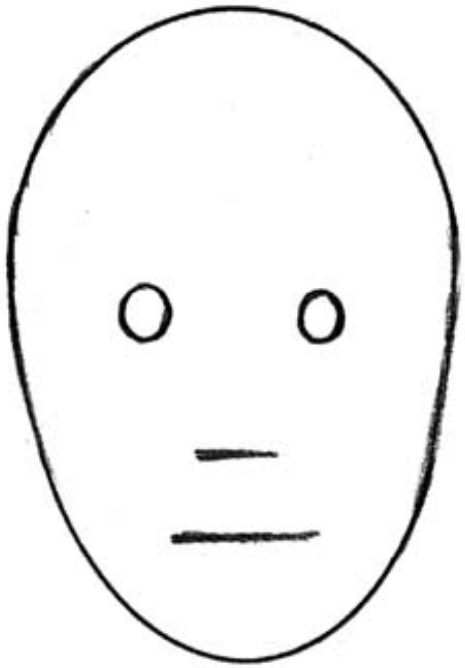
# Managing profiles

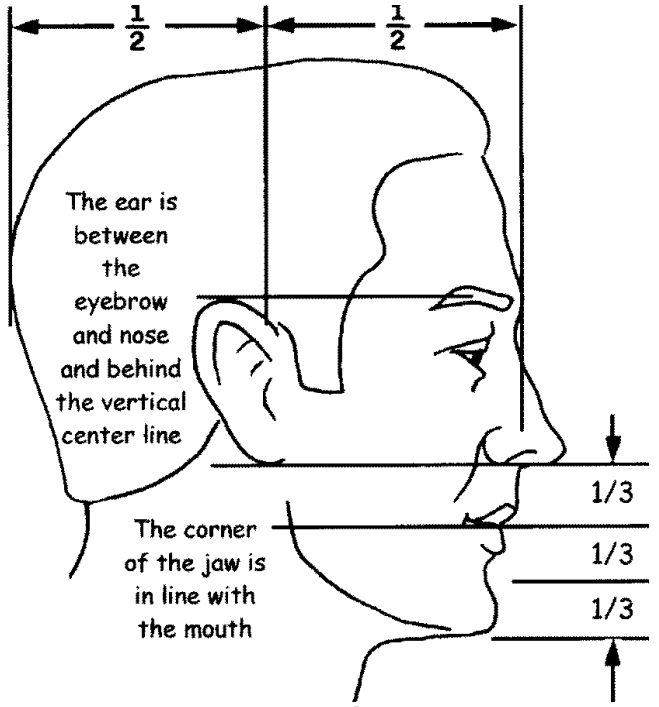
Kantara Initiative work shop
München, 2012_04_17
David Simonsen, david@wayf.dk

SAML specification

SAML profile

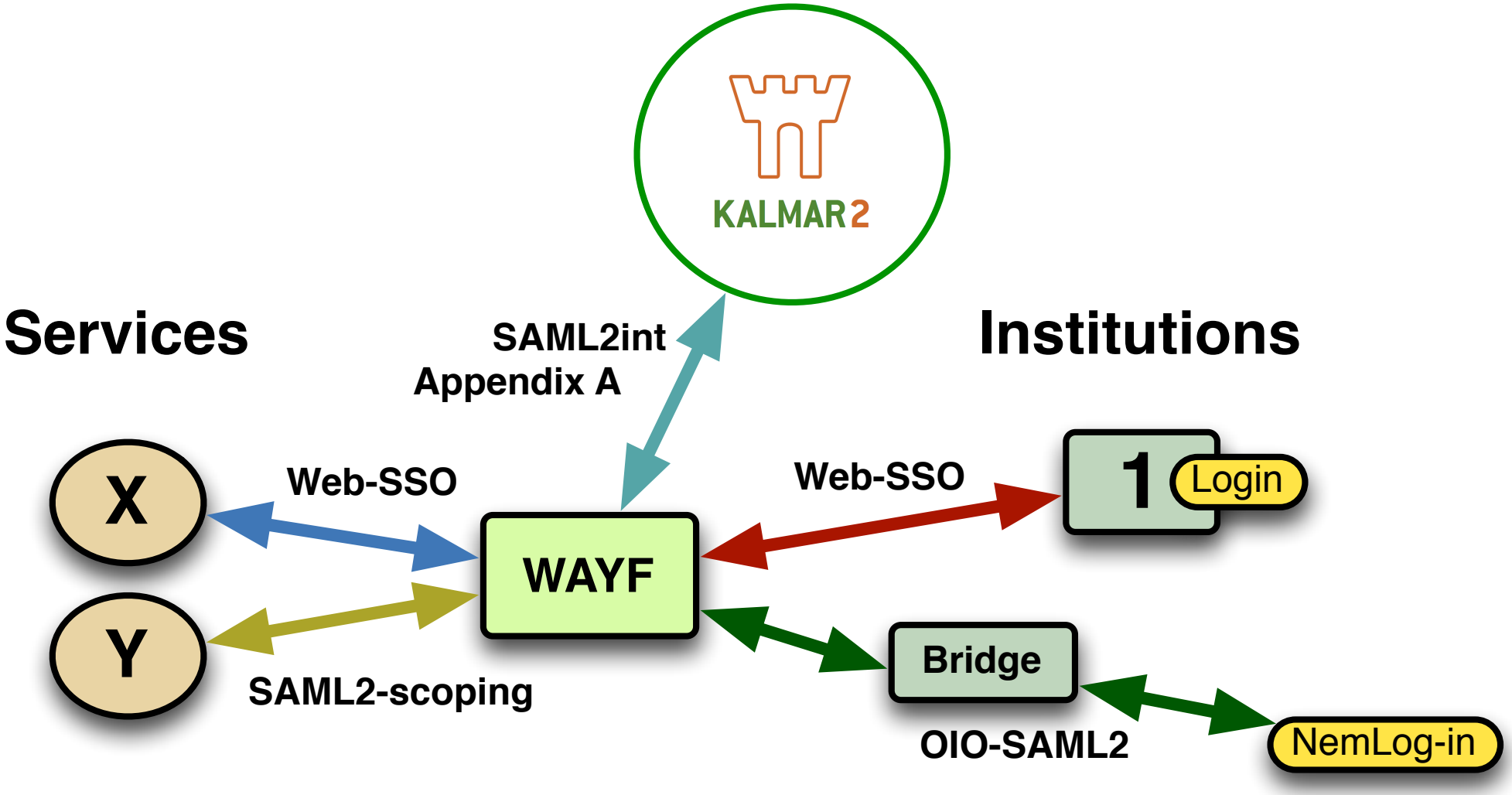


Face

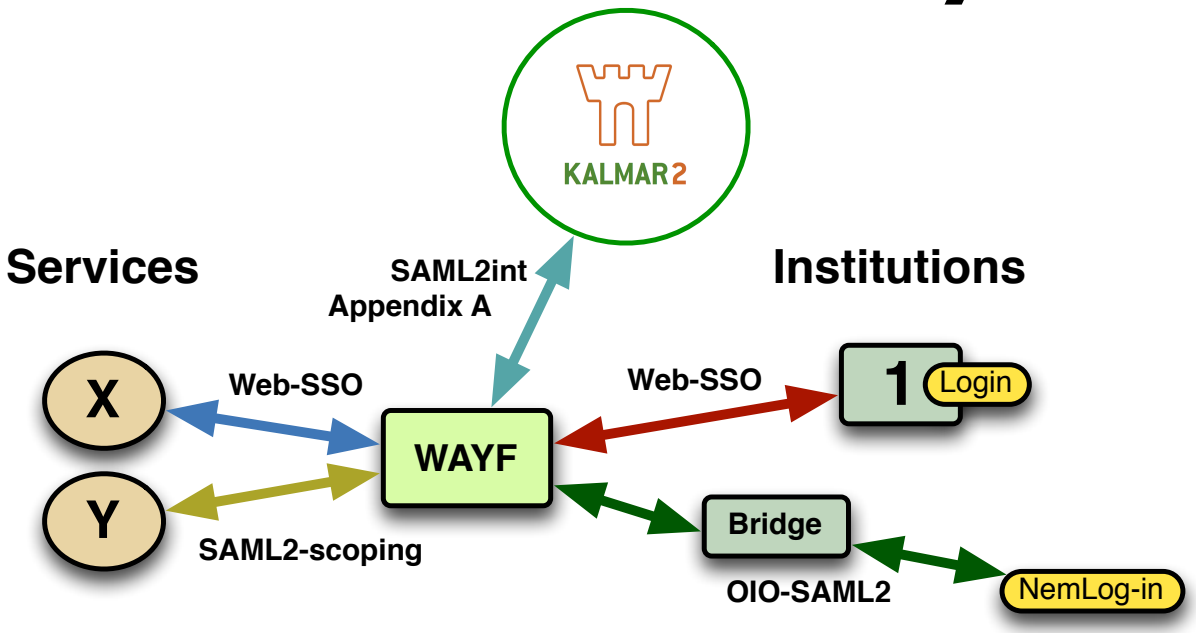



Profile

# WAYF.dk today

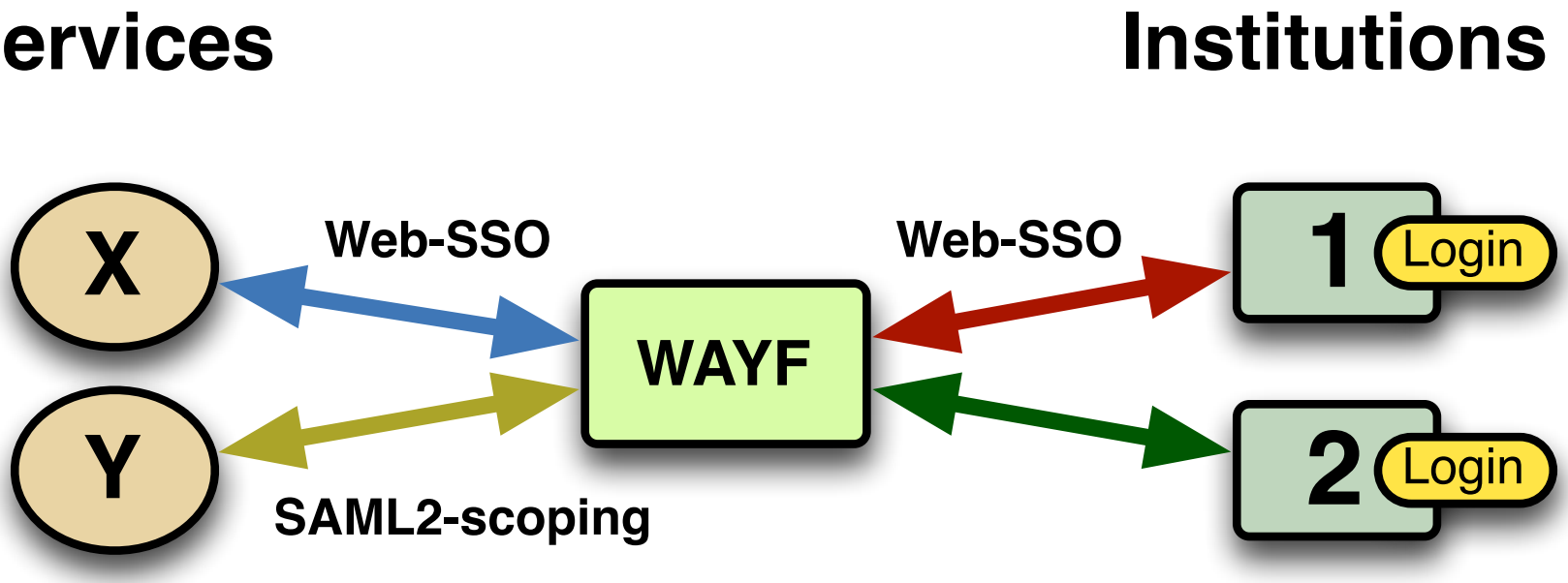


# The story




2007 - added simpleSAMLphp support for the OIO-SAML profile (Danish eGov profile) (encryption etc.)
2008 - WAYF operational, SAML2 Web-SSO in operation
2009 - added support for SAML2 scoping elements, still using Web-SSO profile
2009 - installed OIO-SAML2 bridge for NemLogin (national authentication system)
2008/2009 work on SAML2int profile
2009 - adjustment of WAYF metadata to comply with SAML2int
(Kalmar2 Union, Nordic Inter-federation effort, www.kalmar2.org)
2010 - SAML2int v 0.2, appendix A rewrite
2010 - introduction of Kalmar2 metadata validation service (SAML2int v 0.2)
2011 - adjustment of Kalmar2 metadata from WAYF
2011 - introduction of BIRK, IdP SAML2 proxy end points, possibly multiple BIRKs if profile conflicts
2012 - New NemLogin, operational changes, new reference implementations, no adjustments needed

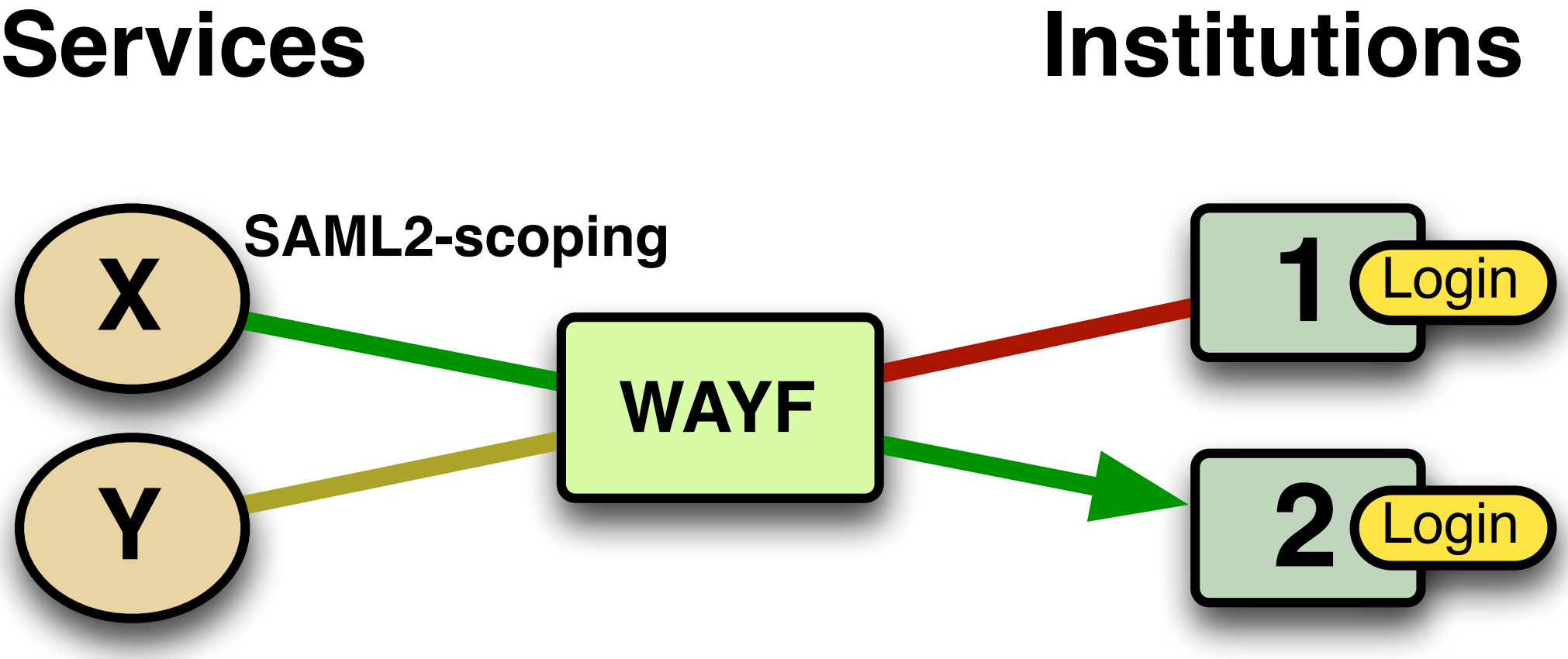
# SimpleSAMLphp Web-SSO profile



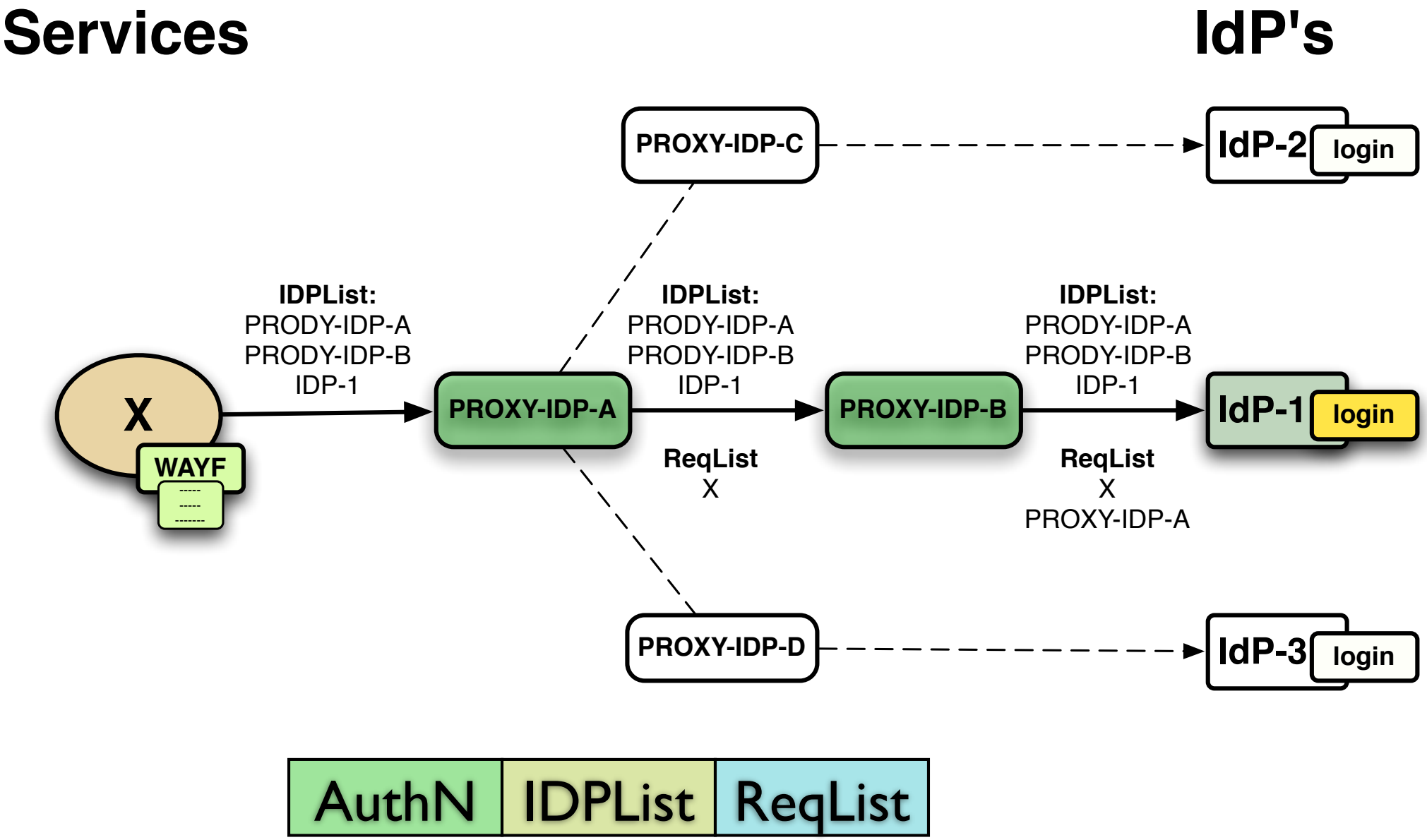

Web-SSO characteristics @ WAYF

- Https encryption
- SAML2 requests not signed
- Responses signed, not encrypted
- Front end Single-Log-out

# SAML2 authN scoping

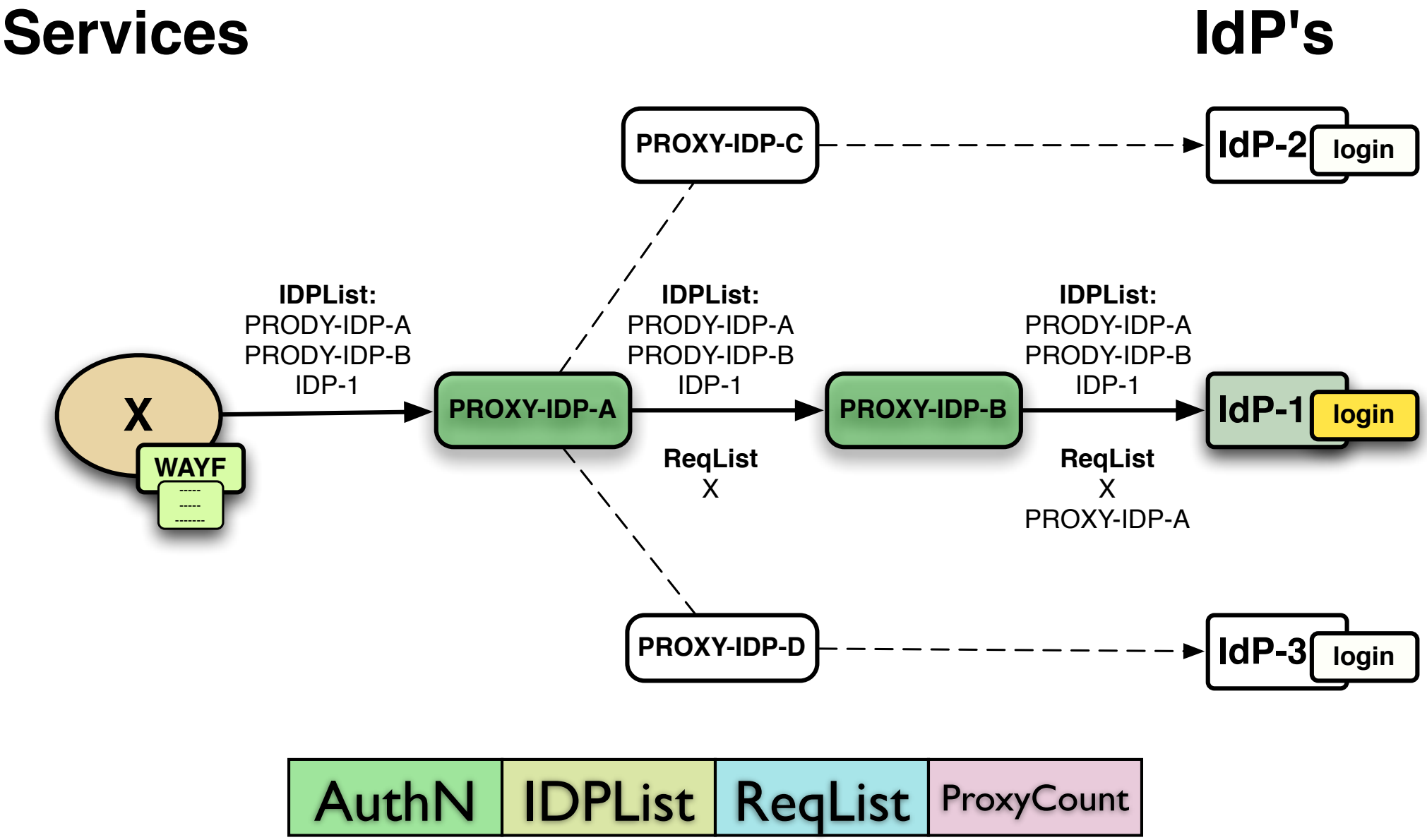


# SAML2 scoping elements




| AuthN | IDPList | ReqList |
|---|---|---|

# SAML2 scoping elements




| AuthN | IDPList | ReqList | ProxyCount |
|---|---|---|---|

# SAML2 authN scoping

Problem
ADFSv2 does not support SAML2 scoping, silently refuses to issue responses

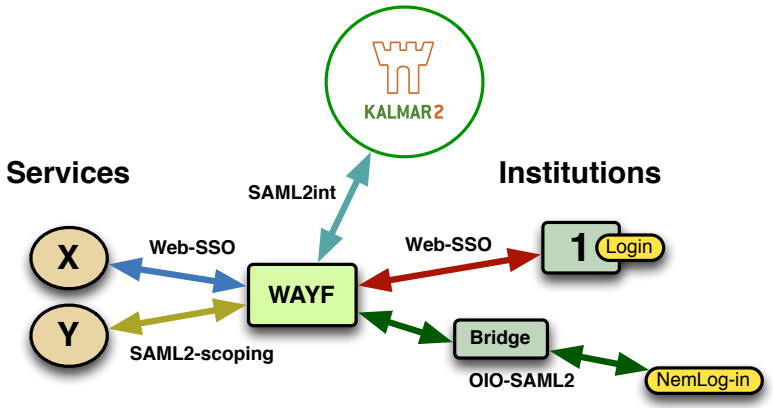
Solution
Break the protocol, recieve-and-remove scoping elements (keep functionality)

# National eID (NemLog-in)

## Profile: OIO-SAML2

Requirements

Encrypted assertions (we added support to SSP)



# SAML2int.org

Written for inter-federation, www.kalmar2.org
(Allows scoping elements)

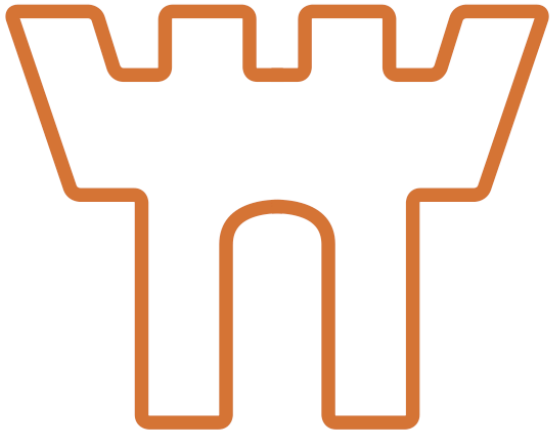
Added
- tech contact info to WAYF metadata

# Kalmar, Appendix A

- Publishing entities from local federation to Kalmar
- SAML 2.0 Web Single Sign-On Profile
- SAML 2.0 Single Logout
- Attributes in Kalmar
- SAML 2.0 Metadata
- Name and description of entities
- Metadata validity period
- Attribute Release Policy
- Extensions
- Scopes
- Monitoring
- User consent
- Identity Provider discovery
- Signing and encryption keys
- Identity Management
- Persistent identifier
- Privacy policy
- Contacts for administrative and technical issues

# Kalmar, Appendix A

- Publishing entities from local federation to Kalmar
- SAML 2.0 Web Single Sign-On Profile
- SAML 2.0 Single Logout
- Attributes in Kalmar
- SAML 2.0 Metadata
- Name and description of entities
- Metadata validity period
- Attribute Release Policy
- Extensions
- Scopes
- Monitoring
- User consent
- Identity Provider discovery
- Signing and encryption keys
- Identity Management
- Persistent identifier
- Privacy policy
- Contacts for administrative and technical issues



KALMAR 2

# Kalmar2, Appendix A

- Org element added (in English as minimum)
  - Diplay name
  - Name
  - URL
- Metadata Validity Period
  - cachedDuration
  - validUntil
- OID-format (of attritbutes) introduced
- Scopes introduced (list of attribute scope values, a 'Shib-thing')
-