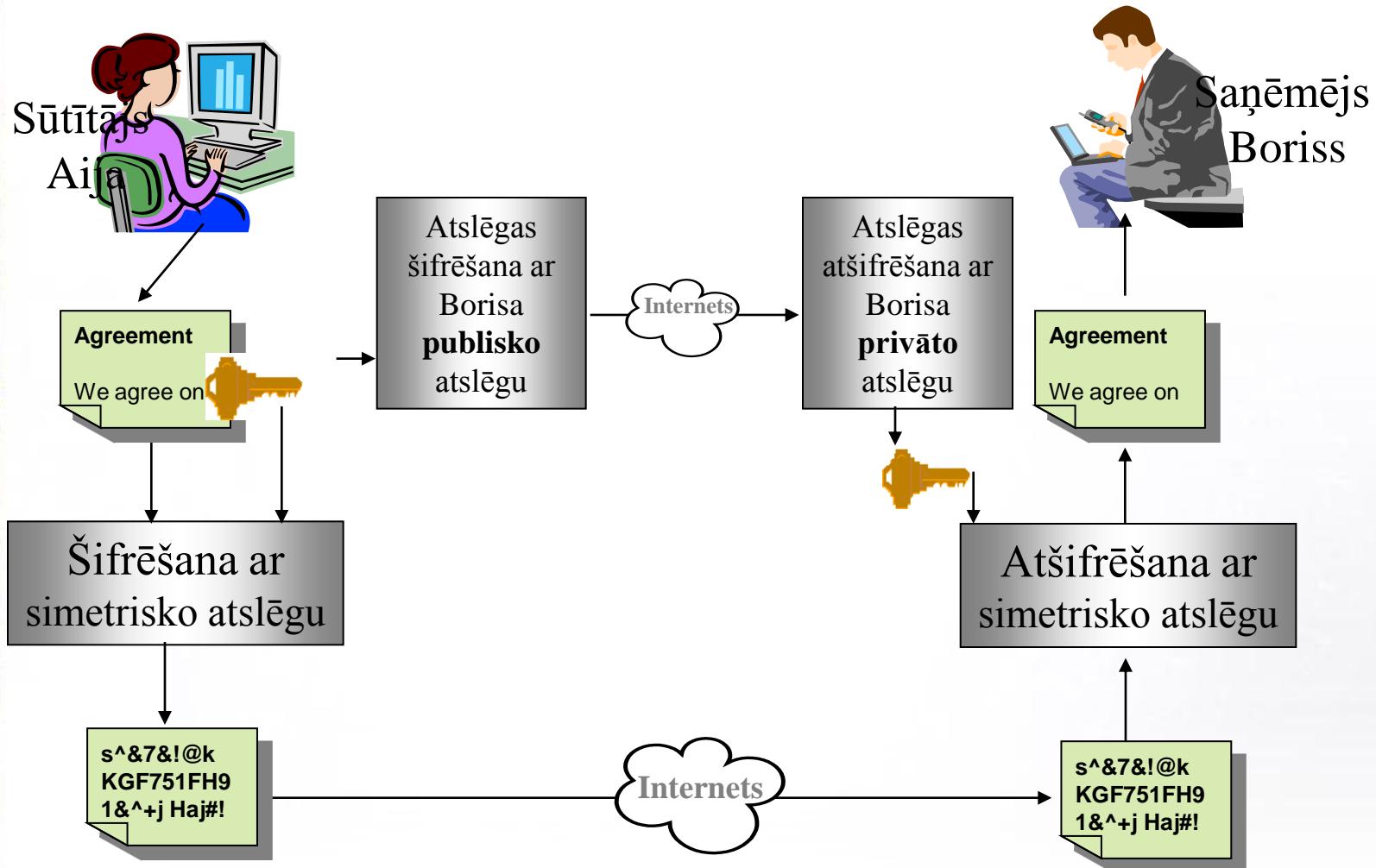
- Katram dalībniekam ir divas saistītas atslēgas:
 - **privātā atslēga**
 - **publiskā atslēga**
- Ja ziņojums ir šifrēts ar vienu no šīm atslēgām, tad to atšifrēt var tikai ar otru
- Privātā atslēga ir konfidenciāla un ir tikai vienas personas rīcībā
- Publiskā atslēga ir publiski pieejama visiem
- Visizplatītākie asimetriskās šifrēšanas algoritmi:
 - DSA (Digital Signature Algorithm, US Federal Information Processing Standard (FIPS) 186-2
 - RSA (Rivest, Shamir, Adleman) RSA Cryptography Standard
 - ECC/ECDSA (Elliptical Curve Digital Signature Algorithm) ANSI X9.62 Public Key Cryptography for the Financial Services Industry.

Asimetriskā šifrēšana

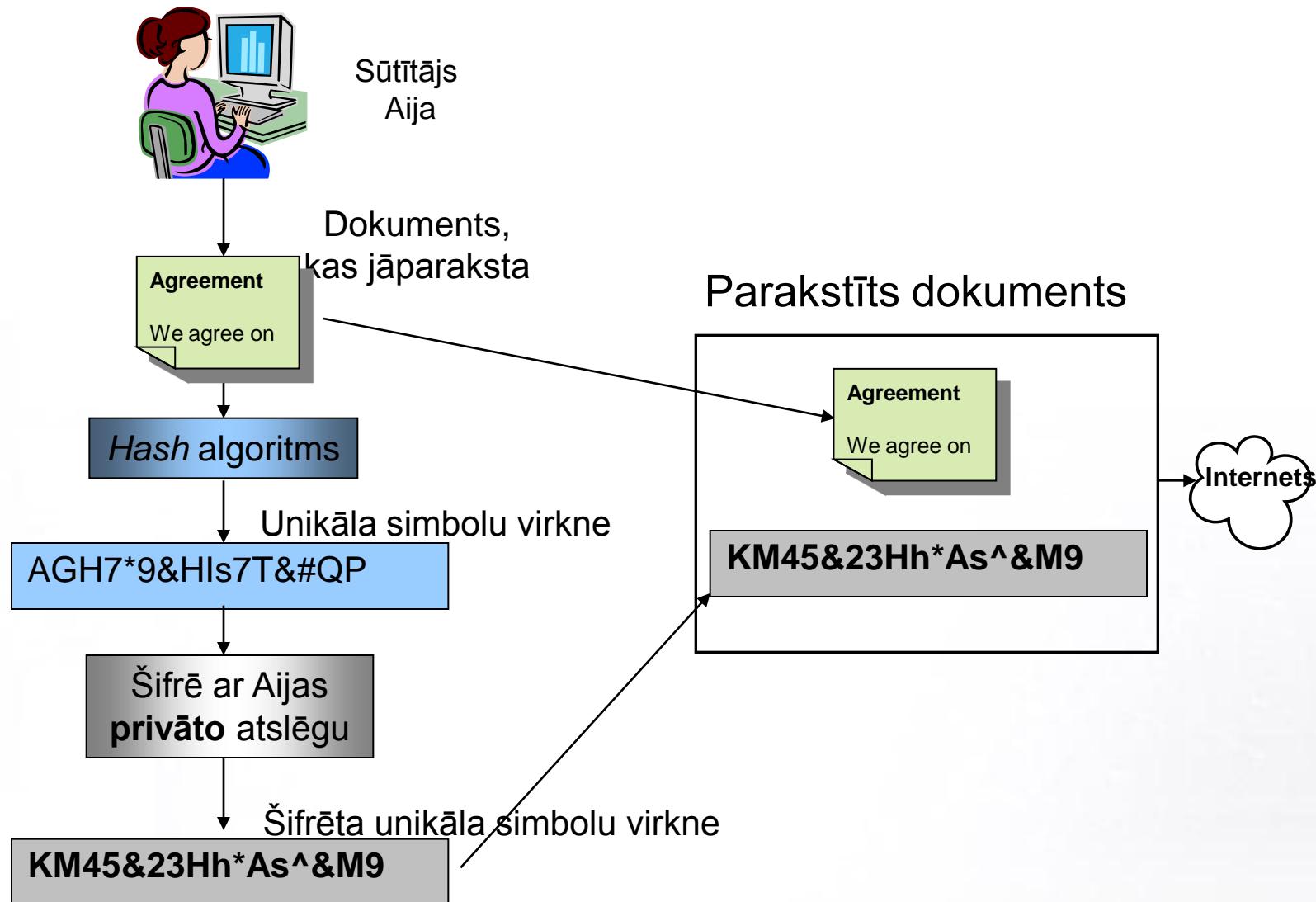


Kombinētā šifrēšana

- Dokumentu šifrē ar ātru simetrisko metodi
- Atslēgas nodošanai lieto lēnāko asimetrisko metodi



Elektroniskā paraksta pievienošana

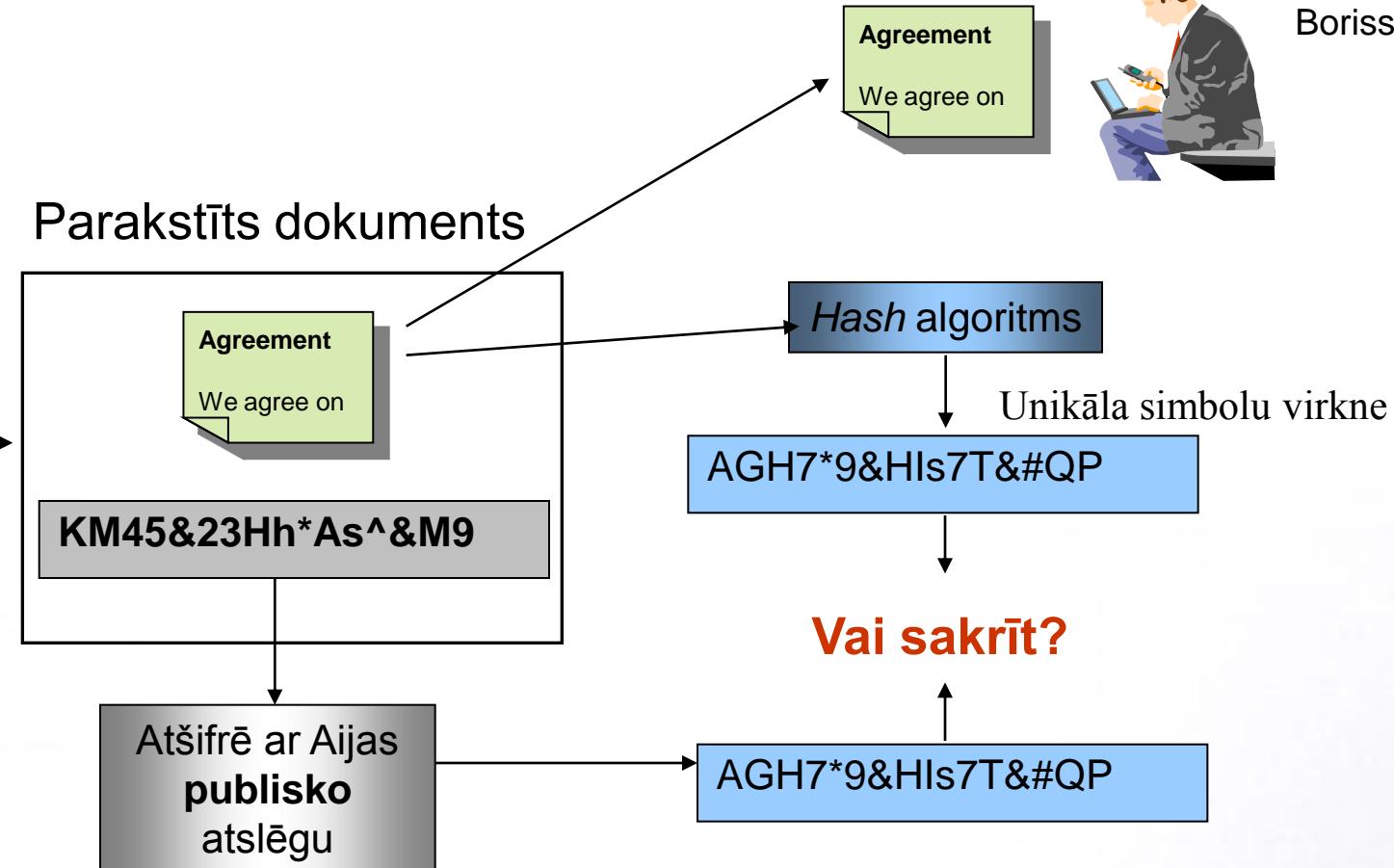


Parakstīta dokumenta saņemšana



Saņemējs
Boriss

Parakstīts dokuments



Elektroniskais paraksts nodrošina:

- parakstītāja autentificēšanu
- dokumenta integritāti
- nenoliedzamību (*non-repudiation*)

Hash function - jaucējfunkcija

- No ziņojuma teksta izviedo fiksēta garuma bitu virkni (hash value, message digest – īsziņojums)
- Divas īpašības:
 - vienvirziena (t.i. no īsziņojuma nav iespējams atjaunot ziņojumu),
 - nav kolīziju (t.i. nevar atrast divus ziņojumus, kuriem būtu vienādi īsziņojumi).
- Izmanto SHA-1 (Secure Hash Algorithm) algoritmu, kas veido 160 bitus garu īsziņojumu.
- 2005.gada 13.februārī publicēts Ķīnas zinānieku paziņojums par veiksmīgu uzbrukumu SHA-1 algoritmam, kas atrod kolīziju mazāk kā ar 2^{69} hash-operācijām.

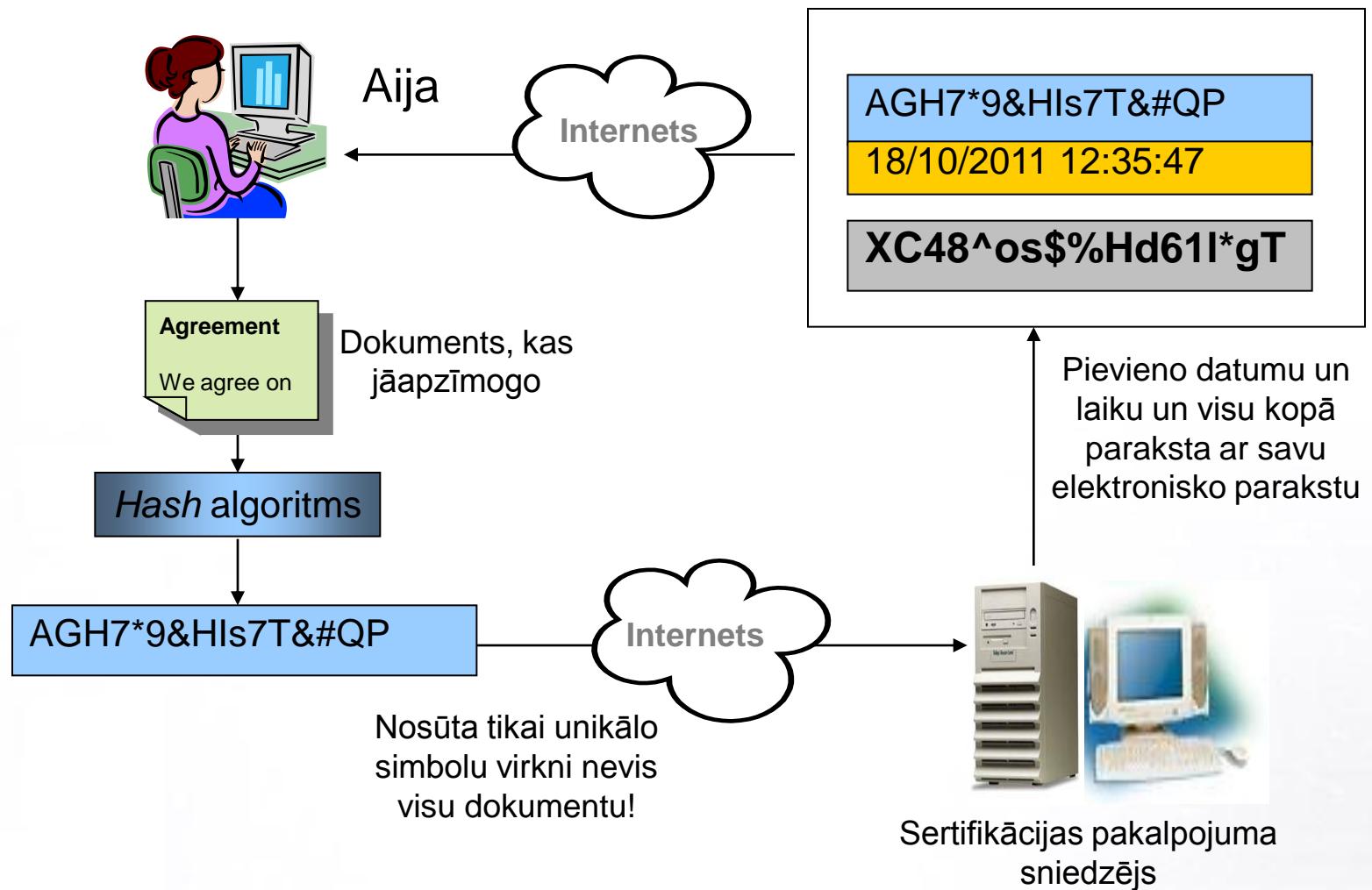
Laika zīmogs

- Laika zīmogs (*time stamp*):
 - pievieno elektroniskam dokumentam datumu un laiku
 - nodrošina ilglaicīgu apstiprinājumu dokumentam
- Izmanto drošu un uzticamu avotu laika vērtībai zīmogā, piemēram, *Coordinated Universal Time (UTC)*
- Laika zīmogu paraksta tā izsniedzējs ar savu privāto atslēgu
- Jābūt nodrošinātai iespējai pārbaudīt laika zīmoga likumību arī pēc tā izsniedzēja sertifikāta derīguma termiņa beigām



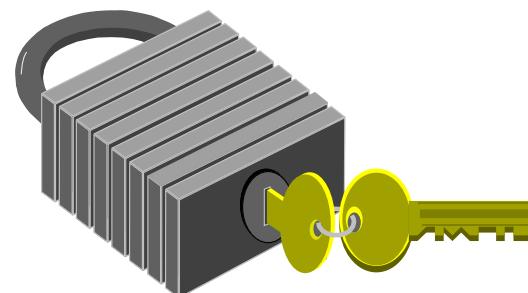
Automatic Time Stamp
Patented 1894-97 ~
Advertised 1899-1923
The Automatic Time Stamp
Co. Boston, MA

Laika zīmoga pievienošana



Elektroniskais paraksts darbojas, ja:

- sūtītāja (Aijas) privātā atslēga ir zināma tikai sūtītājam
- saņēmējs (Boriss) ir pārliecināts, ka sūtītāja (Aijas) publiskā atslēga tiešām pieder sūtītājam



- Risinājums:
 - abas puses apliecina, ka tās droši glabās savas privātās atslēgas
 - **ir trešā puse**, kas apstiprina publiskās atslēgas piederību

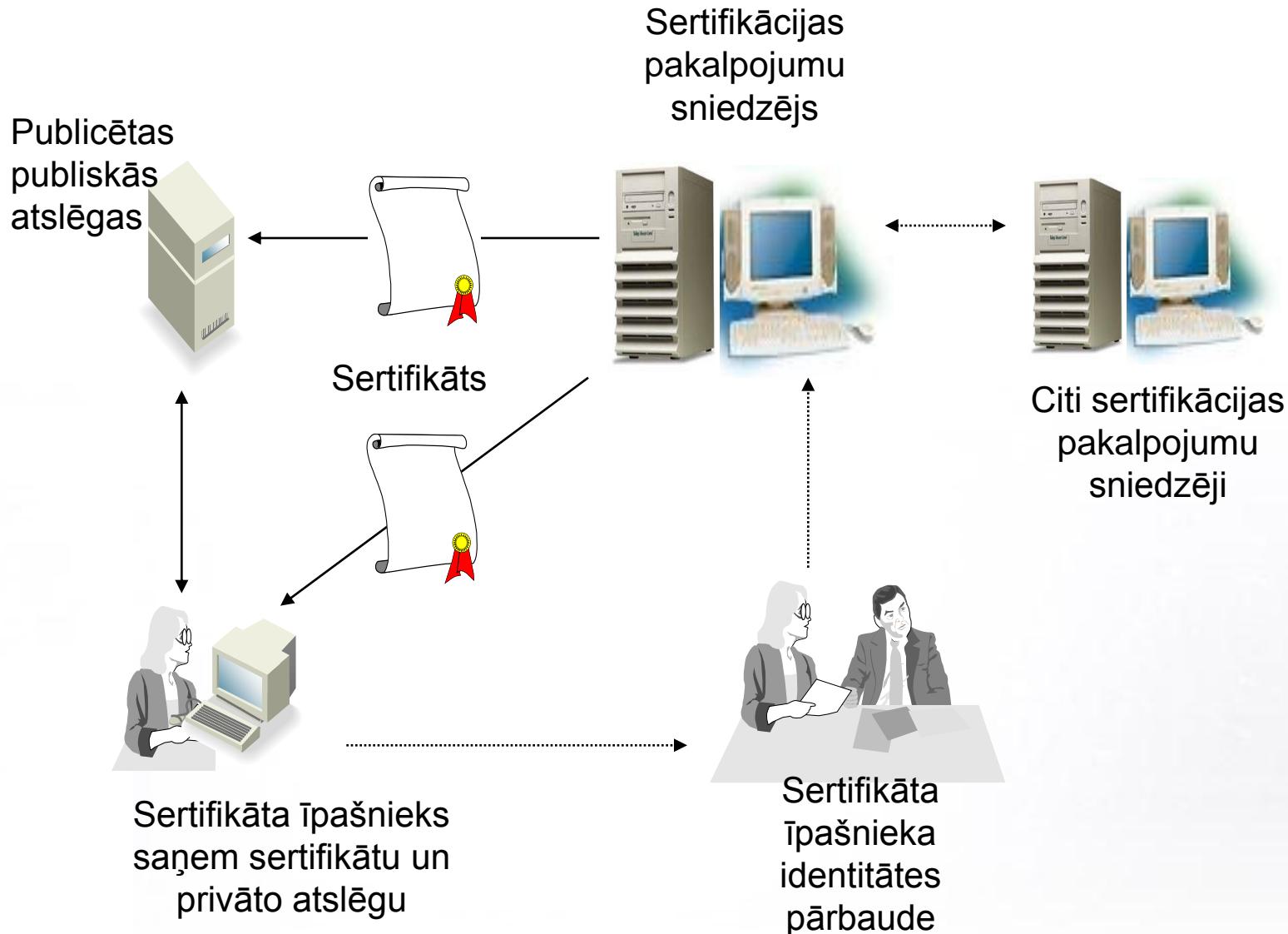
Sertifikācijas pakalpojumi

- **Sertifikāts** — elektronisks apliecinājums, kas saista elektroniskā paraksta pārbaudes datus ar parakstītāju un kalpo parakstītāja identitātes noteikšanai
- Elektroniskos sertifikātus personām izsniedz **sertifikācijas pakalpojumu sniedzējs**
CSP - Certification Service Provider,
CA - Certification Authority
- Sertifikātiem ir derīguma termiņš
- Elektroniskie sertifikāti
 - glabājas īpašā failā
 - glabājas viedkartē
- Prasības sertifikātiem nosaka standarts ITU-T X.509

Sertifikācijas pakalpojumu sniedzēji

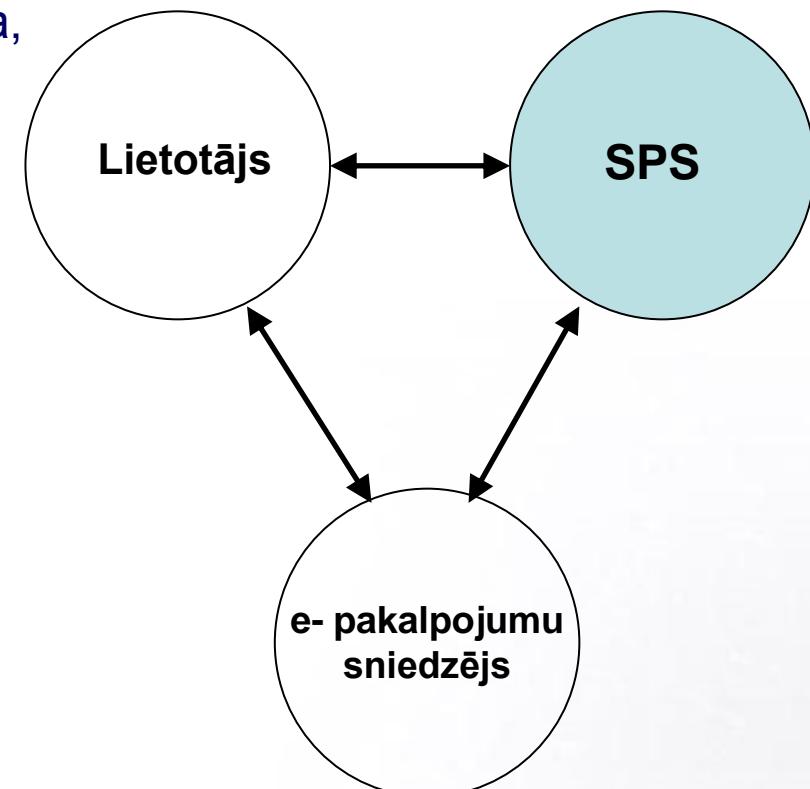
- Sertifikācijas pakalpojumu sniedzējs ir fiziskā vai juridiskā persona, kas sniedz sertifikācijas pakalpojumus
- **Uzticams sertifikācijas pakalpojumu sniedzējs** atbilst likumā noteiktajām drošības un citām prasībām, kā arī ir akreditēts Datu valsts inspekcijā

Sertifikācijas pakalpojums



Sertifikācijas pakalpojumu sniedzēja galvenās funkcijas

- Sertifikātu izsniegšana
- Sertifikātu reģistrēšana, anulēšana, darbības apturēšana un atjaunošana
- Elektroniskā paraksta pārbaudes līdzekļu nodrošināšana
- Elektroniskā dokumenta iezīmēšana ar laika zīmogu
- Informācijas par sertifikātu izsniegšanas un izmantošanas kārtību nodrošināšana
- Konsultāciju sniegšana par sertifikātu lietošanu, elektroniskajiem parakstiem, e-pakalpojumu veidošanu



Starptautiskie standarti

- Eiropas telekomunikāciju standartizācijas institūta tehniskie standarti
 - "Politikas prasības sertifikācijas pakalpojumu sniedzējiem, kas izsniedz kvalificētos sertifikātus" (ETSI TS 101 456)
 - "Politikas prasības laika zīmoga pakalpojumu sniedzējiem" (ETSI TC 102 023)
- CEN (European Committee for Standardization) Workshop Agreements - CWA 14169, 14355, 14365 utt.
- U.C.

Saites internetā

- www.nais.lv
- www.dvi.gov.lv
- www.e-me.lv
- **The Legal and Market Aspects of Electronic Signatures**
- http://europa.eu.int/information_society/eeurope/2005/all_about/security/index_en.htm
- **ICT Standards Board**
- **European Electronic Signature Standardization Initiative (EESI)**
-
- **European Telecommunications Standards Institute (ETSI)**
- <http://www.etsi.org>
- <http://portal.etsi.org>
- **ETSI Technical Committee Electronic Signatures and Infrastructures (ESI)**
- **International Telecommunication Union**
- <http://www.itu.int/>

E-paraksts Latvijā

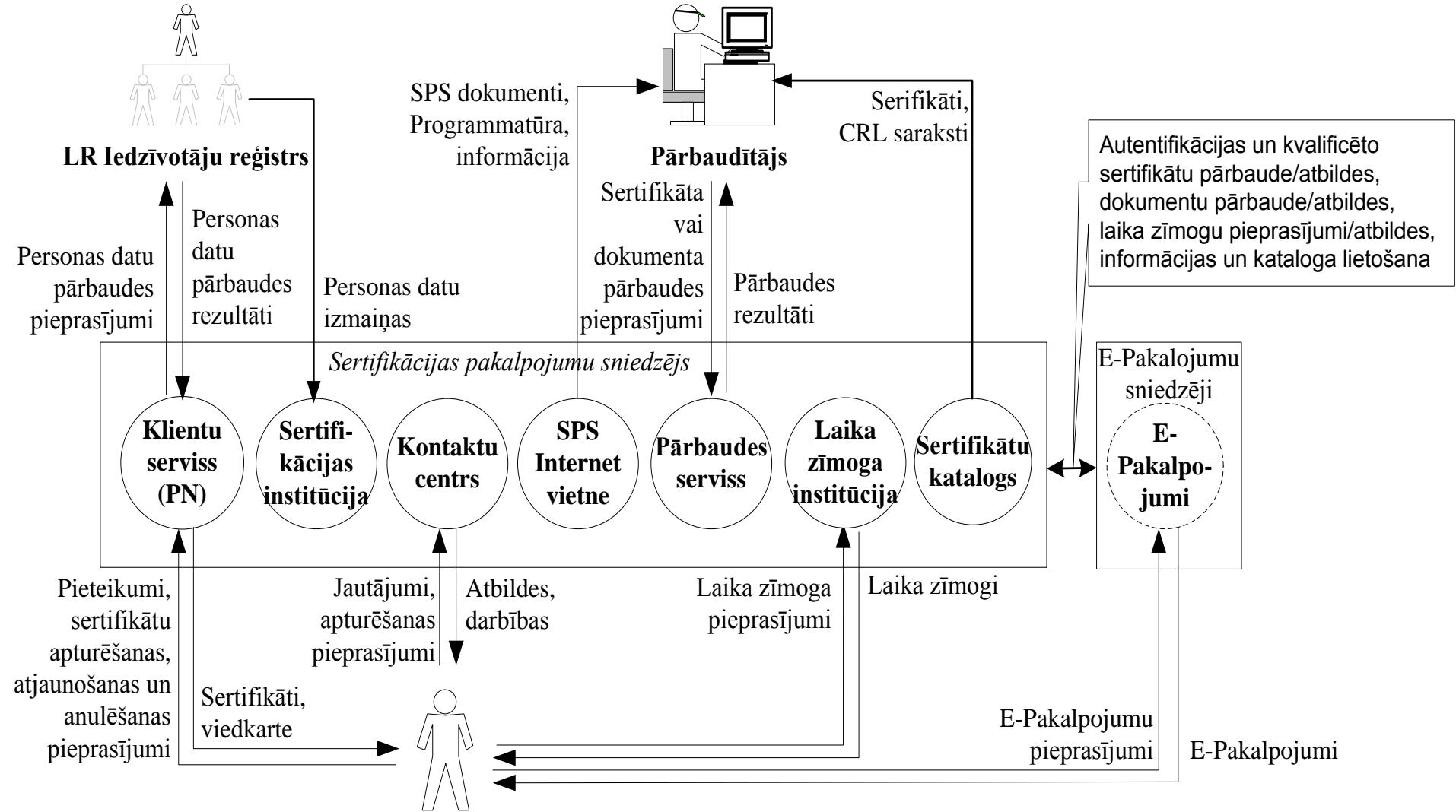


E-paraksts Latvijā

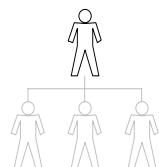
www.eparaksts.lv



- Uzticams sertifikācijas pakalpojumu sniedzējs Latvijā no 01.06.2009. ir VAS Latvijas Valsts radio un televīzijas centrs (LVRTC),
- kas pārņēma šīs funkcijas no VAS “Latvijas Pasts”
- Piedāvātie produkti:
viedkartes, eID kartes, virtuālais e-paraksts
- Viedkartes un eID kartes ir aizsargātas ar PIN kodu
- Viedkartēs un eID kartēs glabājas
 - elektroniskā paraksta radīšanas līdzekļi (t.i. privātās atslēgas)
 - sertifikāti kas apliecina parakstītāja identitāti
- Katrā viedkartē un eID ir divi atslēgu komplekti un sertifikāti:
 - autentifikācijai
 - parakstīšanai



Parakstītājs (fiziska persona, var būt saistīta ar Pasūtītāju)



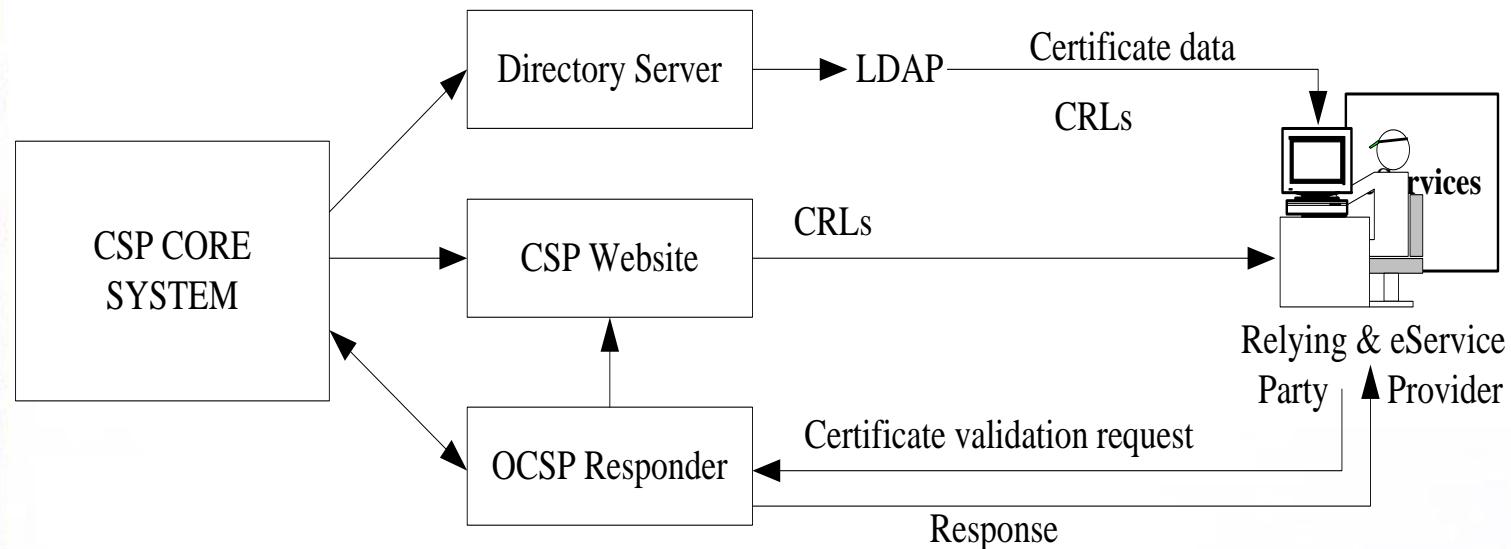
Pasūtītājs (juridiska persona, saistīta ar Parakstītāju)

Parakstīšanas programmatūra



- Parakstīšanas programmatūra dokumentam (datiem) pievieno e-paraksta un/vai laika zīmoga datus saskaņā ar XAdES-C standartu [ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES)],
- Tieka radīts Open Packaging Conventions (EDOC) formāta dokuments (parakstīts fails).
- Specifikācijas darbam ar e-dokumentiem publicētas majas lapā

Sertifikāta statusa pārbaude

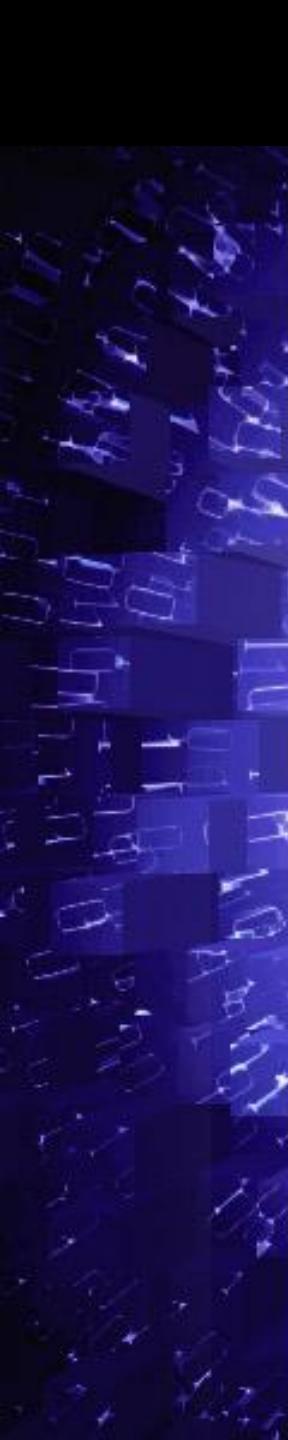


- SPS nodrošina sertifikāta derīguma pārbaudi, izmantojot:
 - *LDAP Directory Server*
 - *OCSP Responder*
 - CRL SPS mājas lapā

Ko var darīt ar autentifikācijas un e-paraksta viedkarti ?



- Apliecināt savu identitāti dažādu pakalpojumu izmantošanai:
 - piekļuve valsts reģistru datiem
 - dzīves vietas deklarēšana
 - laikrakstu abonēšana
 - interneta banku izmantošana
 - u.tml.
- Parakstīt dokumentus
- Informācija par esošajiem e-pakalpojumiem portālā www.latvija.lv



Kas nepieciešams organizācijai, kas ieviesīs elektroniskos dokumentus?

- Skaidrība par dokumentu plūsmām
- Elektronisko dokumentu aprites instrukcija
- Tehniskie līdzekļi elektronisko dokumentu apstrādei
- Sakārtota un efektīva IS pārvaldības un drošības sistēma