

OASIS Digital Signature Services and ETSI standards

Juan Carlos Cruellas – UPC
Stefan Drees - DSS-X co-chair
Nick Pope – Thales eSecurity

Contents

- ETSI and ESI TC
 - Introduction to ETSI and ETSI ESI TC
 - ESI standardization work overview
- DSS and DSS-X OASIS TC
 - DSS concept
 - DSS TC standardization work overview
 - DSS-X overview
- ESI and DSS-X standards relationship
- Questions and Answers

ETSI and ESI TC

Introduction to ETSI and ETSI ESI TC

- European Telecommunications Standards Institute (ETSI) website reports that ETSI:
 - Is recognised as an official European Standards Organisation by the European Commission.
 - Produces globally applicable standards for Information and Communications Technologies (including internet)
 - Websites: <http://www.etsi.org> and <http://portal.etsi.org>

Introduction to ETSI and ETSI ESI TC

- Electronic Signatures and Infrastructures (ESI) TC:
 - Is responsible for Electronic Signatures and Infrastructures standardisation within ETSI.
 - Develops generic standards, guides and reports related to electronic signatures and supporting infrastructures.

Introduction to ETSI and ETSI ESI TC

- Liases with both internal and external bodies to ETSI related to electronic signatures in order to harmonize specifications at the international level.
- Website: http://portal.etsi.org/esi/ESI_ToR.asp

ESI standardisation work overview

- Standardisation work background:
 - Publication in 1999 of the European Directive that allows use digital signatures for legally binding transactions and defines the Advanced Electronic Signature.

ESI standardisation work overview

- ESI TC standardises in different electronic signature related areas:
 - Electronic Signature Formats
 - Infrastructure, including:
 - Specification of new architectural elements
 - Profiling of architectural elements
 - Policies, including:
 - Signature Policy formats
 - Policies for Trusted Service Providers

ESI standardisation work overview

- Guidance material, including:
 - Guidance on algorithms and parameters for electronic signatures.

ESI standardisation work overview

- Electronic signatures formats.
 - Technical Specification TS 101 903: “XML Advanced Electronic Signatures (XAdES)”
 - TS 101 733: “CMS Advanced Electronic Signatures (CAdES)”
 - These specifications:
 - Build on XMLDSig and CMS formats respectively.
 - Standardise a set of properties that may be incorporated to XMLDSig-based electronic signatures fulfilling a number of common requirements (such as the long term validity of the signature)

ESI standardisation work overview

- Identify a set of different combinations of properties (Signature Forms), each one offering its own set of features relevant in specific contexts and phases of the signatures life cycle.
- They have been further profiled by:
 - TS 102 904: “Profiles of XML Advanced Electronic Signatures based on TS 101 903”
 - TS 102 734: “Profiles of CMS Advanced Electronic Signatures based on TS 101 733”
 - They define an electronic signatures baseline profile and profiles for e-Government and e-Invoicing.

ESI standardisation work overview

- Infrastructure. This includes:
 - Profiling infrastructural elements:
 - TS 101 862: “Qualified Certificate Profile”
 - Defines a technical format for Qualified Certificates aligned with annexes I and II of the European Directive.
 - TS 102 280: “X.509 v3 Certificate Profile for Certificates Issued to Natural Persons”.
 - TS 101 861: “Time stamping profile”.
 - Profiles IETF RFC 3161 time-stamps regarding electronic signatures time-stamping.

ESI standardisation work overview

- Specifying new infrastructural elements:
 - TS 102 231: “Provision of Harmonized Trust Service Provider status information”.
 - Defines a way for publishing information on the status of Trusted Service Providers and the services that they provide, as assessed against certain assessment schemes. This is specially useful for supporting cross-domain and international transactions. ASN.1 and XML formats are specified.

ESI standardisation work overview

- Policies. This includes:
 - Signature Policies Formats:
 - Technical Report TR 102 038: XML format for signature policies
 - TR 102 272: ASN.1 format for signature policies
 - These reports define structured formats for signature policies documents that govern the creation and verification of electronic signatures.

ESI standardisation work overview

- Policies that Core Trusted Services Providers must adhere. These include providers of:
 - Public Key Certificates: TS 101 456
 - Attribute Certificates: TS 102 158
 - Qualified Certificates: TS 101 456
 - Time-stamps: TS 102 023

ESI standardisation work overview

- Specifications covering electronic signatures when used in specific application areas.

These include:

- TS 102 573: “Policy requirements for trust service providers signing and/or storing data for digital accounting”.
 - Specifies security management and policy requirements applicable to TSPs that issue fiscally relevant electronically signed documents and/or store them on behalf of taxable persons

ESI standardisation work overview

- On going work on Registered Electronic mail Systems (REM systems: e-mail systems that provide trusted evidences that certain facts have actually occurred), where ETSI is going to produce a new TS: “Registered Electronic Mail (REM) Architecture, Formats for signed evidences and Policies”, a multi-part document that will specify:
 - A generic architecture for REM systems
 - Data requirements and formats for signed evidences in REM systems.
 - Policy requirements for trust service providers providing signed evidences in REM systems.

ESI standardisation work overview

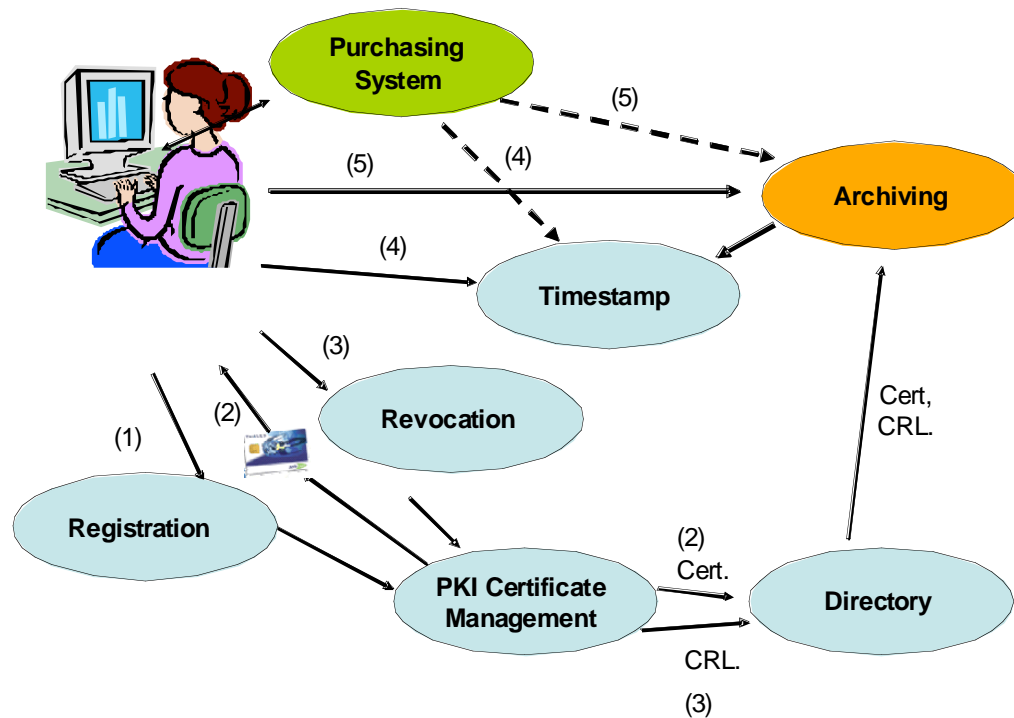
- Guidance. This includes:
 - TS 102 176: “Algorithms and Parameters for Secure Electronic Signatures”. Multipart document:
 - Part 1 deals with hash functions and asymmetric algorithms.
 - Part 2 deals with secure channel protocols and algorithms for signature creation devices.

DSS and DSS-X OASIS TC

DSS concept

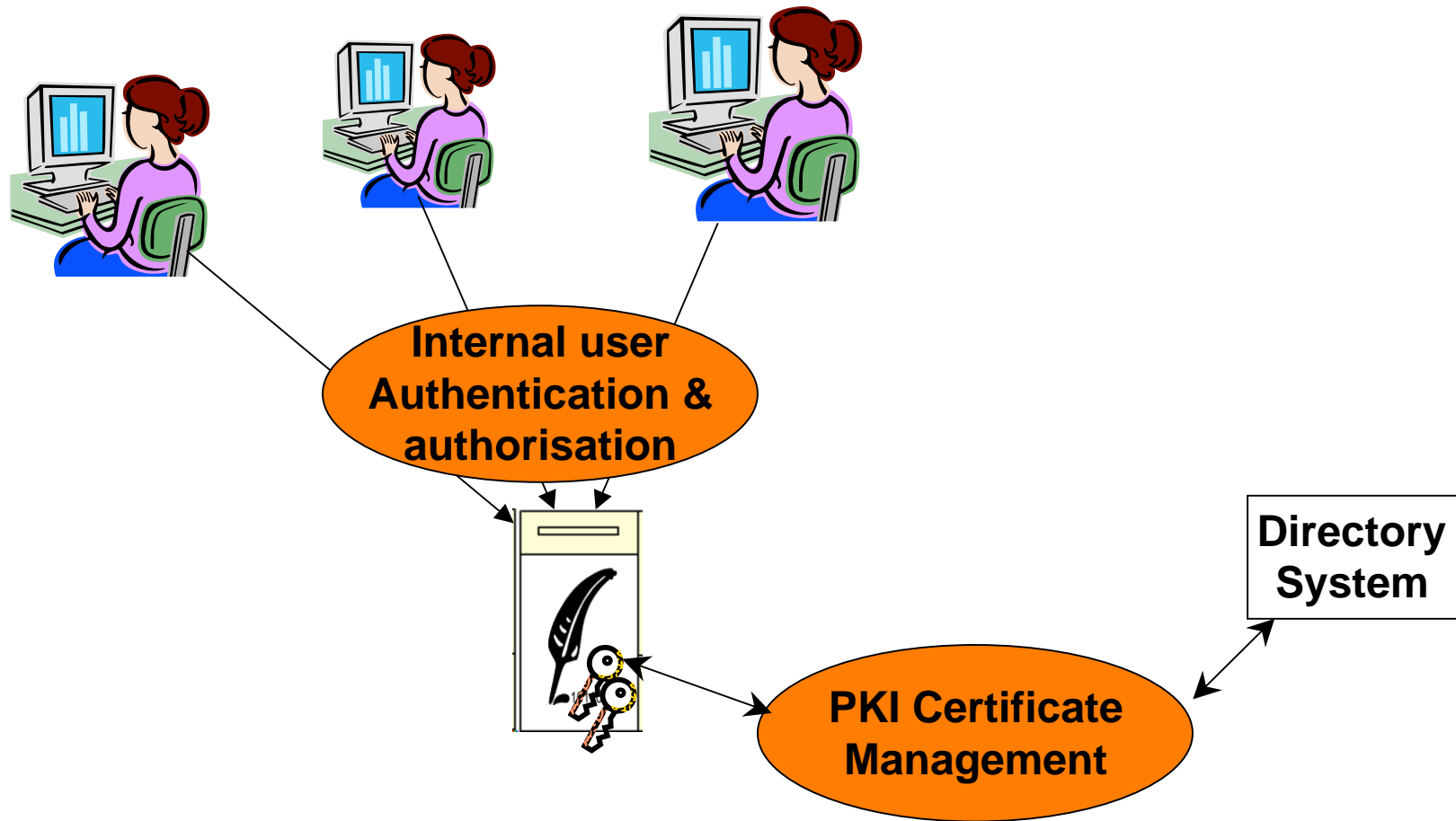
- DSS charter reads:
 - Develop “a protocol for a digital signature creation web service. Providing digital signatures via such a web service facilitates policy-based control of the provision of the signatures”.
 - Develop “a protocol for a digital signature verification web service that can verify signatures in relation to a given policy set”.
 - Develop “an XML-based protocol to produce cryptographic time-stamps”.

DSS concept. Conventional approach



- Deploy key to each user
- Handle Interface to all PKI functions
- Security depends on user

DSS concept. DSS approach



DSS concept. Why DSS

- Avoid burden of deployment of signing on individual basis
- Shared server for generation and verification of digital signatures
- Support of signing as corporate function

DSS concept. Main features

- DSS supports :
 - Creation of digital signatures
 - Verification of signatures
 - Creation / verification of time-stamps
XML (Define in DSS) / Binary (RFC 3161)

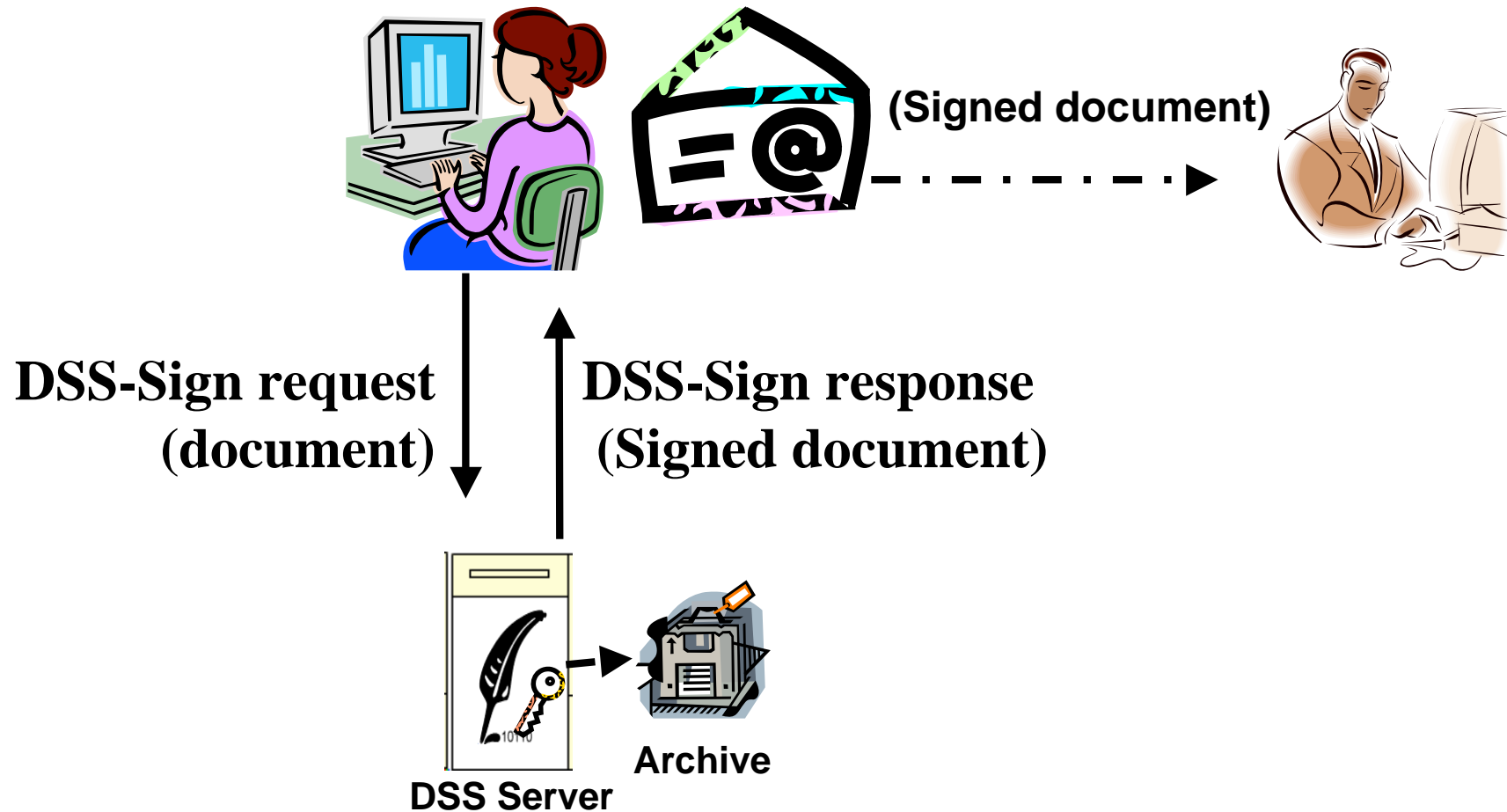
DSS concept. Main features

- Support range of signature formats including:
 - W3C XML Signatures
 - CMS (RFC 3852) Signatures
 - RFC 3161
 - XML time-stamps (defined in DSS)
 - Advanced Electronic Signatures (ETSI TS 101903 and ETSI TS 101733)
- Range of Document / Signature structures
- Optional inputs / outputs for controlling specific features

DSS TC standardization work overview

- Core protocol specification.
 - Defines two protocols: signing and verification.
 - Each protocol two messages: request and response.
 - Defines basic mandatory features and a number of optional features.

DSS Sign Protocol

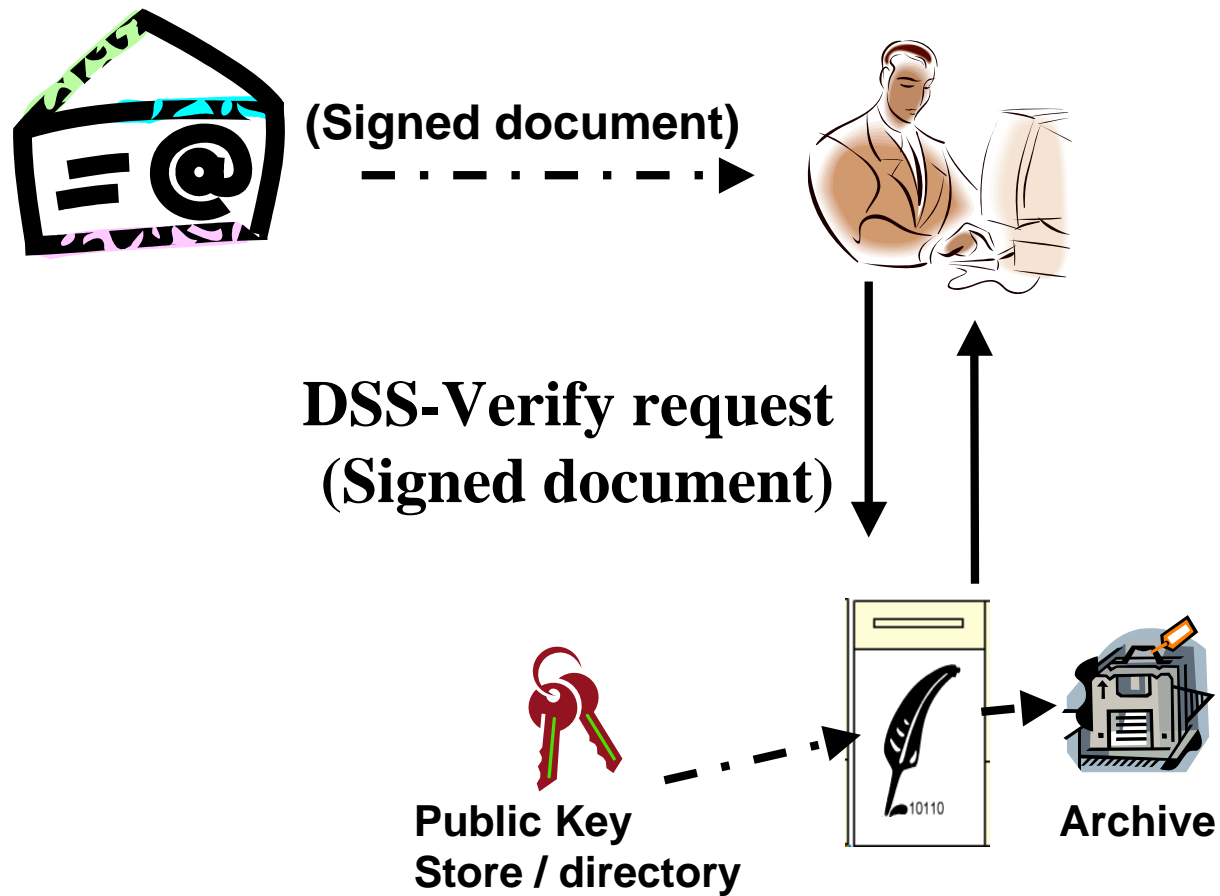


DSS Signature Creation: Advantages

- Authentication of user separated from management of signature key.
 - Controls on who may apply “corporate” signatures
 - Controls on user access to own signing key
 - Based on existing internal security controls using existing authentication and authorisation controls within normal work flow
- If user’s authorisation is revoked, organisation can stop use of signature
 - Immediate
 - No need to publish external revocation
- No need for special device on user system
- Strict organisational controls can be applied to handling of signing key

Improved security & reduced per user cost

DSS Verify Protocol



DSS Signature Verification: Advantages

- Verification complexities taken off user system
- Common verification policy can be directly applied
- Can maintain log of result of signature verification when first received for later re-checking

DSS TC standardization work overview

- Profiles of the core specification:
 - Extend and/or adapt the core to specific needs, use cases and environments.
 - Time-stamp: equivalent of RFC 3161 for XML.
 - Entity-seal: generation/verification of a “seal” (time-stamped signature with information of identity of the requester: proxy signature).

DSS TC standardization work overview

- Advanced Electronic Signature. Supports lifecycle of CAdES and XAdES signatures
- Signature Gateway: creation of signatures at a gateway, translating from an internal format to a standard form
- Code-signing. Support to signing of code authorized for distribution
- Asynchronous Processing. Supports deferred delivery of server responses

DSS-X Overview

- New DSS-X TC “Digital Signature Services eXtended” opened in 23rd July 2007.
- DSS-X TC has joined OASIS IDTrust member section.
- Charter at:
<http://www.oasis-open.org/committees/dss-x/charter.php>

DSS-X overview

- Main goals in the charter:
 - Produce new profiles based on DSS core.
 - Produce dissemination material.
 - Produce analysis of inter-relationship among profiles.
 - Maintenance of existing DSS OASIS standards.

DSS-X overview

- Contacting coordinates:
- Website:
<http://www.oasis-open.org/apps/org/workgroup/dss-x/>
- Public comments e-mail list:
dss-x-comment@lists.oasis-open.org

Anyone willing to contribute is very welcomed!

DSS-X overview

Current status (I):

- Identified a number of profiles to develop:
 - Profile for visible signatures.
 - Profile for PDF signatures
 - Profile for ebXML
 - Profile for individual reports on every signature verified in multi-signature documents
 - Profile for requesting signed verification responses

DSS-X overview

- Profiles for basic functions in support of generation and verification of XML signatures, CMS signatures, XML time-stamps and RFC 3161 time-stamps ("baseline" profiles).
- Profile for handling of signature & service policy
- Profile for supporting centralized encryption and decryption services

DSS-X overview

- Received some external and internal contributions that will be assessed in a near future.
- Currently TC is working in producing requirements documents for the different profiles.
- Rough time-line estimation: work completed by the end of 2008.

ESI and DSS, DSS-X standards relationship

ESI and DSS-X standards relationship

- ESI has:
 - Standardised electronic signature formats and profiled infrastructural elements.
- DSS (and its successor DSS-X) has:
 - Defined protocols for remotely requesting generation and verification of electronic signatures to specialized services and has also ...
 - Specified a profile for requesting generation and validation of AdES signatures specified by ESI.

ESI and DSS-X standards relationship

- DSS and DSS-X:
 - Have made possible the provision of new services that are directly related to standards previously developed by IETF, W3C and ESI, but at the same time...
 - These services will make use of infrastructural elements defined by ESI TC and ...
 - Also, within Europe, they need to be aligned with the policy requirements specified by ESI TC

ESI and DSS-X standards relationship

- Future:
 - ESI and DSS-X could in a certain point of time establish a peer-review/comment mechanism to ensure the alignment of specifications produced by both bodies.

Thank you
Questions ?