

Certificate Information Expression

Stefan Santesson

AAA-sec.com

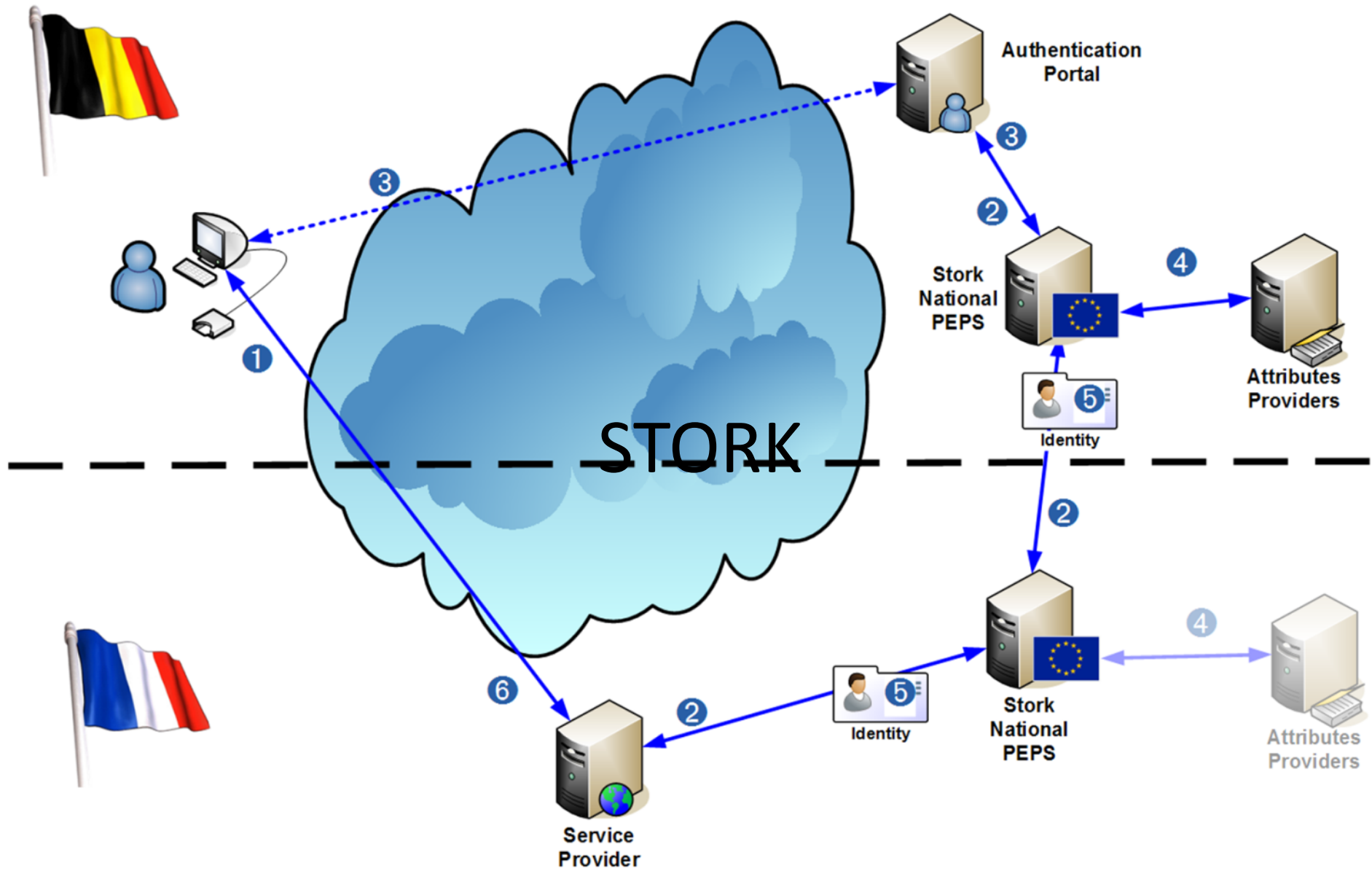
Background

- Presented at Stockholm IETF
- Addresses the need to map certificate subject and issuer attributes and identifiers to adequate semantic definitions

Current ID Semantics

- Presence of an attribute says very little about what information it holds
 - Organization
 - Country
 - SERIALNUMBER
 - etc

Identification through STORK



But for electronic signatures

- User centric model – not applicable
- Does not address authorization
 - Less attributes
- Identification as post processing
- Need for improved semantic definitions

Development since last IETF

- ETSI has approved work item to address improved semantics definitions for signature certificates
- Meeting in Istanbul in October decided to investigate different approaches
 - Pure ETSI Standard
 - Profiling an IETF standard







Basic approach

- Metadata to map between attributes and more precise semantics
- Choice 1: Extending RFC 3739 QC statement
- Choice 2: New extension

Information Card Foundation

ICF Claims Catalog

2008

Claim-Name	Data Type	Value Range 	Description	Status	URI
verification-method	xs:string	URI	The verification method claim provides a URI representing the verification method employed for verifying the verified claims enumerated in the verified-claims/2008-11 claim. The claim value may utilize any of the verification method URIs defined at Verification Methods  . Other URI values may also be defined and used.	Approved 	http://schemas.informationcard.net/@ics/verification-method/2008-12
coppa-certified-adult	xs:token	tri-boolean	True if the subject is a COPPA-certified adult who has been verified using one of the COPPA-specified methods. Some of these methods are documented in the COPPA Rules, which can be found at http://www.ftc.gov/os/1999/10/64fr59888.pdf  .	Approved 	http://schemas.informationcard.net/@ics/coppa-certified-adult/2008-12
us-registered-voter	xs:token	tri-boolean	True if the subject is a registered voter in the United States.	Provisional 	http://schemas.informationcard.net/@ics/us-registered-voter/2008-12
age-18-or-over	xs:token	tri-boolean	True if the subject is 18 or over years of age.	Approved	http://schemas.informationcard.net/@ics/age-18-or-over/2008-11

Well Known Claims

<http://schemas.xmlsoap.org/ws/2005/05/identity/claims>

The above base URI as well as the following claim names have been defined in [ISIP 1.5](#). The claim names are appended to the above base XML namespace URI to form the complete claim type URI (as shown in the right-most column):

Claim name	Data Type	Description	URI
givenname	xs:string	(givenName in RFC 2256) Preferred name or first name of a subject. According to RFC 2256 : "This attribute is used to hold the part of a person's name which is not their surname nor middle name."	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
surname	xs:string	(sn in RFC 2256) Surname or family name of a subject. According to RFC 2256 : "This is the X.500 surname attribute which contains the family name of a person."	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
emailaddress	xs:string	(mail in inetOrgPerson) Preferred address for the "To:" field of email to be sent to the subject, usually of the form @. According to inetOrgPerson using RFC 1274 : "This attribute type specifies an electronic mailbox attribute following the syntax specified in RFC 822 ."	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Way forward

- Initiate discussion to accept new PKIX work item
- Submit first draft for discussion