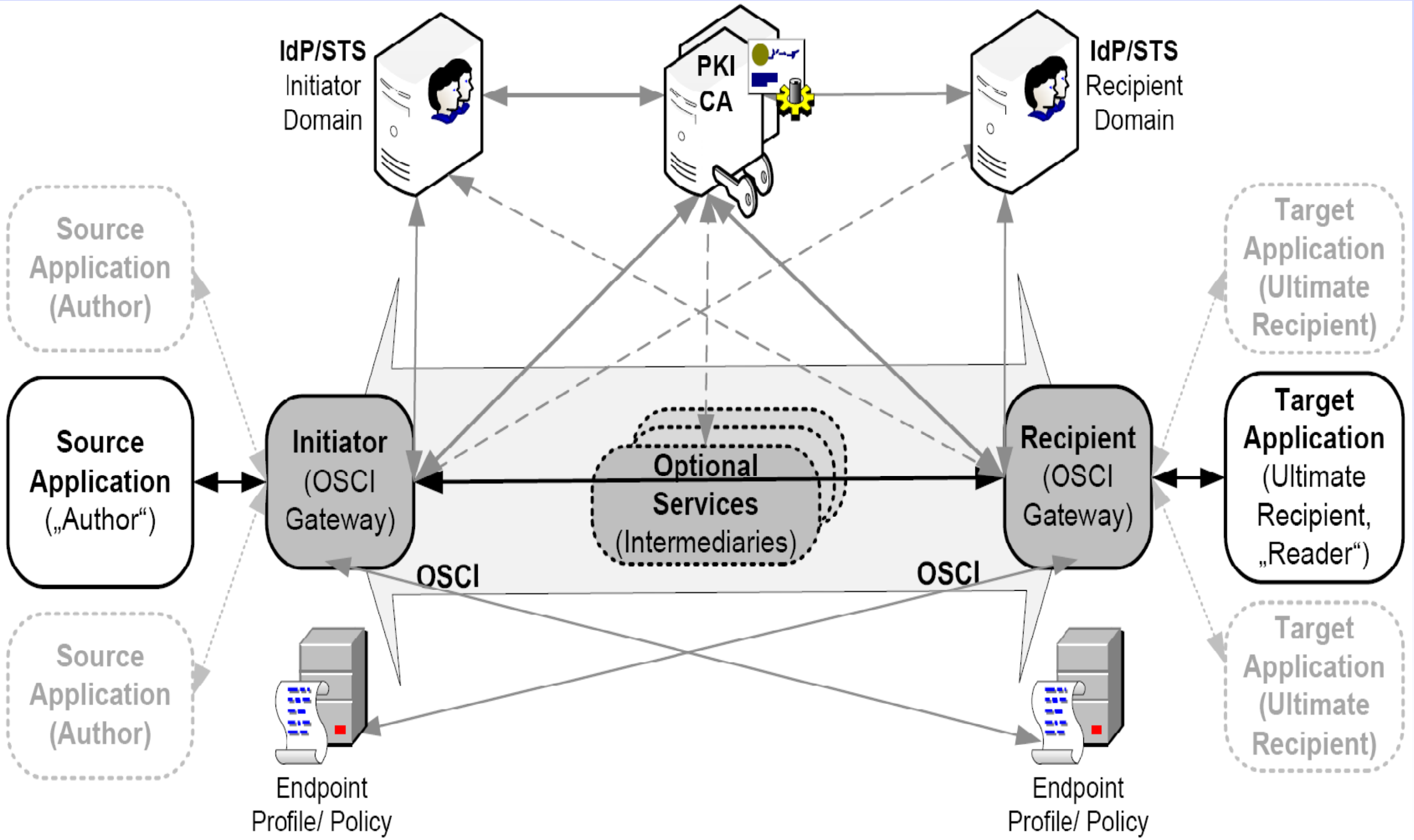
IDABC Middleware Expert Meeting
Brussels, October 9th 2008

OSCI Transport 2.0

- Design Details –

Jörg Apitzsch
CTO at bos GmbH & Co. KG, Bremen
Editor of the OSCI 2.0 Specification

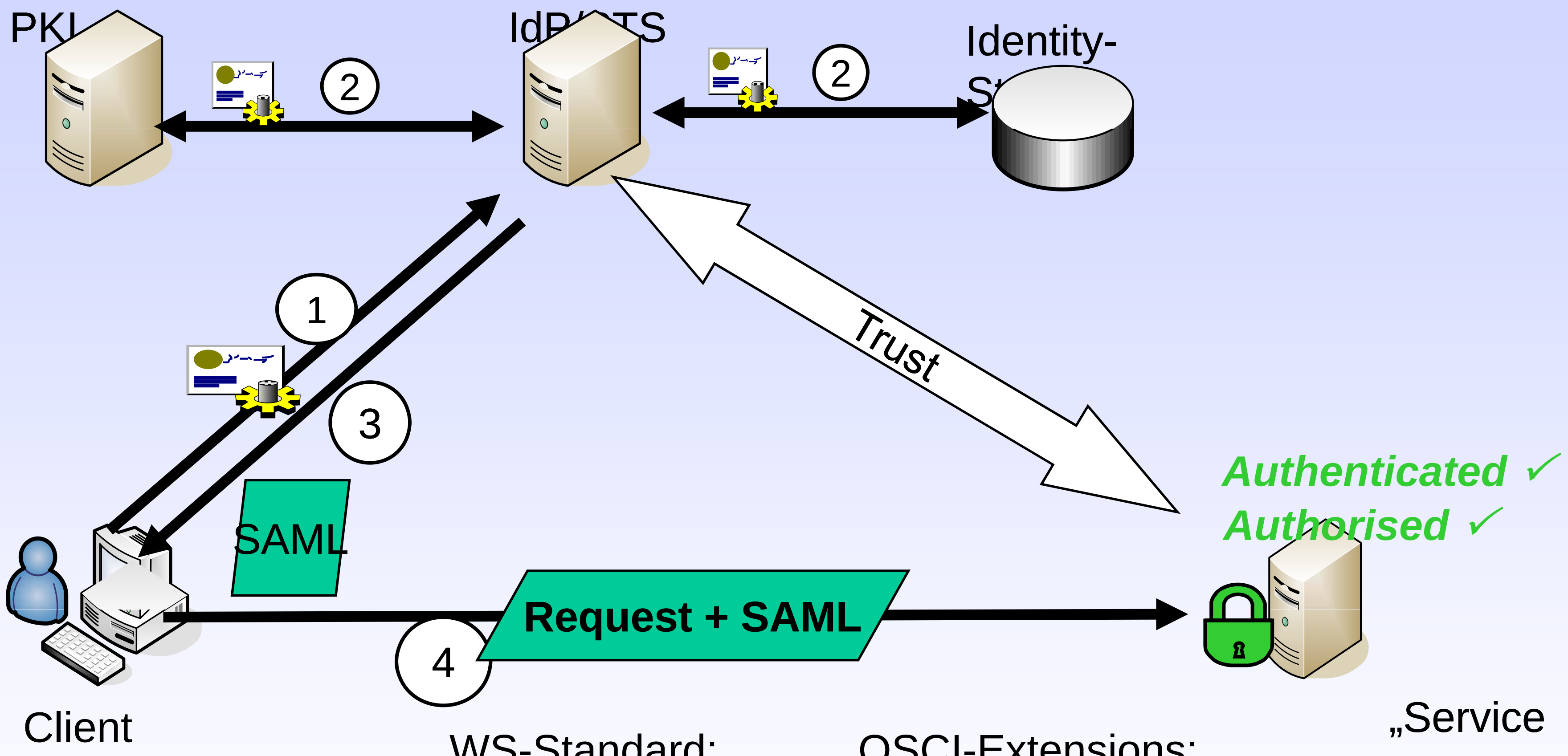
OSCI 2.0 role and communication model



Version 2.0 – Using/Profilng WS-Stack

- Referencing and profiling the major - meanwhile stable - intl. standards (selection):
  - General message structure: SOAP 1.2, MTOM and XOP
  - WS Security (including xdsig/xenc)
  - WS Reliable Messaging, WS Secure Conversation
  - WS Addressing, WS Make Connection
  - WS Trust, WS Federation
    - »Profiling relies on works of WS▸I WEB SERVICES INTEROPERABILITY ORGANIZATION

Services based on WS-Stack



WS-Standard:

- *Addressing*
- *Confidentiality*
- *Integrity*
- *Reliability*

OSCI-Extensions:

- *Proofability*
- *Non repudiation*
- *Legally binding*
- *Asynchronity via Msg-Relay*

Some „Specials“

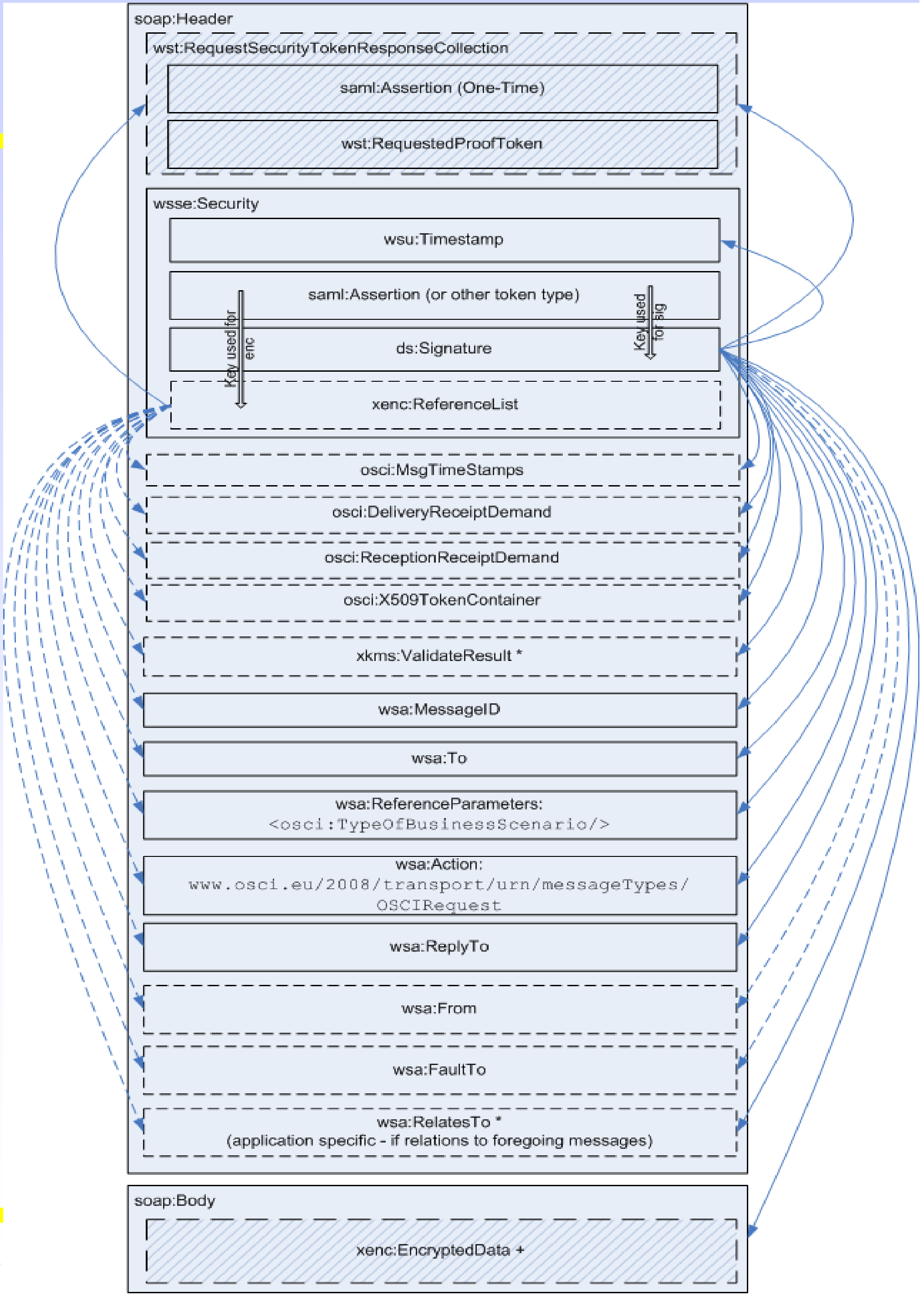
- WS-Trust / WS-Federation:
  - Proof of identity: validation of credentials (i.e. X509-Certificates, SAML-Token)
  - Authorization: validation of claims (i.e. claimed roles) by a standard interface to Attribute Services
- XKMS:
  - To reduce repeated validation requests on each node, it must be possible to include validation request results into the message
- XDISG/#PKCS7, OASIS DDS/eCardAPI:
  - Service for source- / target applications: applying / validating (qualified) digital signatures (PKCS#7 and xdsig)
    - Interface defined as subset of “eCard-API” specification
    - The latter is proposed for the EU eSignature-Framework

OSCI specific requirements

- Message Relay (MsgBox service):
  - customers of administration are supposed to drive their electronic communication in a mostly sporadic way. This leads to the requirement of msg-box services for fully asynchronous message exchange
  - OSCI defines a common interface (SOAP custom header, detailed by selection criteria carried in body) for retrieving and accessing messages in a MsgBox service instance
- Traceability of Communication:
  - DeliveryReceipt – cryptographically secured receipt - what has been delivered when (this can be a receipt from a MsgBox service, "what" is an information about encrypted data)
  - ReceptionReceipt - cryptographically secured receipt, what has been received when; can only be delivered from the recipient of a message
  - FetchedNotification – initiator is informed, when a recipient pulls the message out of his MsgBox service

Transport Security

- WS-Trust
  - Signed/Encrypted Parts
  - Sig/Enc with sym. Key from SAML-Token
- Msg-Box Access
  - using WS Secure Conversation, derived Keys
- Defined in Security Policy (Specific for Classes of Scenarios)



soap:Header

wst:RequestSecurityTokenResponseCollection

saml:Assertion (One-Time)

wst:RequestedProofToken

wsse:Security

wsu:Timestamp

saml:Assertion (or other token type)

ds:Signature

xenc:ReferenceList

osci:MsgTimeStamps

osci:DeliveryReceiptDemand

osci:ReceptionReceiptDemand

osci:X509TokenContainer

xkms:ValidateResult *

wsa:MessageID

wsa:To

wsa:ReferenceParameters:
`<osci:TypeOfBusinessScenario/>`

wsa:Action:
`www.osci.eu/2008/transport/urn/messageTypes/OSCIRequest`

wsa:ReplyTo

wsa:From

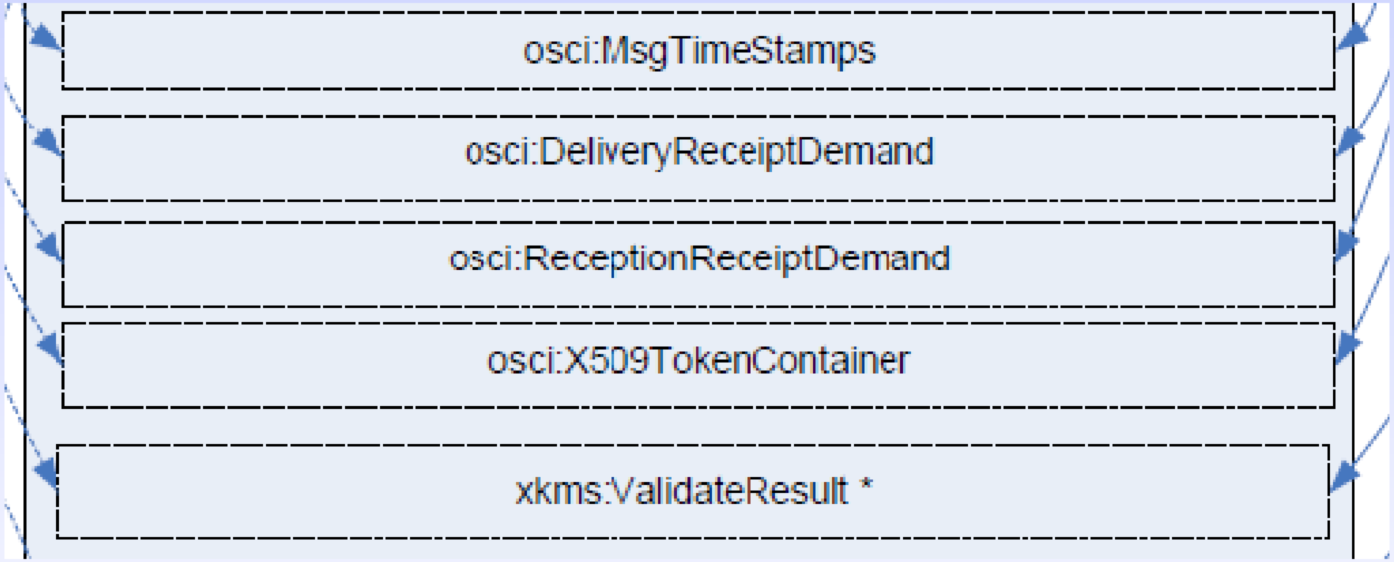
wsa:FaultTo

wsa:RelatesTo *
(application specific - if relations to foregoing messages)

soap:Body

xenc:EncryptedData +

OSCI Header (Request)



osci:MsgTimeStamps

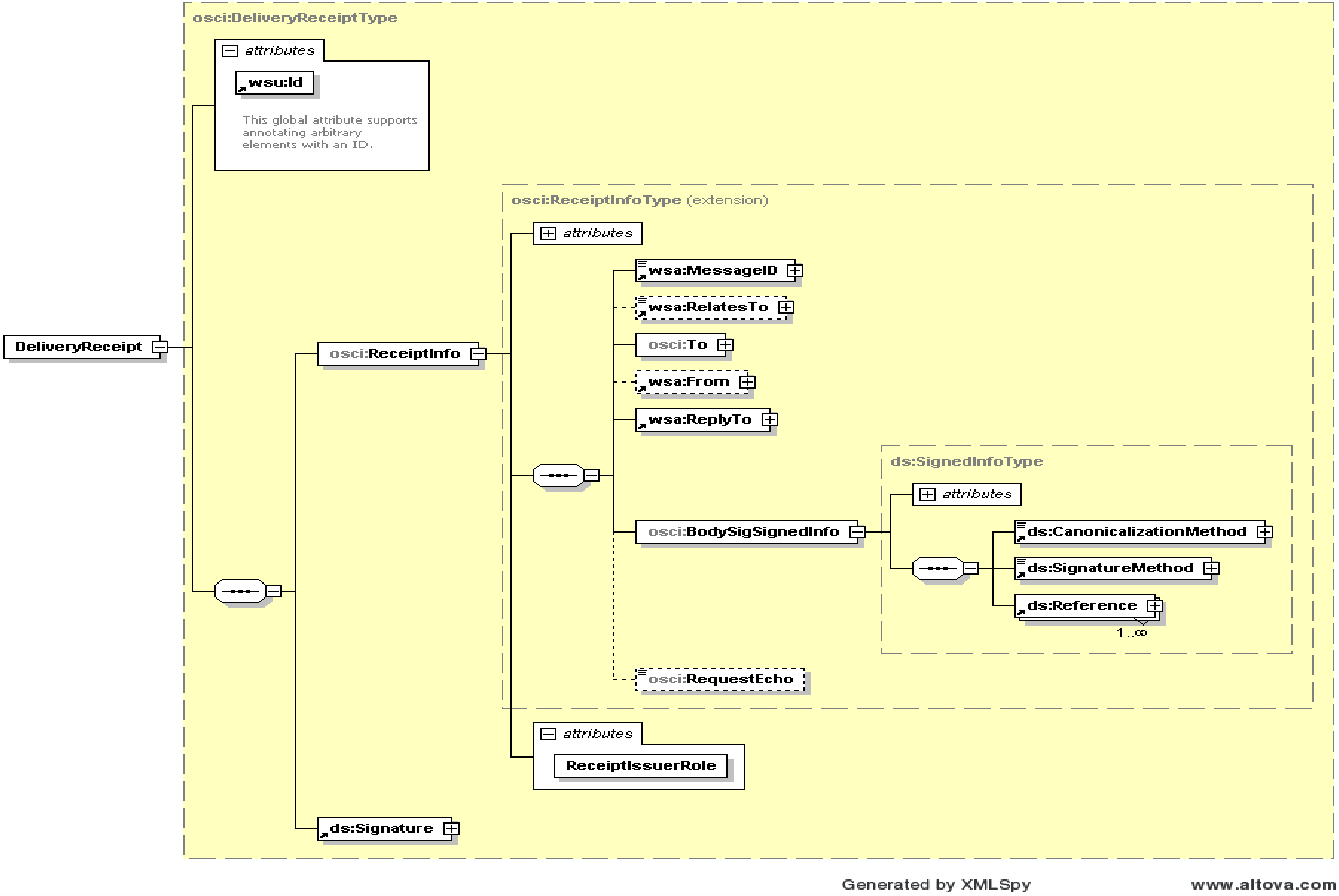
osci:DeliveryReceiptDemand

osci:ReceptionReceiptDemand

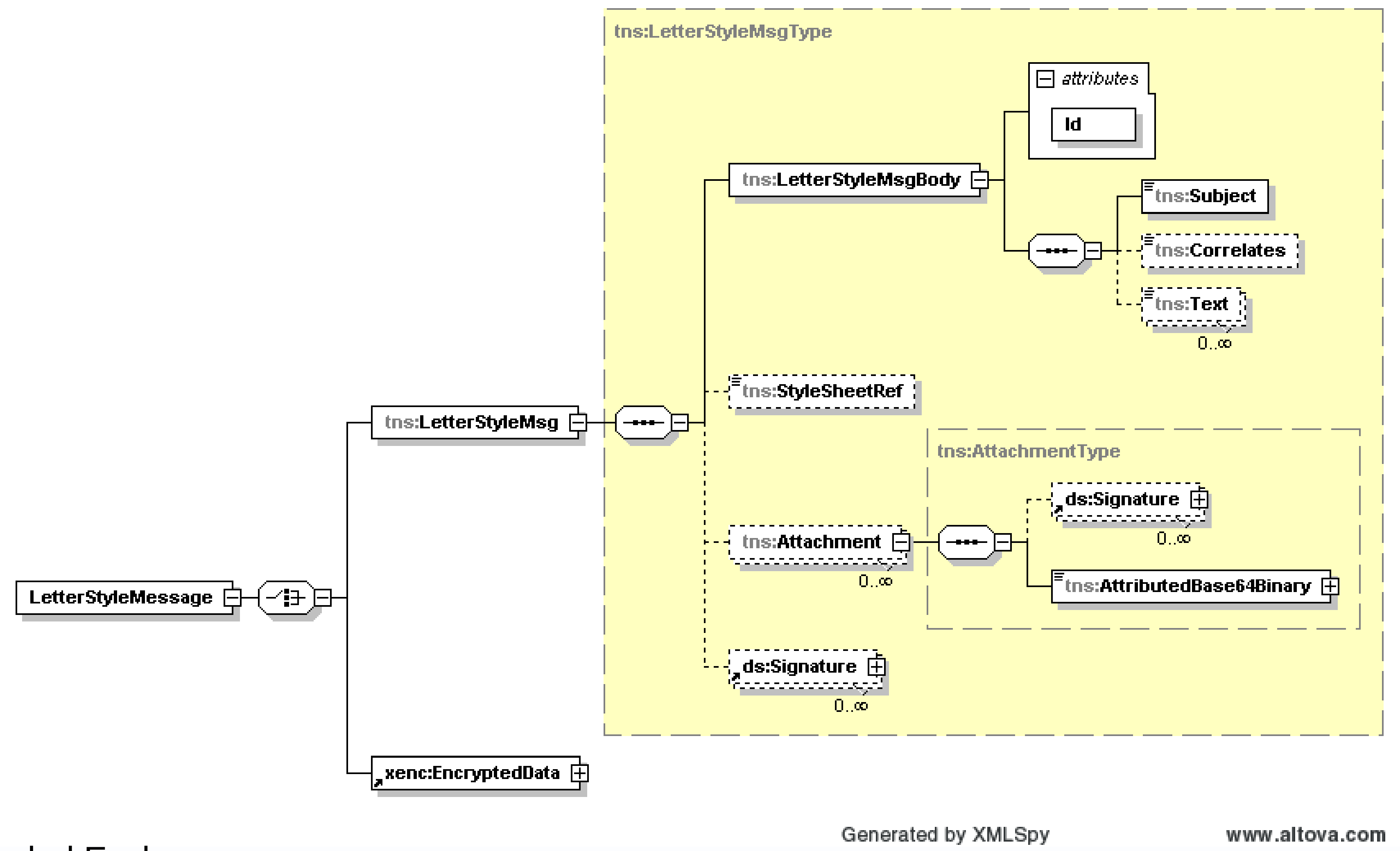
osci:X509TokenContainer

xkms:ValidateResult *

Example: DeliveryReceipt



Body for unbounded Msg Exchange



Bounded Exchange:
„XÖV“ standarsizes XML-Schemas for different public business affair classes

eIDM Link – Project SAFE

Safe WS-* based communication needs authentication and authorization of each message – cross reference to:

- Deutschland-Online project

  Secure **A**cces to **F**ederated **e**-Justice / e-Government

- Goal:
  - **Uniform communication infrastructure for the electronic justice**
- Objectives:
  - **advancement of electronic communication in justice**
  - **secure web-service based end-to-end communication via OSCI**
  - **redesign of an existing registration and authentication procedure**

Revised actual schedule

- Final acknowledgement of specification December 2008
  - Including final versions of all related documents
  - English translation of architecture document to follow afterwards
- PoC Implementation based on Sun Metro framework will be ready end of January, 2008
- SAFE planned to be available mid 2009
- Goal for bos: Realized and integrated in Governikus until end of 2009

Steps to be done

(1) Exchanging Specifications for detailed Comparison

(2) Exchange of Comments hereon

(3) Selection of represantative Business Scenarios

- i.e. from EU e-Procurement Project PEPPOL
- i.e. from EU Service Directive, Project SPOCS)
    - SPOCS WP 3: „Interoperable delivery, eSafe, secure and interoperable exchanges and acknowledgement of receipt"

(4) Modelling and Exchanging WSDL's / Policies, first Tests in own Environment

(5) Bilateral alignment