The Standards People

Protocols for Remote Digital Signature Creation

Presented by: **Anders Tornqvist**

Francesco Barcellini

Luigi Rizzo

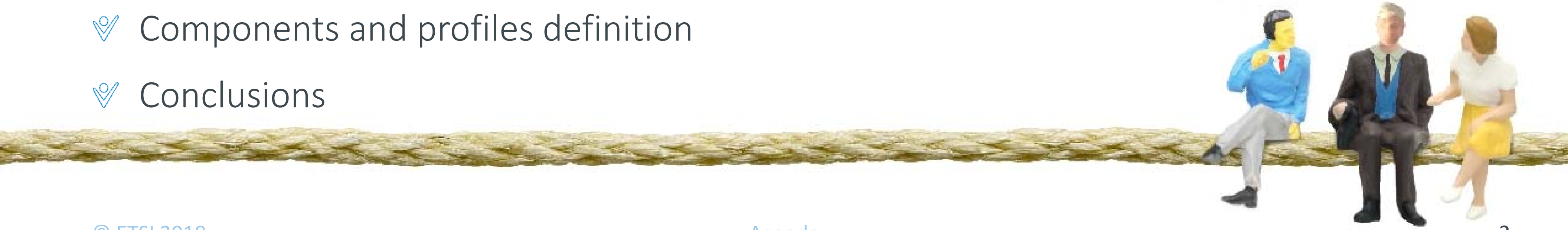
For: **ETSI Security Week:**

Remote Signature Creation Services

13.6.2018

Agenda

- Scope
- Signature creation process
  - Signature Creation Application
  - Server Signing Application
- Server signing architectures
  - SCAL1
  - SCAL2
- Technical approach of TS 119 432
- Components and profiles definition
- Conclusions



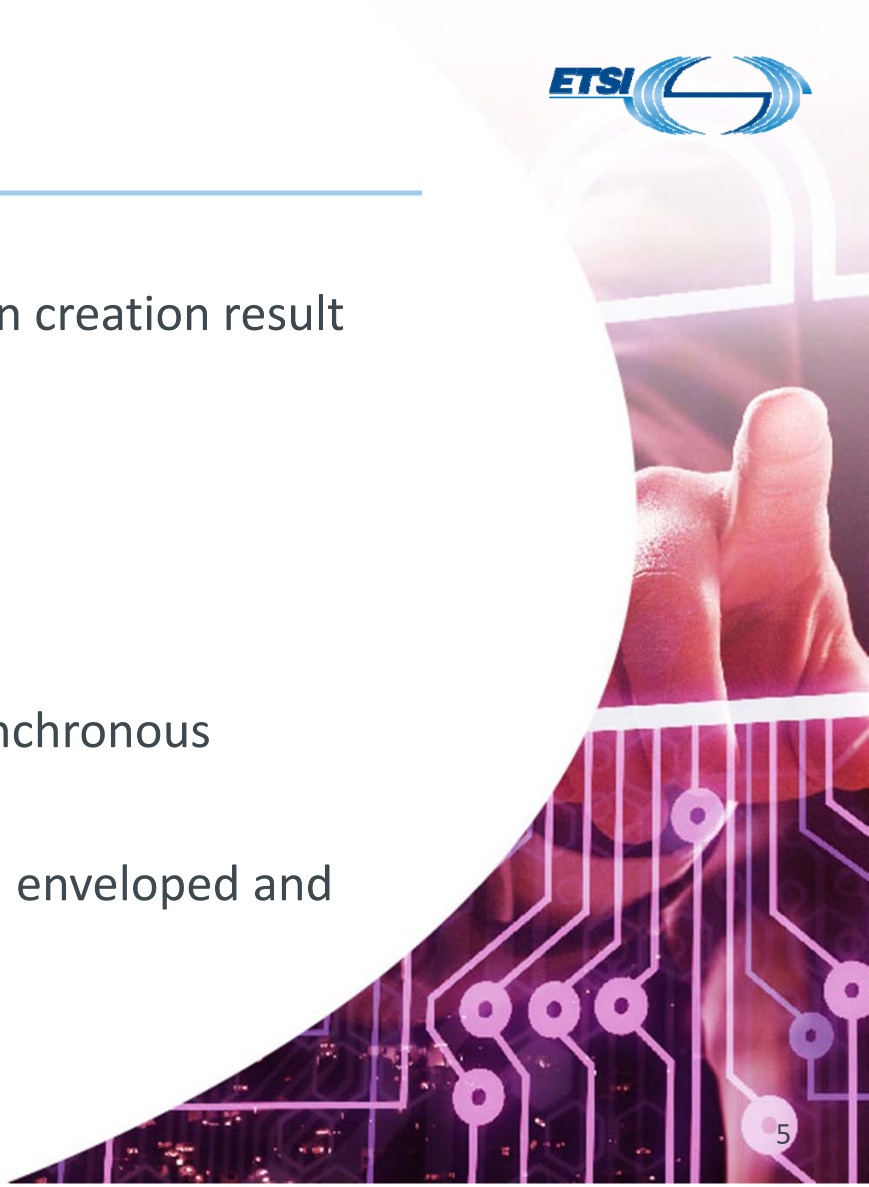
Scope

Scope

- ETSI TS 119 432 defines protocols and interfaces that allow a client to request the creation of AdES digital signatures as defined by ETSI EN 319 102-1 and/or a Digital Signature Values, as result of DTBSRs signature, to a remote signing server and allow the aforementioned server to return the signature creation results and, when possible, the AdES or DSV requested.
- ETSI TS 119 432 specification is limited to remote server signing, that is the context in which the signing key is held in a remote shared service.
- ETSI TS 119 432 defines two implementations of the aforementioned protocol, one in XML and one in JSON syntaxes.

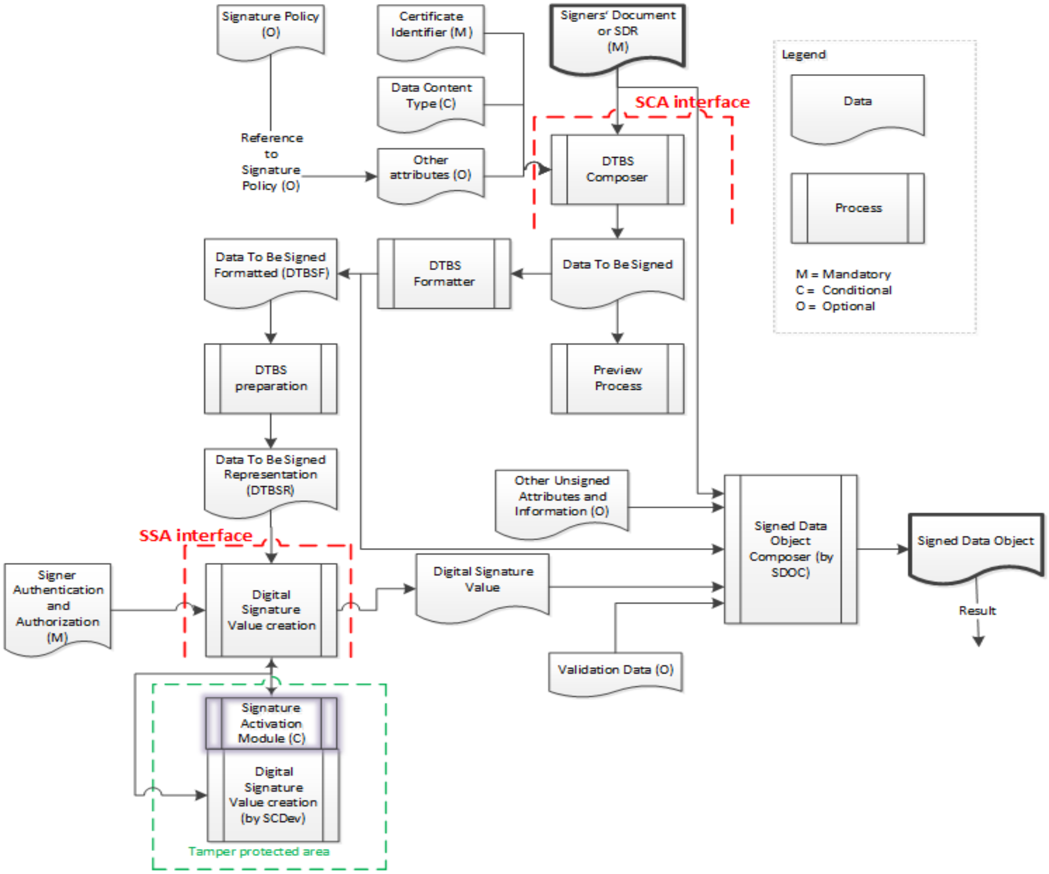
Scope

- The protocol allows to request creation and return creation result for the following types of digital signatures:
  - Digital Signature Values
  - CAdES signatures
  - PAdES signatures
  - XAdES signatures
- The protocol supports both synchronous and asynchronous management of requests and responses.
- The protocol supports the creation of enveloping, enveloped and detached signatures.



Signature creation process

Steps and data elements


Signature Policy (O)
Certificate Identifier (M)
Signers' Document or SDR (M)
Data Content Type (C)
Reference to Signature Policy (O)
Other attributes (O)
SCA interface
DTBS Composer
Legend
Data
Process
M = Mandatory
C = Conditional
O = Optional
Data To Be Signed Formatted (DTBSF)
DTBS Formatter
Data To Be Signed
DTBS preparation
Preview Process
Data To Be Signed Representation (DTBSR)
Other Unsigned Attributes and Information (O)
Signed Data Object Composer (by SDOC)
Signed Data Object
SSA interface
Signer Authentication and Authorization (M)
Digital Signature Value creation
Digital Signature Value
Result
Validation Data (O)
Signature Activation Module (C)
Digital Signature Value creation (by SCDev)
Tamper protected area

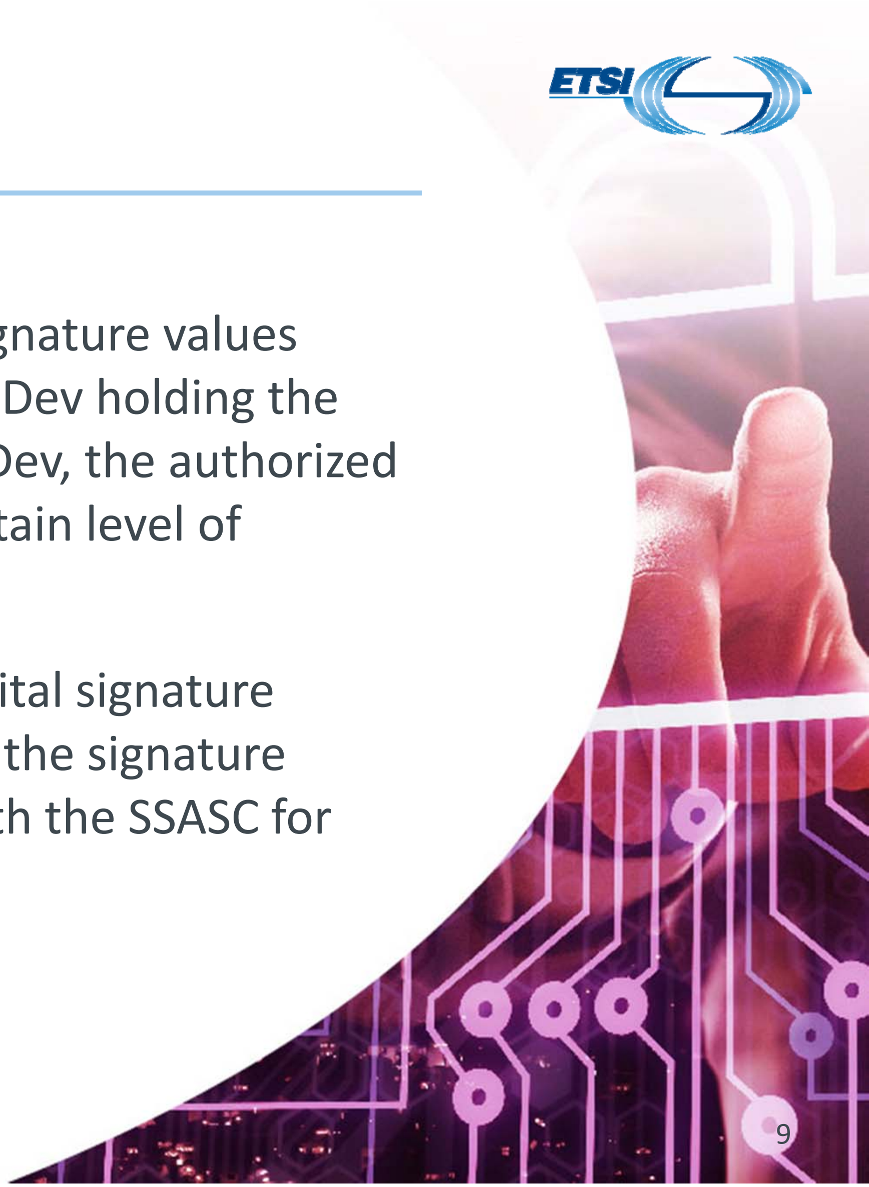
Signature creation process steps and related data elements taken from ETSI EN 319 102-1

SSASC and SCASC

- The above process points out a scenario where the AdES and/or Digital Signature Value (DSV) are created using a signing key held within a cryptographic security module, named Signature Creation Device (SCDev), operated by a Signature Creation Service Provider (SCSP).
- Based on the different types of data managed in requests and responses, two main components can be identified in the above process providing different interfaces for signing management.
  - The Server Signing Application Service Component (SSASC)
  - The Signature Creation Application Service Component (SCASC)

SSASC and SCASC

- The SSASC is the component supporting digital signature values creation. The SSASC is able to interact with the SCDev holding the signer’s private key. When the SSASC uses the SCDev, the authorized signer is able to control the signing key with a certain level of confidence.
- The SCASC is the component supporting AdES digital signature creation and carrying out several specific parts of the signature creation process. The SCASC is able to interact with the SSASC for requesting digital signature values creation.



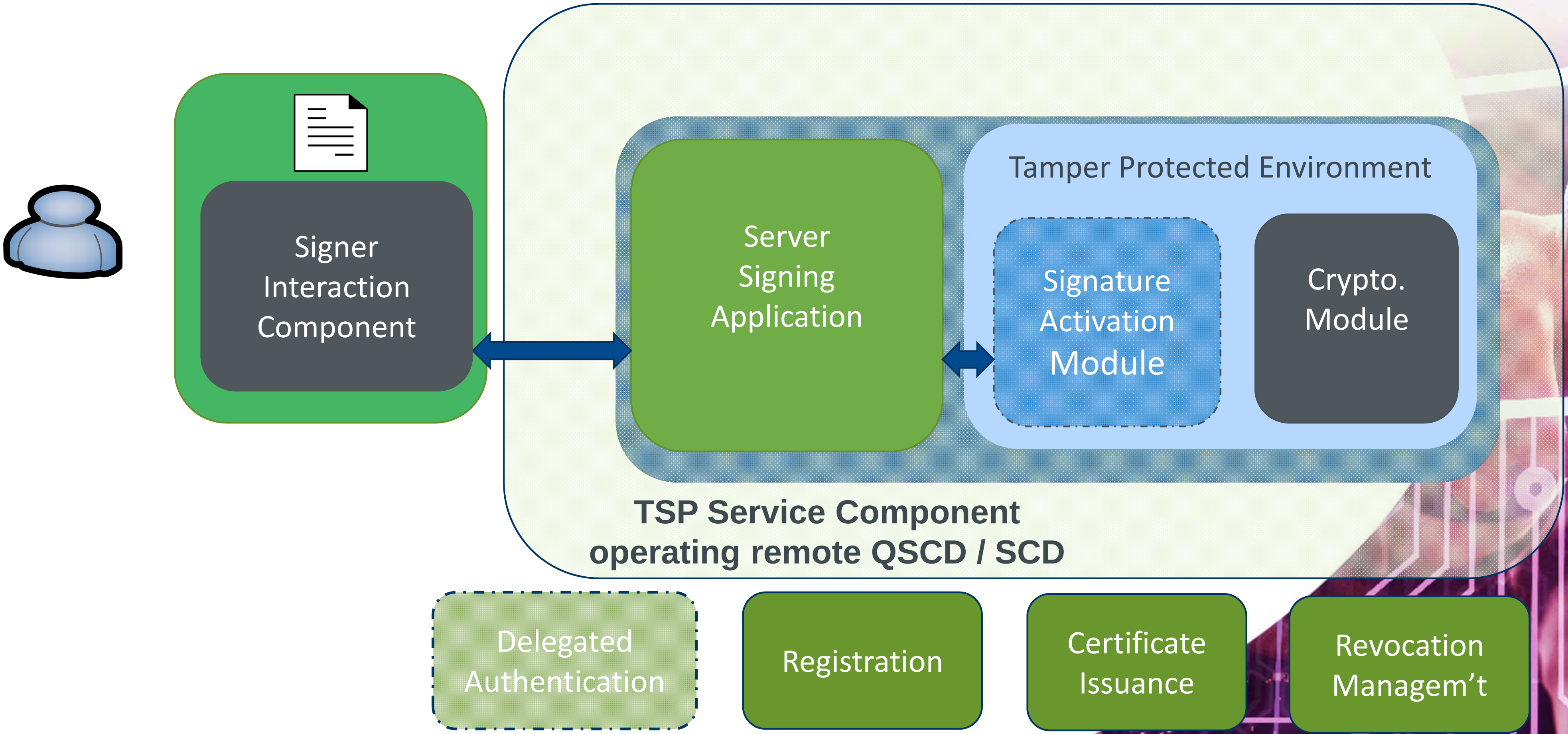
SSASC and SCASC

- Signature Creation Application
  - Signer’s document and hashing
  - DTBS composition and formatting
  - DTBS preparation
  - SDO composer
- Server Signing Application
  - Signature creation
    - Signature activation
    - Signature creation by SCDev

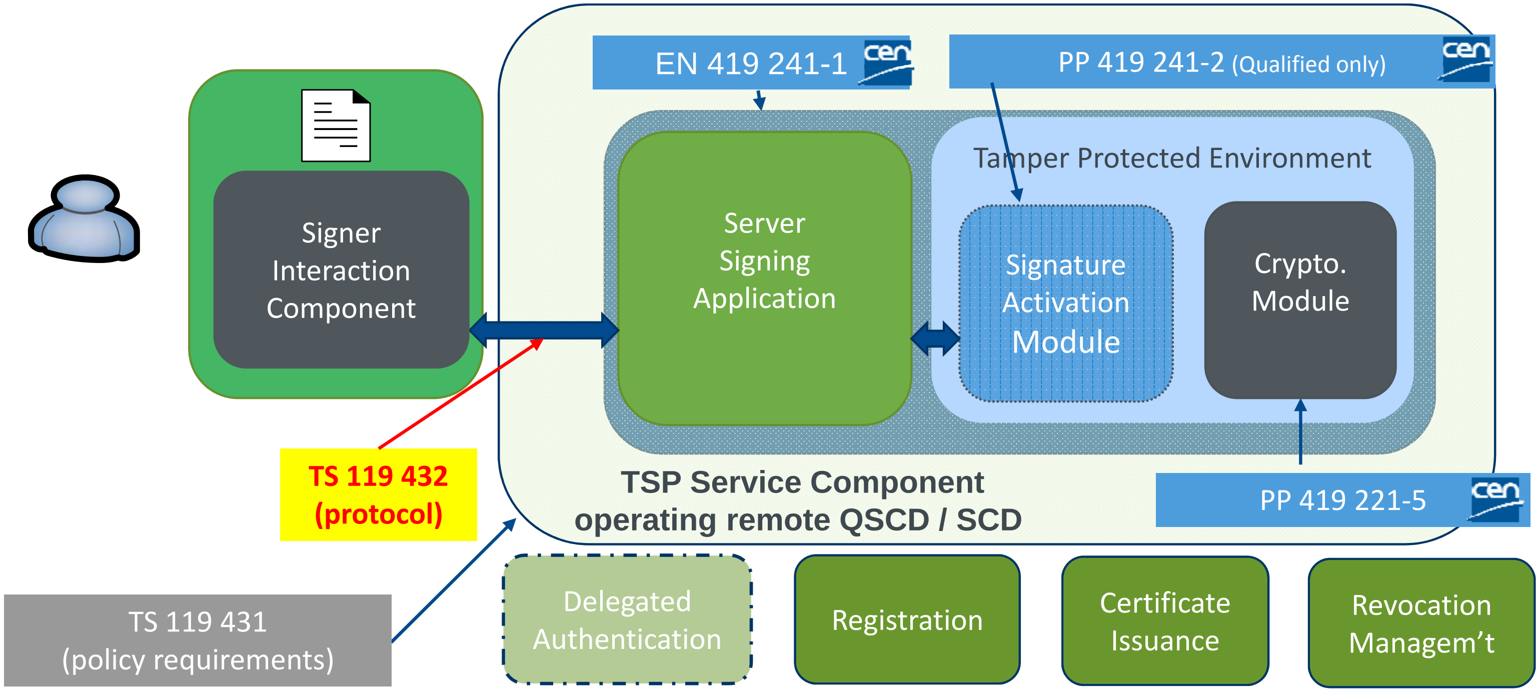
© ETSI 2018

Server signing architectures

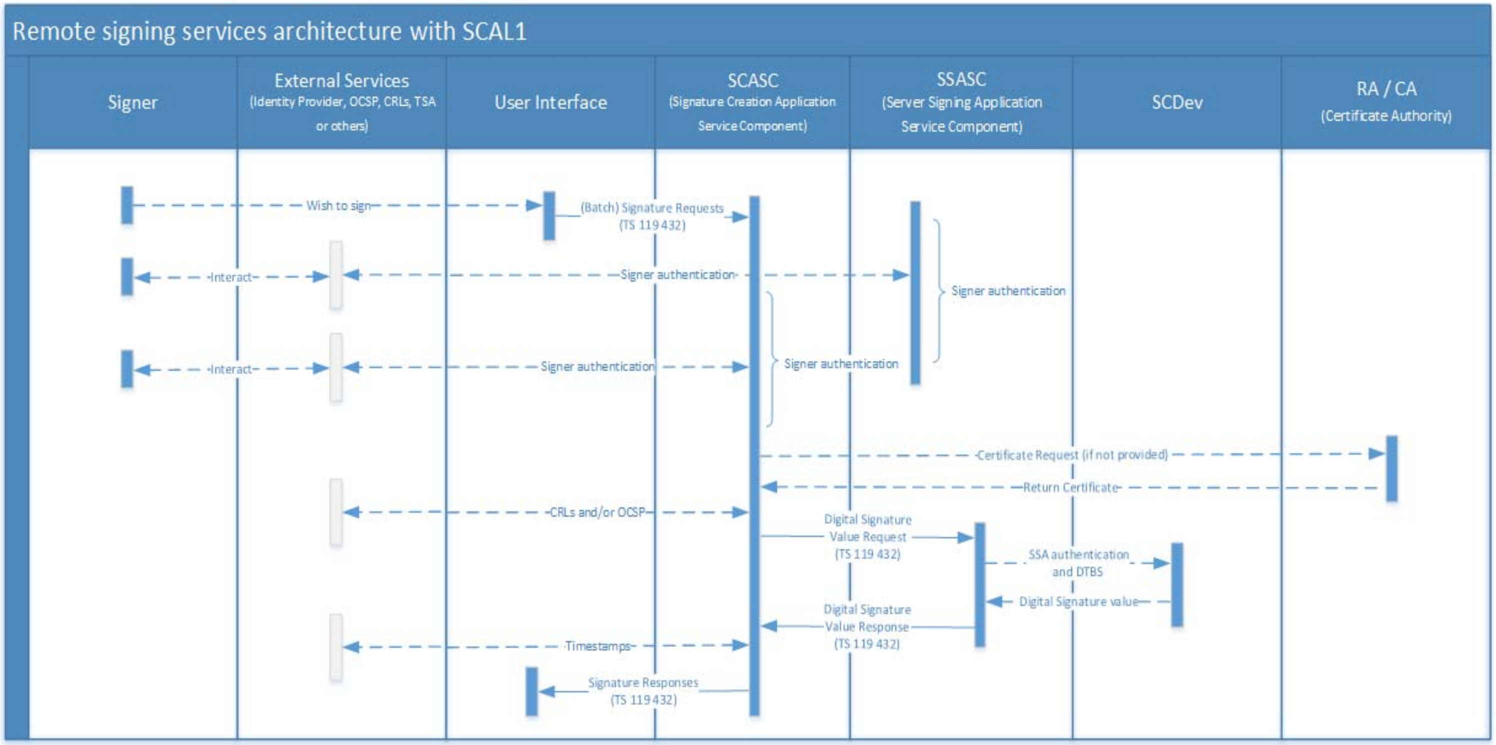
Model for remote signing


Signer Interaction Component
Server Signing Application
Tamper Protected Environment
Signature Activation Module
Crypto. Module
TSP Service Component operating remote QSCD / SCD
Delegated Authentication
Registration
Certificate Issuance
Revocation Managem’t

Scope of remote signing standards


EN 419 241-1
PP 419 241-2 (Qualified only)
Signer Interaction Component
Server Signing Application
Tamper Protected Environment
Signature Activation Module
Crypto. Module
TS 119 432 (protocol)
TSP Service Component operating remote QSCD / SCD
PP 419 221-5
TS 119 431 (policy requirements)
Delegated Authentication
Registration
Certificate Issuance
Revocation Managem’t

Remote signing services with SCAL1



Remote signing services architecture with SCAL1

Signer

External Services
(Identity Provider, OCSP, CRLs, TSA or others)

User Interface

SCASC
(Signature Creation Application Service Component)

SSASC
(Server Signing Application Service Component)

SCDev

RA / CA
(Certificate Authority)

Wish to sign

(Batch) Signature Requests
(TS 119 432)

Interact

Signer authentication

Signer authentication

Interact

Signer authentication

Signer authentication

Certificate Request (if not provided)

Return Certificate

CRLs and/or OCSP

Digital Signature
Value Request
(TS 119 432)

SSA authentication
and DTBS

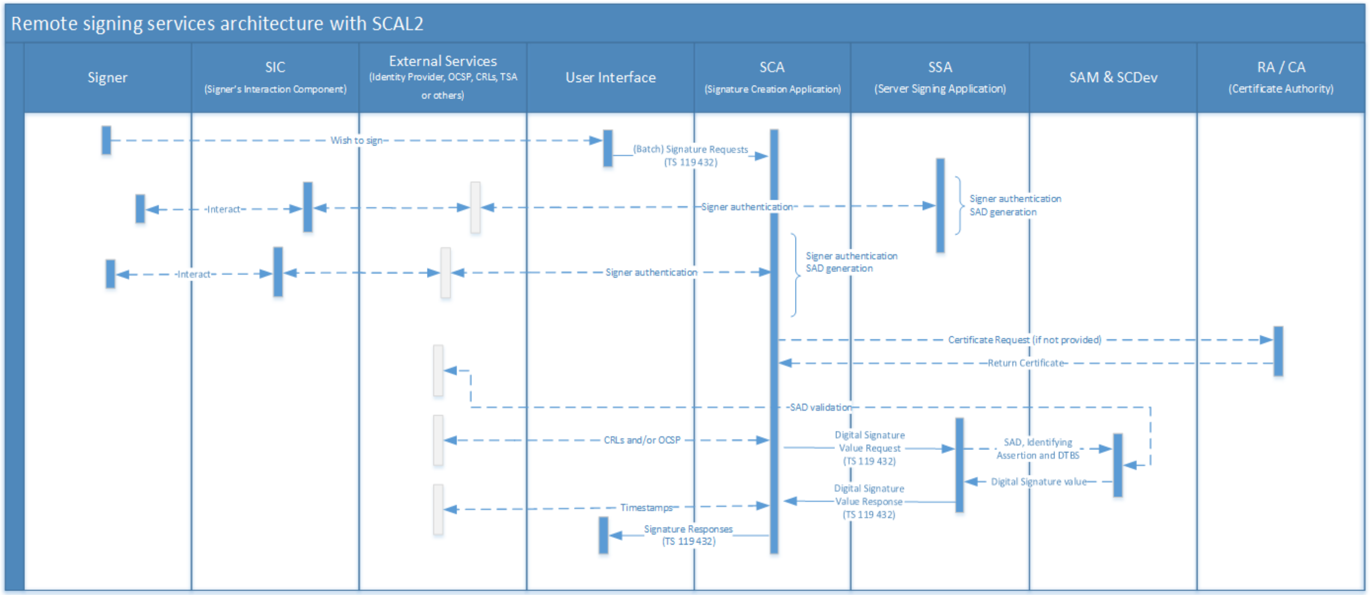
Digital Signature value

Digital Signature
Value Response
(TS 119 432)

Timestamps

Signature Responses
(TS 119 432)

Remote signing services with SCAL2



Remote signing services architecture with SCAL2

Signer

SIC
(Signer's Interaction Component)

External Services
(Identity Provider, OCSP, CRLs, TSA or others)

User Interface

SCA
(Signature Creation Application)

SSA
(Server Signing Application)

SAM & SCDev

RA / CA
(Certificate Authority)

Wish to sign

(Batch) Signature Requests
(TS 119 432)

Interact

Signer authentication

Signer authentication
SAD generation

Interact

Signer authentication

Signer authentication
SAD generation

Certificate Request (if not provided)

Return Certificate

SAD validation

CRLs and/or OCSP

Digital Signature
Value Request
(TS 119 432)

SAD, Identifying
Assertion and DTBS

Digital Signature value

Digital Signature
Value Response
(TS 119 432)

Timestamps

Signature Responses
(TS 119 432)

Technical approach for ETSI TS 119 432

Implementations

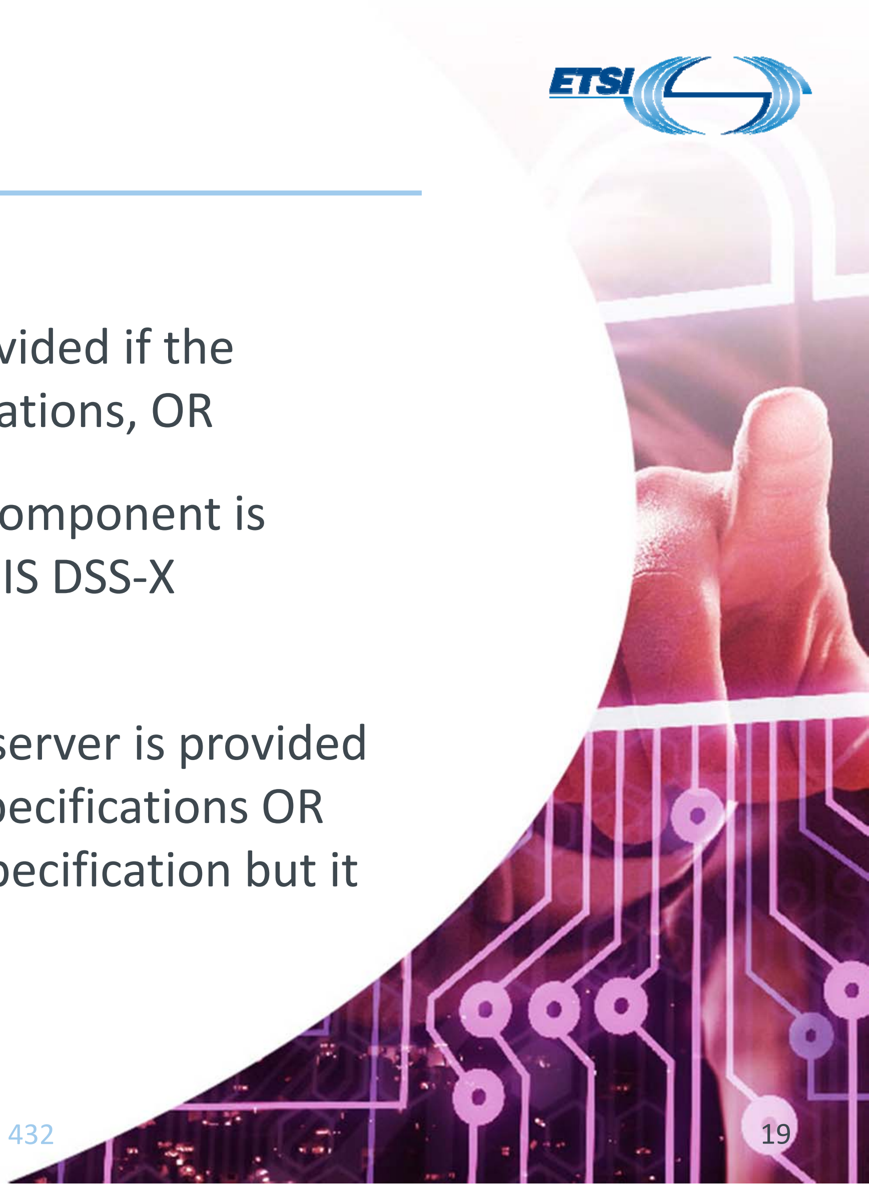
- The implementations of the protocol defined in ETSI TS 119 432 take as starting point the protocols specified by.
  - OASIS Digital Signature Services eXtended Technical Committee (DSS-X TC hereinafter);
  - Cloud Signature Consortium (CSC hereinafter).
- The implementations of the protocol in XML are profiles of the OASIS DSS-X TC core document version 2.0 which is under production by OASIS.
- The implementations of the protocol in JSON are profiles of the CSC document “Architectures, Protocols and API Specifications for Remote Signature applications” version 0.1.7.9.

OASIS DSS-X TC and CSC

- ETSI ESI and OASIS DSS-X TC as well as ETSI ESI and CSC have signed a MOU that allows them fluent exchange of information and attendance of representatives of one body to meetings of the other body.
- For each component of the protocol, ETSI TS 119 432 defines: its semantic specification, a complete XML specification, and a complete JSON specification.
- The semantic specification includes the functionality of the component and is independent of the specific implementation of the protocol (XML or JSON).

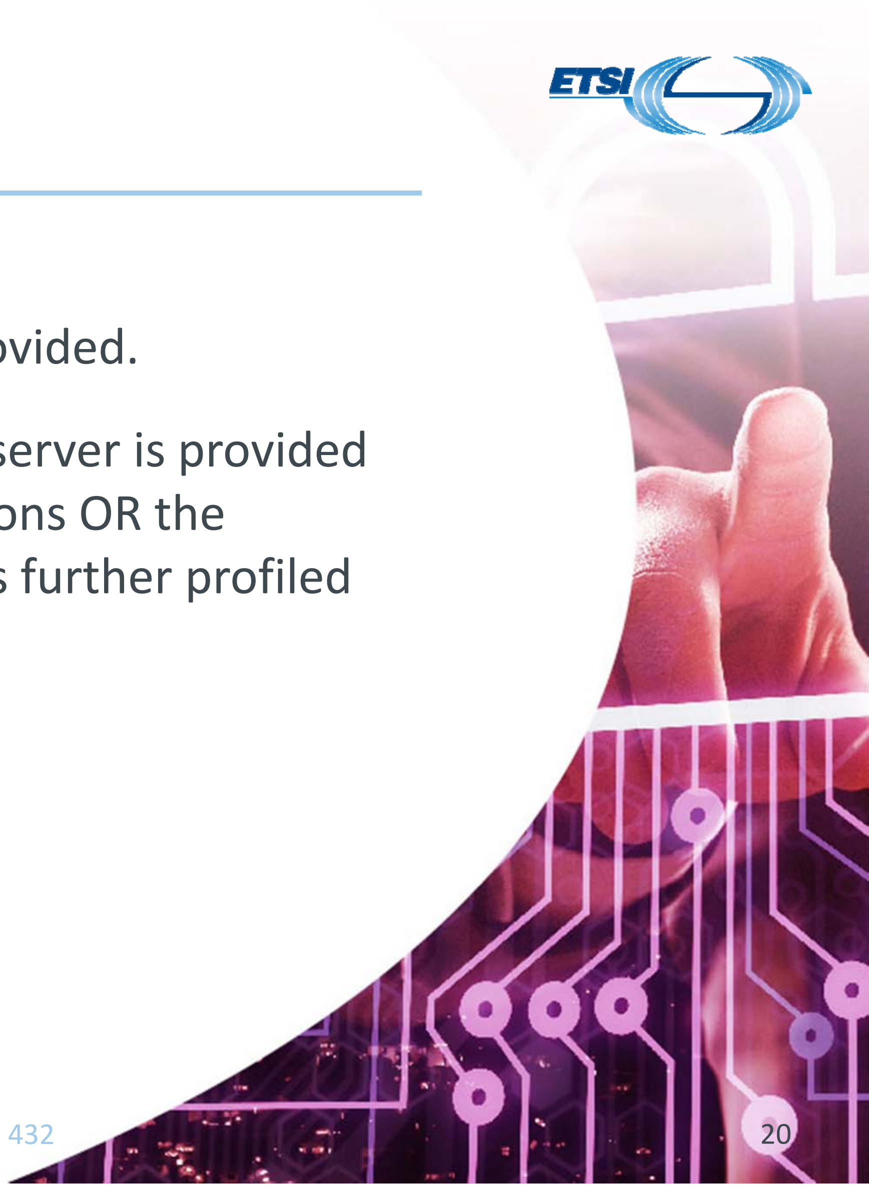
OASIS DSS-X profile

- A XML Schema definition of the component is provided if the component is not taken from OASIS DSS-X specifications, OR
- A reference to the XML Schema definition of the component is provided if the component is defined in some OASIS DSS-X specification and is further profiled here.
- The specification of the processing model for the server is provided if the component is not taken from OASIS DSS-X specifications OR the component is taken from some OASIS DSS-X specification but it is further profiled here.



CSC profile

- A JSON Schema definition of the component is provided.
- The specification of the processing model for the server is provided if the component is not taken from CSC specifications OR the component is taken from CSC specification but it is further profiled here.



Components and profile definitions

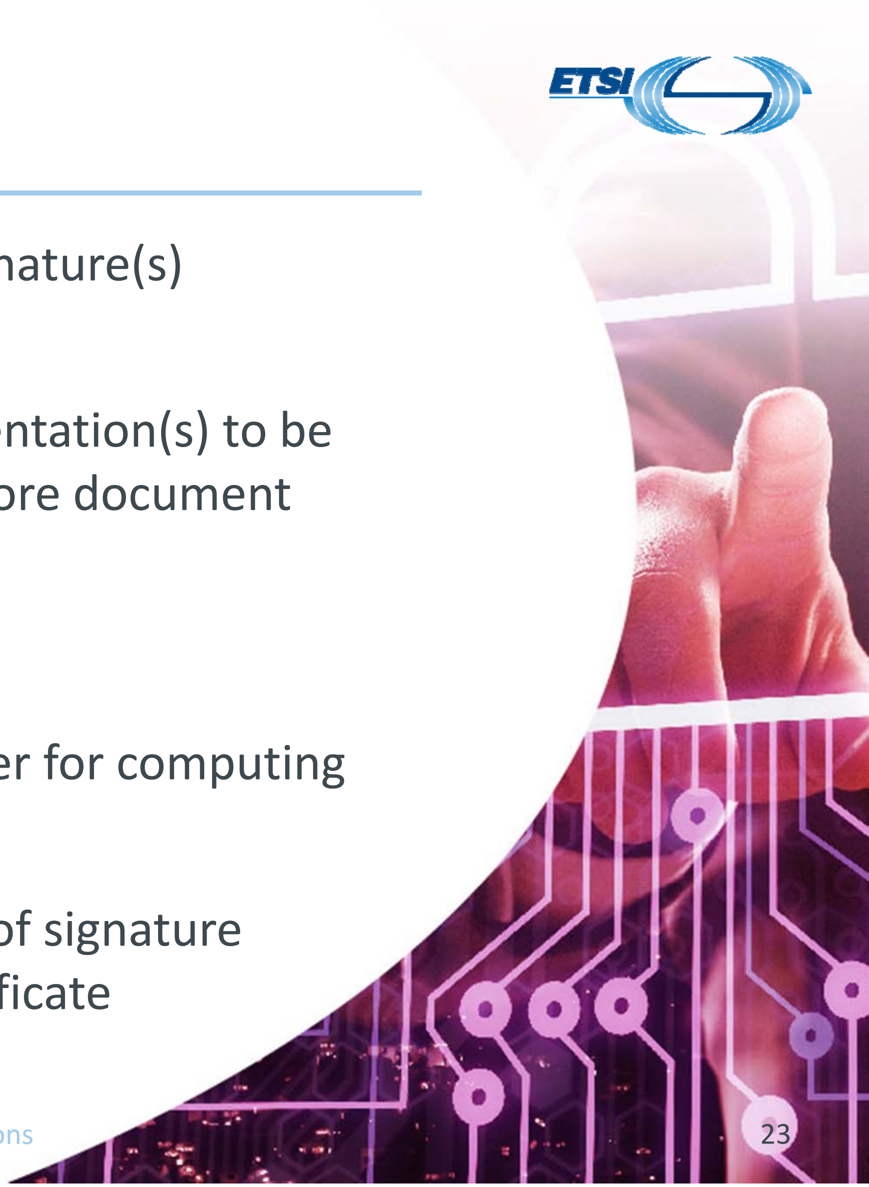
General notes

- Components represent messages that can be passed to or returned by the Signature Creation Service in order to request and execute the Signature Creation Service functionalities.
- Components for managing authentication/authorization functionalities are considered out of scope and have not been included in ETSI TS 119 432.
- Profiles represent functionalities that are implemented by the Signature Creation Service making use of the above defined components.

Overview for AdES creation requests

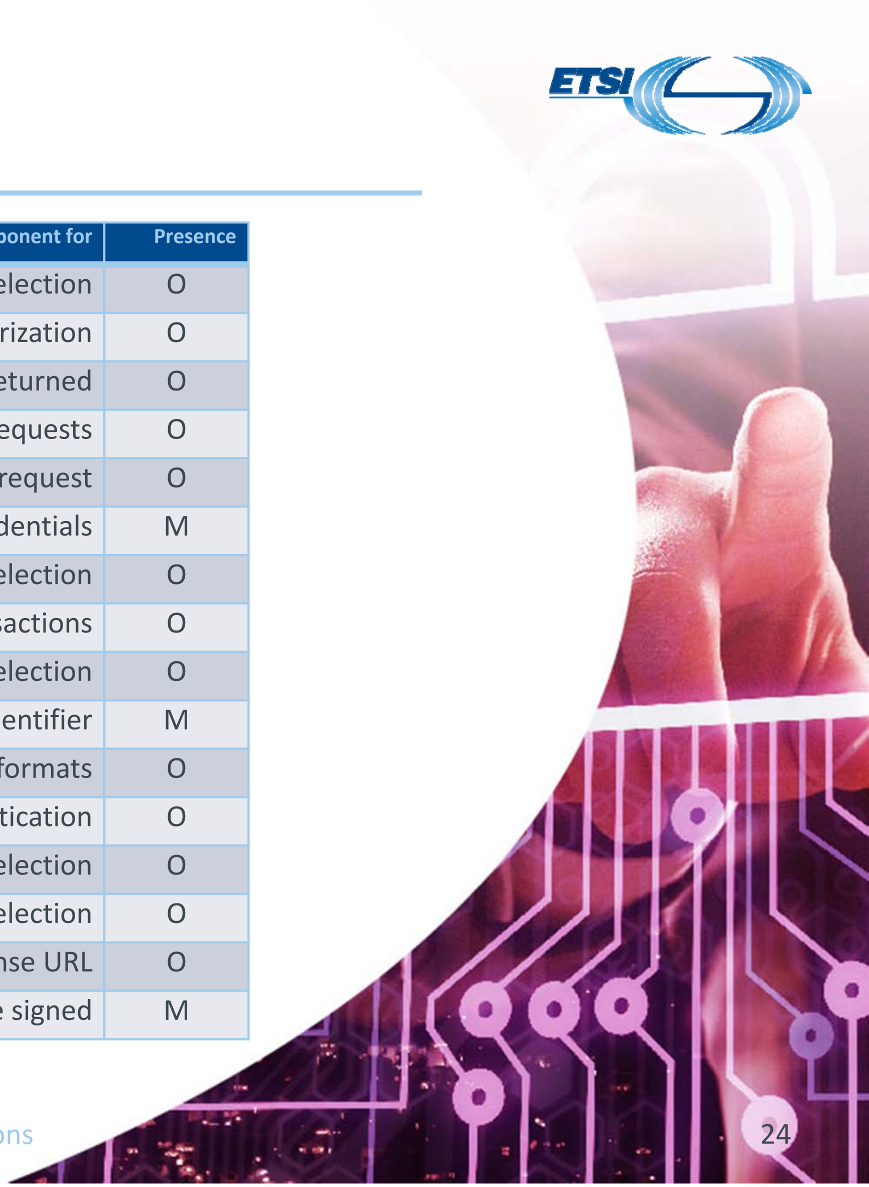
The message for requesting the creation of AdES signature(s) includes / can include components for …

- submitting the document(s) or document representation(s) to be signed (one or more documents and/or one or more document representations can be managed);
- notifying which profile is to be used;
- identifying the signing key to be used by the server for computing the requested signature operations;
- requesting additional features (i.e. identification of signature creation policy and/or service policy, signing certificate information).



Components for AdES creation requests

Ref.	Component for	Presence
7.2	asynchronous/synchronous operation mode selection	O
7.4	credential authorization	O
7.5	defining optional data to be returned	O
7.6	defining the validity period for asynchronous requests	O
7.7	identification of the request	O
7.8	identifying signature credentials	M
7.9	language and region selection	O
7.11	managing digital signatures transactions	O
7.13	optional signature attributes/properties selection	O
7.15	protocol identifier	M
7.16	requesting specific signature formats	O
7.24	service authentication	O
7.26	service policy selection	O
7.28	signature creation policy selection	O
7.30	specifying response URL	O
7.31	submitting document(s) or hash(es) of document(s) to be signed	M



Example

Component for submitting document(s) or hash(es) of document(s) to be signed

Component semantics

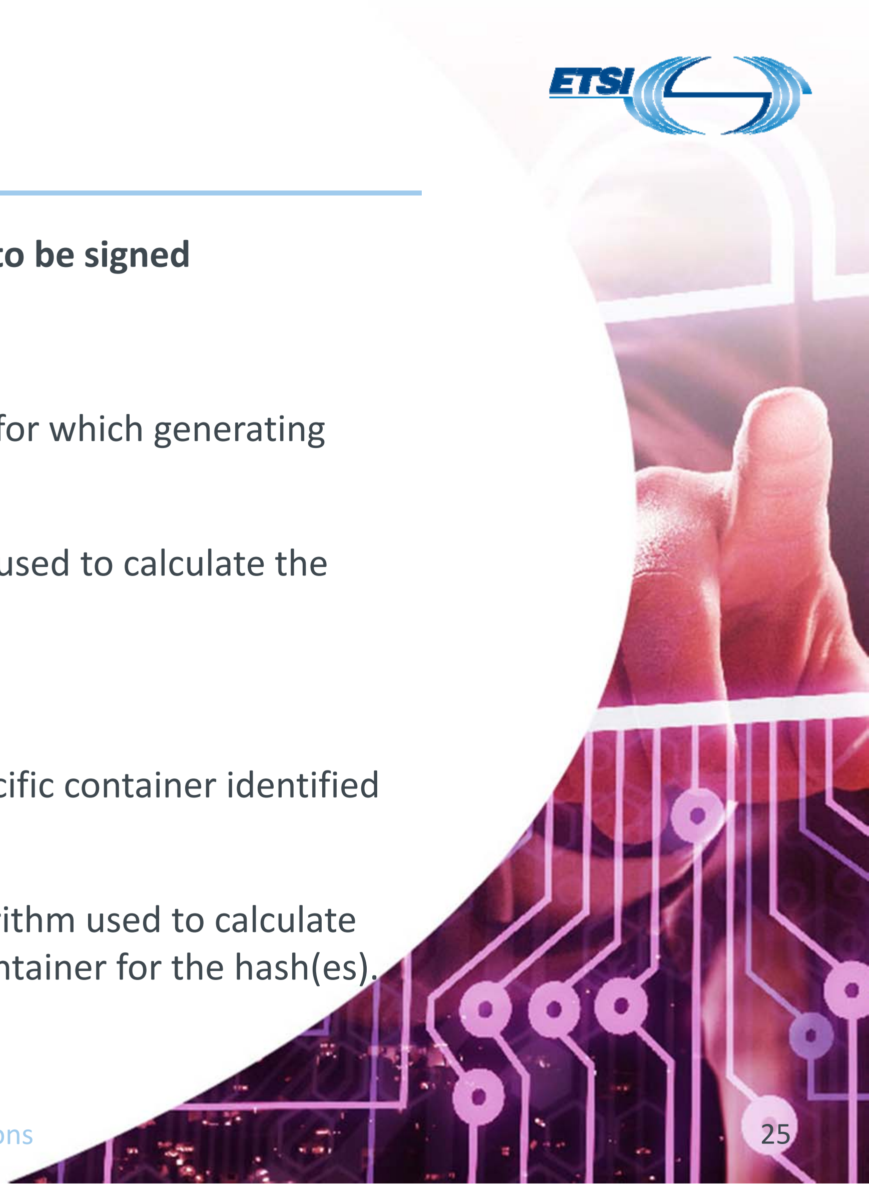
The protocol shall allow including the document(s) or a list of hashes for which generating signature(s) in two different containers.

When using hashes, the information concerning the digest algorithm used to calculate the hash of the document at the client side shall be supplied too.

The information that shall be supplied is:

- The content(s) of the document(s) to be signed, included in a specific container identified as the container for the document(s).

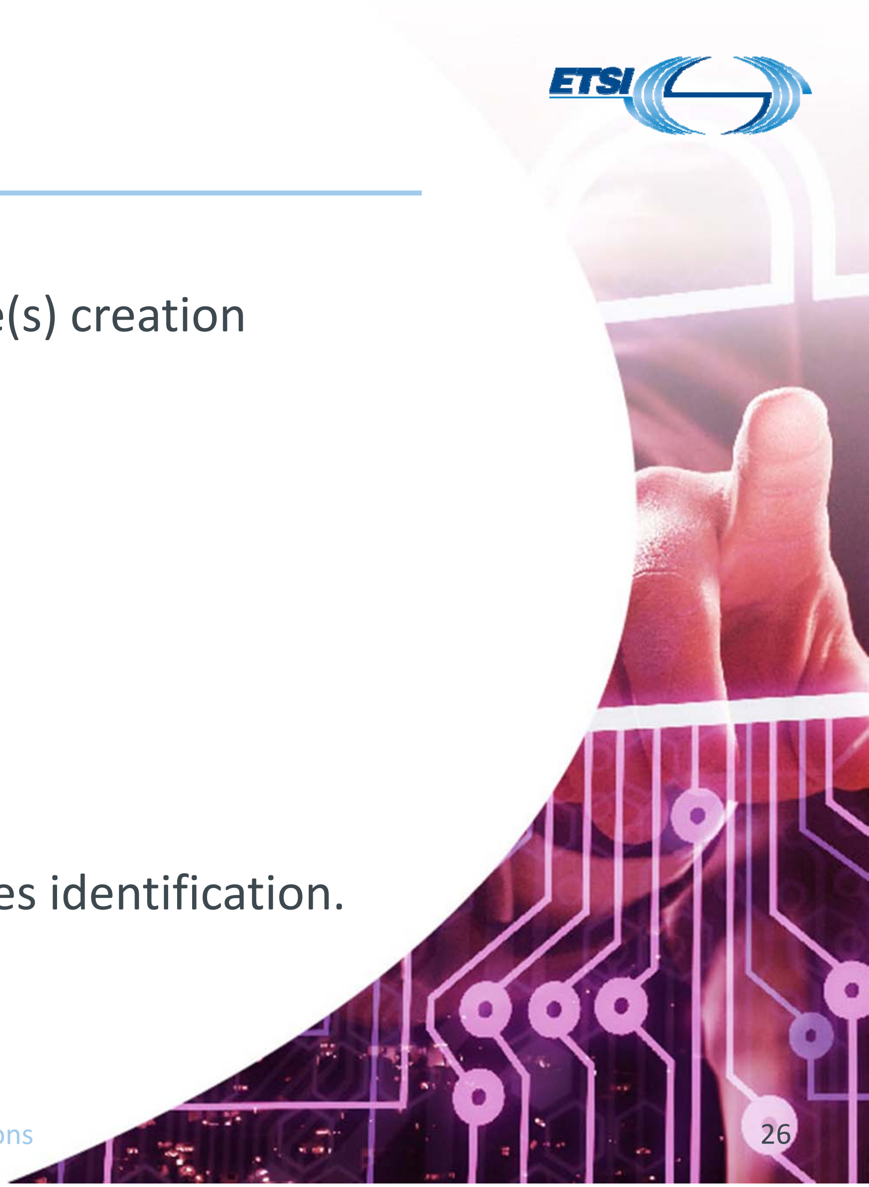
- The hash(es) of the document(s) to be signed and the digest algorithm used to calculate such hash(es), included in a specific container identified as the container for the hash(es).



Overview for AdES creation responses

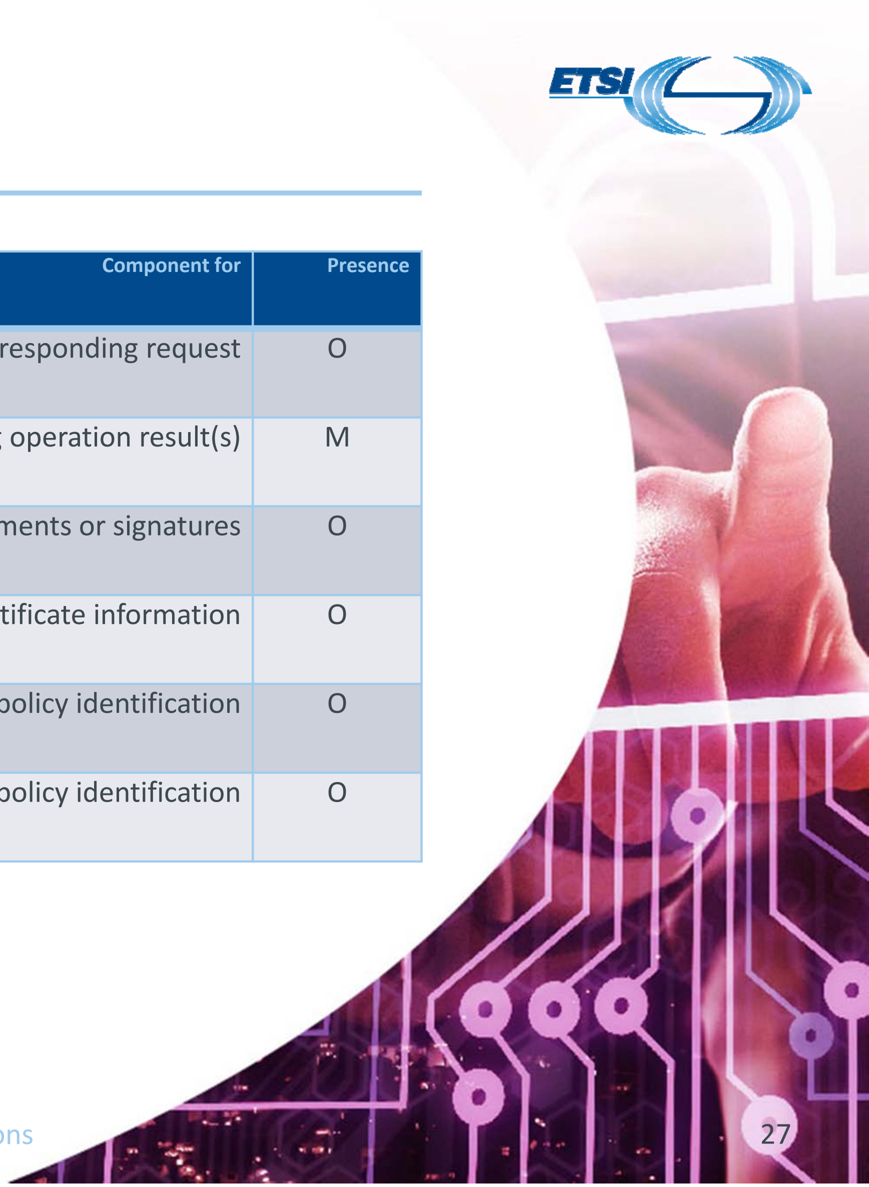
The message returned in response of AdES signature(s) creation request includes / can include components for …

- notifying operation results
- returning signed documents or signatures
- returning signing certificate information
- correlating response to corresponding request
- returning service and/or signature creation policies identification.



Components for AdES creation responses

Ref	Component for	Presence
7.3	correlating response to corresponding request	O
7.12	notifying operation result(s)	M
7.21	returning signed documents or signatures	O
7.22	returning signing certificate information	O
7.25	service policy identification	O
7.27	signature creation policy identification	O



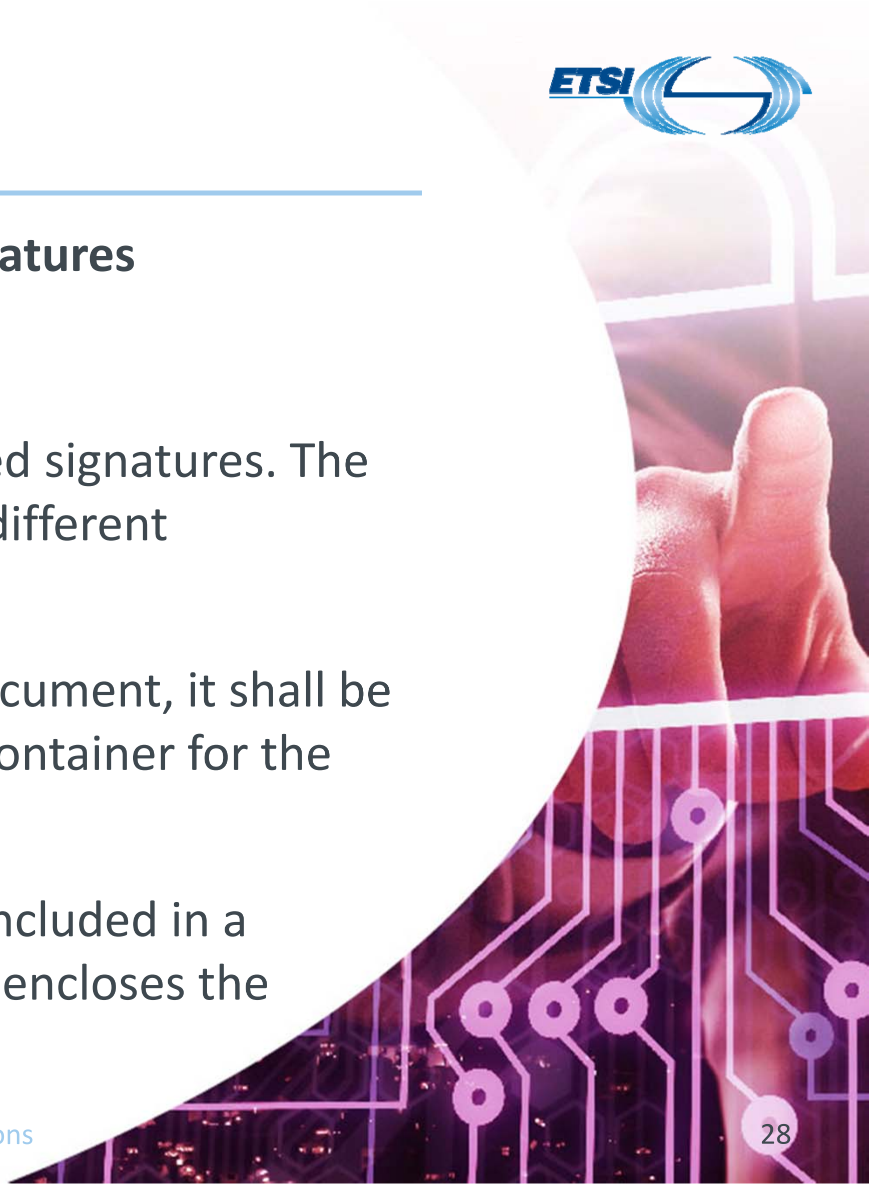
Example

Component for returning signed documents or signatures

Component semantics

This component shall be used to return the requested signatures. The protocol shall allow returning the signatures in two different containers according to the following rules:

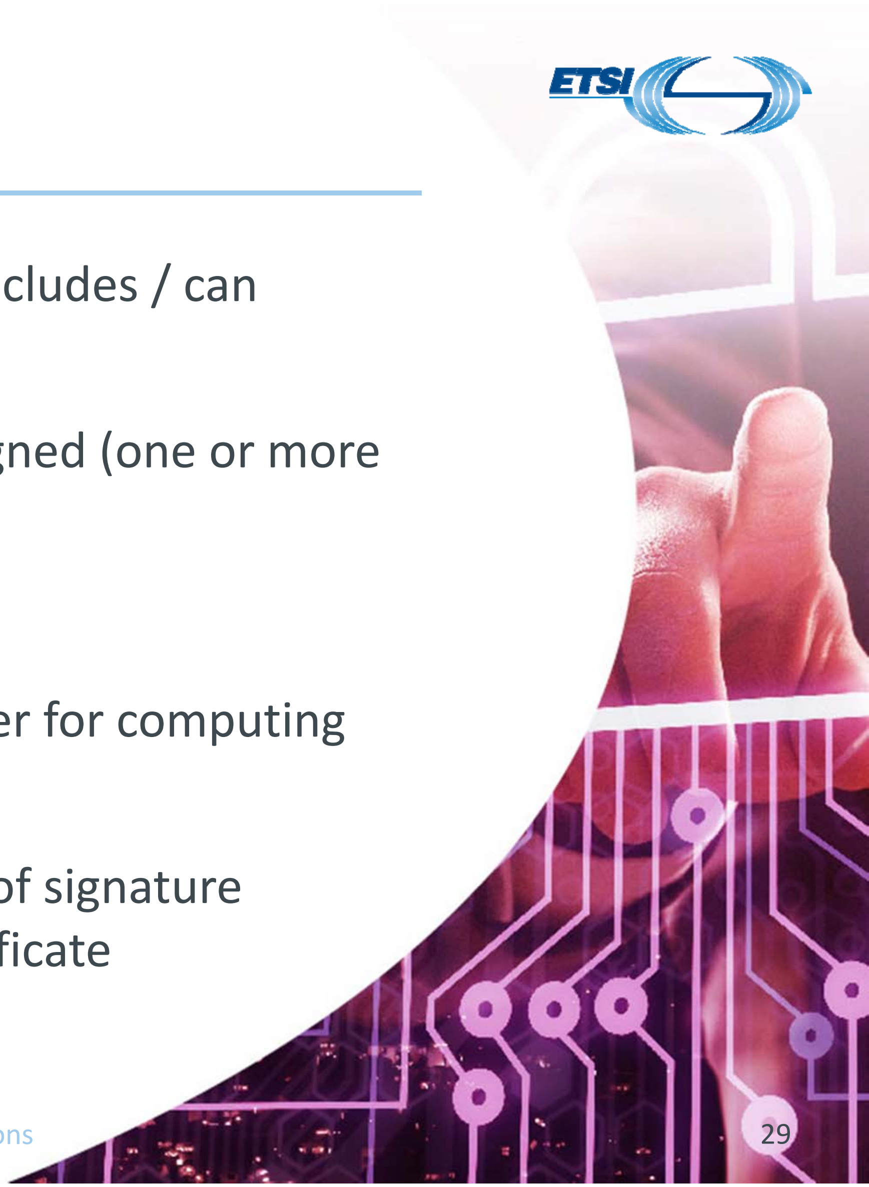
- If the signature is enveloped within the signed document, it shall be included in a specific container identified as the container for the signed document.
- If the signature is not enveloped then it shall be included in a specific container identified as the container that encloses the signature.



Overview for DSV creation requests

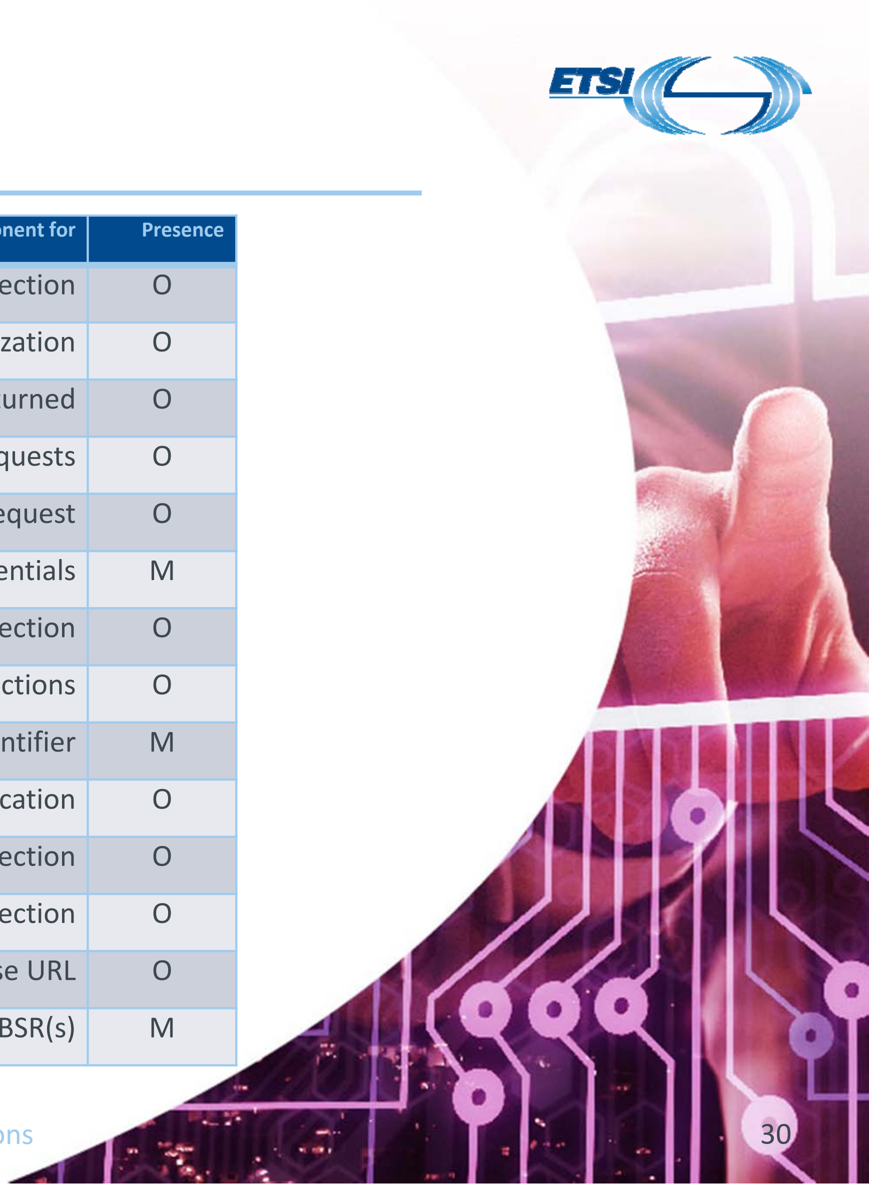
The message for requesting the creation of DSV(s) includes / can include components for …

- submitting the DTBS(s) representation(s) to be signed (one or more DTBS(s) representation(s) can be managed);
- notifying which profile is to be used;
- identifying the signing key to be used by the server for computing the requested signature operations;
- requesting additional features (i.e. identification of signature creation policy and/or service policy, signing certificate information).



Components for DSV creation requests

Ref	Component for	Presence
7.2	asynchronous/synchronous operation mode selection	O
7.4	credential authorization	O
7.5	defining optional data to be returned	O
7.6	defining the validity period for asynchronous requests	O
7.7	identification of the request	O
7.8	identifying signature credentials	M
7.9	language and region selection	O
7.11	managing digital signatures transactions	O
7.15	protocol identifier	M
7.24	service authentication	O
7.26	service policy selection	O
7.28	signature creation policy selection	O
7.30	specifying response URL	O
7.32	submitting DTBSR(s)	M



Example

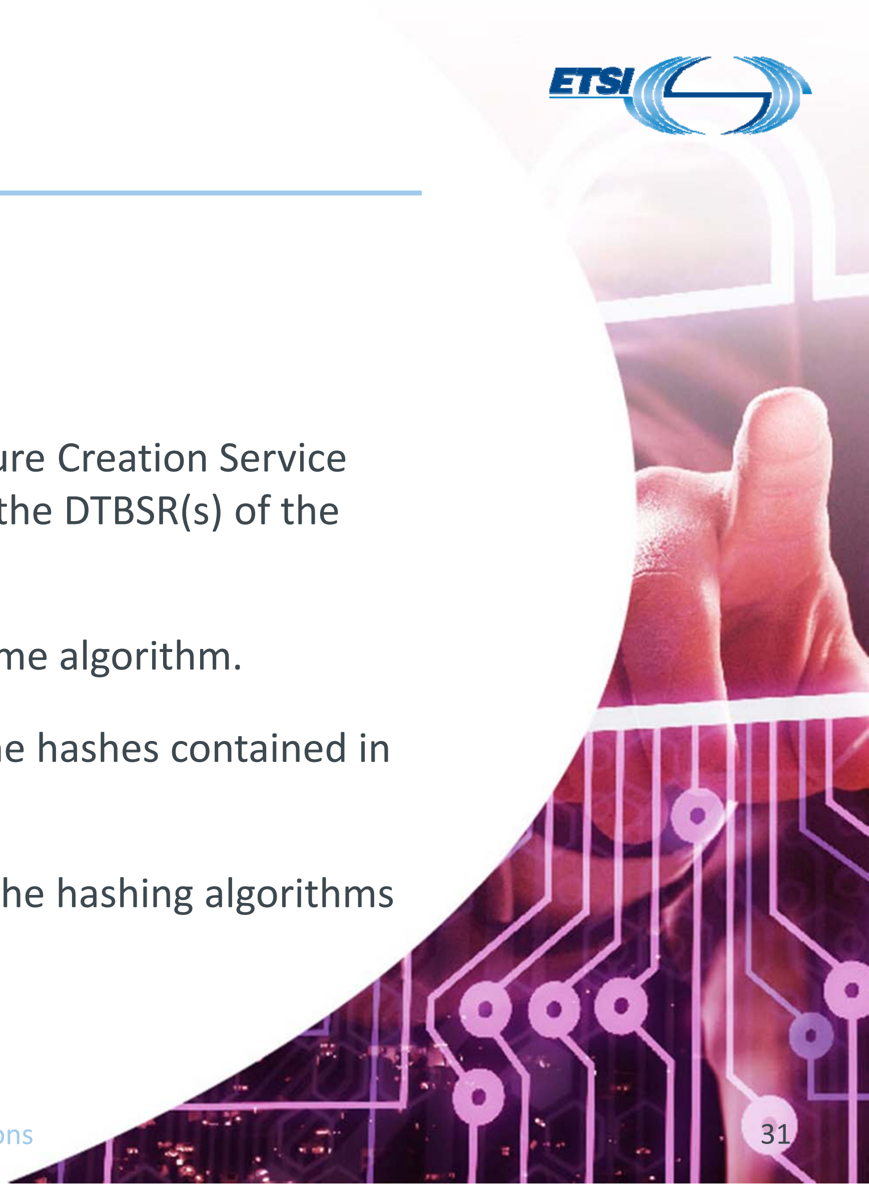
Component for submitting DTBSR(s)

Component semantics

The component shall be used in order to provide to the Signature Creation Service the list of DTBSR(s). The protocol shall allow the inclusion into the DTBSR(s) of the following information:

- a list of hashes that shall have been calculated using the same algorithm.
- the identification of the hash algorithm used to calculate the hashes contained in the DTBSR(s).

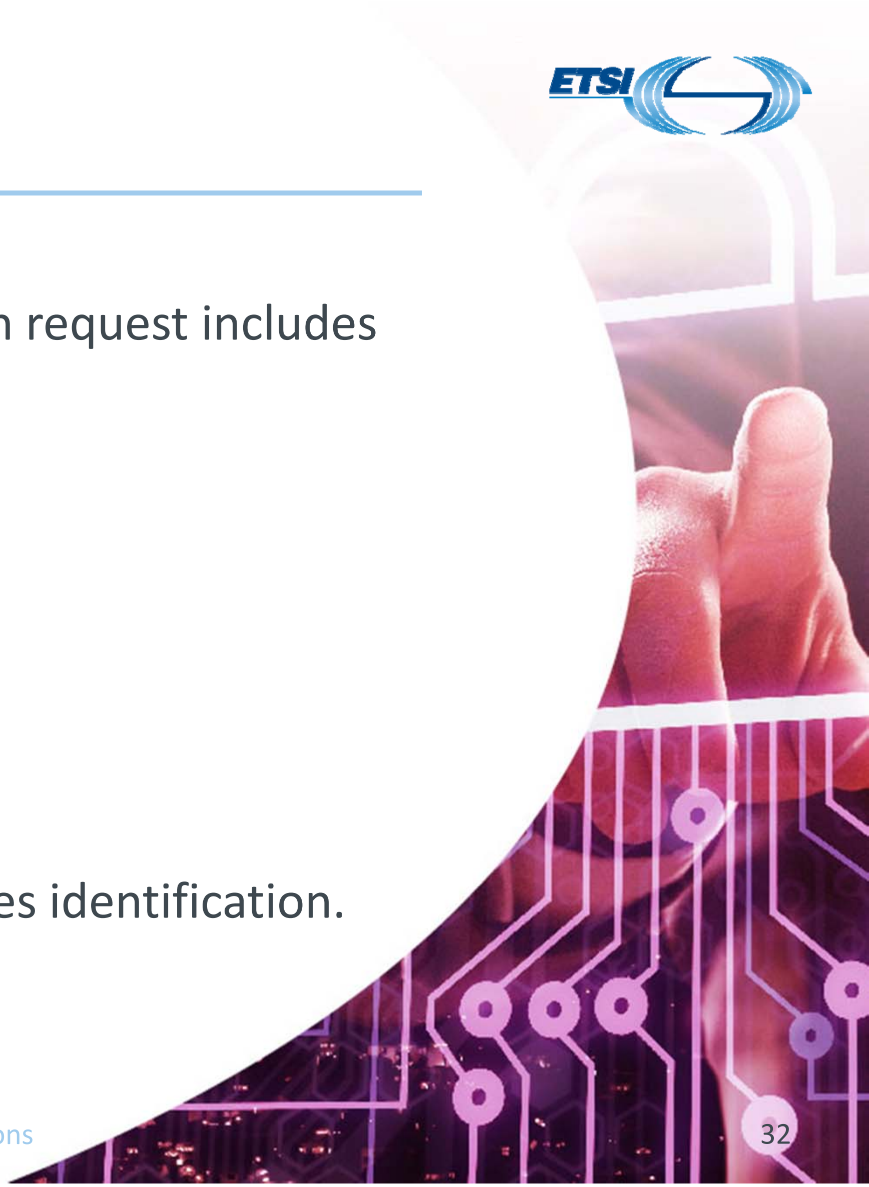
NOTE: ETSI TS 119 312 should be considered for the choice of the hashing algorithms to be used.



Overview for DSV creation responses

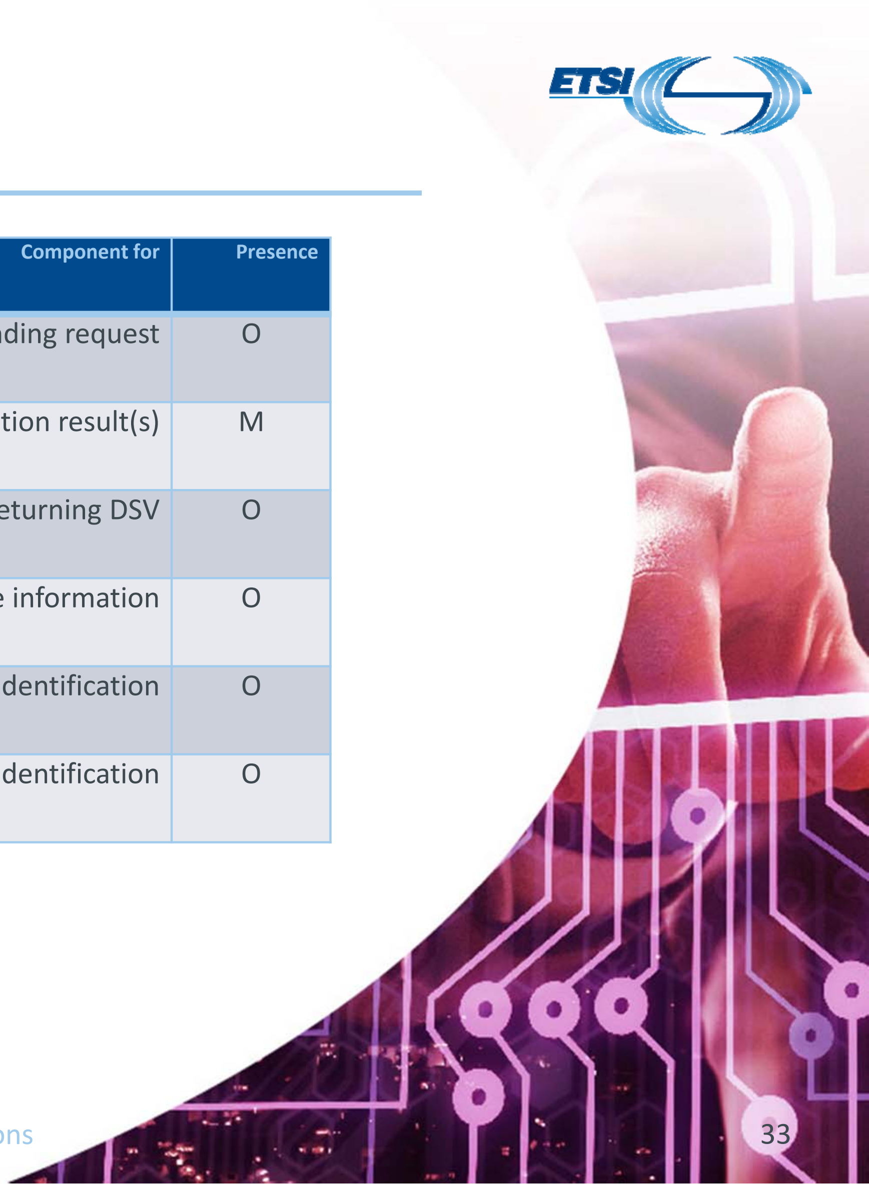
The message returned in response of DSV(s) creation request includes / can include components for …

- notifying operation results
- returning DSV(s)
- returning signing certificate information
- correlating response to corresponding request
- returning service and/or signature creation policies identification.



Components for DSV creation responses

Ref	Component for	Presence
7.3	correlating response to corresponding request	O
7.12	notifying operation result(s)	M
7.18	returning DSV	O
7.22	returning signing certificate information	O
7.25	service policy identification	O
7.27	signature creation policy identification	O



Example

Component for returning digital signature value(s)

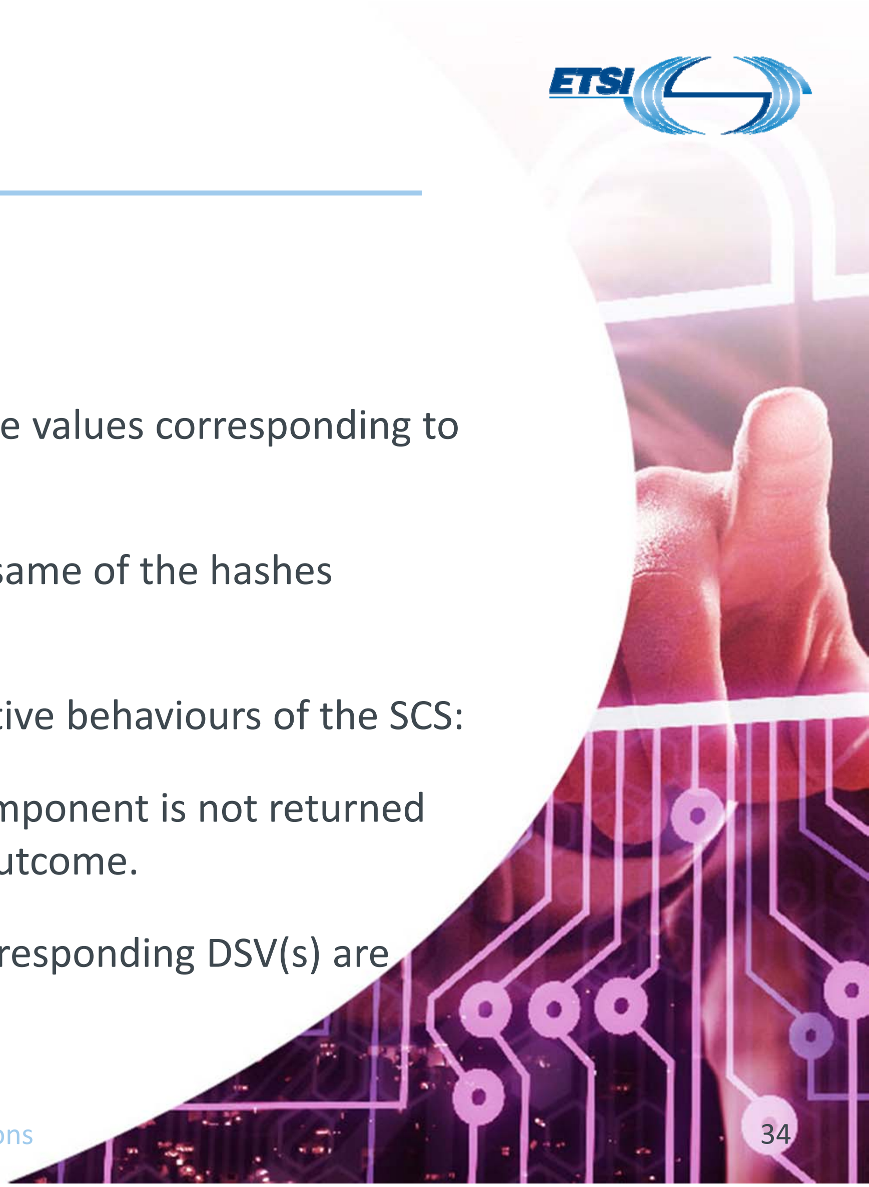
Component semantics

This component shall contain a list of base64 encoded signature values corresponding to the hashes passed in the DTBSR(s) component.

The digital signature value(s) position into the list shall be the same of the hashes included in DTBSR(s) component.

This component can be specified according to possible alternative behaviours of the SCS:

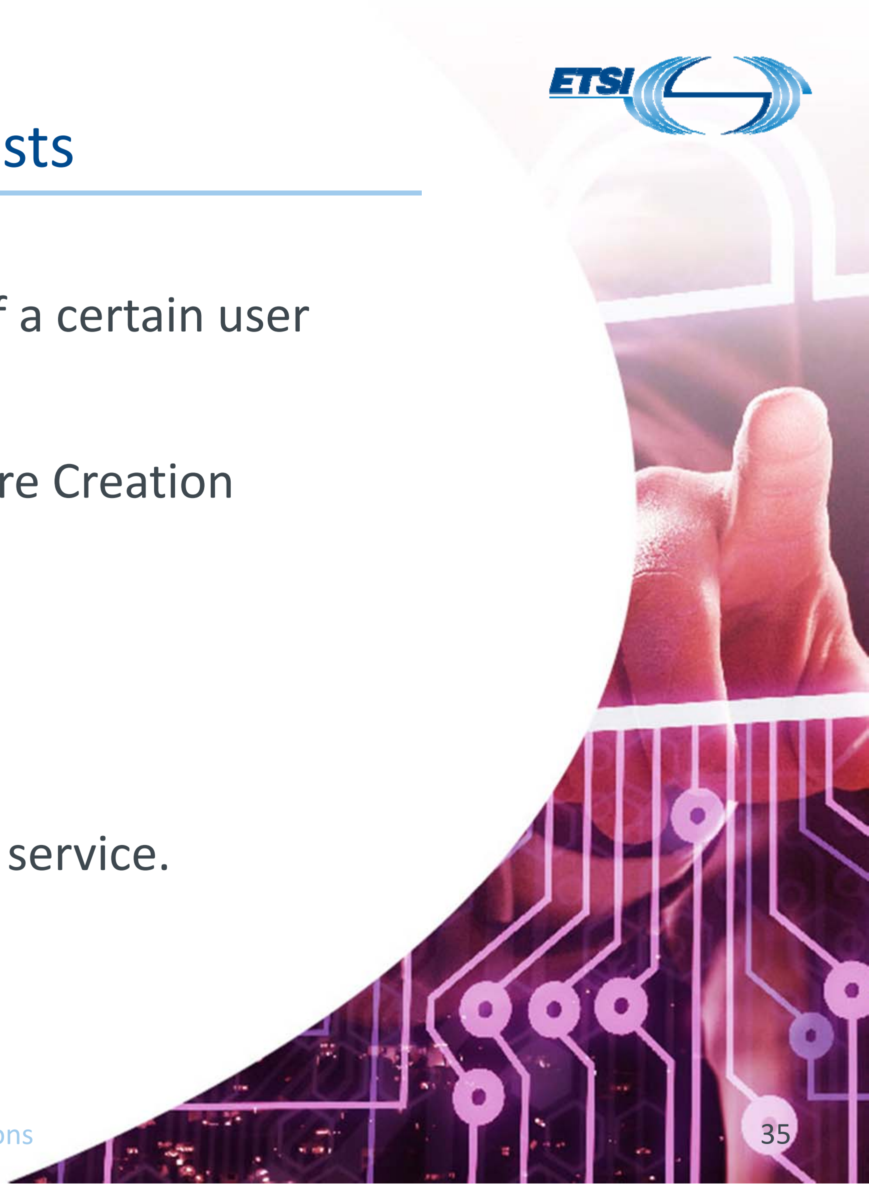
- When one or more of the requested signatures fail, this component is not returned and an error code is returned as signature creation result outcome.
- When one or more of the requested signatures fail, the corresponding DSV(s) are returned as empty values.



Overview for signing certificates list requests

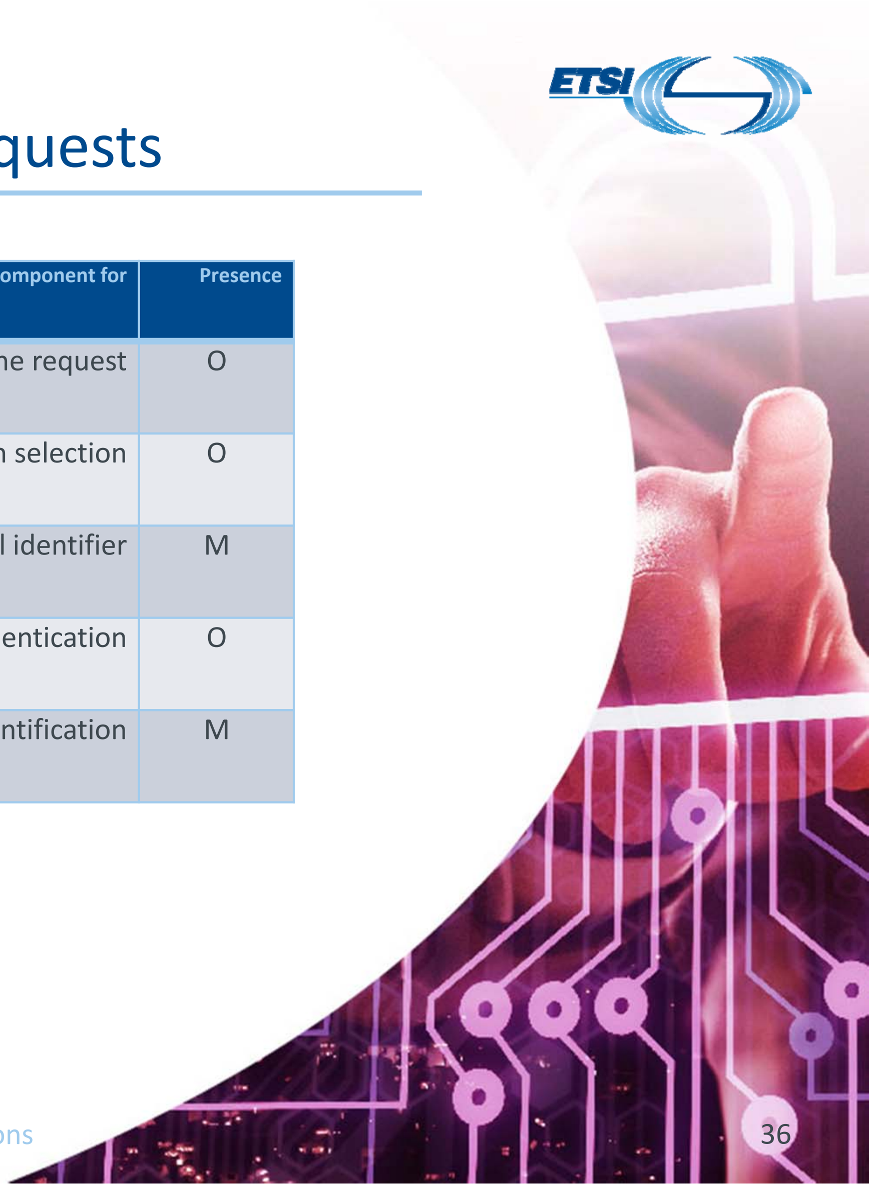
The message for requesting the list of signing keys of a certain user includes / can include components for …

- uniquely identifying the signer within the Signature Creation Service;
- notifying which profile is to be used;
- identifying the request;
- authenticating the client in order to access to the service.



Components for signing certificates list requests

Ref	Component for	Presence
7.7	identification of the request	O
7.9	language and region selection	O
7.15	protocol identifier	M
7.24	service authentication	O
7.29	signer identification	M

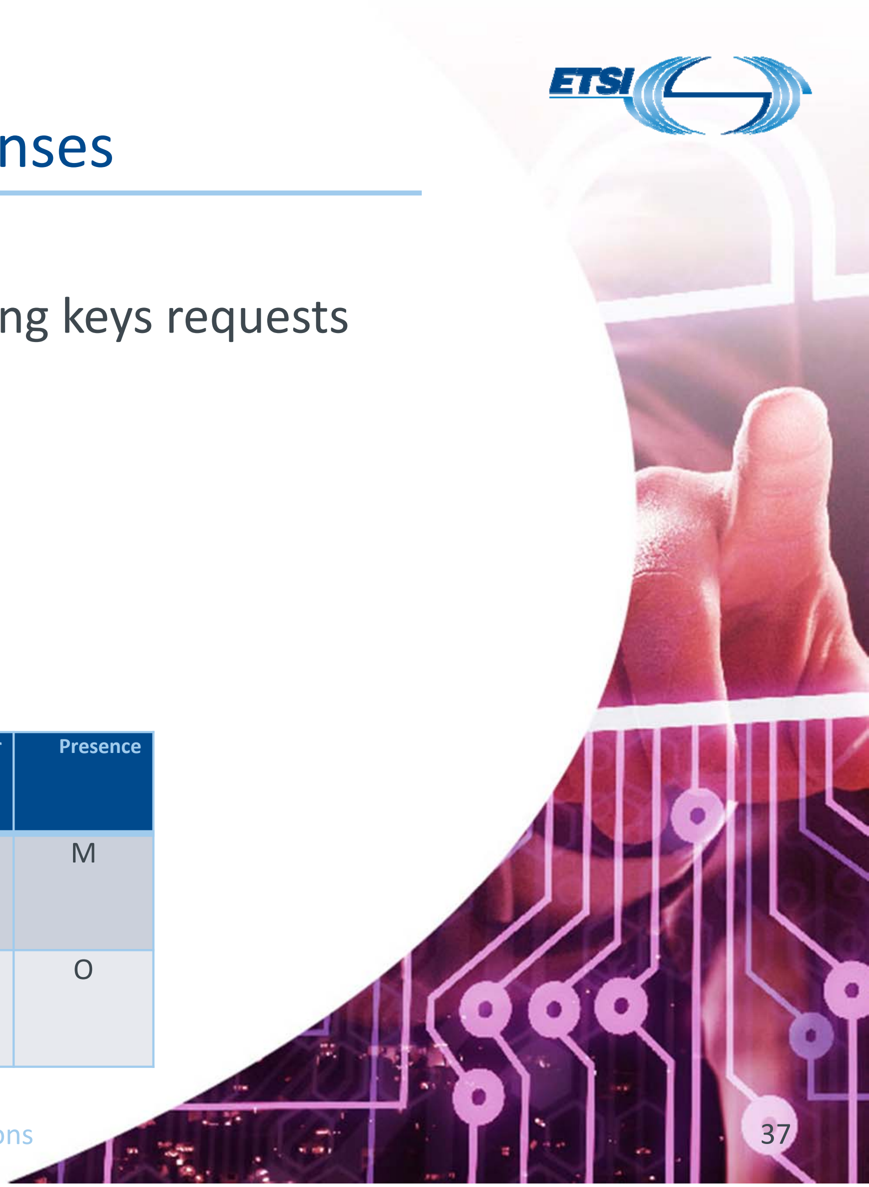


Overview for signing certificates list responses

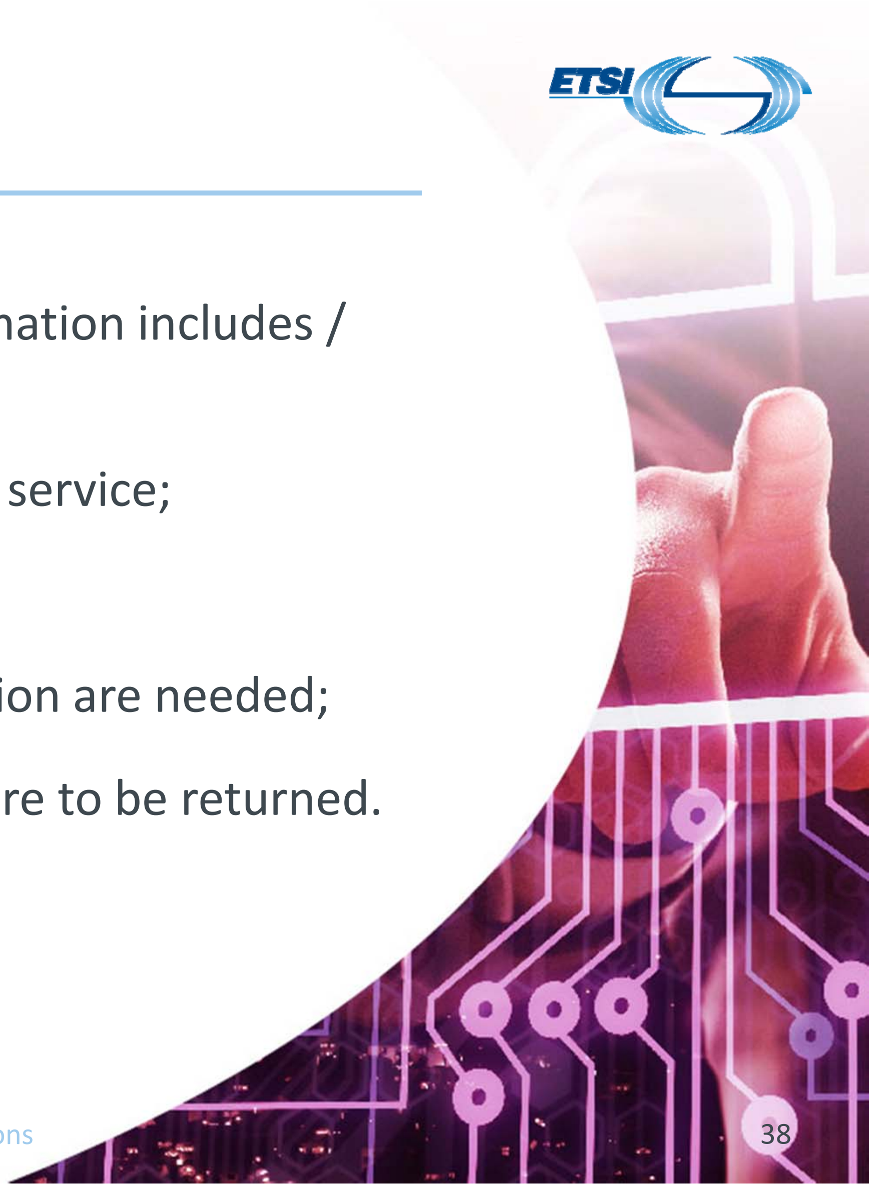
The message returned in response of the list of signing keys requests includes / can include components for …

- notifying operation results;
- returning signing certificate(s) list.

Ref	Component for	Presence
7.12	notifying operation result(s)	M
7.23	returning the list of the signing certificate(s)	O



Overview for credential info requests

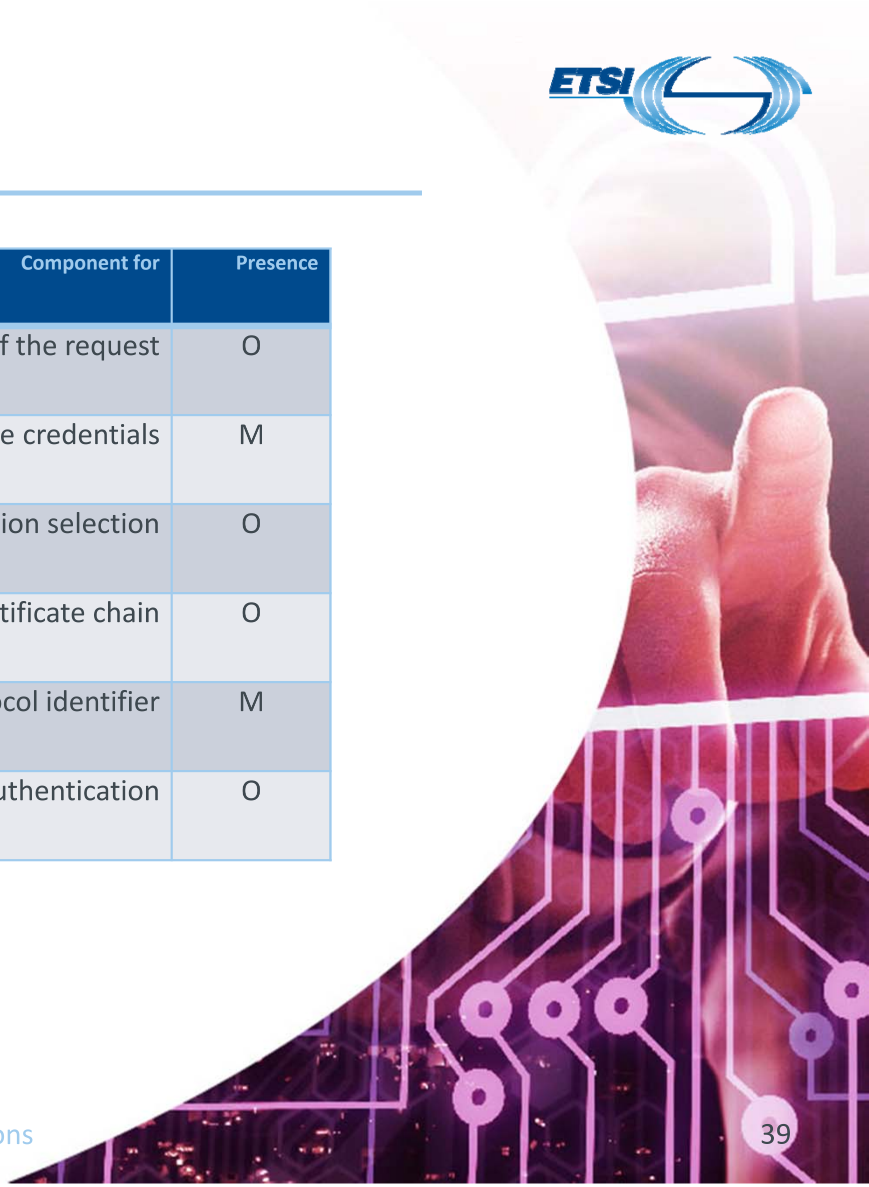


The message for requesting signing credential information includes / can include components for …

- authenticating the client in order to access to the service;
- notifying which profile is to be used;
- identifying the signing credential whose information are needed;
- specifying which contents from certificate chain are to be returned.

Components for certificate info requests

Ref	Component for	Presence
7.7	identification of the request	O
7.8	identifying signature credentials	M
7.9	language and region selection	O
7.10	list the certificate chain	O
7.15	protocol identifier	M
7.24	service authentication	O



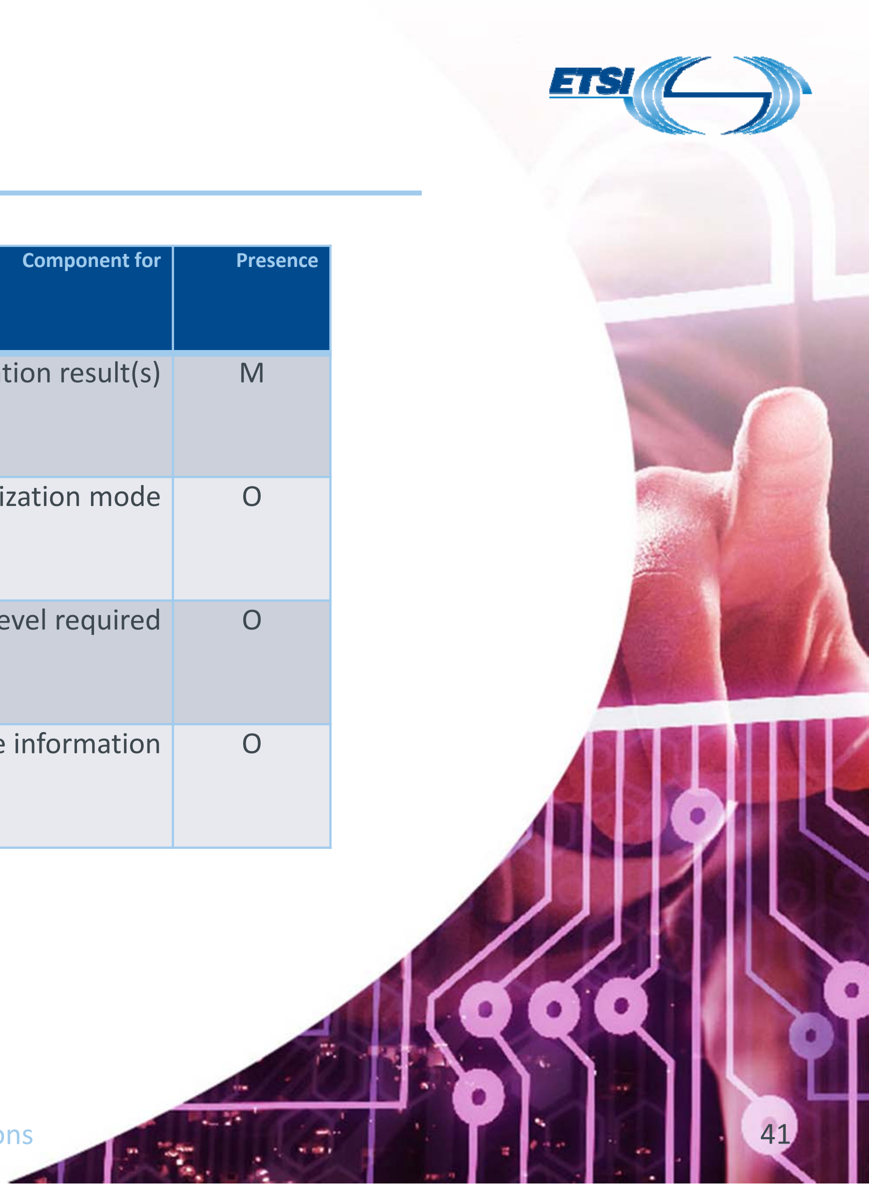
Overview for credential info responses

The message returned in response of the signing credential information requests includes / can include components for …

- notifying operation results;
- returning credential authorization mode;
- returning credential SCAL level required;
- returning signing certificate information.

Components for credential info responses

Ref	Component for	Presence
7.12	notifying operation result(s)	M
7.17	returning credential authorization mode	O
7.19	returning SCAL level required	O
7.22	returning signing certificate information	O



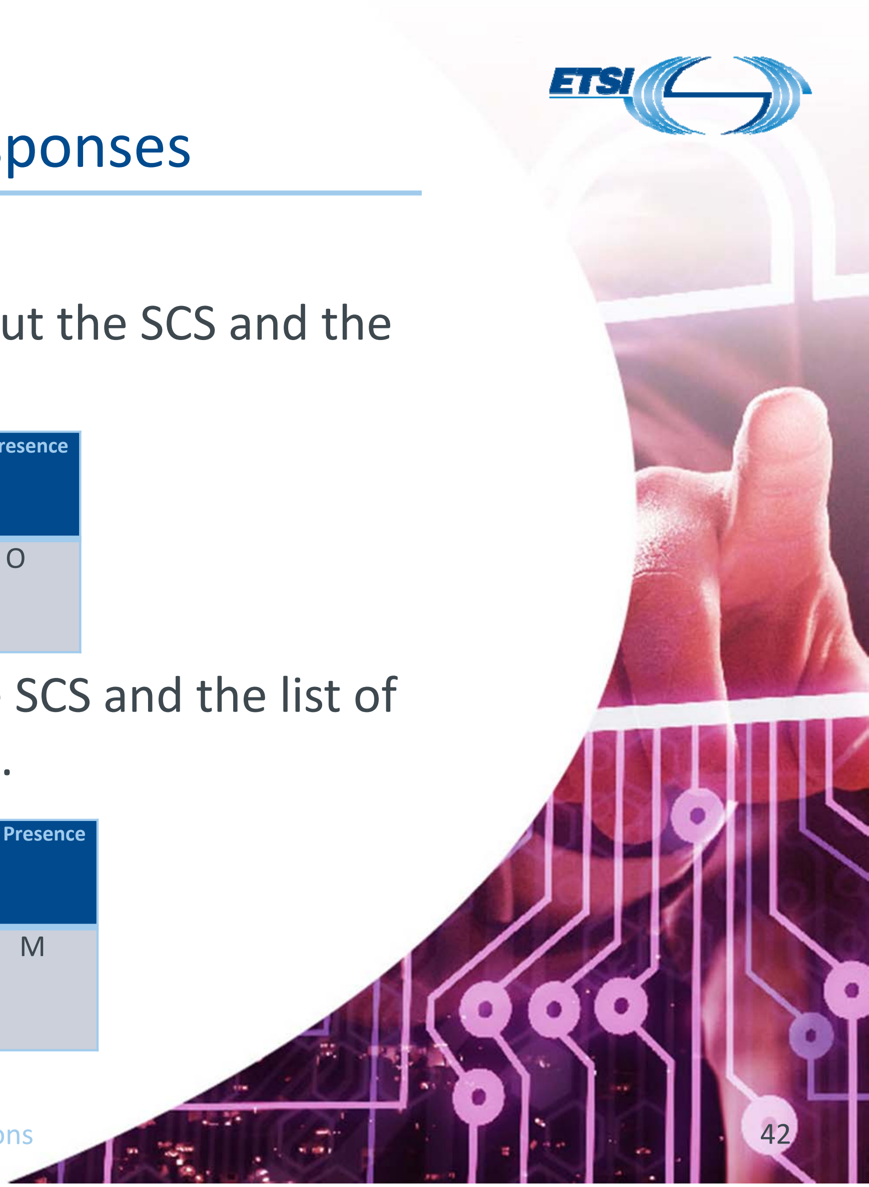
Overview for service info requests and responses

This profile shall be used to request information about the SCS and the functionalities implemented and supported by it.

Ref	Component for	Presence
7.10	language and region selection	O

This profile can return several information about the SCS and the list of the functionalities implemented and supported by it.

Ref	Component for	Presence
7.20	returning service information	M



Overview for all profiles

Ref.	Component for:	A	B	C	D	E	F	G	H	I	J	K
7.2	asynchronous/synchronous operation mode selection	O		O								
7.3	correlating response to corresponding request		O		O							
7.4	credential authorization	O		O								
7.5	defining optional data to be returned	O		O								
7.6	defining the validity period for asynchronous requests	O		O								
7.7	identification of the request	O		O			O		O			
7.8	identifying signature credentials	M										
7.9	language and region selection	O		O		O	O		O		O	
7.10	list the certificate chain								O			
7.11	managing digital signatures transactions	O		O								
7.12	notifying operation result(s)		M		M			M		M		
7.13	optional signature attributes/properties selection	O										
7.14	polling results					M						
7.15	protocol identifier	M		M			M		M			
7.16	requesting specific signature formats	O										
7.17	returning credential authorization mode									O		
7.18	returning DSV				O							
7.19	returning SCAL level required									O		
7.20	returning service information										M	
7.21	returning signed documents or signatures		O									
7.22	returning signing certificate information		O		O					O		
7.23	returning the list of the signing certificate(s)							O				
7.24	service authentication	O		O		O	O		O			
7.25	service policy identification		O		O							
7.26	service policy selection	O		O								
7.27	signature creation policy identification		O		O							
7.28	signature creation policy selection	O		O								
7.29	signer identification						M					
7.30	specifying response URL	O		O								
7.31	submitting document(s) or hash(es) of document(s) to be signed	M										
7.32	submitting DTBSR(s)			M								

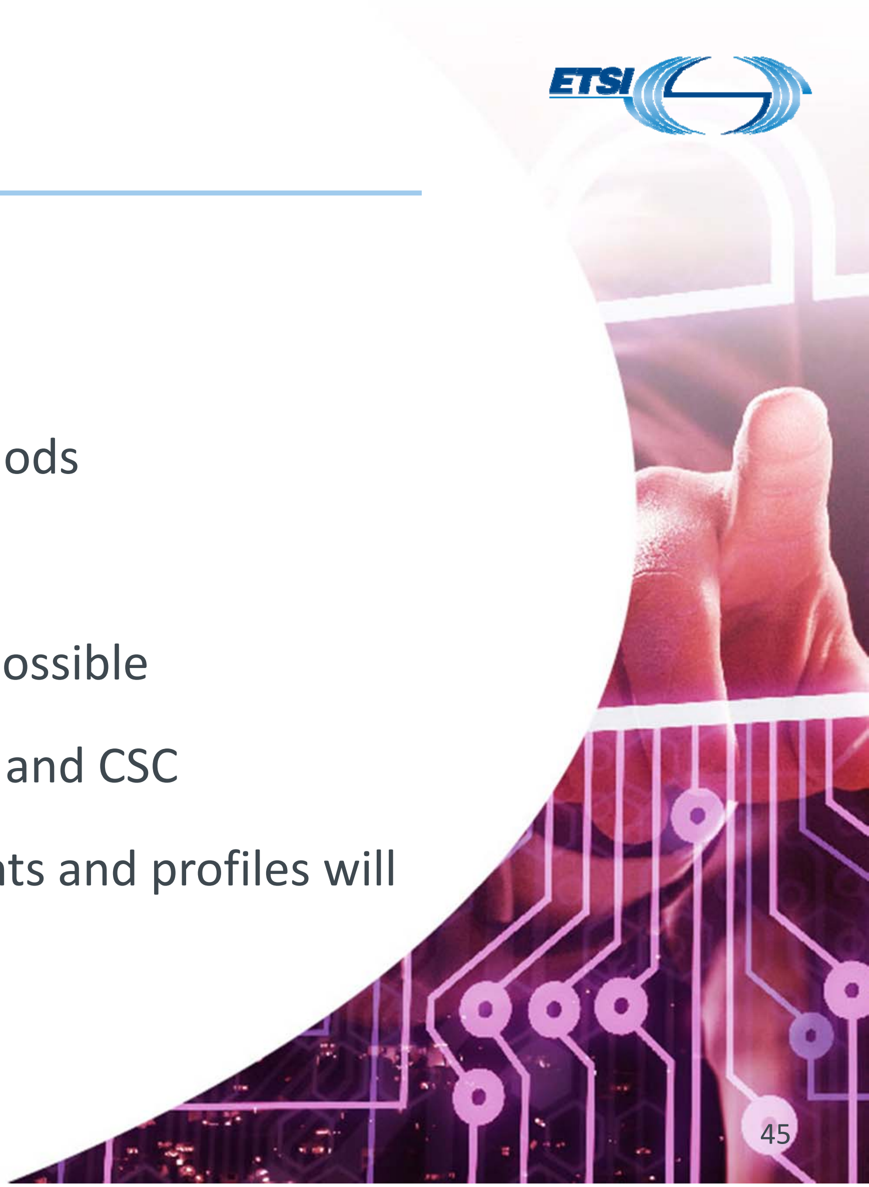
Conclusions

TS 119 432

Protocols for remote digital signature creation

Update in progress

- currently 32 components used by 8 profiles/methods
- conformant to CEN TW4S part 1
- follows OASIS DSS2 (XML) and CSC (JSON) when possible
- liaison and communication is ongoing with OASIS and CSC
- it is very likely that new XML and JSON components and profiles will need to be defined
- digital signature transactions management…



TS 119 432

Protocols for remote digital signature creation

What about

- digital signature transactions management…
- visual representation of signatures…
- conformance level AdES vs other signatures (-BES, -EPES, …)…