Ensuring mutual recognition of electronic signatures

Aleksandr Sazonov

25th September 2014
Background

The task
Ensure e-documents *genuineness* (*integrity* + *authenticity*) in cross-border scenarios

Best practice
Electronic signature usage (PKI-technology)

- Secure
- Scalable
- Widely used
Users in one domain

Anton trusts CA and Berta trusts CA ->
Anton can verify Berta’s e-signature
To verify Berta’s e-signature Anton has to:
a) trust CA2
b) be able to technically verify Bertha’s electronic signature
The usage of trusted services of a third party (or TTP services):

• X.842 Information technology – Security techniques – Guidelines for the use and management of trusted third party services

• Electronic identification and trust services (eIDAS)

• Documents on TTP within the framework of Eurasian Economic Union, such as IISFMT (Integrated Information System of Foreign and Mutual Trade)
Single TTP service

TTP service (international)

CA1

Anton

CA2

Berta
TTP services architecture

Single TTP service per country

TTP service 1 (national)

CA1

Anton

TTP service 2 (national)

CA2

Berta
Usage in eTIR framework

- Alignment with frameworks on eIDAS and/or IISFMT
- Reusability, further development / extension
- Adopted for specific requirements of eTIR
- Reasonable implementation period
- Another local solution
- Much time to become operational
Questions?

*Let's ensure trusted trans-boundary electronic interaction!*

Aleksandr Sazonov

deputy general director on development

“National Certification Authority Rus” CJSC

sazonov@nucrf.ru