

How to reconcile citizen eID schemes and business identity needs ?

Olivier Delos, Sylvie Lacroix
Partners SEALED

Current situation and issue

- Electronic Identity Cards are currently rolled-out or in preparation all over Europe (and beyond)
- On board PKI facilities enable citizens to benefit from:
 - Strong Authentication
 - (Qualified) Electronic Signatures
 - [Encryption facilities]
- Business use of such schemes ? ... Free highly secure PKI token
- But eID scheme is based on minimal set of information to uniquely identify a person, ... what about association of:
 - Business characteristics
 - Delegation of powers
 - Mandates
 - Roles
 - Profiles, ...

Current situation and issue

- Focusing on the Electronic Signature schemes ...
- How to use an eID card to electronically sign ?
 - As a Lawyer
 - As a nurse
 - As a doctor working in the context of an hospital
 - As an accountant being mandated by a company
 - As a consulting company partner
 - As a company legal representative
 - ...
- How to securely associate such « characteristics » to an eID scheme ?

Current situation and issue

- Specific Use cases
 - Doctor working in an hospital and has to sign medical reports
Not keen to use his personal identity only reflecting his citizen info since he is actually working as a doctor on behalf of the hospital and is covered by the hospital insurance in that context
 - Partner in a Big (4) consulting company
Every official document getting out the company must be signed by a Partner ... How to associate this « partner characteristic » to the eID
 - Company VAT declaration in Belgium
Accountants mandated by a company to deposit company VAT declarations have to use another « professional certificate » based credential to sign such declarations
- How to use eID cards/schemes and securely associate such « characteristics » to an eID based electronic signature ?

Possible solutions

Possible solutions to the problem of using eID schemes (cards) in a business context are using:

- Context based
- Claimed role (in a specific context or not)
- Certified role – Attribute Certificate
- Additional credentials / cards
- Additional roles in eID certificates
- **New type of Trusted Third Party
(ROLE Stamping Authorities)**



Possible solutions – Context based

- The context of usage is determining the context in which the electronic signature has to be validated and taken into account
- Context can be explicit or implicit, supported by a policy or not
- Advantage:
 - Easy to implement at signer's side
- Disadvantages:
 - May be difficult to prove (Decentralised validation schemes may help)
 - no formal guarantee
 - Short term only
 - May be difficult to determine context
 - when several possible
 - At a later stage

Possible solutions – Claimed Role

- Same as previous but signer indicates (signs) a claimed role in the signed data
- Advantages:
 - Easy to implement at signer's side
 - Context better determined
- Disadvantages:
 - May be difficult to prove (decentralised validation schemes may help), especially at a later stage
 - no formal guarantee
 - Short term only

Possible solutions – Certified role (Attribute Certificate)

- The electronic signature contains a « certified role » indication and is signed by the signer
- « Certified role » can be explicit or implicit, and is usually based on Attribute Certificate issued by an Attribute Authority
- Attribute certificate can also be used as « signing certificate »
- Advantage:
 - Formal guarantee
- Disadvantages:
 - Relatively heavy investment at Attribute Authority side
 - Costly infrastructure
 - Lifecycle Management (issuing, publication, revocation/suspension)
 - Attribute certificates have a validity period (start/end) and should be validated against revocation

Possible solutions – Additional credentials (cards)

- Signer is issued an additional credential (card) reflecting a specific role (characteristic, attribute, mandate, delegation of power, role, etc.)
- Advantage:
 - Formal guarantee
- Disadvantages:
 - Costly !!
 - Infrastructure and lifecycle management
 - Additional token (card, USB token, etc.)
 - Several may be needed when several characteristics

Possible solutions – Additional characteristics in eID

- eID certificates are issued with additional characteristics completing the « basic » identity (e.g., attribute, mandate, delegation of power, role, etc.)
- Advantage:
 - Can help to solve the problem in the limited context of the additional characteristic
- Disadvantages:
 - Which characteristic rather than another
 - Costly !!
 - Infrastructure and lifecycle management
 - Lifecycle is likely to be shorter than for « basic identity » schemes



New scheme – New kind of TTP

- New kind of TTP (Role Authority) is requested and trusted to confirm a claimed signer role according to a validation context:
 - Either based on an extended Time Stamping Authority (ROSA)
 - Or based on an extended OCSP Responder (AUROR)
- Advantages:
 - Fully solves the problem
 - Fully standard as based on extension of existing standards and authorities
 - Provide formal guarantee on claimed role
 - Timely related (guarantee at a precise trusted time)
 - Low cost infrastructure compared to Attribute Certificates
 - Relying on Authentic Validation Sources (keeping control on authentic information)
 - Can complete eID schemes or any PKI based identity scheme
- Requisites:
 - OID/URI harmonisation to identify Roles and Roles Authorities

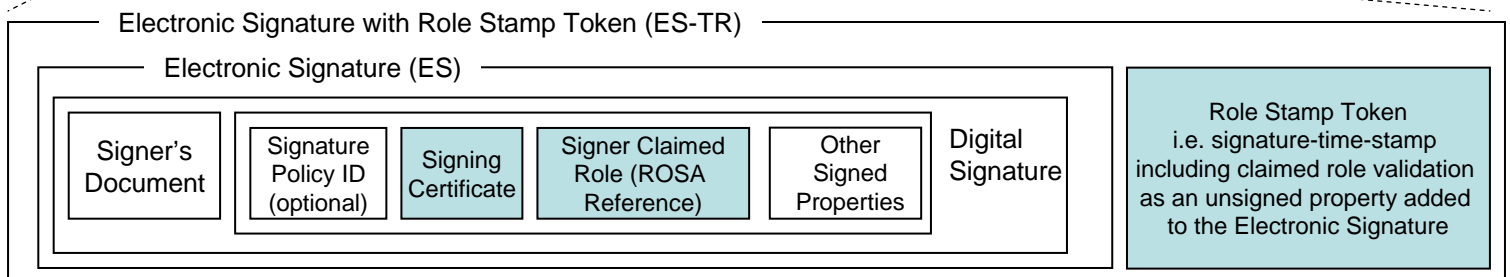
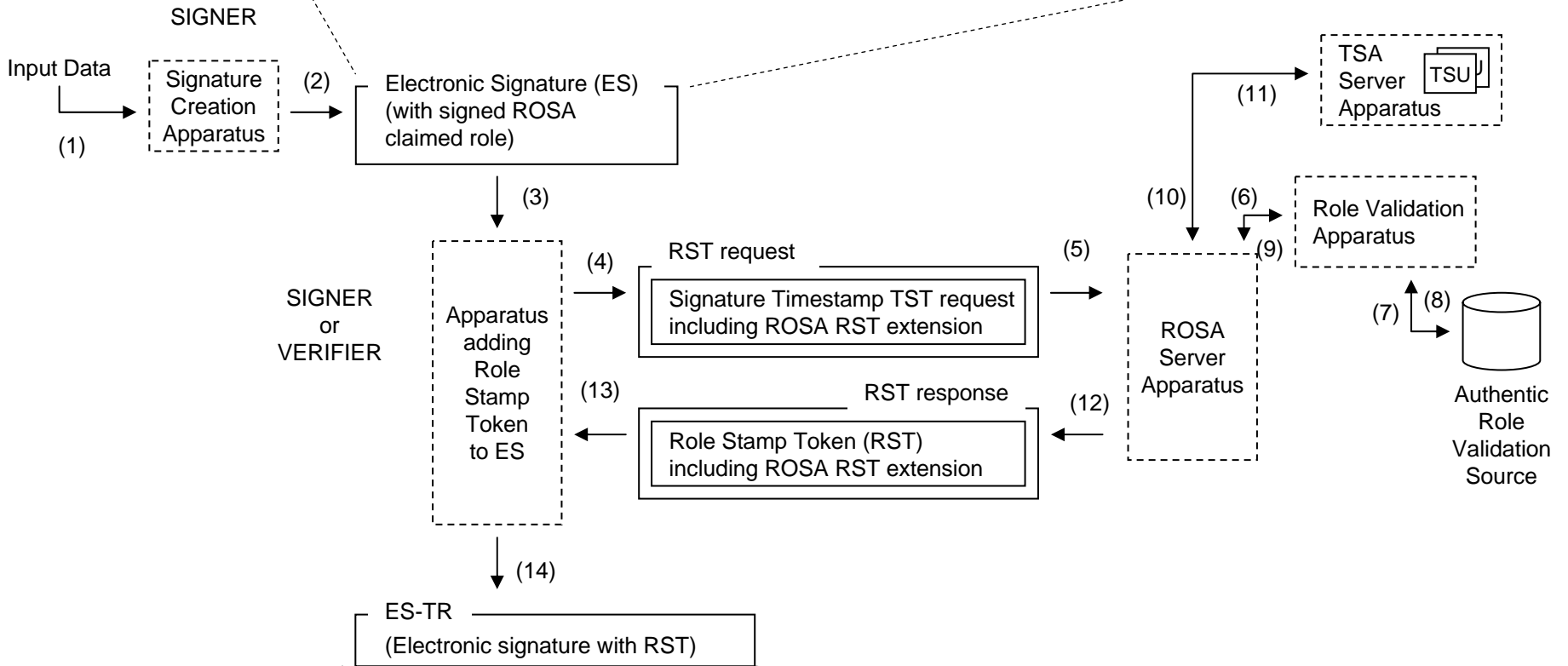
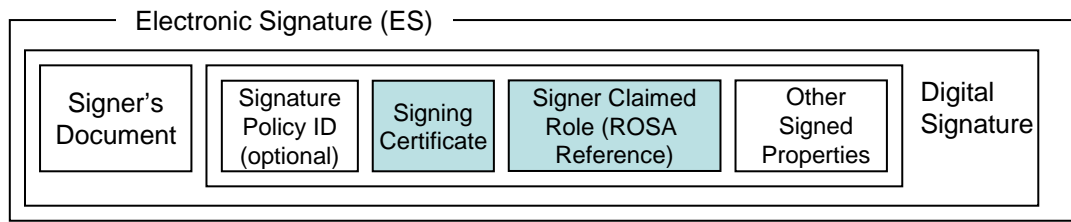
ROle Stamping Authority (ROSA) – How it works

- Signature step (Signer):
 - Signer completes the signature format (any) with specific signed attributes
 - Signer's identity information (may be the signing certificate)
 - Signer's claimed role and
 - Associated Role Stamping Authority (ROSA) Identifier
 - ROSA Policy identifier

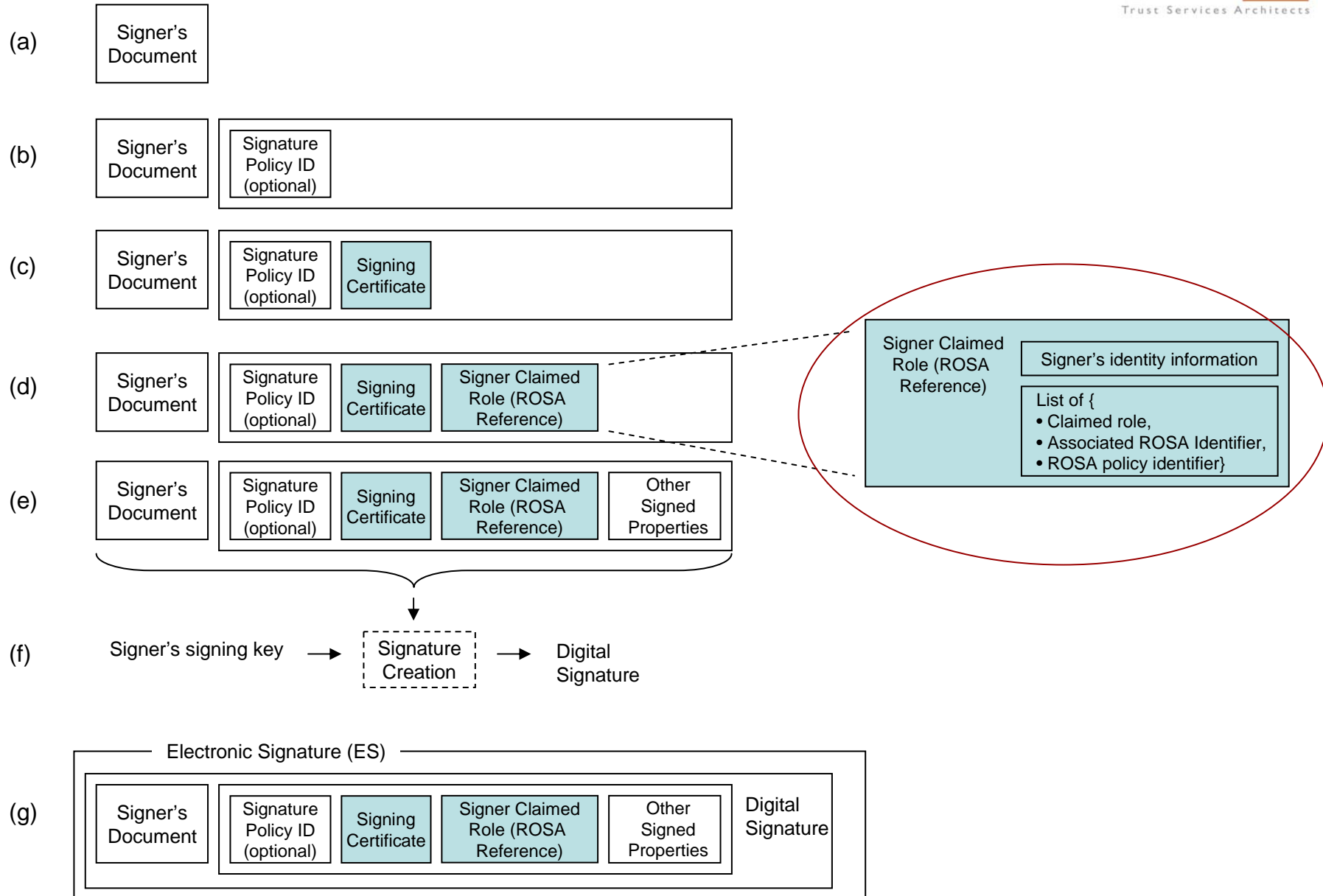
- Role Validation Request step (Signer / Verifier):
 - Signer / Verifier creates request towards ROSA from information included in the signature
 - Format of the request is an **extended Time-Stamping Request**

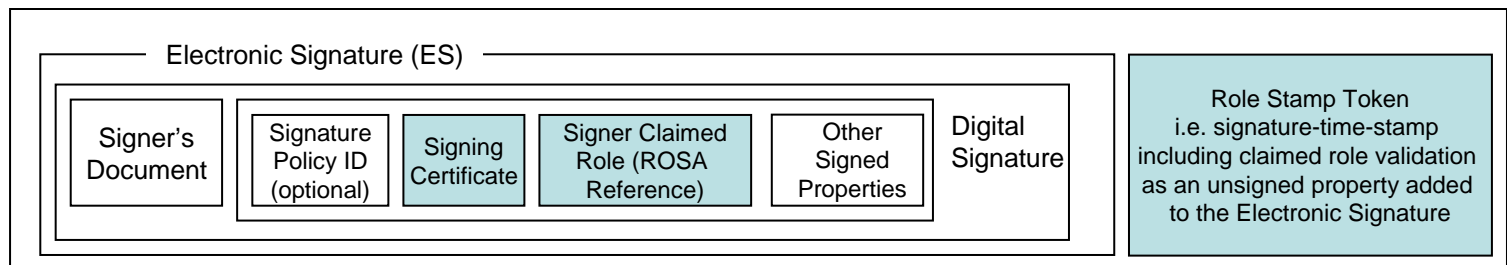
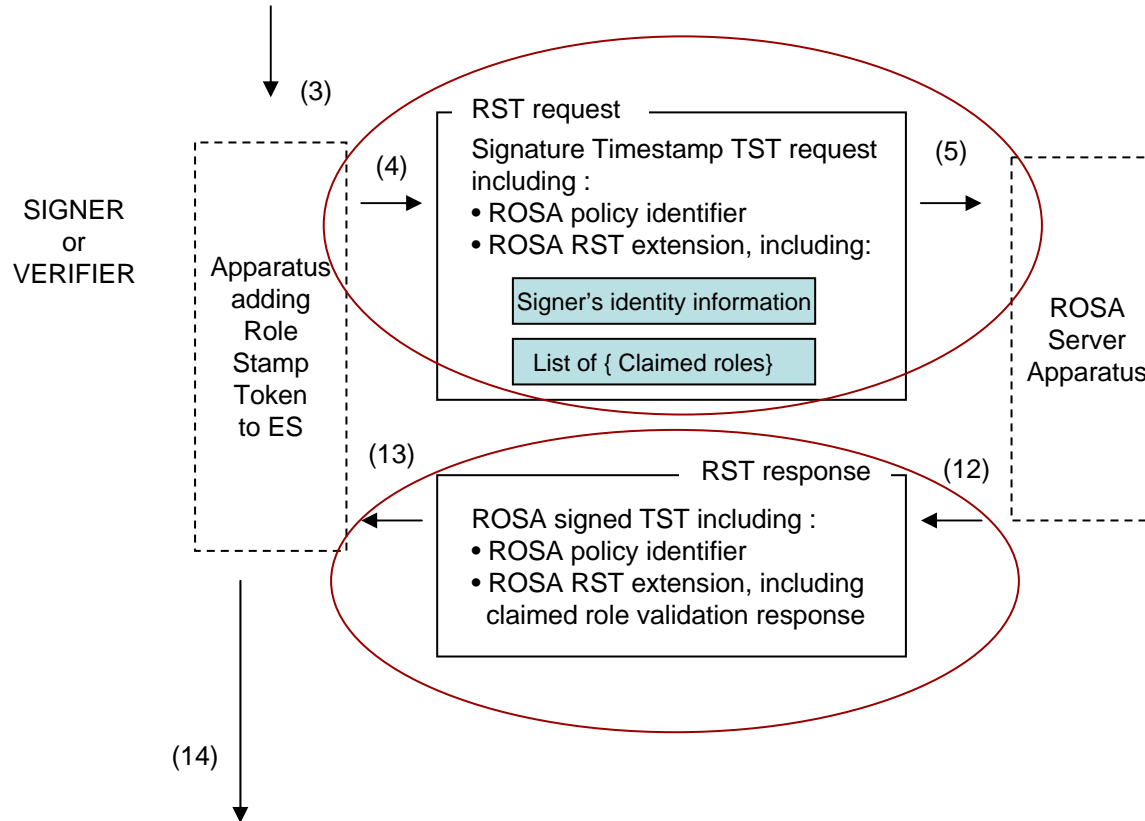
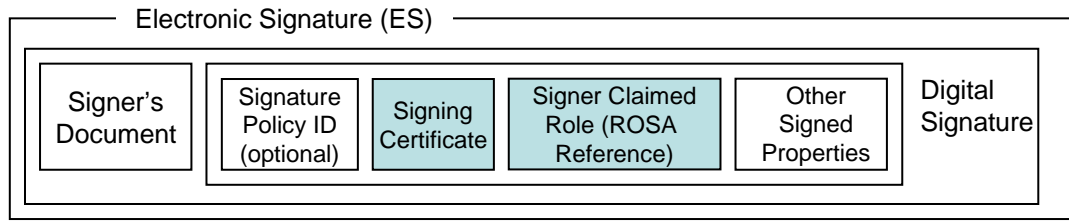
- Role Validation Answer step (ROSA):
 - Role Stamp Token** as an **extended Time Stamp Token** including confirmation of validated claimed role

- Integration in Signature Format (Signer / Verifier)



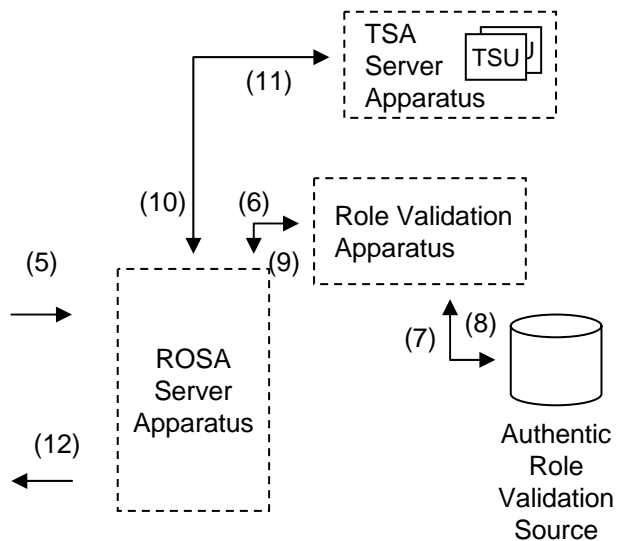
- (1) The Signer uses the following input data to be able to create an Electronic Signature with a signed claimed role to be validated by a ROSA: the Signer's document, several properties that shall be signed together with the Signer's document among which the optional signature policy identifier and associated commitment type, the signing certificate, the Claimed Role extension that contains the Signer's identity information (that must be consistent with the Signer's identity information that is certified in the signing certificate), and a list of claimed role, associated ROSA identifier, and ROSA policy identifier. Other properties to be signed can be added.
- (2) The Signer shall use its private signing key to create the Electronic Signature on the Signer's document and the signed properties. Additional unsigned properties can be added to the created Electronic Signature (ES). This ES can be of any form among which but not limited to S/MIME, PKCS#7, XMLDSIG, CMS, AESIG, CAdES, XAdES, etc.
- (3) The Signer can send the created ES to a Verifier that shall add the Role Stamp Token (RST) to the ES. The Signer can also be the one that shall add the RST to the ES.
- (4) The Signer/Verifier shall create the RST request from the information that it will collect from the ES, i.e., the Signer's identity information, the ROSA policy identifier, the ROSA identifier, and the list of claimed roles. The RST request is created from a Time-Stamp Request (e.g., as defined in RFC 3161) and include a specific extension related to the claimed role(s) to be validated by the ROSA. The Signer/Verifier should perform some checks on the information collected in the ES among which whether the Signer's identity information placed in the signed claimed role property, if present, is consistent with the Signer's identity information found in the signing certificate.
- (5) The request is sent by the Signer/Verifier to the identified ROSA.
- (6) The ROSA Server shall proceed to the request verification as done for a classic time-stamp request and shall perform an additional check against the role(s) that is(are) claimed to be associated to the Target Entity identity (Signer's identity information). The ROSA Server shall request confirmation to or use a Role Validation Apparatus (RVA).
- (7) This Role Validation Apparatus shall interrogate an Authentic Role Validation Source (ARSV) to obtain or not the validation of the association between the Target Entity Identity Information (Signer's Identity Information in this case) and the claimed associated role(s).
- (8) The Authentic Role Validation Source provide the response to the Role Validation Apparatus.
- (9) The Role Validation Apparatus provide the response to the ROSA server. Note that different configuration can be possible: the ROSA Server, the RVA, and the ARSV can be combined in one, two or three (or split into even more) entities, they can be located and operated by different entities, etc.
- (10) Once the ROSA Server receives confirmation on the claimed role(s), it can create the RST response and have it signed in a time-stamp. The response is requested for being timestamped by a Time Stamping Unit (TSU).
- (11) The TSU sends back the generated timestamp.
- (12) The ROSA Server then sends the RST response to the requestor.
- (13) The Signer/Verifier then verifies the RST response.
- (14) The Signer/Verifier then adds the RST to the ES to generate the ES-TR.



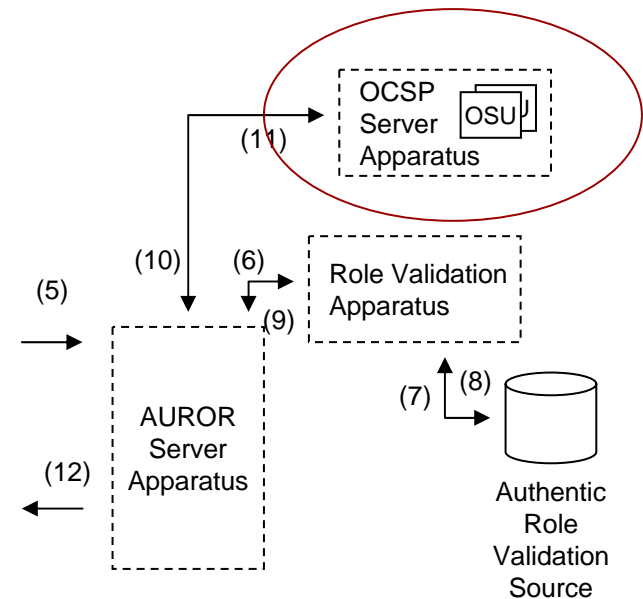


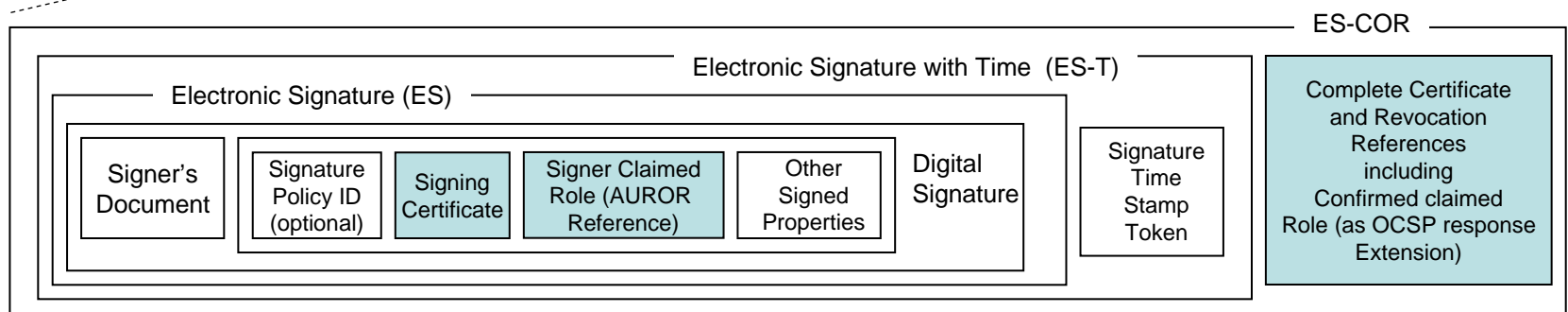
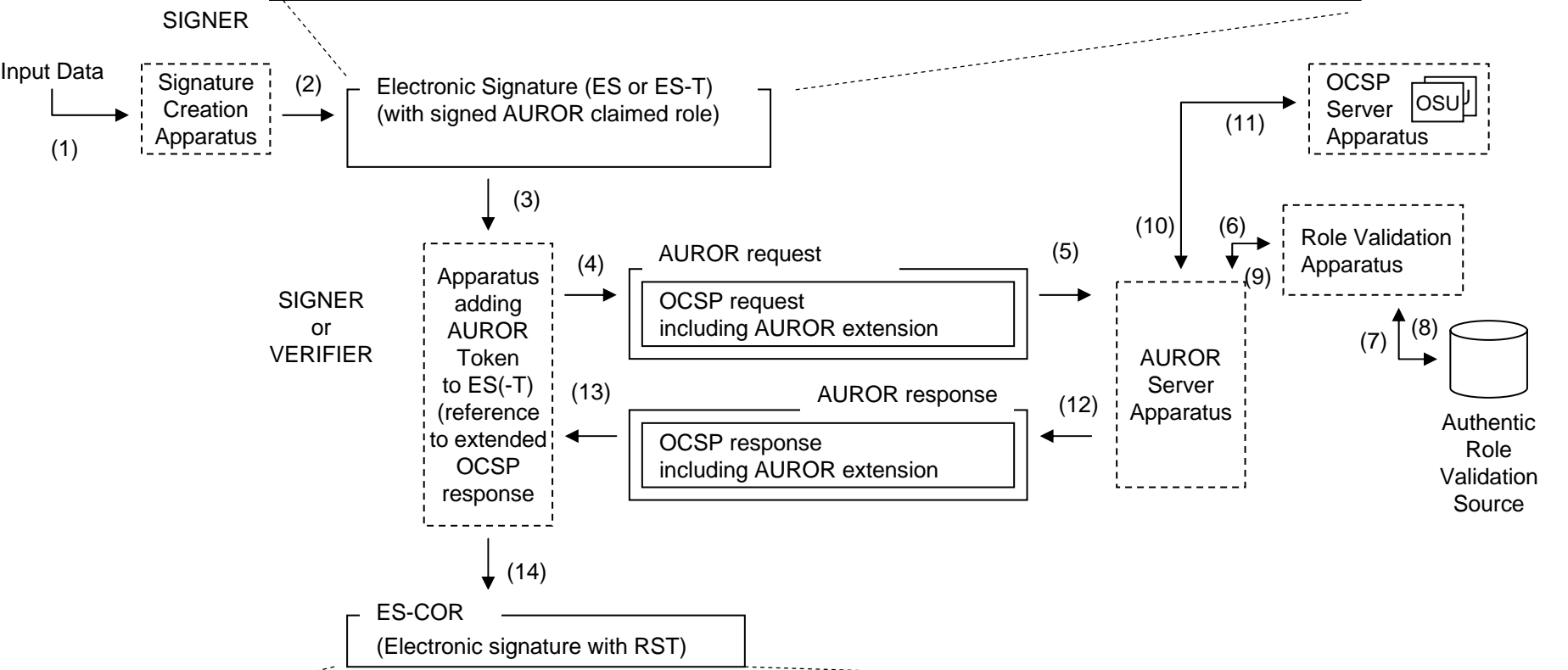
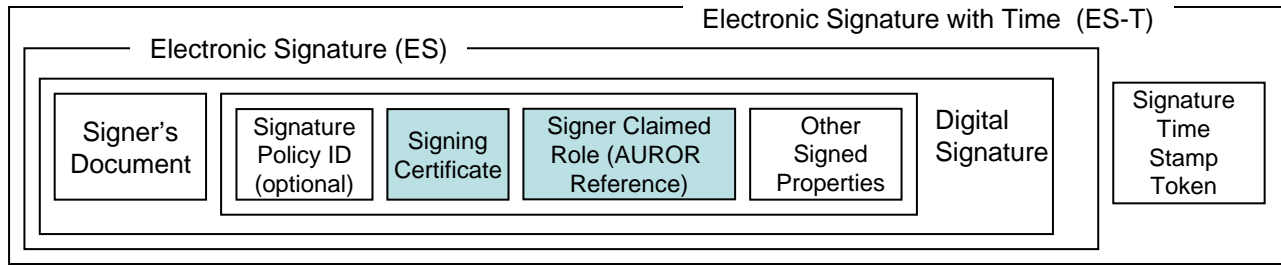
Authorised Role OCSP Responder (AUROR) – How it works

Extended Time-Stamping Authority Based Scheme



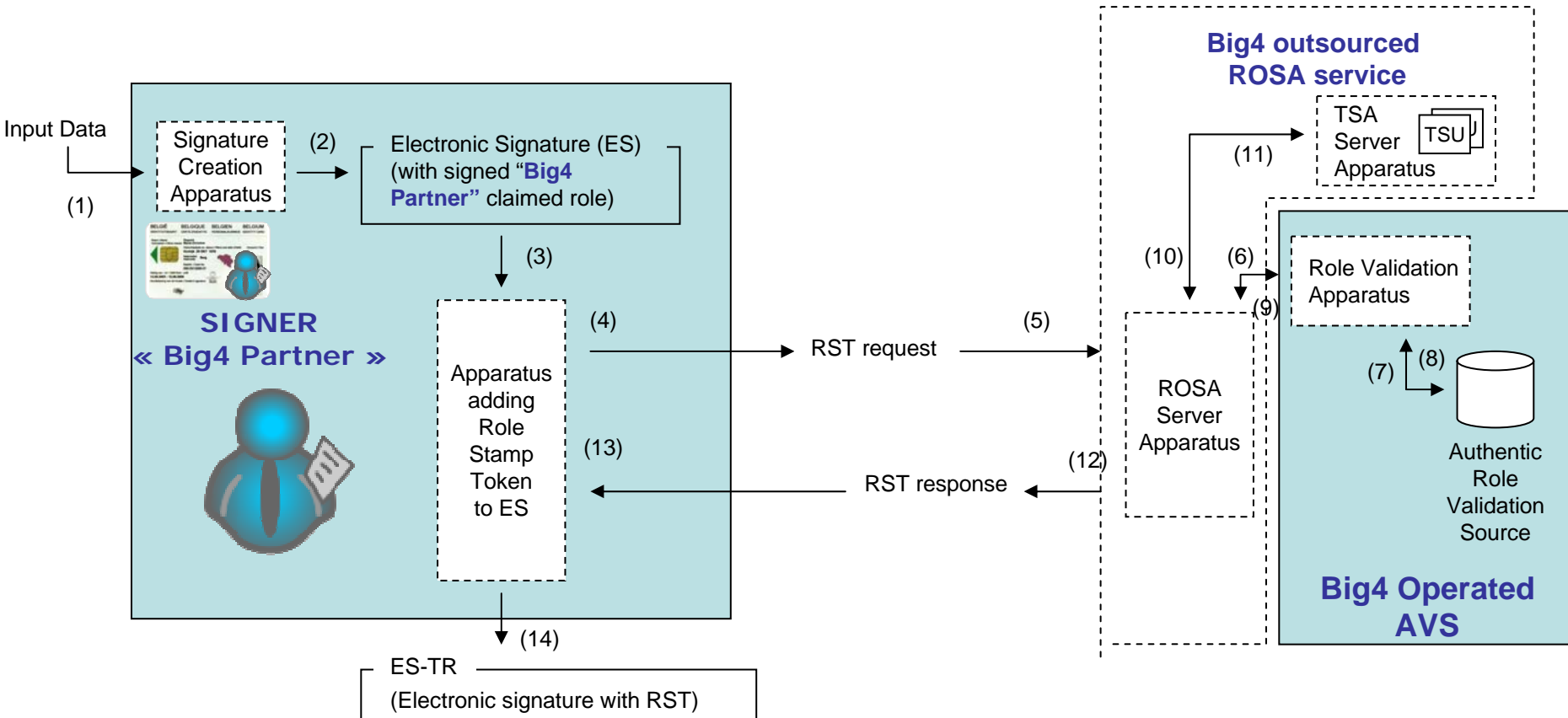
Extended OCSP Responder Based Scheme



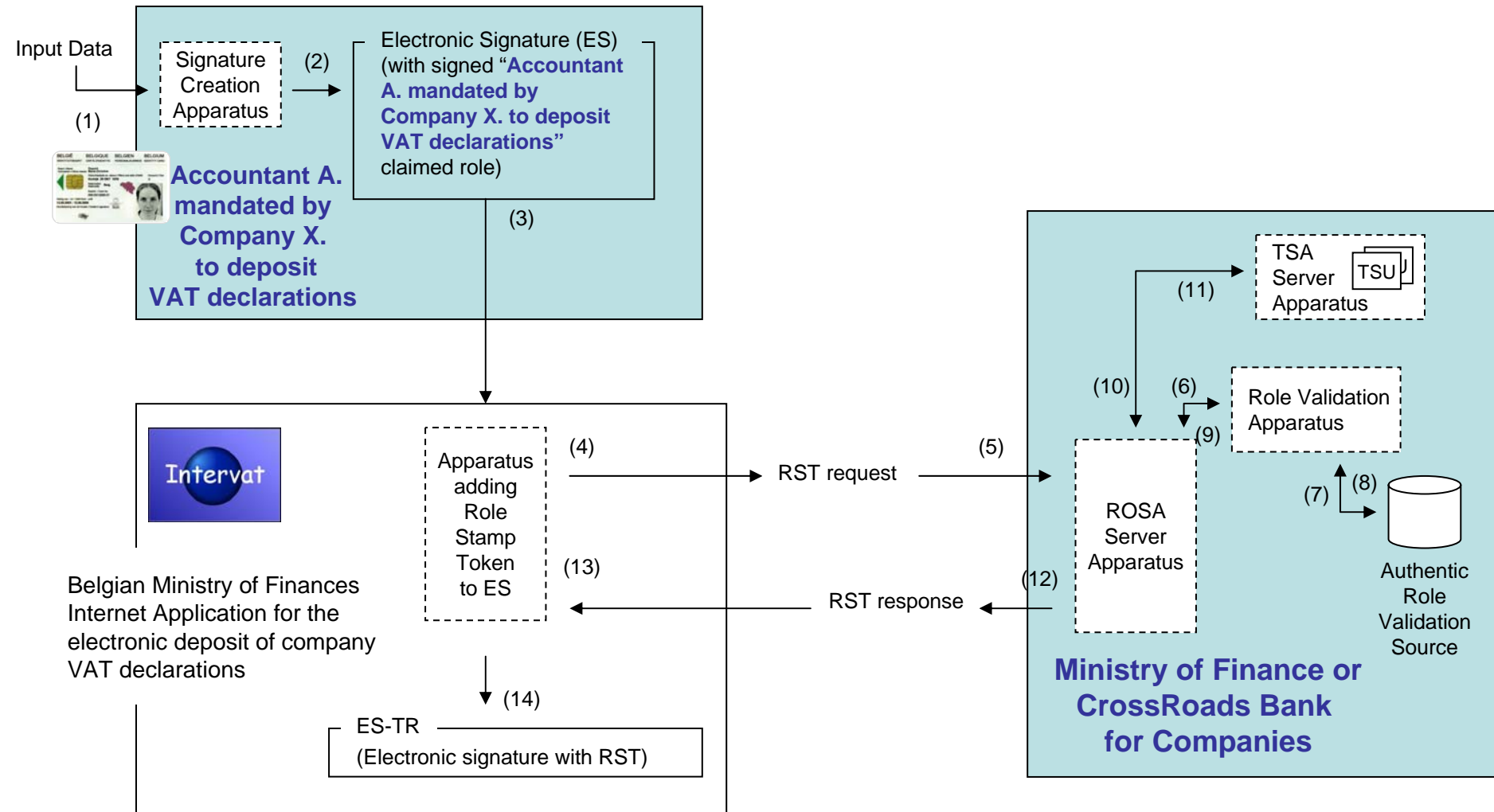


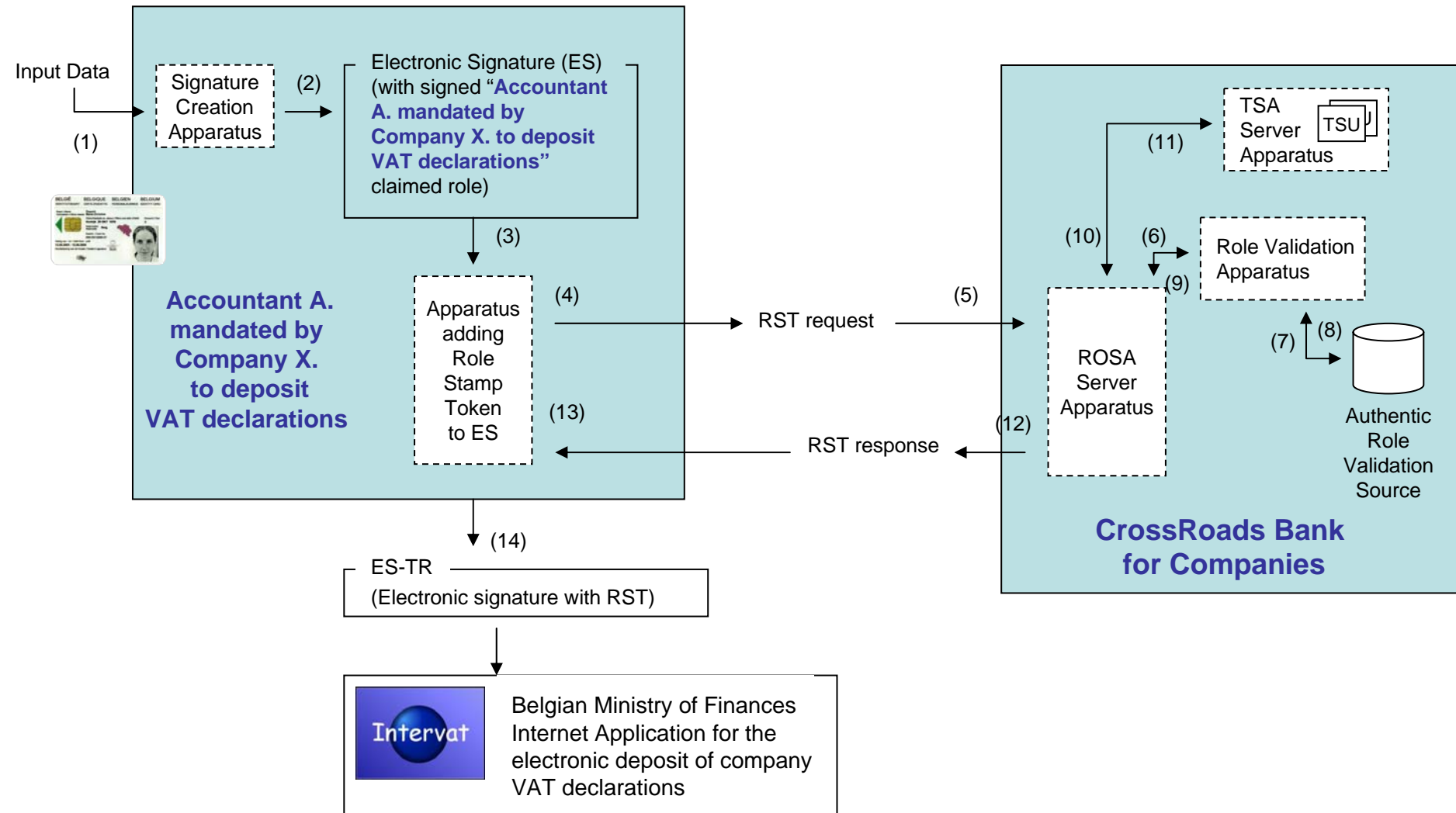
- (1) The Signer uses the following input data to be able to create an Electronic Signature with a signed claimed role to be validated by an AUROR: the Signer's document, several properties that shall be signed together with the Signer's document among which the optional signature policy identifier and associated commitment type, the signing certificate, the Claimed Role extension that contains the Signer's identity information (that must be consistent with the Signer's identity information that is certified in the signing certificate), and a list of claimed role, associated AUROR identifier, and AUROR validation policy identifier. Other properties to be signed can be added. In addition this ES scheme can be extended to a format for which there exists a trusted time associated to the signature (e.g., CAdES-T, or XAdES-T, or any ES format).
- (2) The Signer shall use its private signing key to create the Electronic Signature on the Signer's document and the signed properties. Additional unsigned properties can be added to the created Electronic Signature (ES). This ES can be of any form among which but not limited to S/MIME, PKCS#7, XMLDSIG, CMS, AESIG, CAdES, XAdES, etc. The ES can be optionally extended to a form including a signature trusted time-stamp.
- (3) The Signer can send the created ES(-T) to a Verifier that shall add the Complete Certificate and Revocation reference to the ES(-T). The Signer can also be the one that perform that action.
- (4) The Signer/Verifier shall create the "Role and OCSP" request from the information that it will collect from the ES, i.e., the Signer's identity information, the ROSA policy identifier, the ROSA identifier, and the list of claimed roles. The RST request is created from an OCSP Request (e.g., as defined in [RFC2560]) and include a specific extension related to the claimed role(s) to be validated by the AUROR. The Signer/Verifier should perform some checks on the information collected in the ES among which whether the Signer's identity information placed in the signed claimed role property, if present, is consistent with the Signer's identity information found in the signing certificate.
- (5) The request is sent by the Signer/Verifier to the identified AUROR.
- (6) The AUROR Server shall proceed to the request verification as done for a classic OCSP request and shall perform an additional check against the role(s) that is(are) claimed to be associated to the Target Entity identity (Signer's identity information). The AUROR Server shall request confirmation to or use a Role Validation Apparatus (RVA).
- (7) This Role Validation Apparatus shall interrogate an Authentic Role Validation Source (ARSV) to obtain or not the validation of the association between the Target Entity Identity Information (Signer's Identity Information in this case) and the claimed associated role(s).
- (8) The Authentic Role Validation Source provide the response to the Role Validation Apparatus.
- (9) The Role Validation Apparatus provide the response to the AUROR server. Note that different configuration can be possible: the AUROR Server, the RVA, and the ARSV can be combined in one, two or three (or split into even more) entities, they can be located and operated by different entities, etc.
- (10) Once the AUROR Server receives confirmation on the claimed role(s), it can create the Role & OCSP response (i.e., an OCSP response that include the Role extension) and have it signed the OCSP Signing Unit (OSU). The response is requested for being signed by OSU.
- (11) The OSU sends back the generated signature (signed extended OCSP).
- (12) The AUROR Server then sends the Role & OCSP response to the requestor.
- (13) The Signer/Verifier then verifies the Role & OCSP response.
- (14) The Signer/Verifier then adds the Role & OCSP to the ES(-T) to generate the ES-COR.

Case study – Signing as a Big 4 Partner



Case study – Mandated Accountant to deposit Company VAT declaration





Conclusions

- Reconciling eID schemes with business usage is possible through the new presented scheme (ROSA / AUROR) with the advantages
 - Fully standard as based on extension of existing standards and trusted authorities
 - Easy to implement
 - Provide formal guarantee on claimed role
 - Trusted Time related (guarantee at a precise trusted time)
 - Low cost infrastructure compared to Attribute Certificates and other sol^o
 - Relying on Authentic Validation Sources (that keep control on authentic information)
 - Can complete eID schemes or any PKI based identity scheme
 - Legal framework indirectly in place as based on European Directive 1999/93/EC but specific TTP legislation is preferably required (e.g., in preparation in Belgium, already in place in some Member States)
 - Can be extended to authentication scheme

Questions ?

Contact information:



www.sealed.be

- *Sylvie Lacroix*
sylvie.lacroix@sealed.be
- *Olivier Delos*
olivier.delos@sealed.be