ABC4Trust & PrimeLife Tutorial

Part II: Policy Languages

Overview of this talk

- Identity management: SAML
- Access control: XACML
- Trust management: WS-Trust
- Identity federation: WS-Federation
- U-Prove token format
- Card-based access requirements language (CARL)

eXtensible Markup Language (XML)

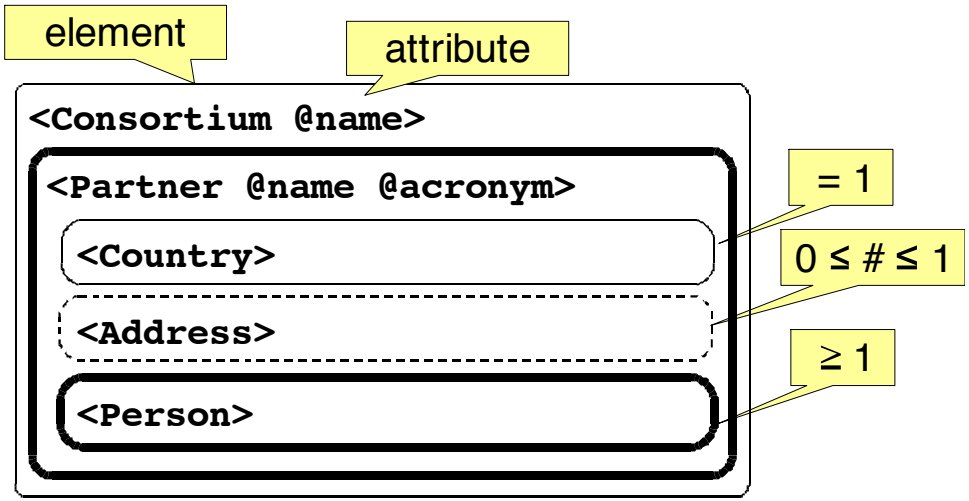
element

attribute

child element

```
<Consortium name="ABC4Trust">
    <Partner name="Alexandra Institute AS" acronym="ALX">
        <Country>Denmark</Country>
        <Address>Aabogade 34, 8200 Aarhus N</Address>
        <Person>Jakob Pagter</Person>
        <Person>Gert Laessoe Mikkelsen</Person>
    </Partner>
    <Partner name="CryptoExperts" acronym="CRX">
        <Country>France</Country>
        <Person>Pascal Paillier</Person>
        <Person>Cecile Delerablee</Person>
    </Partner>
</Consortium>
```

Format specified by *schema*

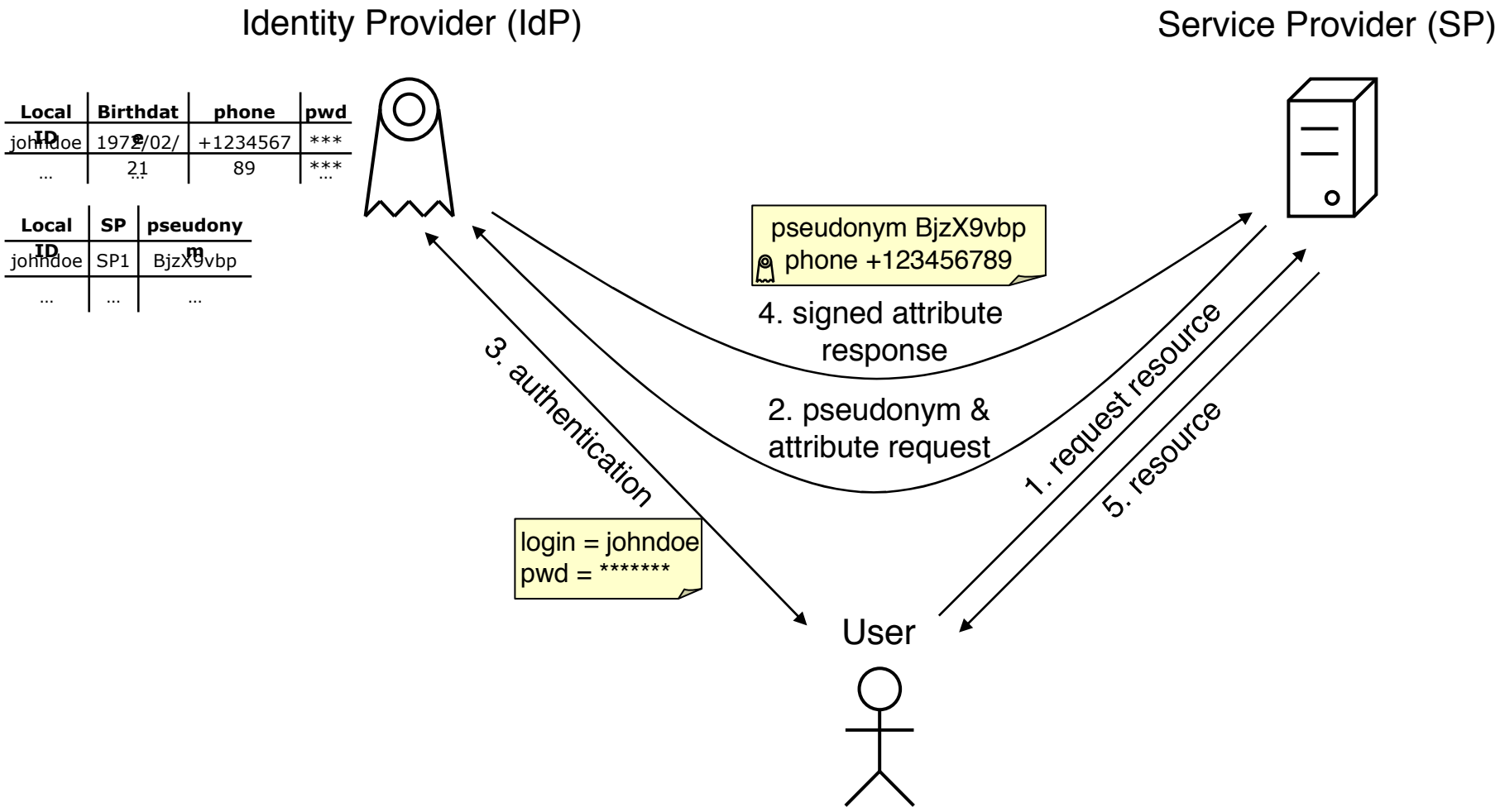


Identity management: SAML

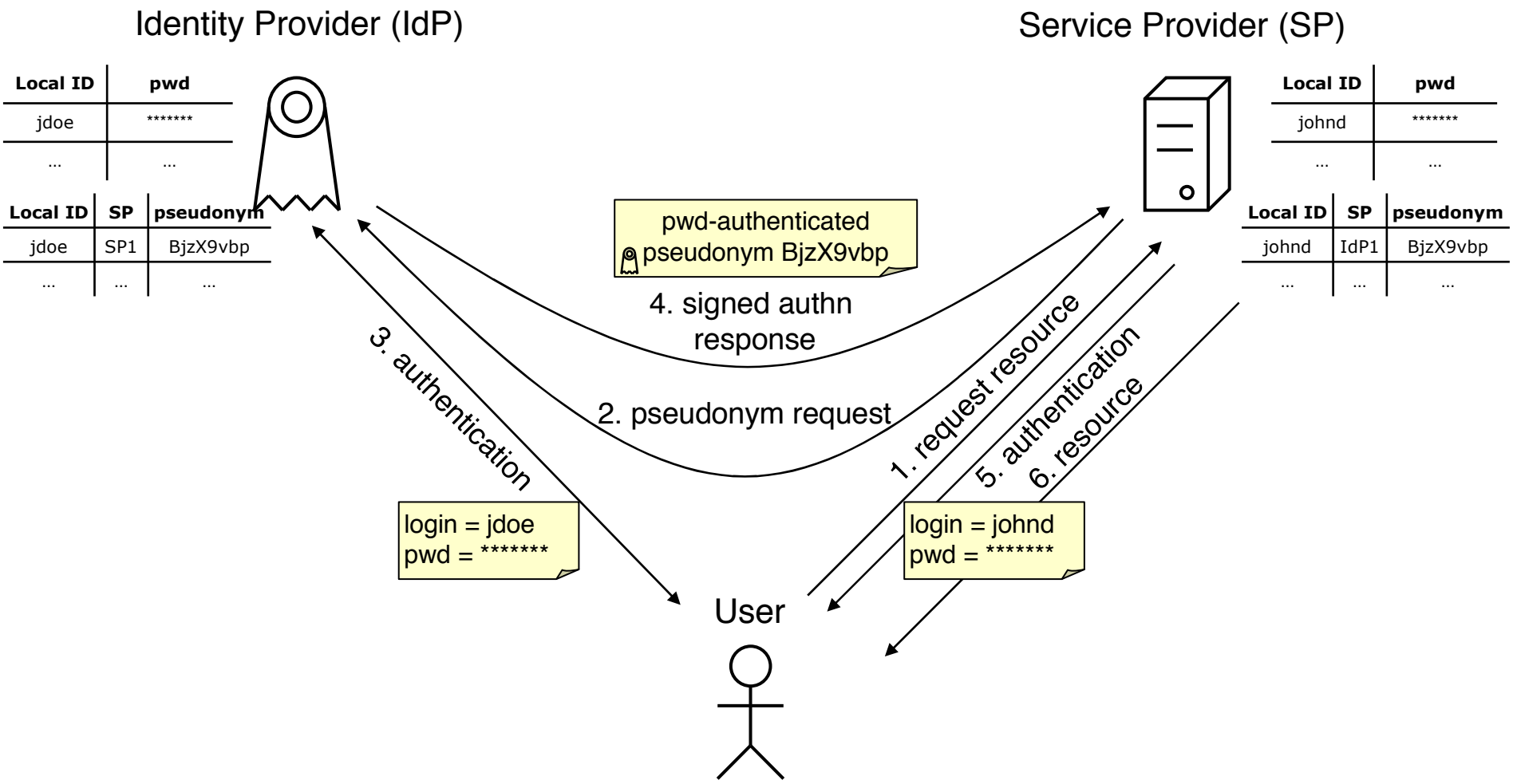
SAML

- Security Assertion Markup Language, by OASIS
- Protocol language for communicating **signed**
  - user authentication information
  - user attribute information
  - authorization decision information
- Main use cases
  - Single sign-on (SSO)
  - Identity federation
  - Attribute provision

SAML use case: attribute provision



SAML use case: identity federation



SAML assertion format

Assertion with unique identifier and time of issuing

SAML authority making the claim

XML signature of assertion by issuer

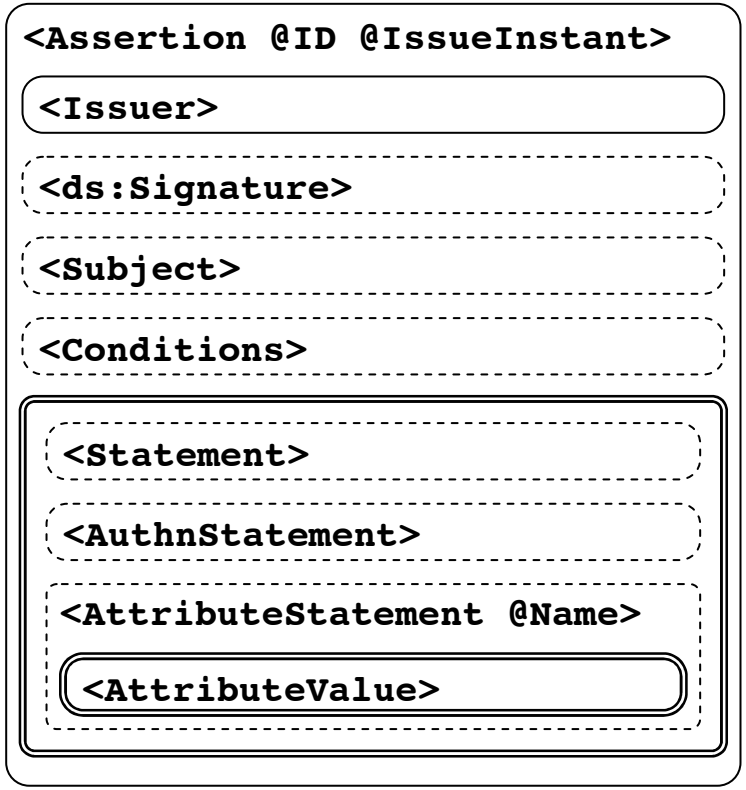
Principal that is subject of the assertion

Constraints on use of assertion (time, audience,…)

Abstract statement type

Statement that (and how) user authenticated at IdP

Statement that subject has specified attribute values.



Access control: XACML

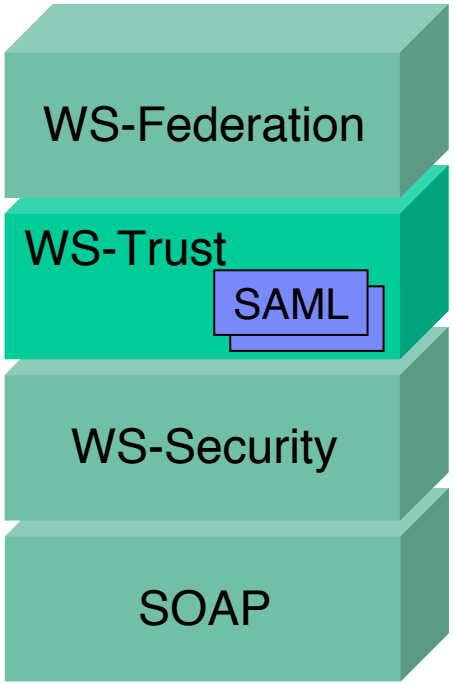
XACML

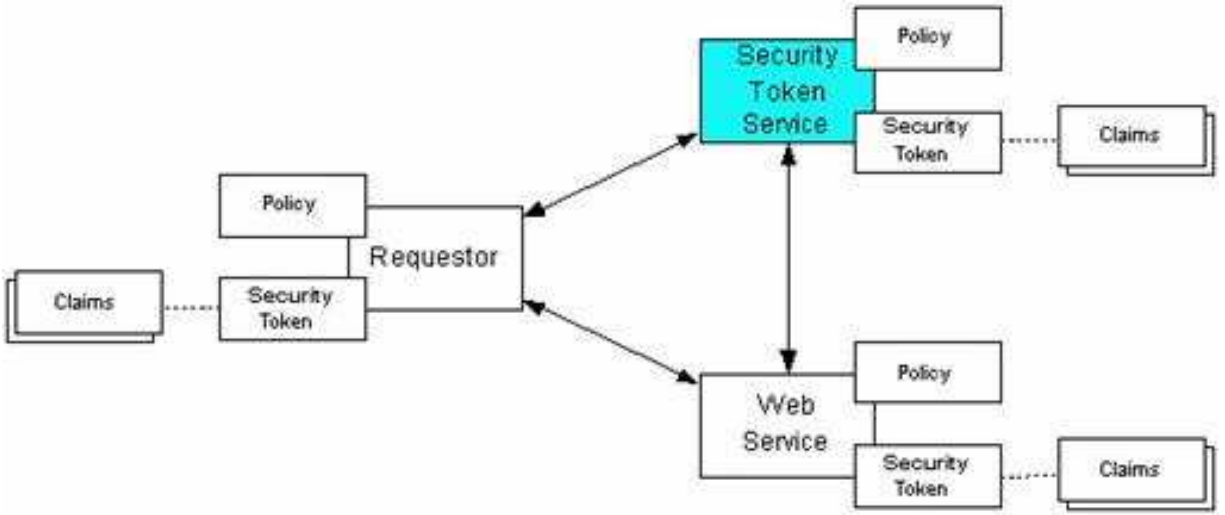
- eXtensible Access Control Markup Language, developed by OASIS
- Industry standard specifying
  - XML-based access control policy language
  - XML-based access request/response protocol language
  - processing model
- Access decisions based on attributes of
  - Subject (e.g., username, role)
  - Protected resource (e.g., file name, URL, content,…)
  - Action (e.g., read, write,…)
  - Environment (e.g., date, time,…)
- Extension points: can define new attributes, data types, functions, obligations, rule/policy combining algorithms

Trust management: WS-Trust

WS-Trust (according to WS-*)

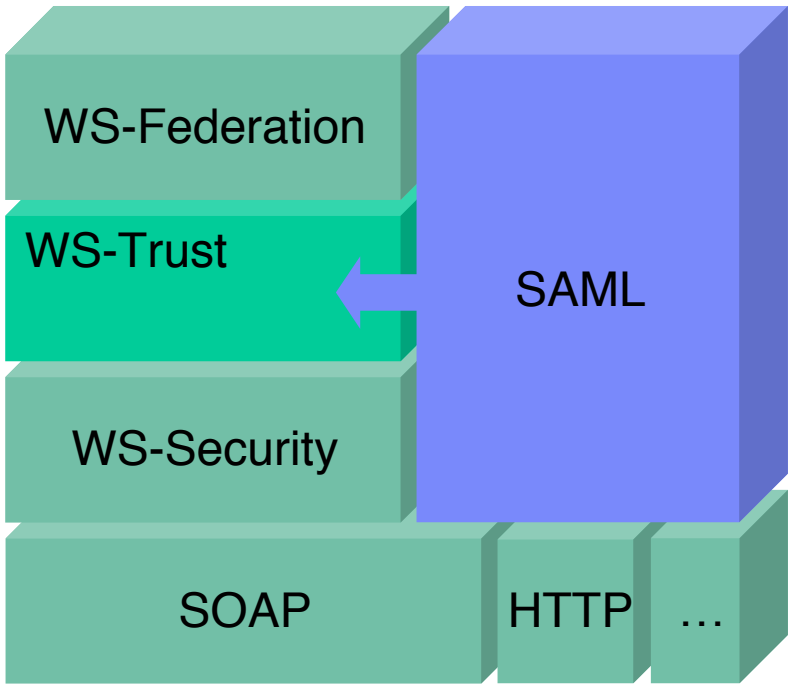
- Goal: trusted SOAP message exchanges through tokens
- Framework for requesting, issuing, and exchanging security tokens, and to broker trust relationships
- Tokens can be in any format: X.509, Kerberos, passwords, **SAML**,…

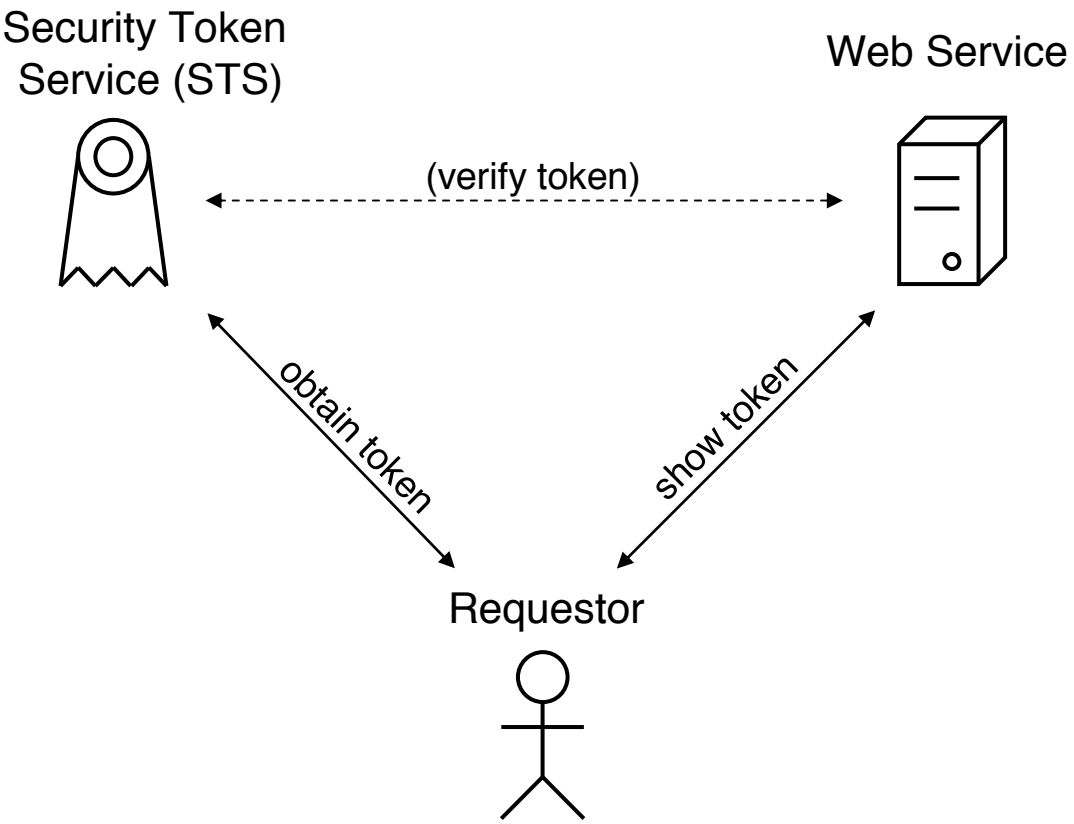




WS-Trust (according to SAML?)

- Goal: trusted SOAP message exchanges through tokens
- Framework for requesting, issuing, and exchanging security tokens, and to broker trust relationships
- Tokens can be in any format: X.509, Kerberos, passwords, **SAML**,...





Identity federation: WS-Federation

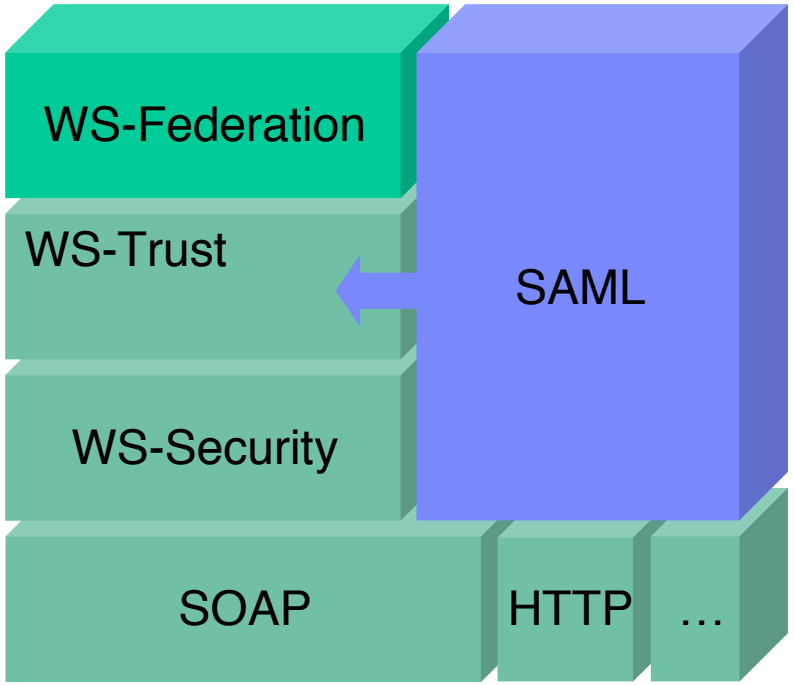
WS-Federation

Goal: federation of security realms

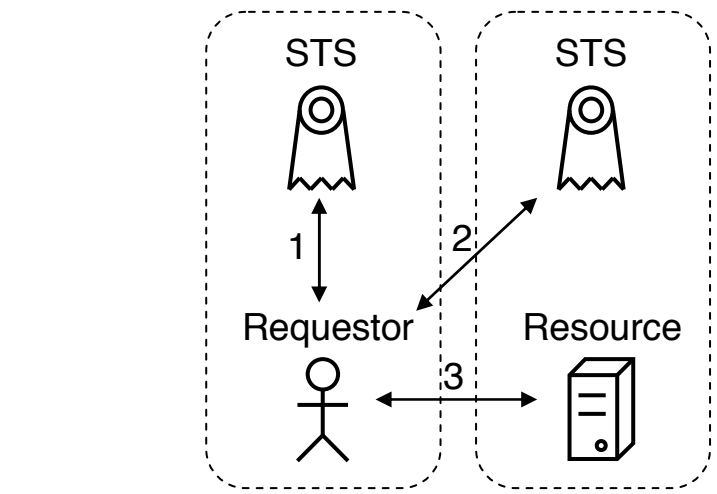
≈ let users from one realm access resources in other realm

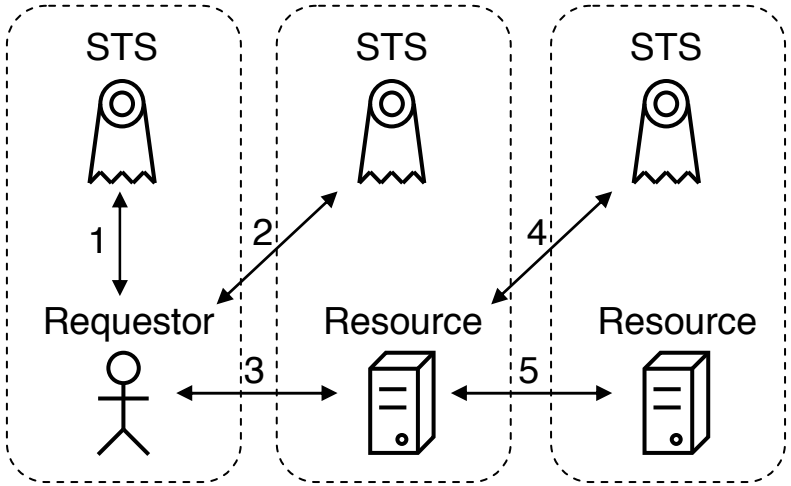
by brokering (i.e., exchanging one for another) assertions about

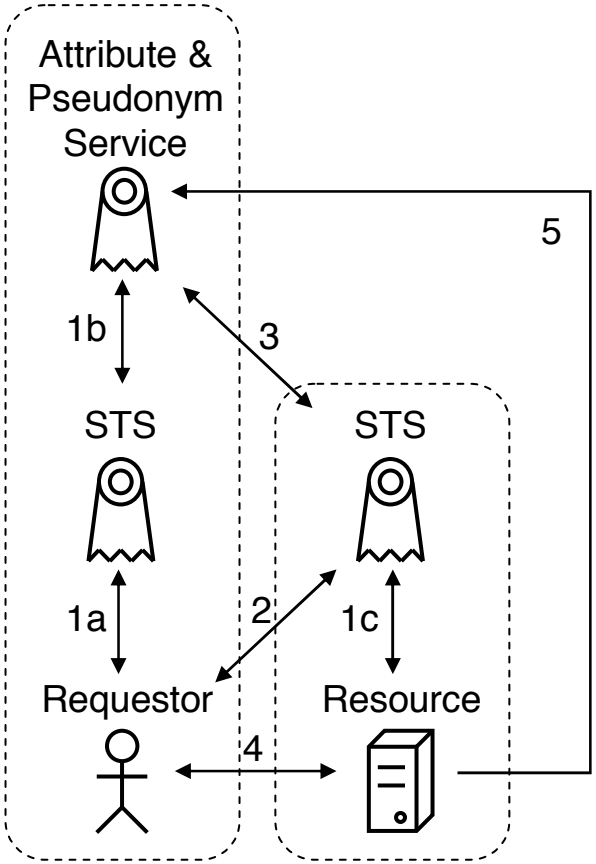
- identity
- attributes
- authentication
- authorization

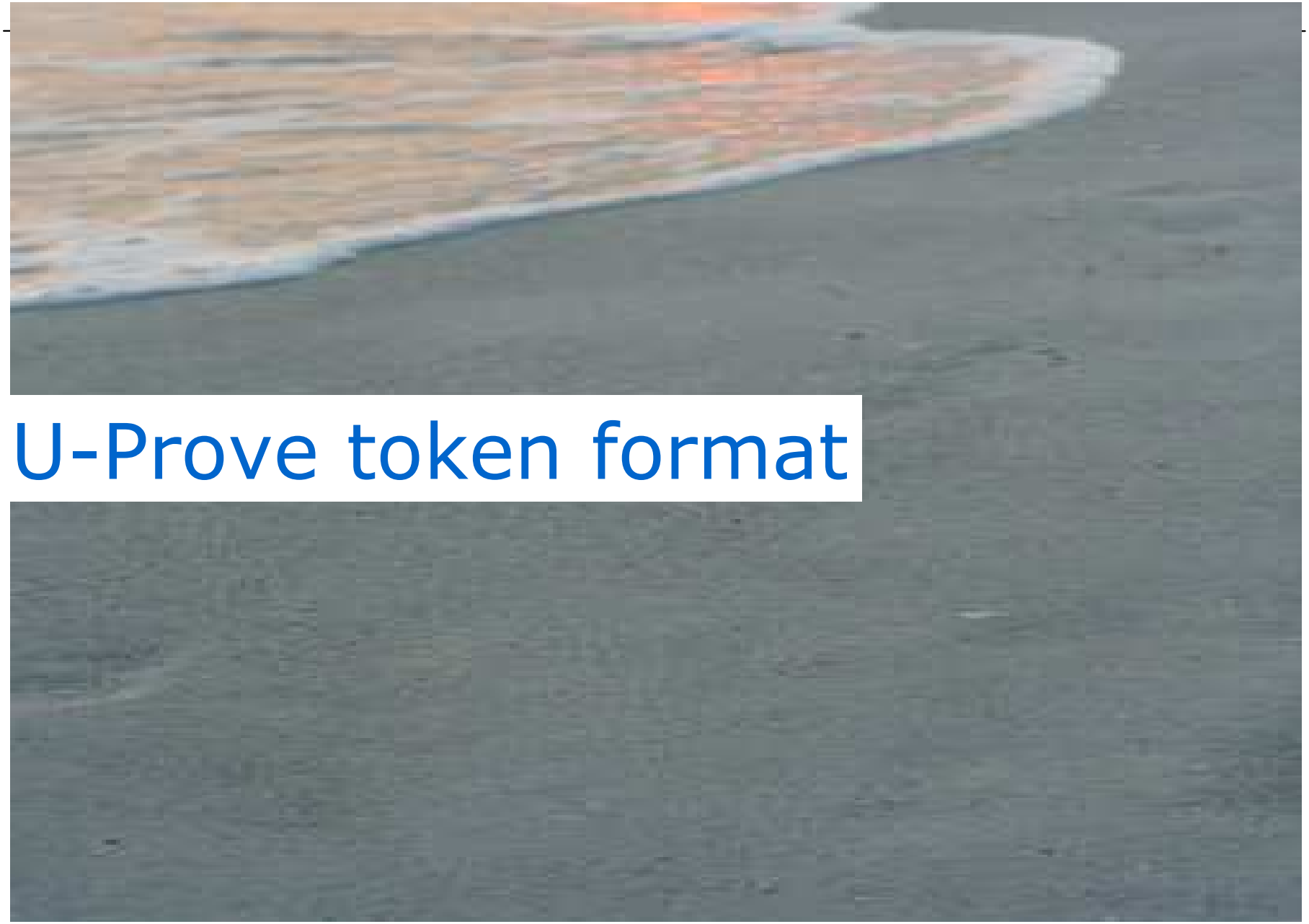


WS-Federation scenarios



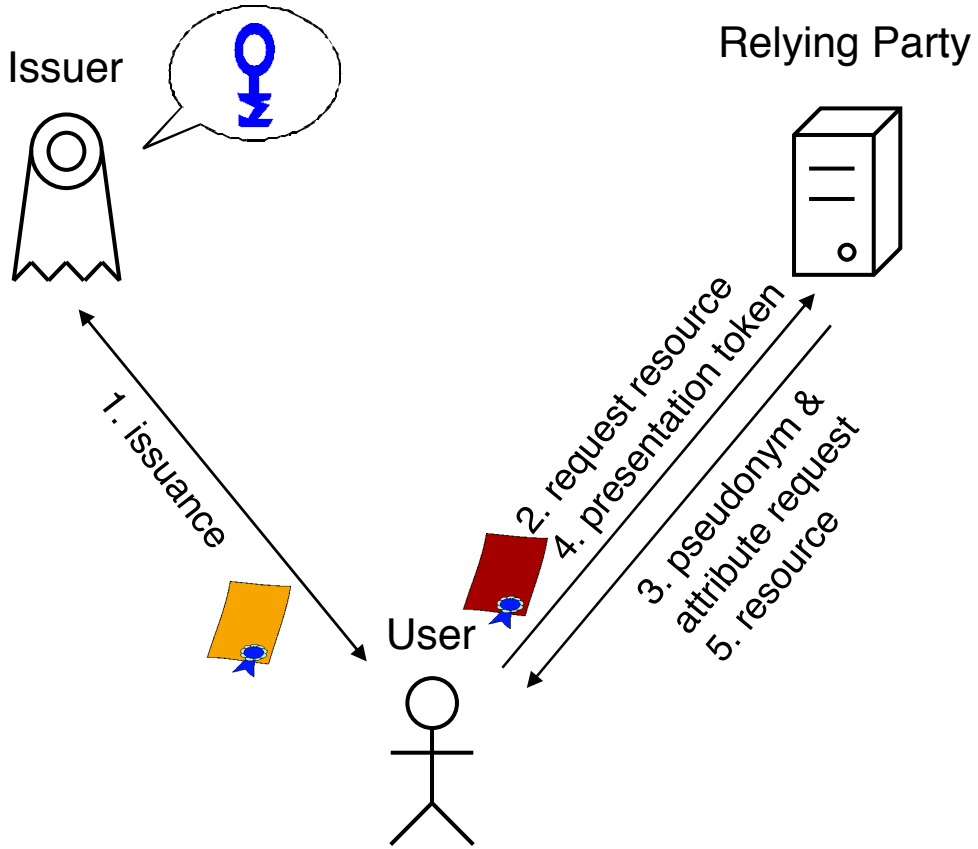




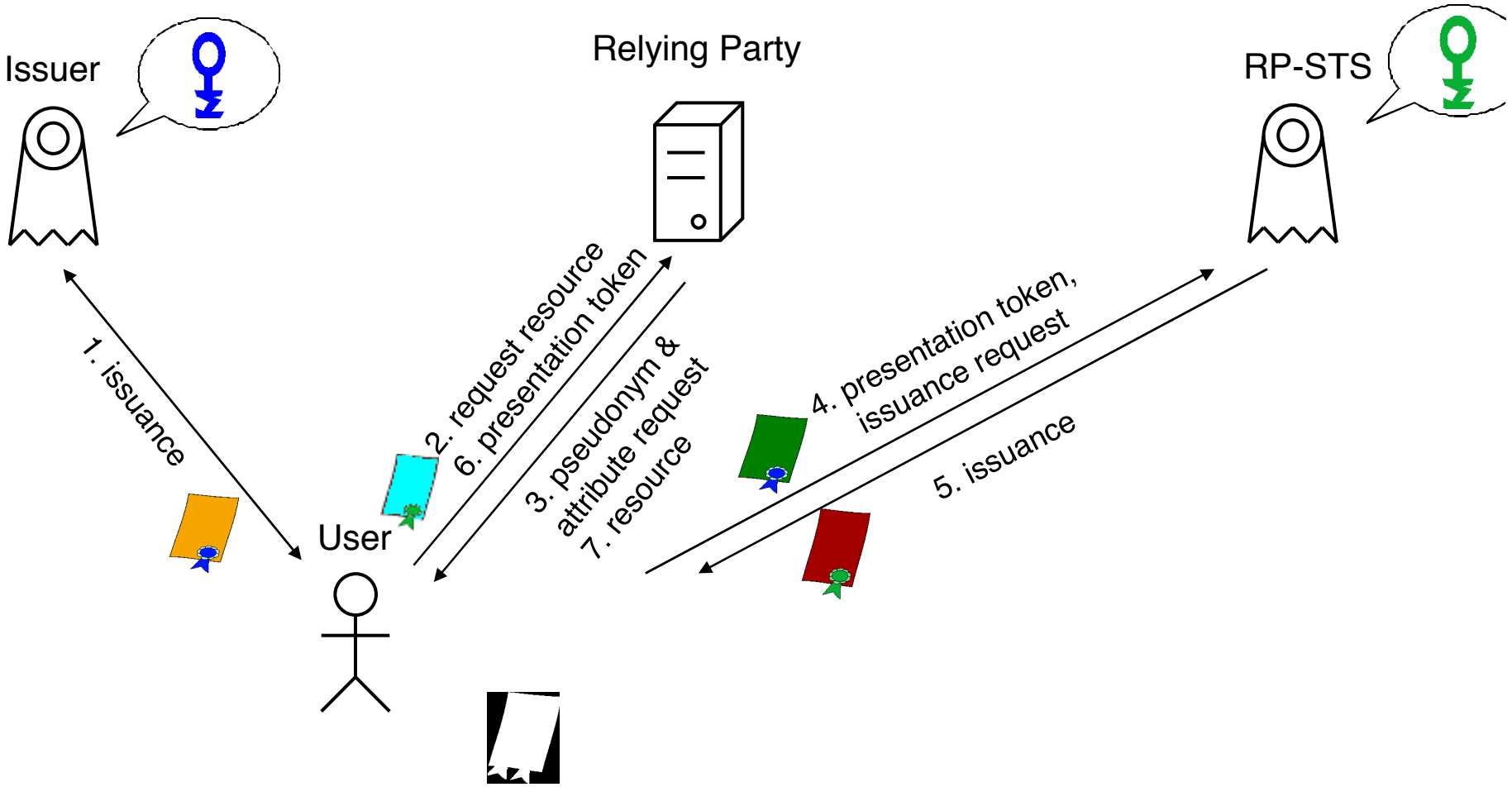


U-Prove token format

SAML / WS-Trust with anonymous credentials



SAML / WS-Trust with anonymous credentials



U-Prove WS-Trust profile

WS-Trust token format for

- issuing (interactive)
- presentation (non-interactive)

Message being signed by this token

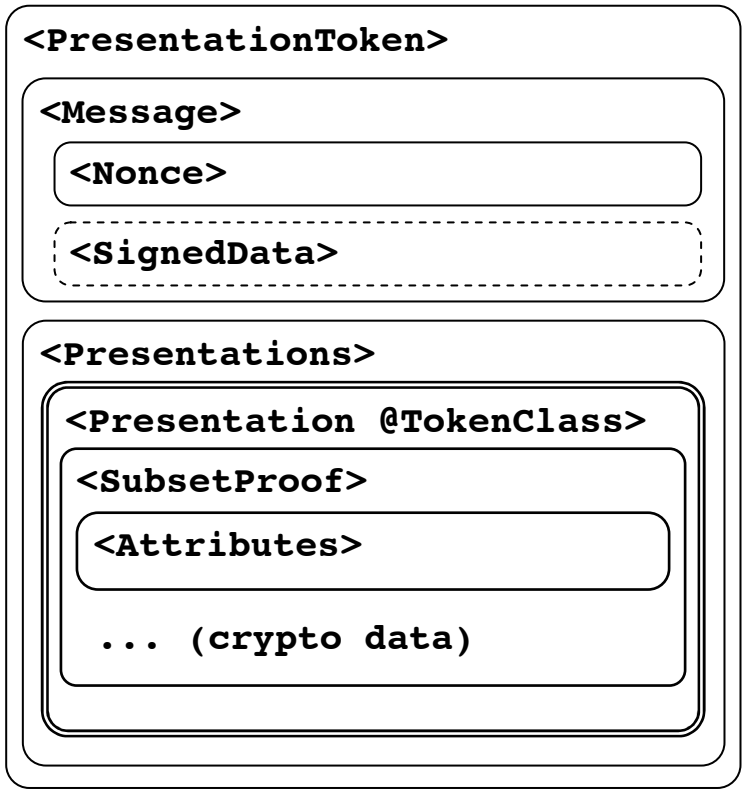
Cryptographic challenge

Application-specific human-readable information

One token can contain one or more presentations

Class is “claim” or “ID”

List of revealed attributes and their values

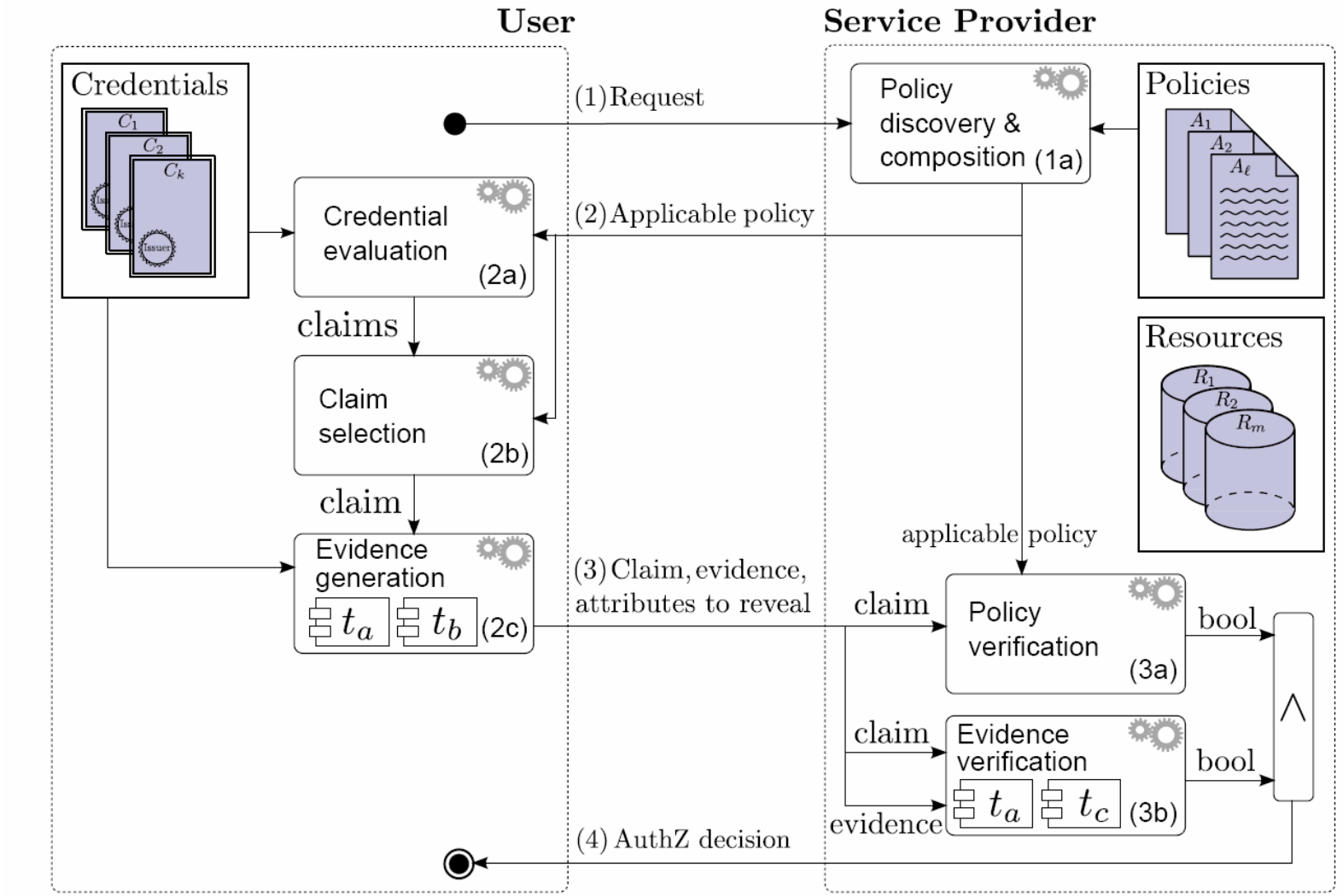


Card-based access requirements language (CARL)

Card abstraction

- Card contains
  - list of attribute-value pairs
  - *pre-evidence*: meta-data to
    - protect attribute integrity
    - prove card ownership
- Card *issuer* vouches for attributes wrt *owner* (identity/authority)
- Hierarchy of card *types:* define attributes contained
- Instantiating technologies: X.509, SAML, CardSpace, OpenID, Kerberos, trusted LDAP, Identity Mixer, U-Prove,…

Card-based access control architecture



Card-based access requirements language (CARL)

Policy and proof presentation in CARL and SAML/XACML

- Policy: requirements on owned cards, e.g.,
  own p::Passport **issued-by** admin.ch, fgov.be, governo.it
  own c::Creditcard **issued-by** visa.com, amex.com
  reveal c.number, c.expdate
  where p.name = c.name ^ p.bdate < today-18Y
  ^ c.expdate > today ^ p.expdate > today+1M

- Authentication = *claim* over owned cards + *evidence*, e.g.,
  own p::Passport **issued-by** admin.ch
  own c::Creditcard **issued-by** visa.com
  reveal c.number = "1234567890"
  reveal c.expdate = "31/12/2012"
  where p.name = c.name ^ p.bdate < 22/03/1993 ^ p.expdate > 22/04/2011

Conclusion

Conclusion

- Identity management/federation standards (SAML, WS-*)
  - traditional public-key cryptography
  - either need IdP for each proof token generation (SAML) or no minimal disclosure (X.509)
- Overall model fits to anonymous credentials
- Extensions or modifications to standards needed
- Common token format: see ABC4Trust