OASIS Standard Digital Signature Services (DSS)

Assures Authenticity of Data for Web Services

Juan Carlos Cruellas – UPC Spain
Nick Pope – Thales eSecurity
(Co-Chairs DSS Technical Committee)

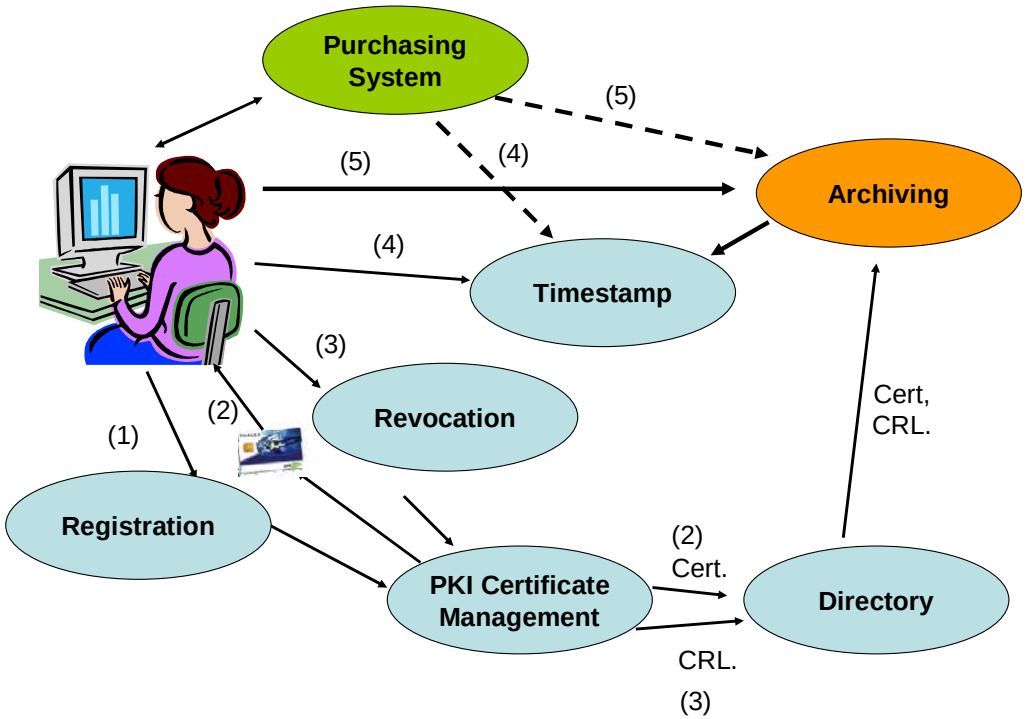
Contents

- Introduction
  - Why DSS
  - Outline features
  - Advantages
  - Set of specifications
  - Use case example: EU invoicing
- Core Protocols
  - Introduction
  - Signing protocol
  - Verifying protocol
- Profiling core
  - Introduction
  - Some relevant profiles
- Present and Future
- Questions and Answers

Why DSS

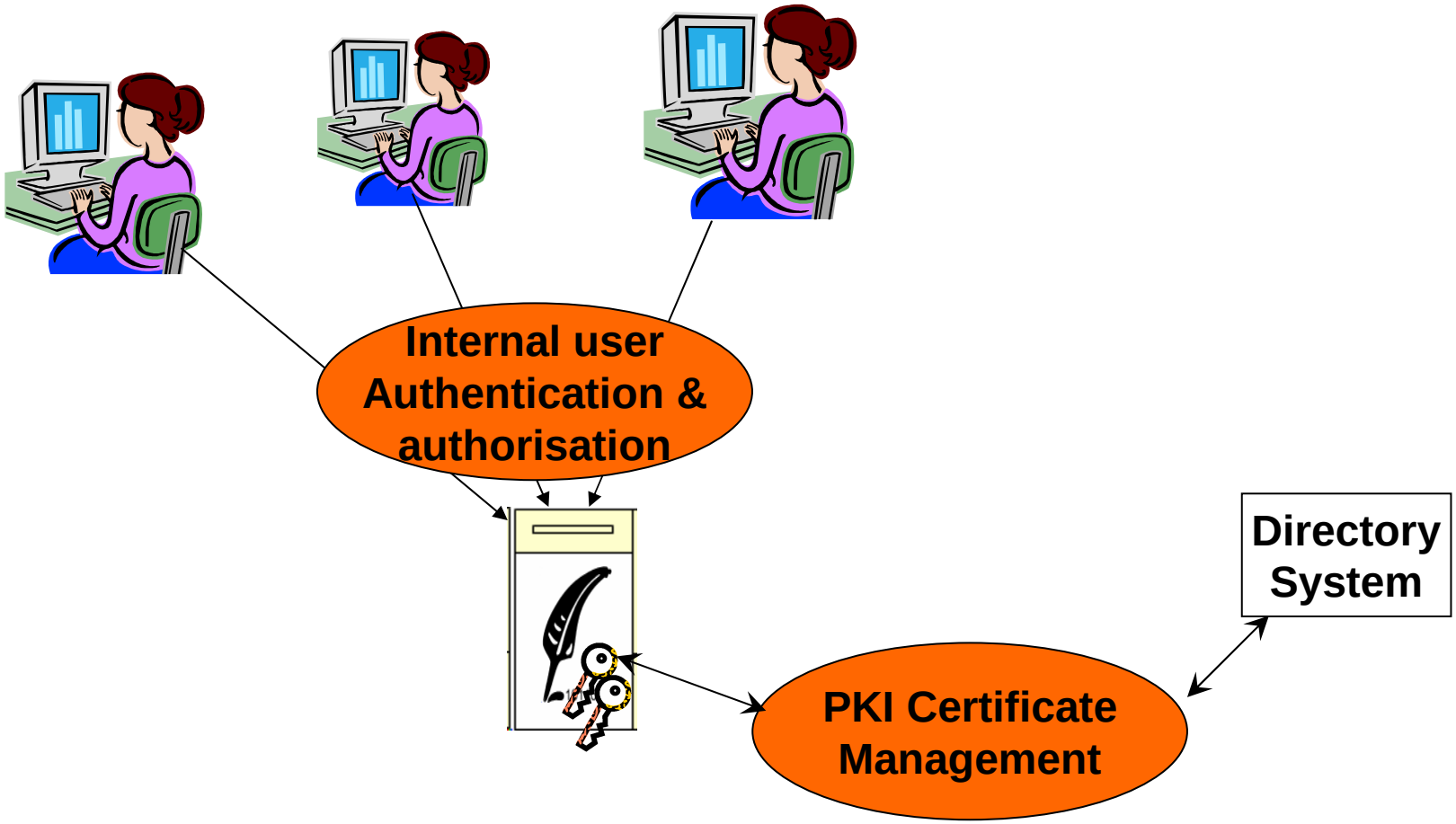
- Avoid burden of deployment of signing on individual basis
- Shared server for generation and verification of digital signatures
- Support of signing as corporate function

Conventional Approach

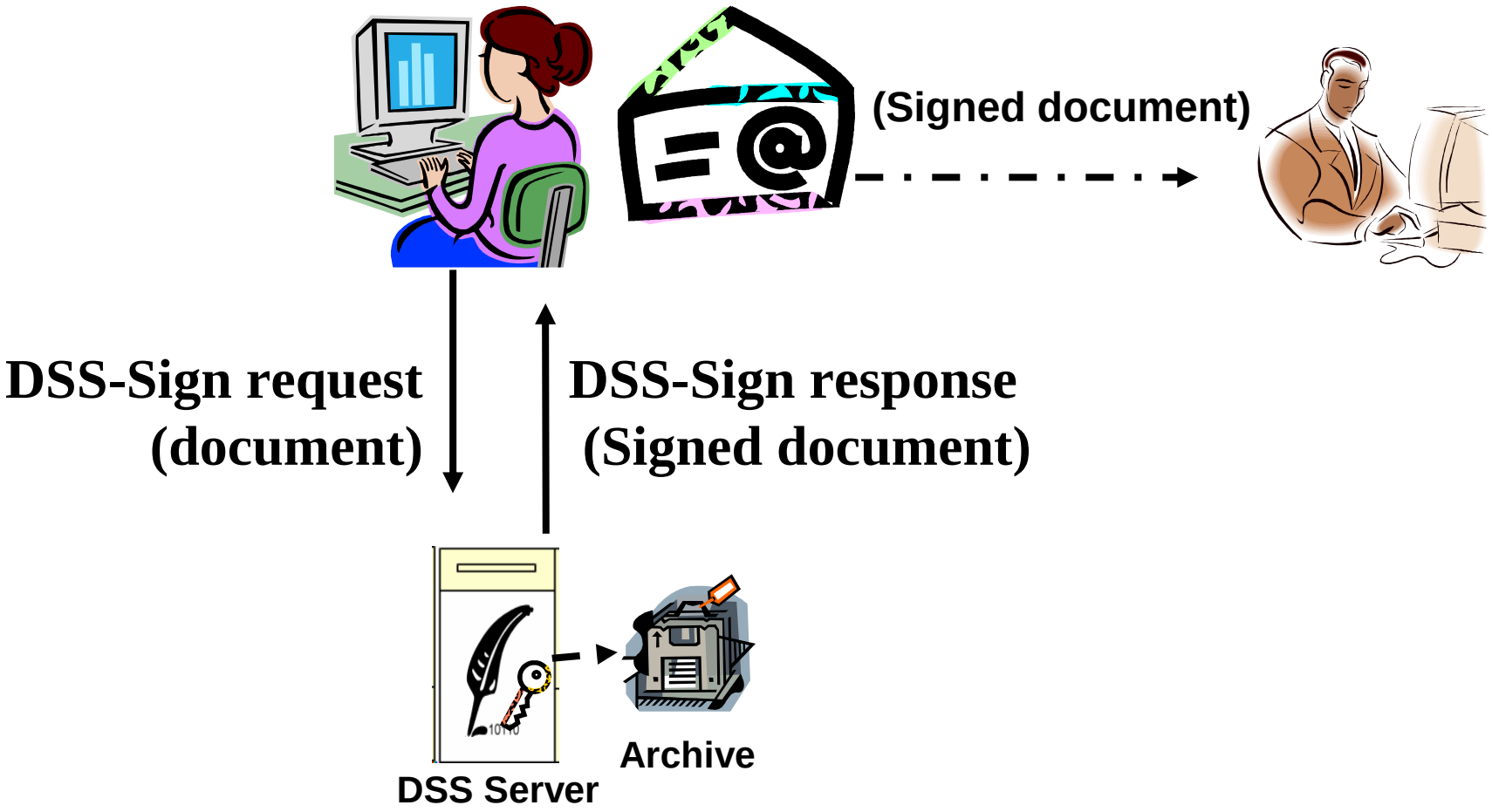


- Deploy key to each user
- Handle Interface to all PKI functions
- Security depends on user

DSS approach



DSS Sign Protocol

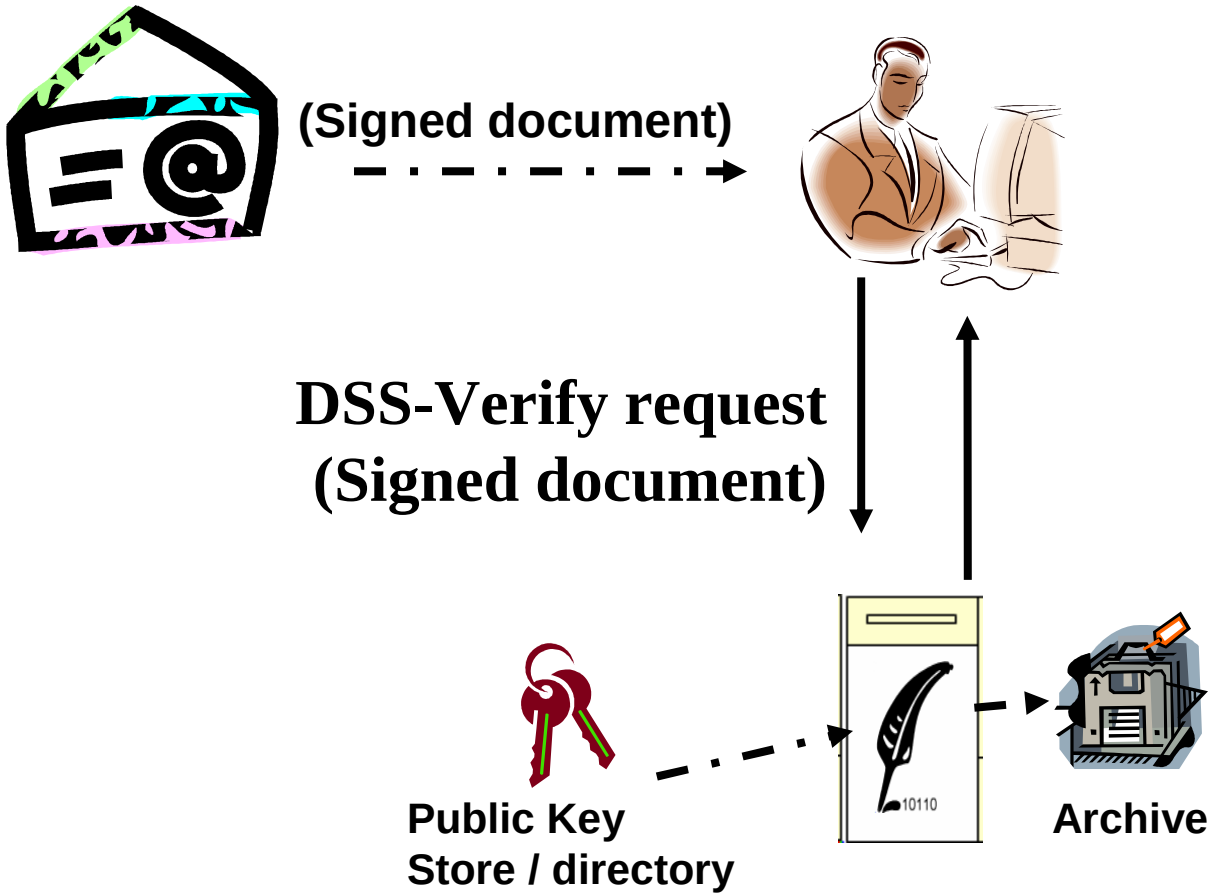


DSS Signature Creation: Advantages

- 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 Features

- Supports :
  - Creation of digital signatures
  - Verification of signatures
  - Creation / verification of time-stamps

    XML (Define in DSS) / Binary (RFC 3161)
- Generic “Core”
- Profiles for particular use cases

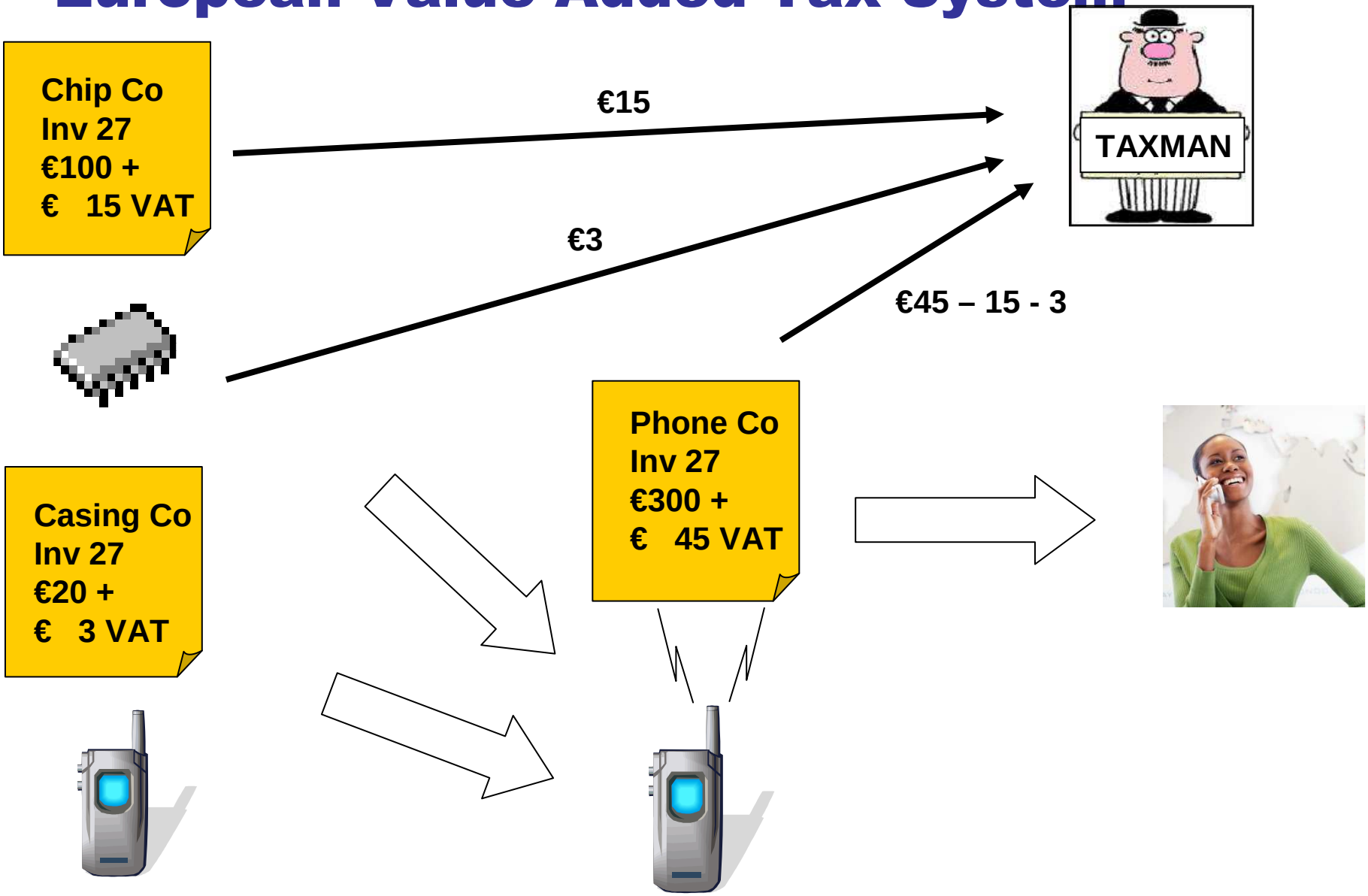
DSS Features

- 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

Set of specifications:

- Core protocol.
- Profiles of the core:
  - XML time-stamping
  - Entity seal
  - Signature gateway
  - “Advanced” / Long term Electronic Signatures (ETSI TS 101 733, TS 101 903, RFC 3126)
  - Code Signing
  - Electronic Post Mark

Use case: e-Invoicing and European Value Added Tax System



EU VAT Harmonisation Directive

- *"Invoices sent by electronic means shall be accepted by Member States provided that the authenticity of the origin and integrity of the contents are guaranteed* .."
- Recognised mechanisms:
  - EDI Service Provider
  - "Advanced Electronic Signature"
    - X.509 based Digital Signature
    - From company / company officer

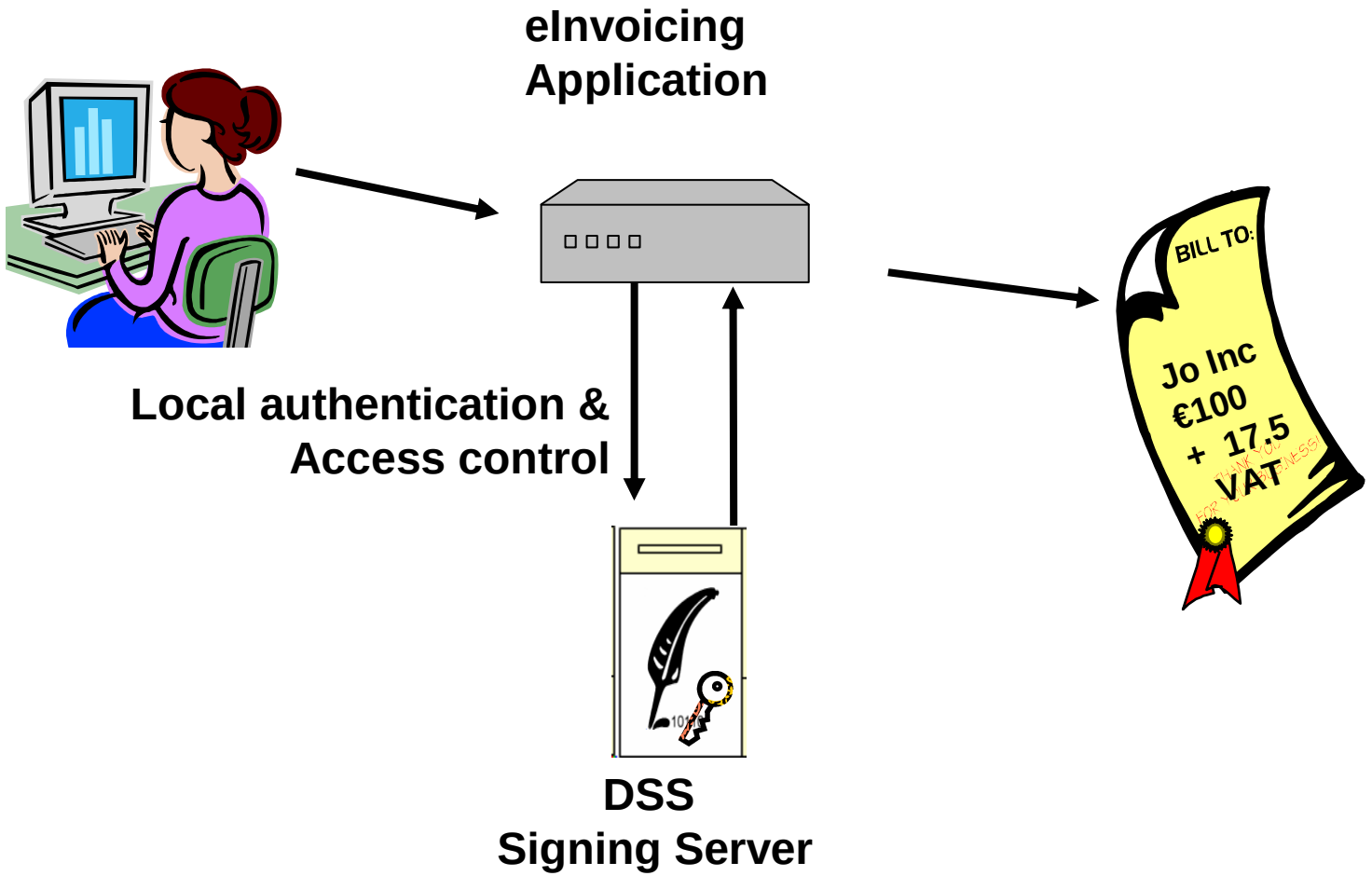
Requirement for Storage of Signed Invoices

Technical Requirements

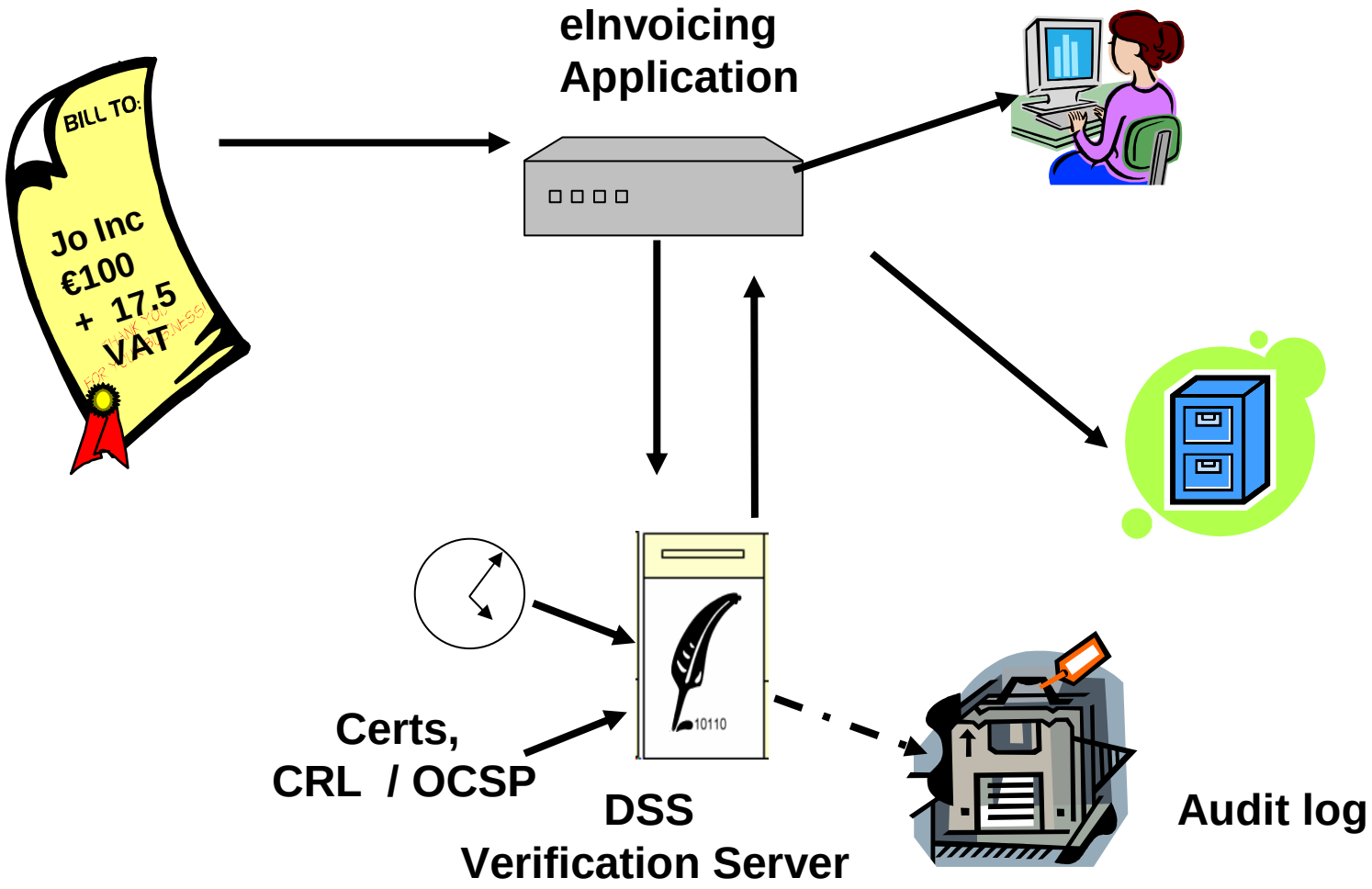
- Information used to verify signature when stored
  - Certificate path
  - OCSPs / CRLs
- Time of verification
  - Signature Time-stamp
- Means to assure validity of signature at signing time during lifetime of documents
  (e.g. 10 years)

- Ref: CWA 15579
  ETSI TS 102 573

DSS Signature Creation applied to eInvoicing



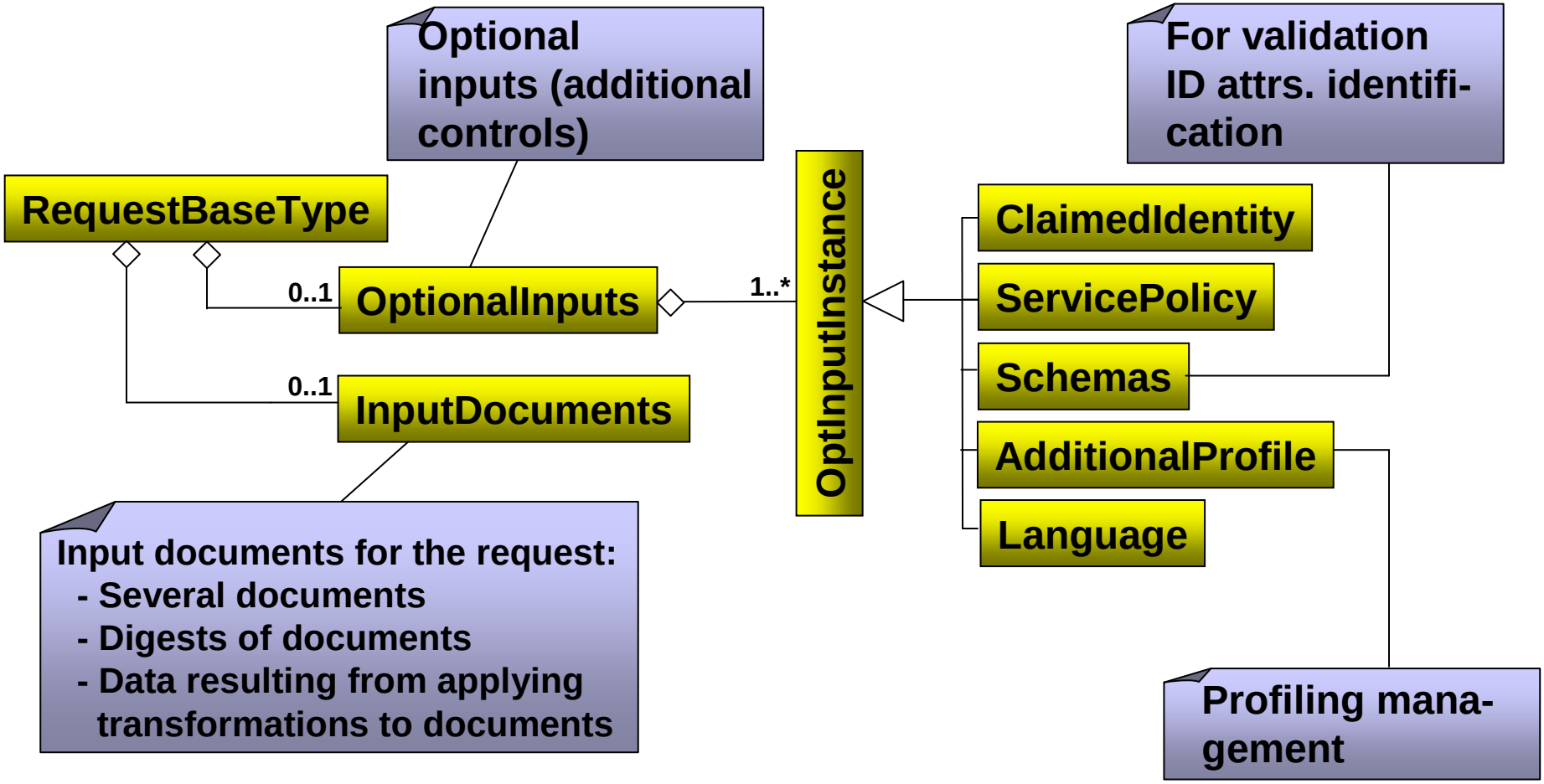
DSS Signature Verification applied to eInvoicing



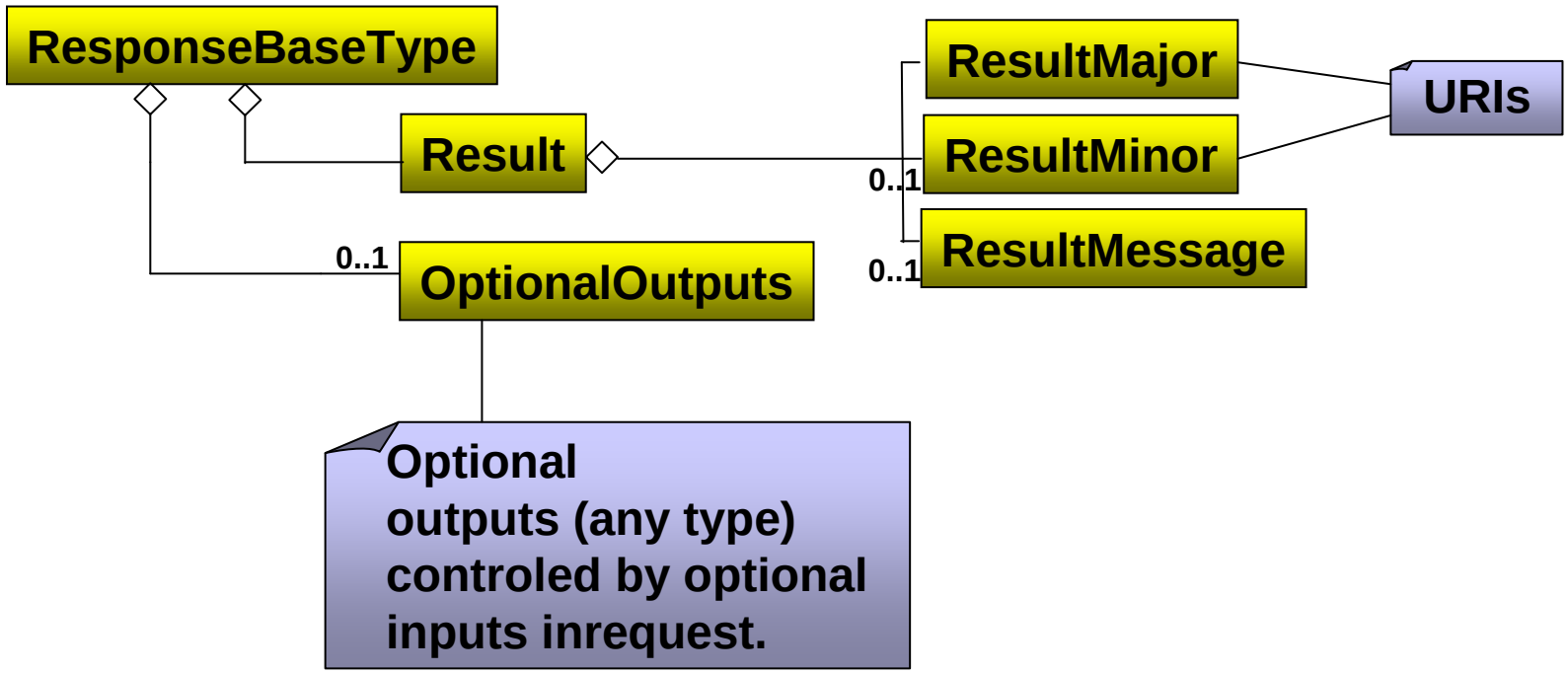
Core Outline

- Basic XML Structures for:
  - SignRequest
  - SignResponse
  - VerifyRequest
  - VerifyResponse
- Common request / response basic structure
- Optional inputs / outputs to handle different ways of signing / verifying
- Range of ways of conveying document
- Transport:
  - HTTP, SOAP
  - SSL, Web Security Services

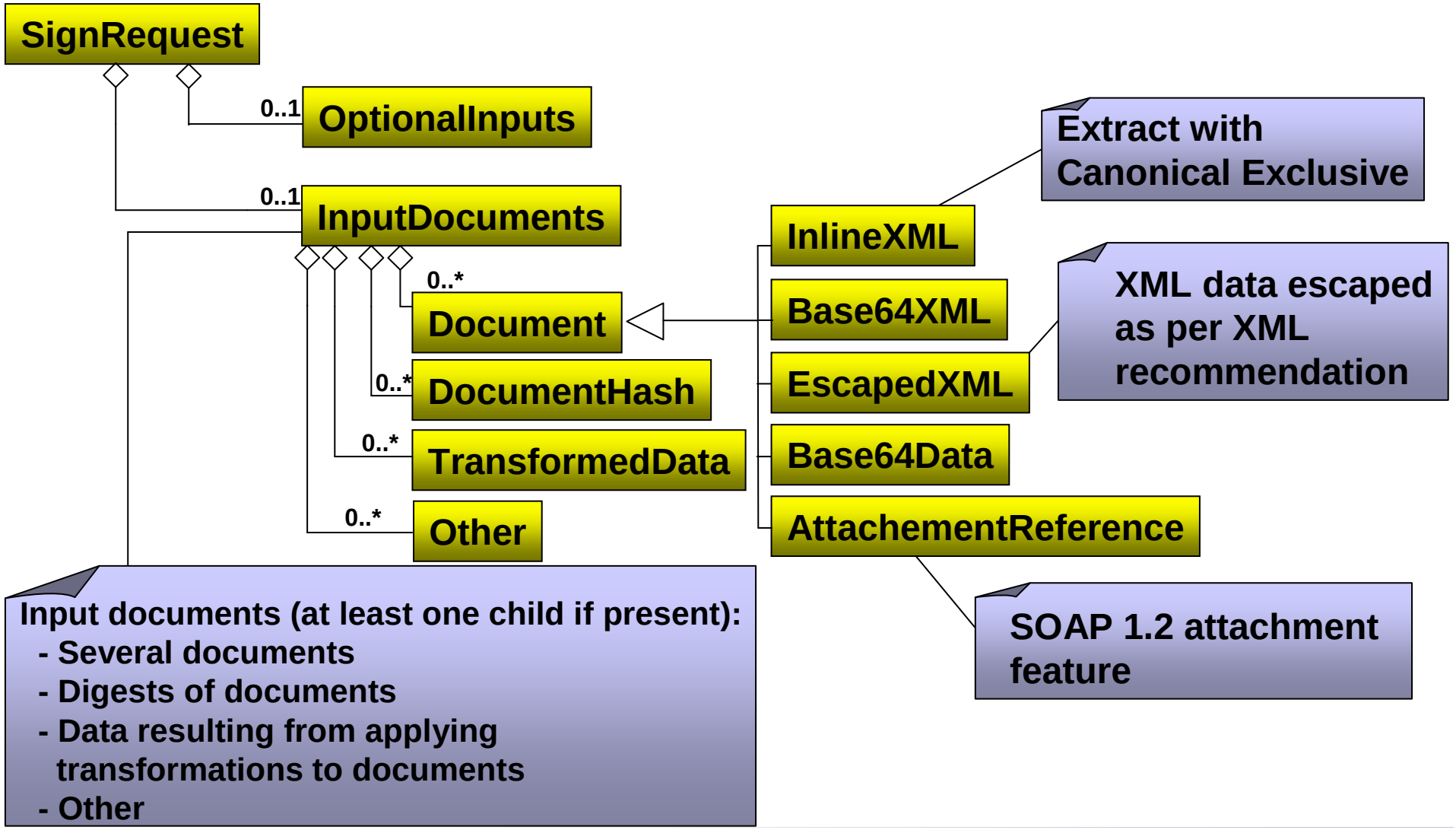
Base request and common controls



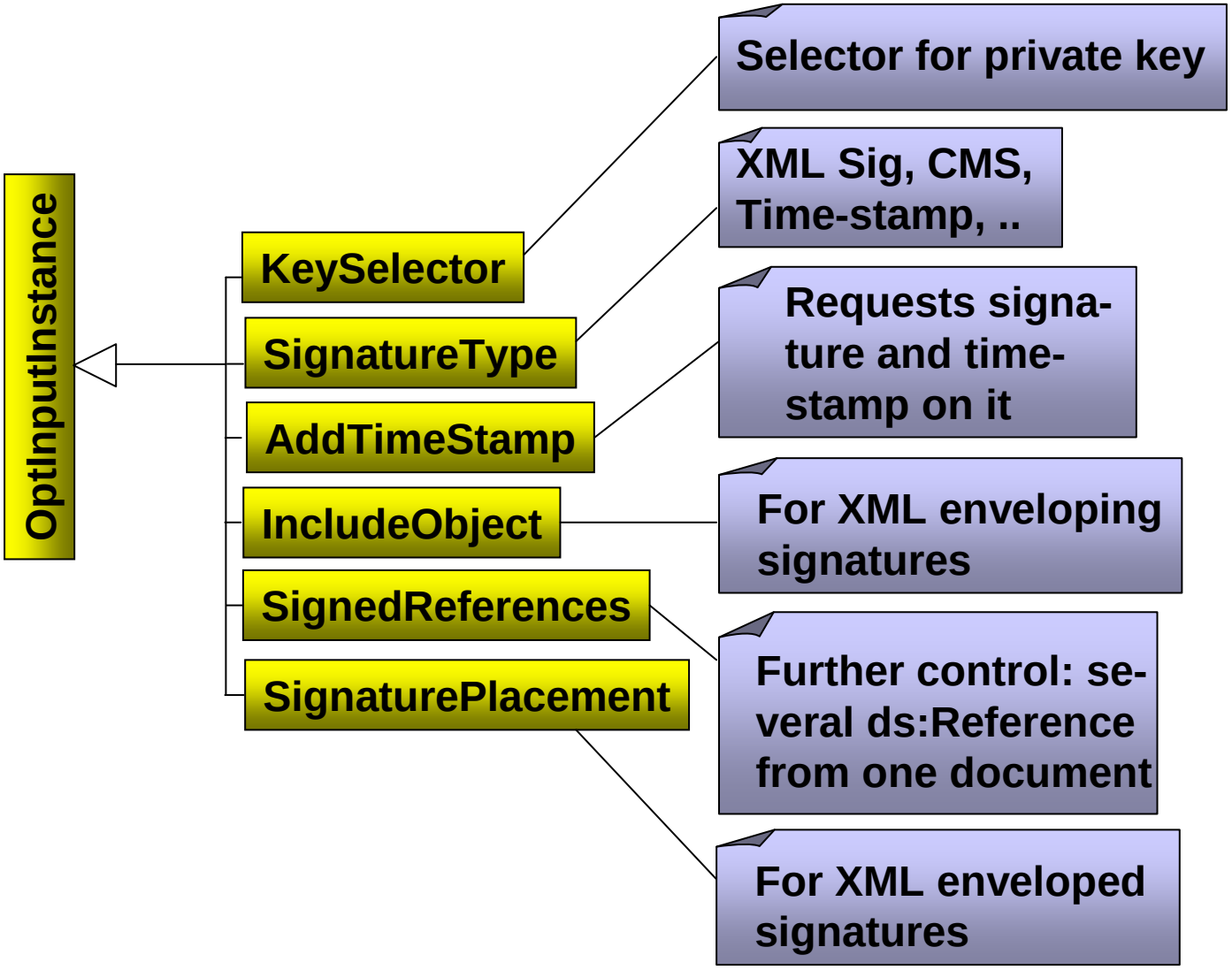
Base response



Signing Protocol: To-be-signed documents and data in request.



Signing Protocol: Additional controls in request.



Core: Signing Protocol Features summary

- To-be-signed documents:
  - Signature may be requested for:
    - More than one document.
    - Digests of documents (confidentiality issues).
    - Data objects resulting from transformations of documents.
  - Documents in several formats: base64-encoded binary, XML (escaped, base-64 encoded, inline), SOAP Attachment

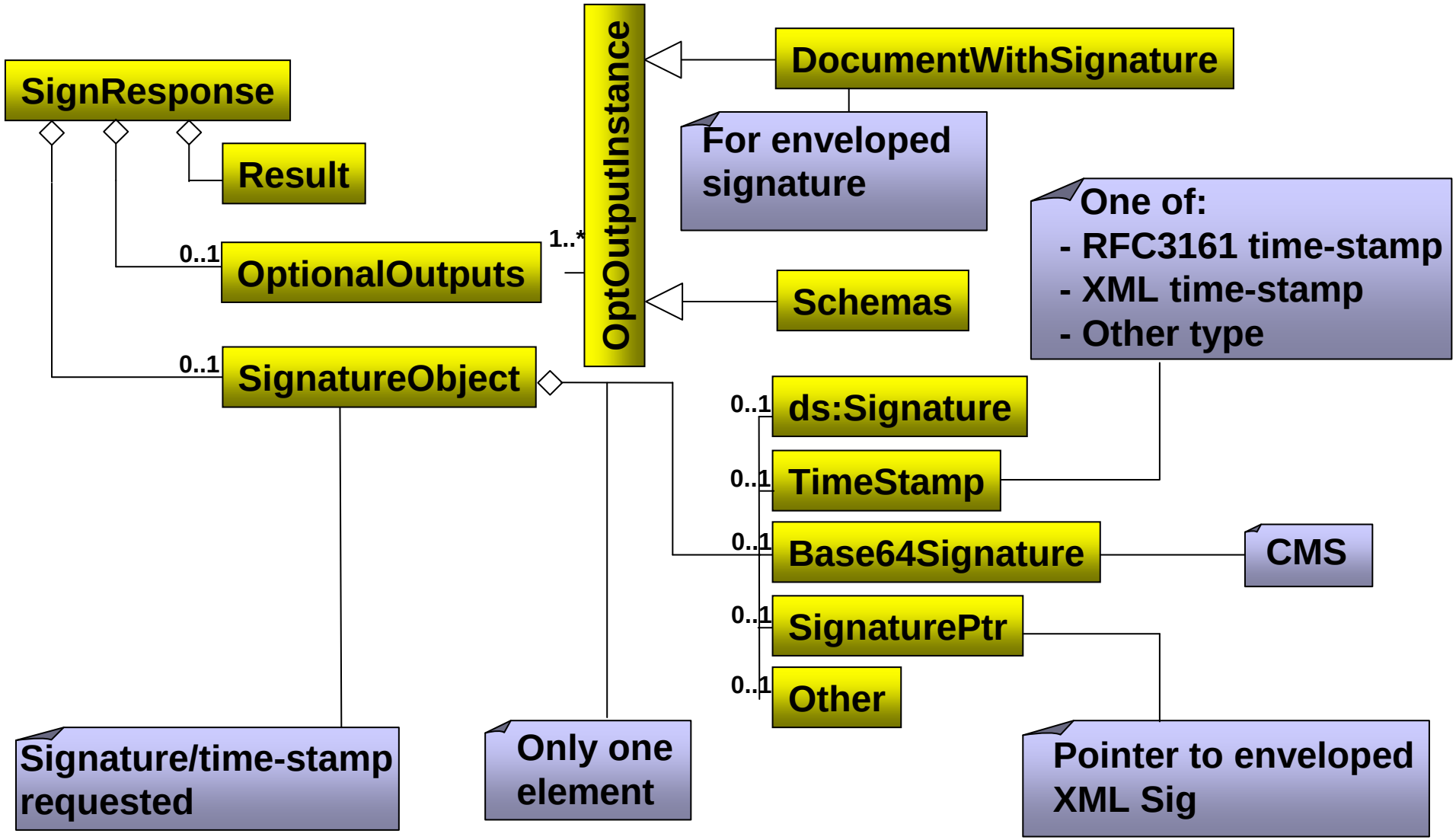
Core: Signing Protocol Features summary

- Specific controls for signature generation. Client may:
  - request a specific type of signature / time-stamp
  - claim his own identity
  - request signing with a specific private key
  - request generation of a time-stamp on the generated signature
  - request that the signature envelopes one or more signed documents.

Core: Signing Protocol Features summary

- Request the server generate several to-be-signed data objects from one input document (using XPath transformations, for instance) and sign each one (one ds:Reference per data object).
- Request to envelope the signature within a XML document.

Signining Protocol: Response

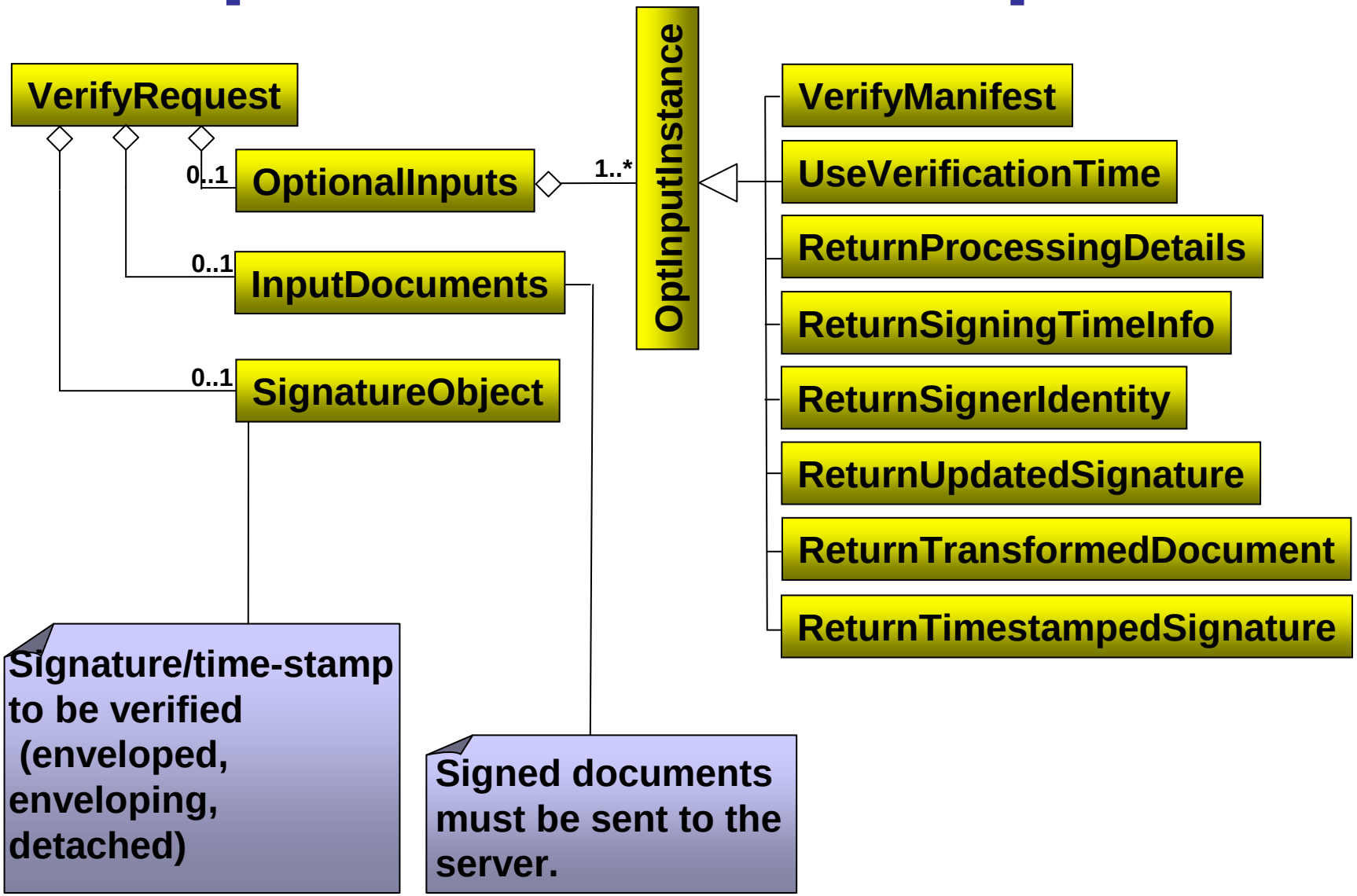


Core: Signing Protocol Response

Relevant features:

- The response may contain one enveloping, one enveloped or one detached signature.
- The enveloped signature appears within the DocumentWithSignature element, and is pointed by SignaturePtr.

Verifying Protocol: Specific controls in request



Core. Verifying Protocol. Features summary

- Signed documents:
  - Enveloping documents:
    - Directly incorporated with the enveloped signatures.
  - Enveloped documents:
    - Signature within SignatureObject with enveloped document.

Core: Verifying Protocol Features summary

- Detached documents:
  - The server DOES NOT retrieve detached documents: must be sent in the request.
  - Incorporated as InputDocuments each one including in one attribute the URI value present in the corresponding ds:Signature’s ds:Reference, so that the server may link the signature with the signed detached document.

Core: Verifying Protocol Features summary

- Specific controls on verification process. The client may:
  - request verification of ds:Manifest.
  - request the server to act as if the verification time is not the present one but another one
  - request to return information on the signing time (good if there is any signature time-stamp)
  - request return of the signer identity

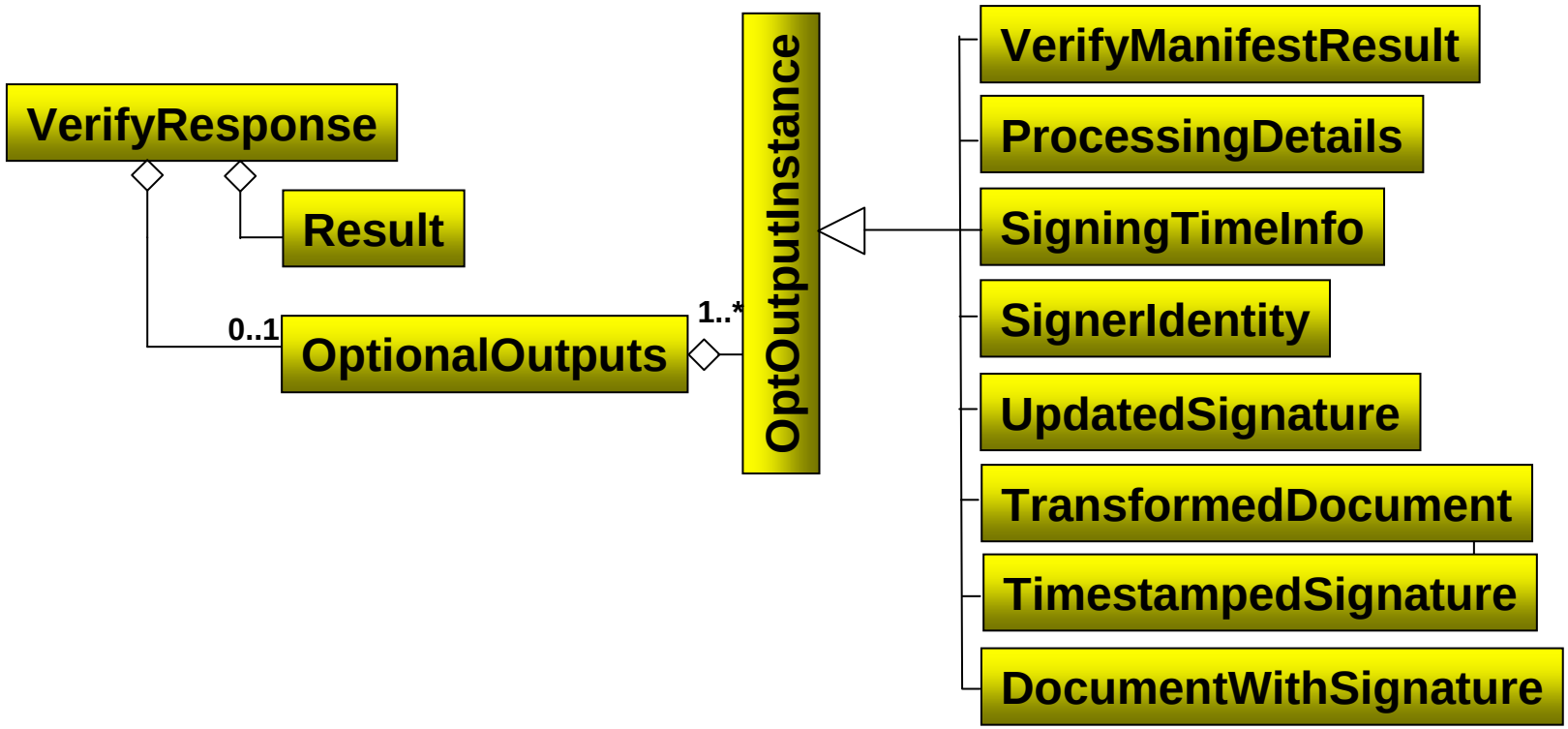
Core: Verifying Protocol Features summary

- request update of the signature (this means incorporation of verification material, time-stamps on verification material, etc). This is related with re-verification of signatures. Alternatively DSS also supports audit log of verification material.
- request transformation of certain documents and return
- request generation of a time-stamp on the verified signature
- request details of the verification process

Core: Verifying Protocol Features summary

- If there are more than one signatures in one document, the server may verify all of them, but not possible to individually report each verification.

Verifying Protocol: Response



DSS profiling

- Support for different scenarios and ways of signing/verifying.
- Profiles:
  - 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).
  - Advanced Electronic Signature. Supports lifecycle of long term electronic signatures

DSS profiling

- 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 profiling

Types of profiles:

- Concrete profiles: may be directly instantiated (entity seal, time-stamp,..)
- Abstract profiles
  - Can be used as building bock for concrete profile
  - Can be used in conjunction with concrete profiles to modify operation
    - E.g. entity seal working with the code-signing profile to allow deferred response.
  - Profiles work jointly for satisfying specific requirements in the given scenarios.

Present Status

- Fully ratified as OASIS standard.
- A number of interoperability tests carried out within the DSS TC
- Several implementations

Example Implementations

- CATCERT implementation for public agencies in Catalonya, Spain
- ARX CoSign - digital signature appliance
- Thales SafeSign appliance
  (Full DSS support prospective)
- UPC
- Netherlands government PDF document signing proof of concept
- Open Source version
  http://sirius-sign.sourceforge.net/

DSS Future

- New DSS-X TC “Digital Signature Services eXtended” opening in 23rd July.
- DSS-X TC will join OASIS IDTrust member section.
- Charter at:

  http://www.oasis-open.org/committees/dss-x/charter.php
- Envisaged work:
  - Development of new profiles.
  - More interoperability testing
  - Production of educational material
  - Maintenance of the core

DSS Future

Prospective profiles identified so far:

- Visible signatures
- PDF Signatures
- Profile for ebXML
- Profile for individual reports on every signature verified in multi-signature documents
- Profile for requesting signed verification responses
- "baseline" profiles. Profiles for basic functions in support of generation and verification of XML signatures, CMS signatures, XML time-stamps and RFC 3161 time-stamps.
- Handling of signature & service policy
- Profile for supporting centralized encryption and decryption services

Thank you

Questions ?

Further information:

DSS – published specifications

http://www.oasis-open.org/committees/dss

DSS-X – Future activities

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