Step-up AuthN-as-a-Service

update

Roland van Rijswijk - Deij

roland.vanrijswijk@surfnet.nl

So where are we?

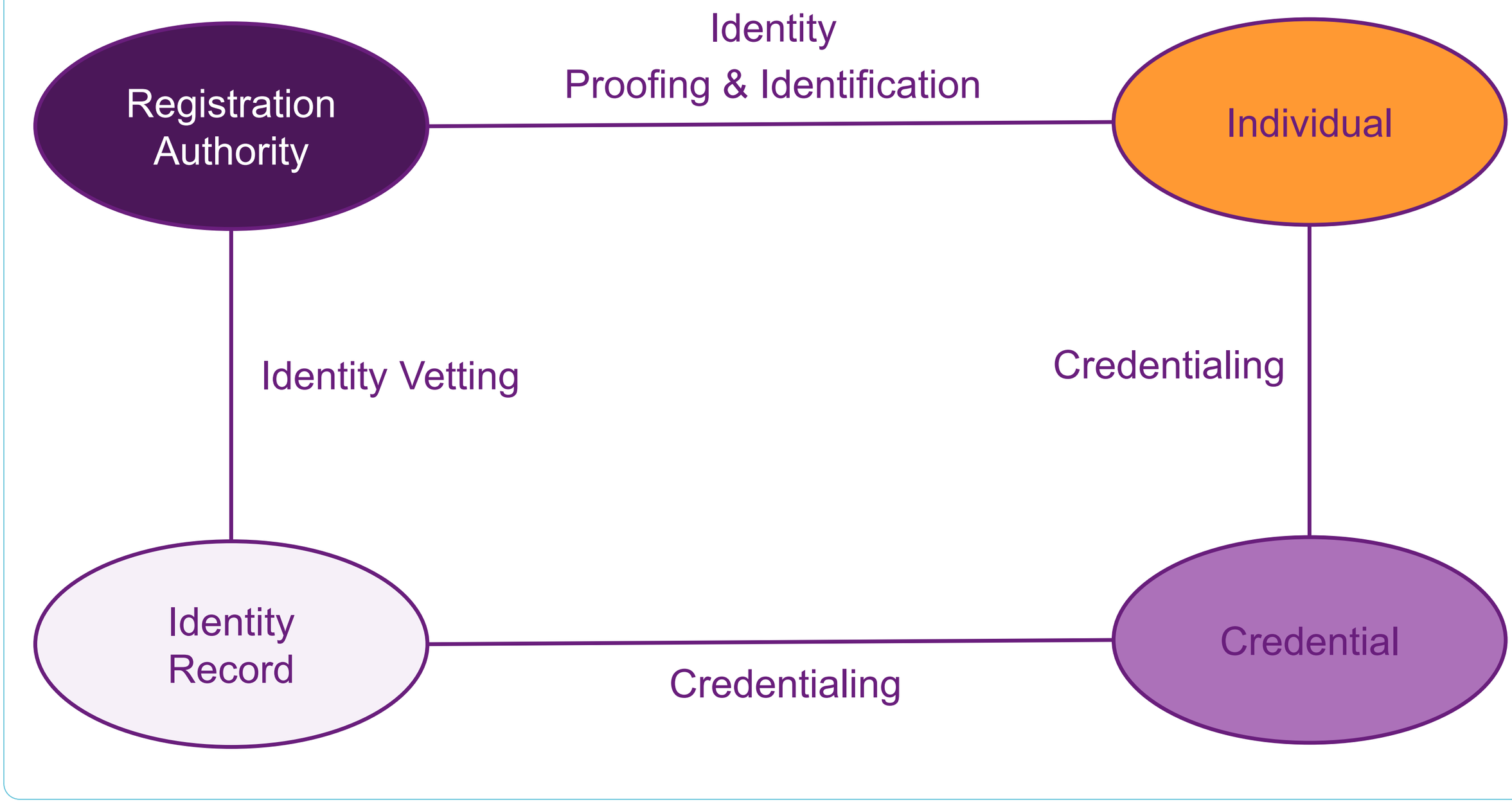
- **Step-up Authentication-as-a-Service:**
  - 2-factor AuthN as add-on to existing federation
  - Goal: easily extend existing federated services with minimal changes to IdP and SP
  - Support range of 2-factor AuthN solutions

Project phase	Done/planned
Interviews with constituency	Q1-Q2 ✔
Market scan	Q1-Q3 ✔
Architecture & process study	Q2-Q3 ✔
Implementation go/no go	Q4
Implementation	Q1-Q2 2013

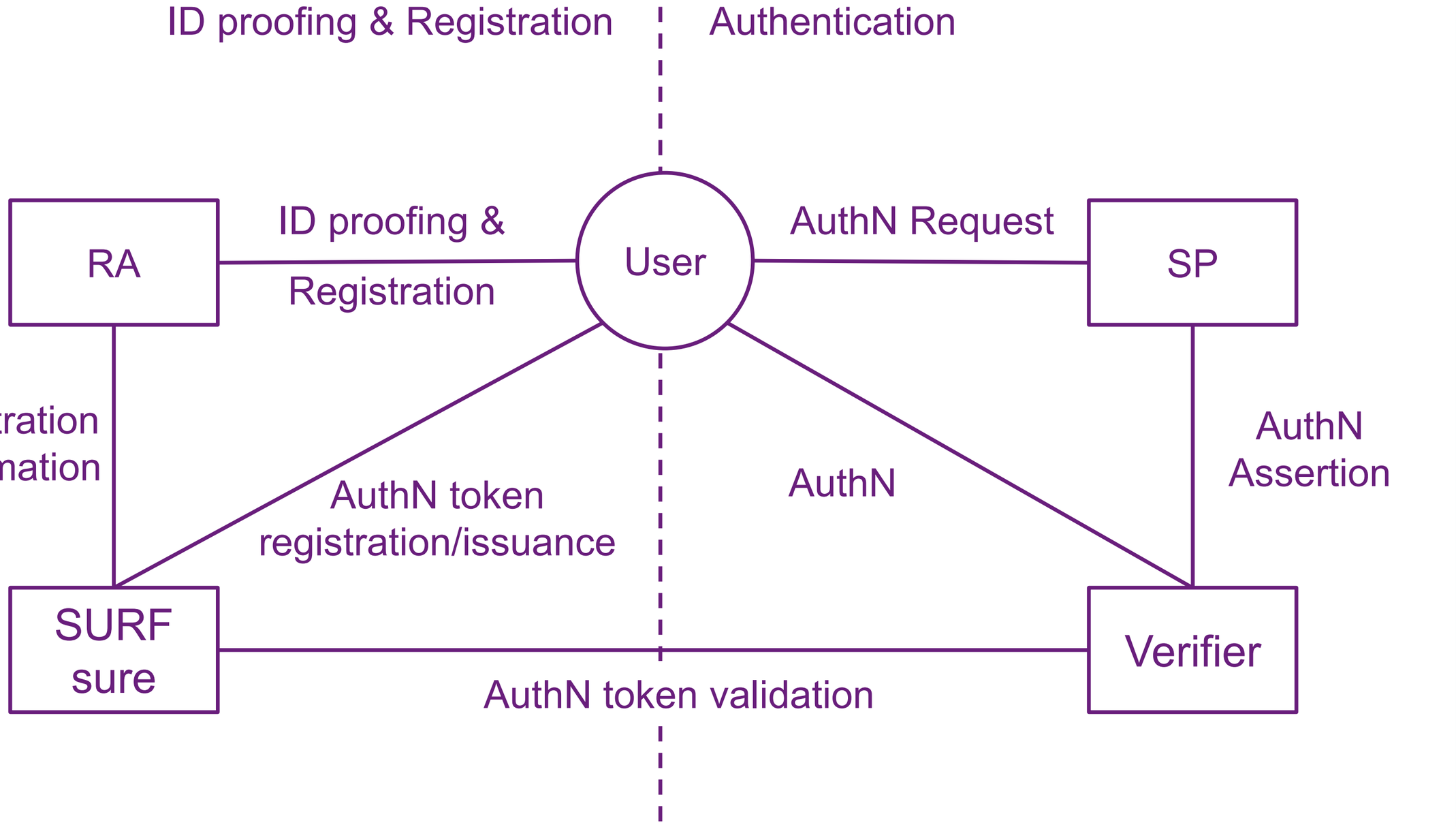
Constituency feedback

- Interest from diverse audience
  - Universities, polytechnics, academic/teaching hospitals, research institutes
- User groups vary in size from tens of users to thousands of users
- Mostly organisation-internal use cases
  - Student grade administration, HR systems, etc.
  - Applications hosted both internally as well as in the cloud
- Most organisations prefer SMS or app-tokens

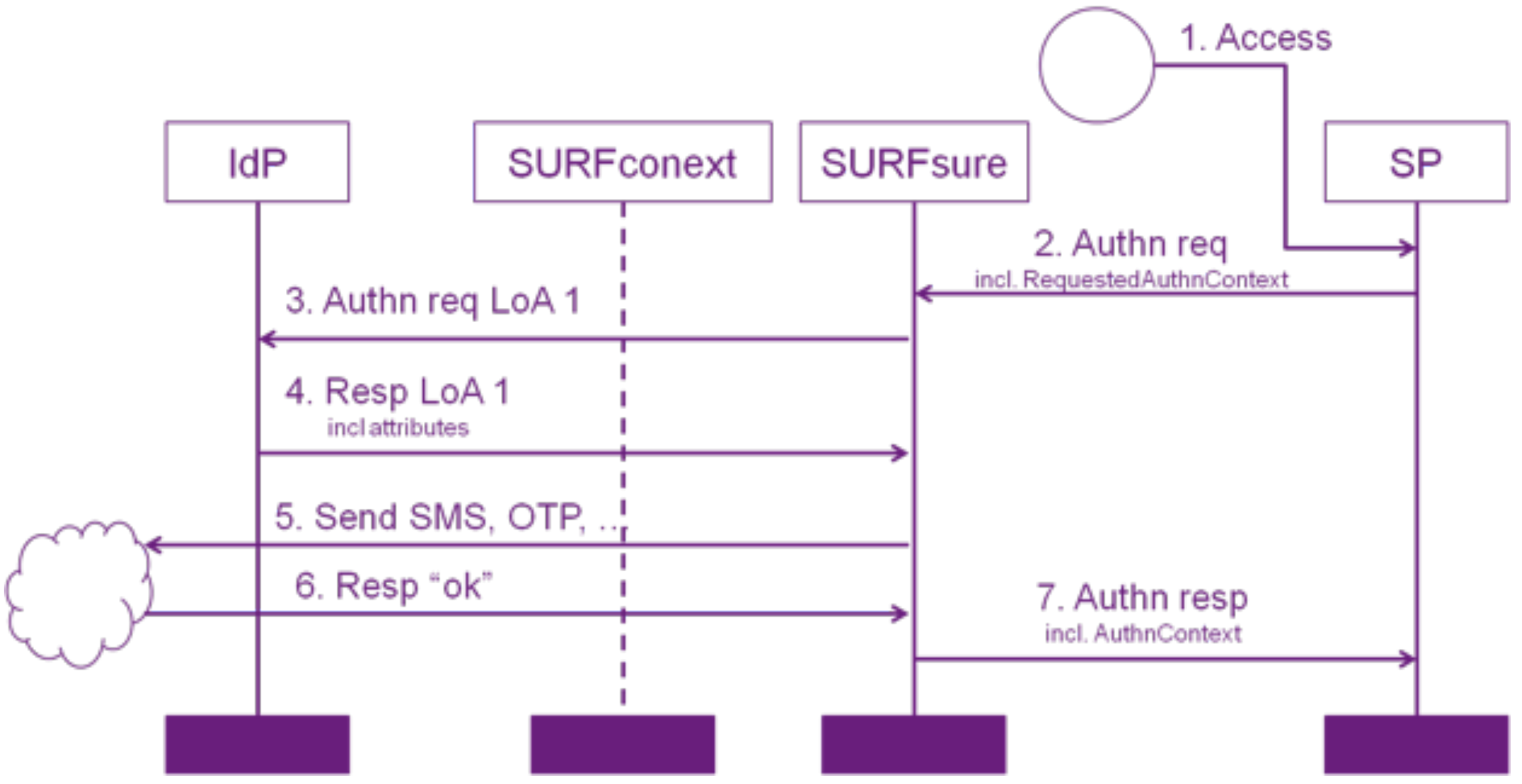
Terminology



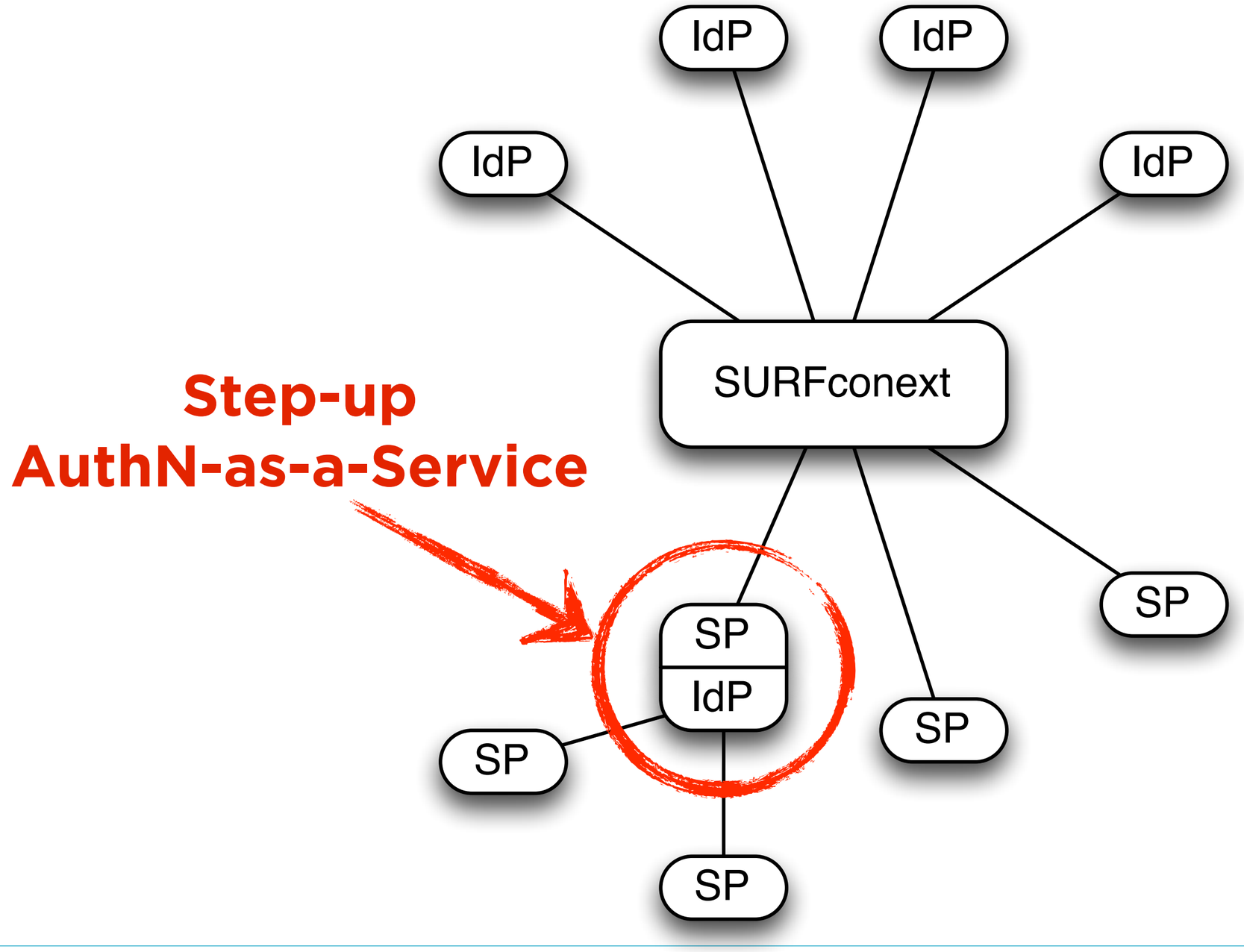
Model for registration and authentication



Service as a SAML proxy



Position vis-a-vis federation



Level-of-Assurance process side

- We use the criteria from ISO 29115 (draft) for the registration process requirements:

LoA	Requirements for registration
1	None
2	Information from an authoritative source
3	Information from an authoritative source and verification
4	Information from an authoritative source, verification and entity witnessed in person

Level-of-Assurance authentication

- We use the criteria from ISO 29115 (draft) for the authentication requirements:

LoA	Requirements for authentication	Example
1	Minimal assurance about the authentication mechanism	Password
2	Like LoA 1 + secure protocol; controls in place to prevent eavesdropping and online guessing attacks; protect stored credentials	SMS OTP
3	Like LoA 2 + secret information exchanged in the protocol must be cryptographically protected	tiqr, other apps
4	Like LoA 3 + tamper-resistant hardware must be used for storage of secrets; all sensitive information must be cryptographically protected	Physical token

Side note: the ‘Google’ use case

- Google, Facebook and others are offering 2-factor on their free services
- User self-registers cell phone or token app
  - Can be used to authenticate from “untrusted” location or to reset password
- So: no assurance, but much easier for the user
- Difference with ‘SURFsure’: protecting user asset vs. protecting organisational assets

Signalling the LoA in SAML

- Several attempts at solving this problem:
  - SAML Authentication Context specification (complicated, verbose)
  - SAML Authentication Context Classes (pre-defined AuthNContext specifications, simple, well-defined)
  - SAML Identity Assurance Profiles (further limits authentication context class reference, refers to external governing agreements like NIST SP800-63 or ISO 29115)

- We choose the last solution, and will use URNs from the registry proposed in RFC 6711 (thanks Leif :-))

Registration process

- Registration will take place at the user's home institution
- 1 trusted RA per organisation appointed by SURFnet, can delegate to others in organisation
- User self-registers token, then goes to RA for face-to-face with ID card and token

Supported tokens in version 1

tiQr

Future plans

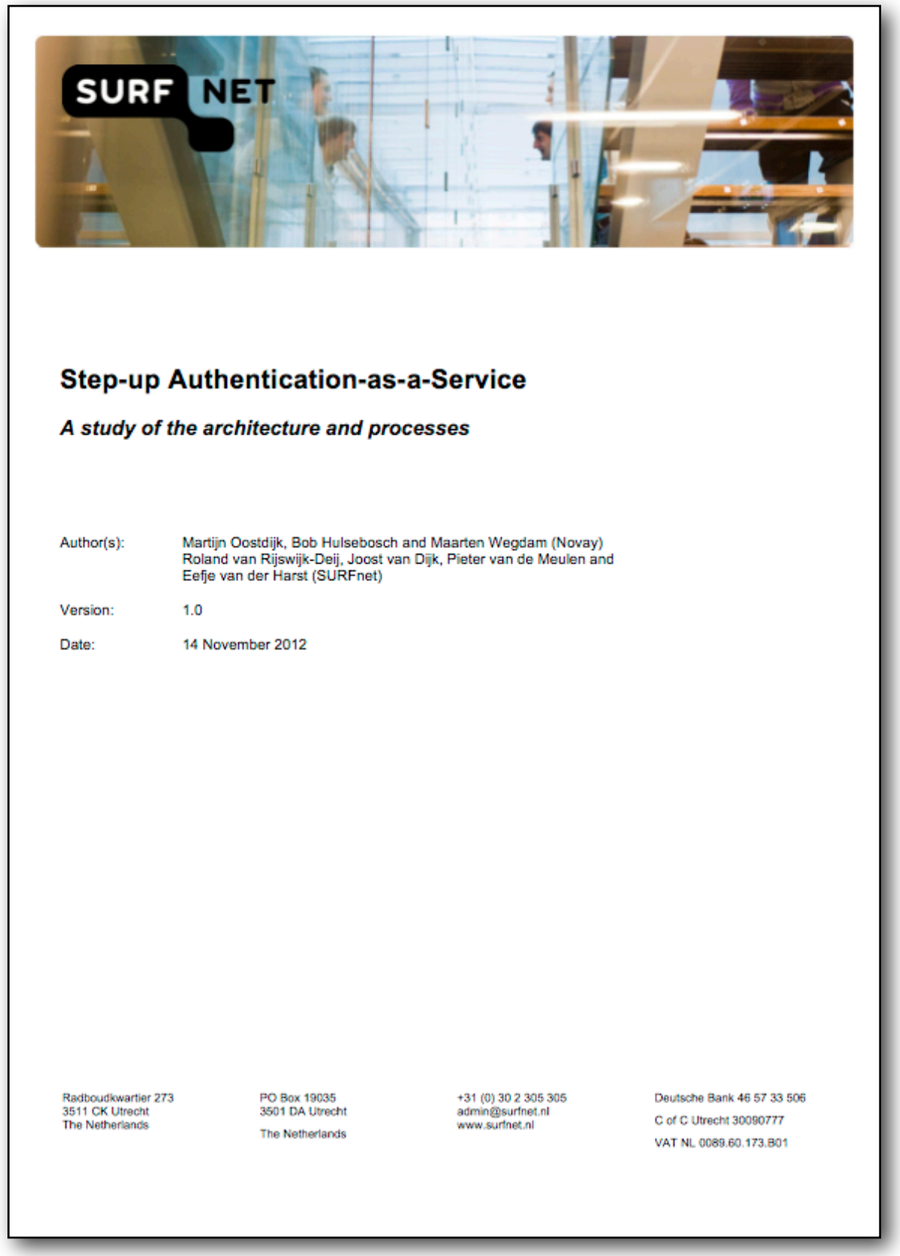
- Support use of tokens for Dutch eGovernment programme "*eHerkenning*"
- Support cloud offerings from token vendors like Vasco and SafeNet
- Extend with RADIUS support (perhaps)

More information

- Our architecture study document is available on request (will be released after “go/no go” decision)

- Looking to collaborate; Come talk to me!

  (already in contact with UnitedID)


SURF NET

Step-up Authentication-as-a-Service

A study of the architecture and processes

Author(s): Martijn Oostdijk, Bob Hulsebosch and Maarten Wegdam (Novay)
Roland van Rijswijk-Deij, Joost van Dijk, Pieter van de Meulen and Eefje van der Harst (SURFnet)

Version: 1.0

Date: 14 November 2012

Radboudkwartier 273
3511 CK Utrecht
The Netherlands

PO Box 19035
3501 DA Utrecht
The Netherlands

+31 (0) 30 2 305 305
admin@surfnet.nl
www.surfnet.nl

Deutsche Bank 46 57 33 506
C of C Utrecht 30090777
VAT NL 0089.60.173.B01

roland.vanrijswijk@surfnet.nl

nl.linkedin.com/in/rolandvanrijswijk

@reseauxsansfil

Questions? Comments?