OASIS Digital Signature Services

Remote Signing

ENISA Trust Services Forum, Berlin

- Digital Signature Services (DSS-X)'s Mission: *"Defining an ~~XML~~ interface to process digital signatures for Web services".*
- OASIS Digital Signature Services TC produced a set of OASIS standards (in 2007), including the core protocols and a number of profiles.
- New OASIS Digital Signature Services eXtended (DSS-X) TC created operating under OASIS RF IPR mode.
- Committee specification, version 2.0
  - Multiple transport representations (e.g. JSON) support
  - Core streamlined
  - Processing feedback

- DSS-X Profile: Local Signature Computation
- Status: Committee draft
- Support different key placement variants
  - Dedicated Key servers
    - May require user‘s explicit consent
  - User‘s smart card
    - User agent not addressable directly
  - Mobile devices
    - User agent addressable by mobile infrastructure
- Signature requestor location
  - Collocated
  - Distributed

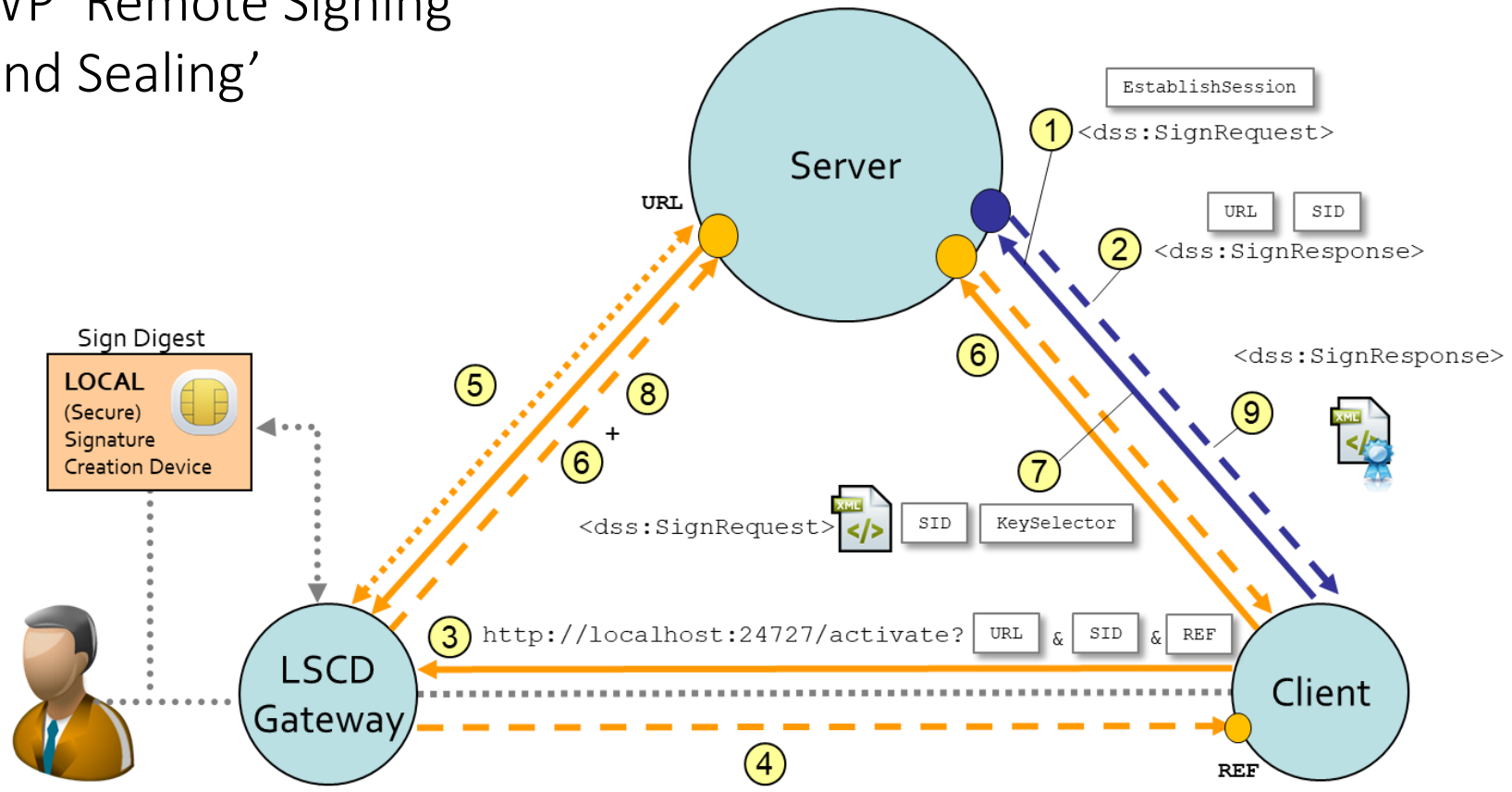
- DSS-X Profile: Local Signature Computation
- Status: Committee draft
- Supp
  - De
    -
  - Us
    -
  - Mo
    - User agent addressable by mobile infrastructure
- Signature requestor location
  - Collocated
  - Distributed

The ‘Local Signing’ scenario is the most complex model. We consider ‘Remote Signing’ as a specialization of the ‘Local’ approach!

DSS-X contribution: Chip Gateway Protocol

- Contributed to foster eIDAS-Regulation(EU) No. 910/2014 by luxtrust and ecsec
- Focus user controlled tokens
  - User‘s smart card
  - Mobile devices
- Implementation by the EU-funded ‚FutureTrust‘ project

WP ‘Remote Signing and Sealing’



5	LG → S : LG → S : <lsp:GetCommand> / command, as requested by Server, including	**Connect**
6	S → LG: <lsp:ListTokensRequest>, followed by <lsp:ListTokensResponse> S → LG: <lsp:ListCertificatesRequest>, followed by <lsp:ListCertificatesResponse>	**List**
8	S → LG: <lsp:SignRequest>, followed by <lsp:SignResponse> S → LG: <lsp:Terminate>, followed by redirect to REF	**Sign**

DSS-X TC Public page:

- https://www.oasis-open.org/committees/dss-x

Document access:

- http://docs.oasis-open.org/dss-x/dss-core/v2.0/csprd01/dss-core-v2.0-csprd01.html
- http://docs.oasis-open.org/dss-x/localsig/v1.0/cs02/localsig-v1.0-cs02.html
- https://www.oasis-open.org/committees/download.php/60049/ChipGateway-Specification-OASIS.pdf

Web www.futuretrust.eu

FutureTrust

@FutureTrust_EU

www.linkedin.com/groups/8562515

kuehne@trustable.de