Step-up-authetication as a service

Internet2 Annual Meeting 2013

Pieter van der Meulen
Technical Product Manager

SURF NET

Introduction

- Step-up-authentication as a service (SuaaS)
- Business case and requirements
- Architecture
- Registration process
- Next steps

Business case

- Demand for stronger authentication
  - Institutional IT systems
    - Financial, student, HR
    - VPN
  - Access to databases with privacy sensitive data
- Offer as a service
  - Reduce cost per use case

Requirements

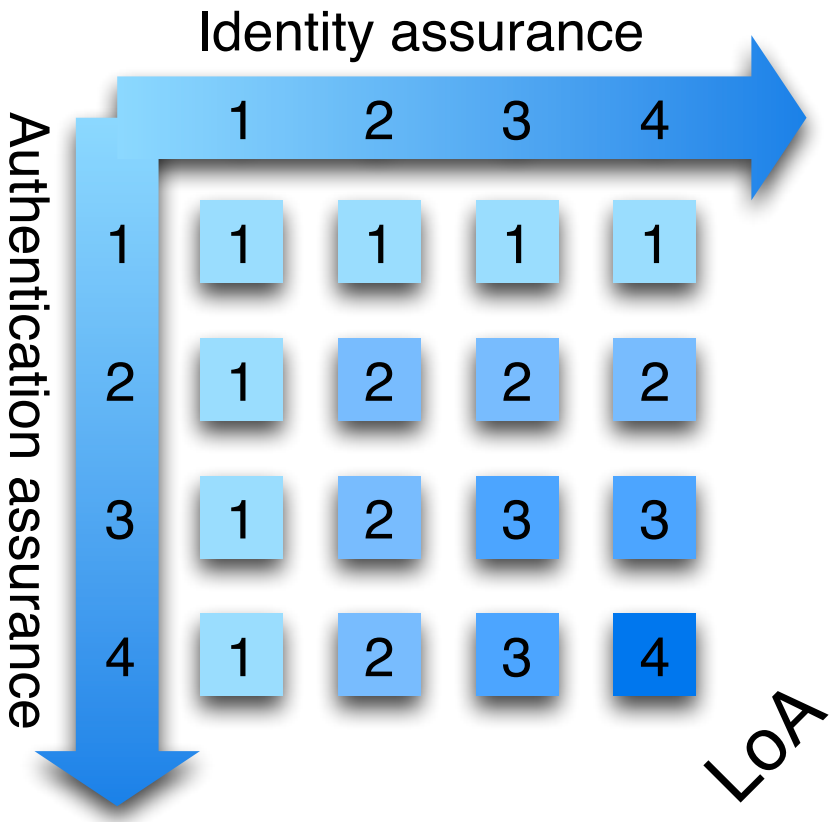
- Offered as a service
- SAML federation
- Support
  - SMS
  - tiqr
  - YubiKey
- Open
  - vendor neutral
  - Standards based

Level of Assurance (LoA)

- Standards define four LoAs
  - NIST SP 800-63, STORK, ISO 29115
- Levels define confidence in the asserted identity
  - LoA 1 - Little or no confidence
  - LoA 2 - Some confidence
  - LoA 3 - High confidence
  - LoA 4 - Very high confidence

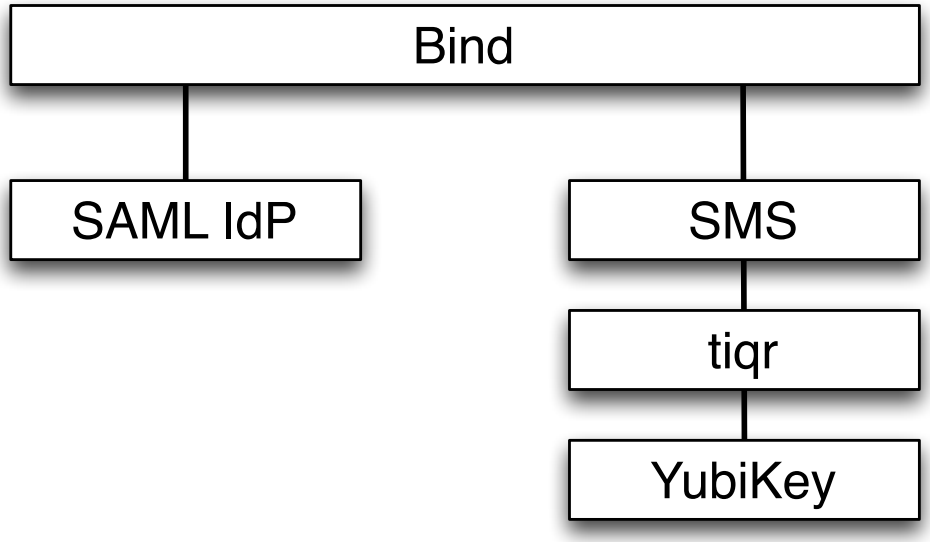
Level of Assurance (LoA)

- LoA is the combination of
  - Identity assurance
  - Authentication assurance



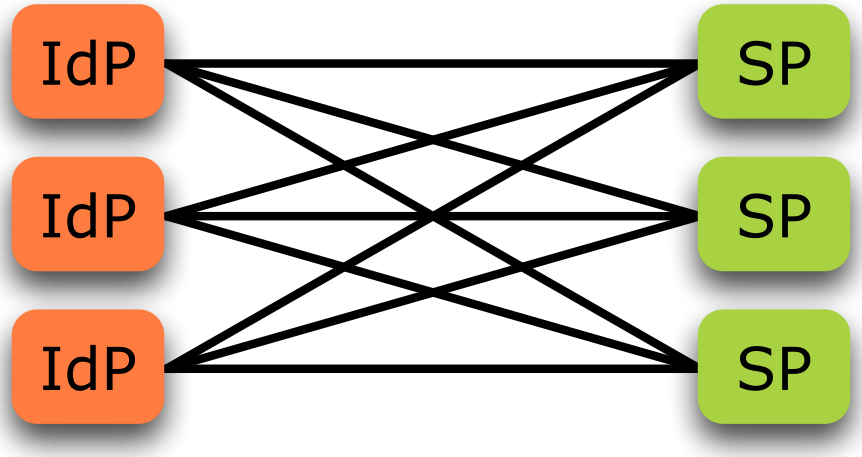
Architecture

- Create a stronger credential from
  - existing institutional authentication (SAML)
  - and second factor: Phone, Token



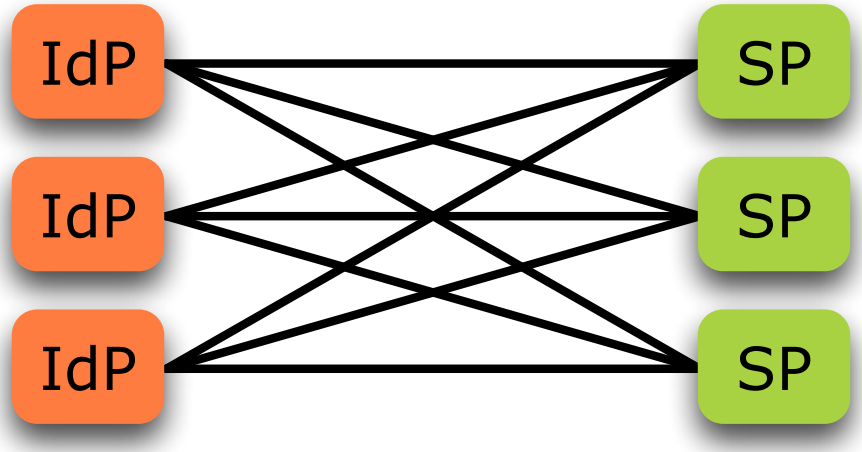
Architecture

- (InCommon) SAML federation

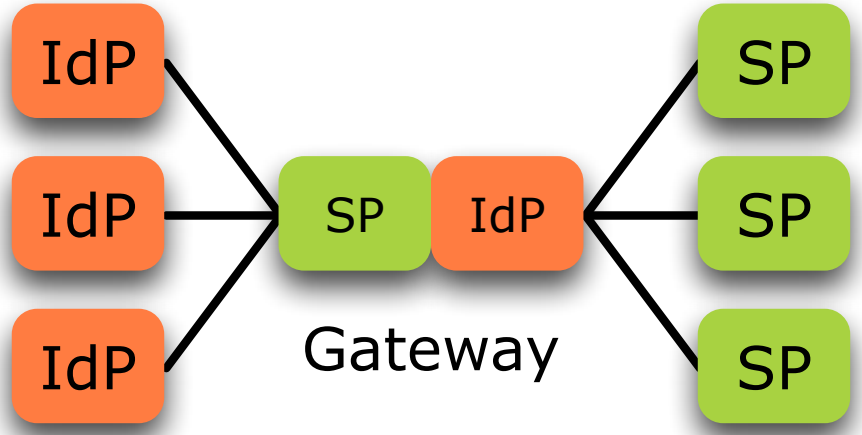


Architecture

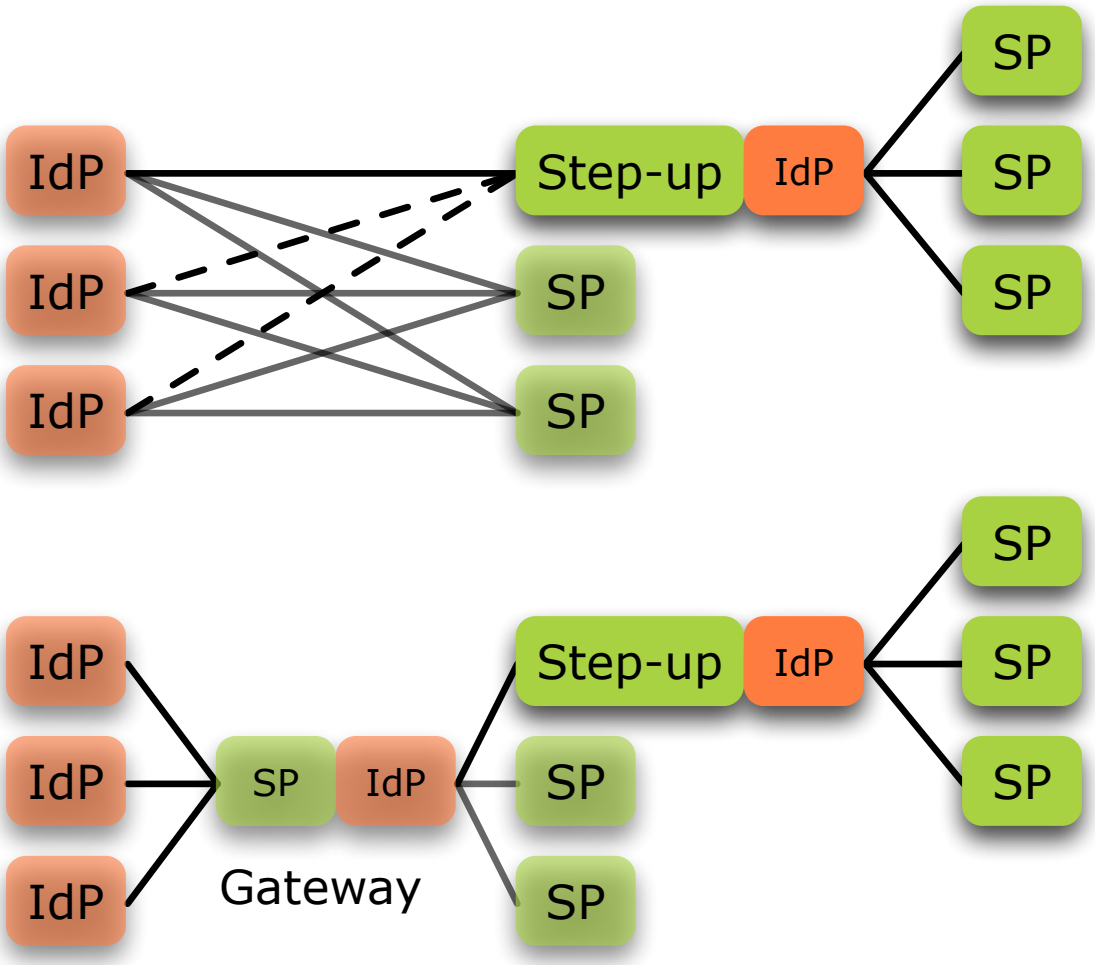
- (InCommon) SAML federation



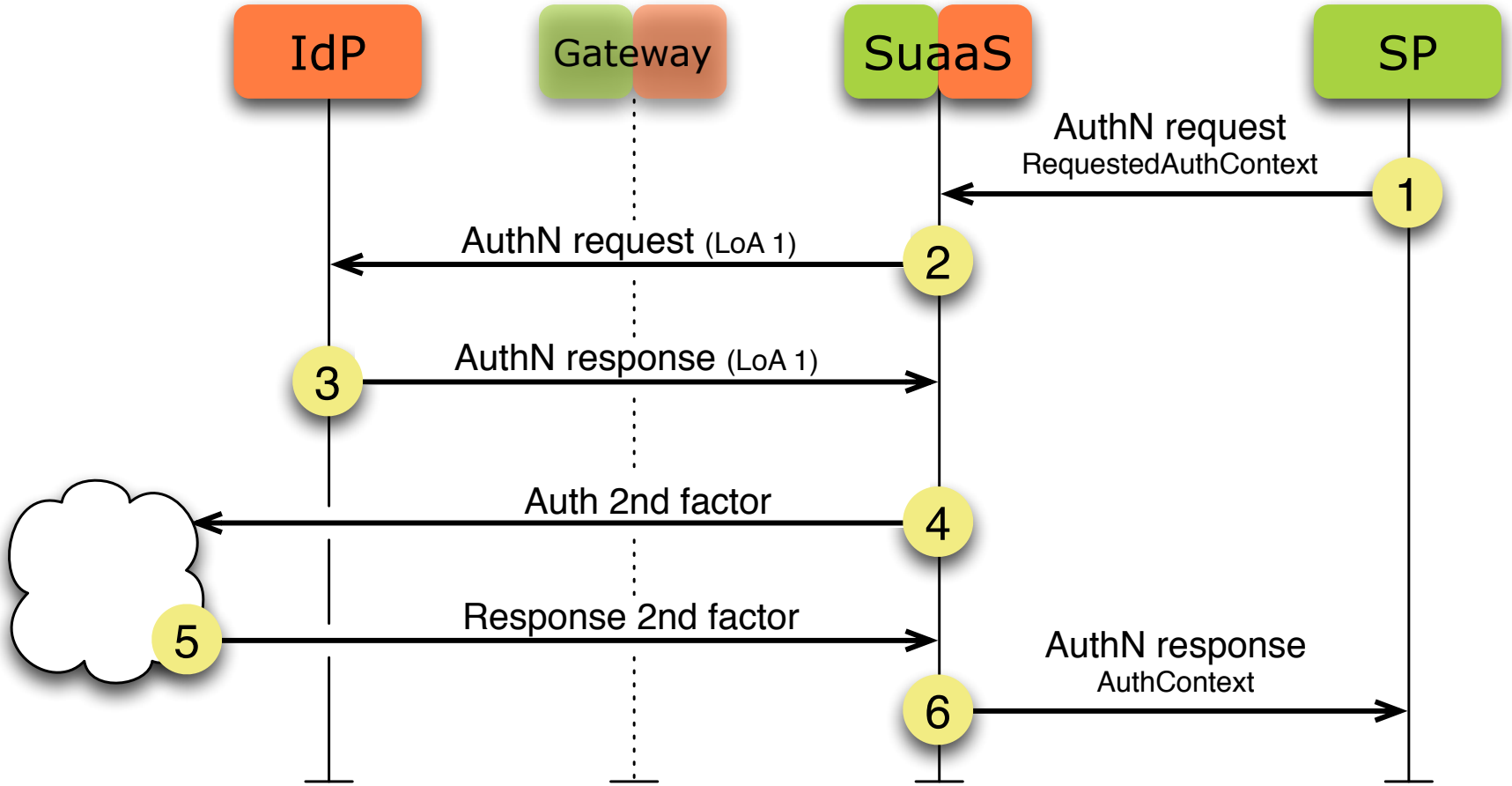
- SURFnet federation



Architecture

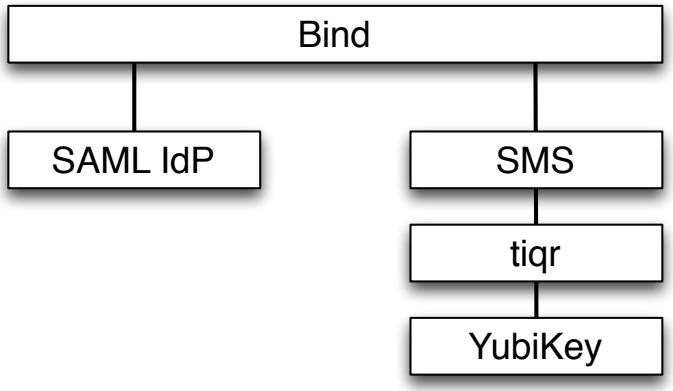


Authentication Flow

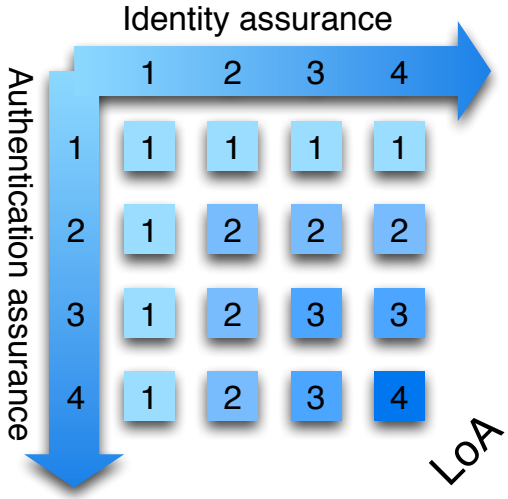


Registration process

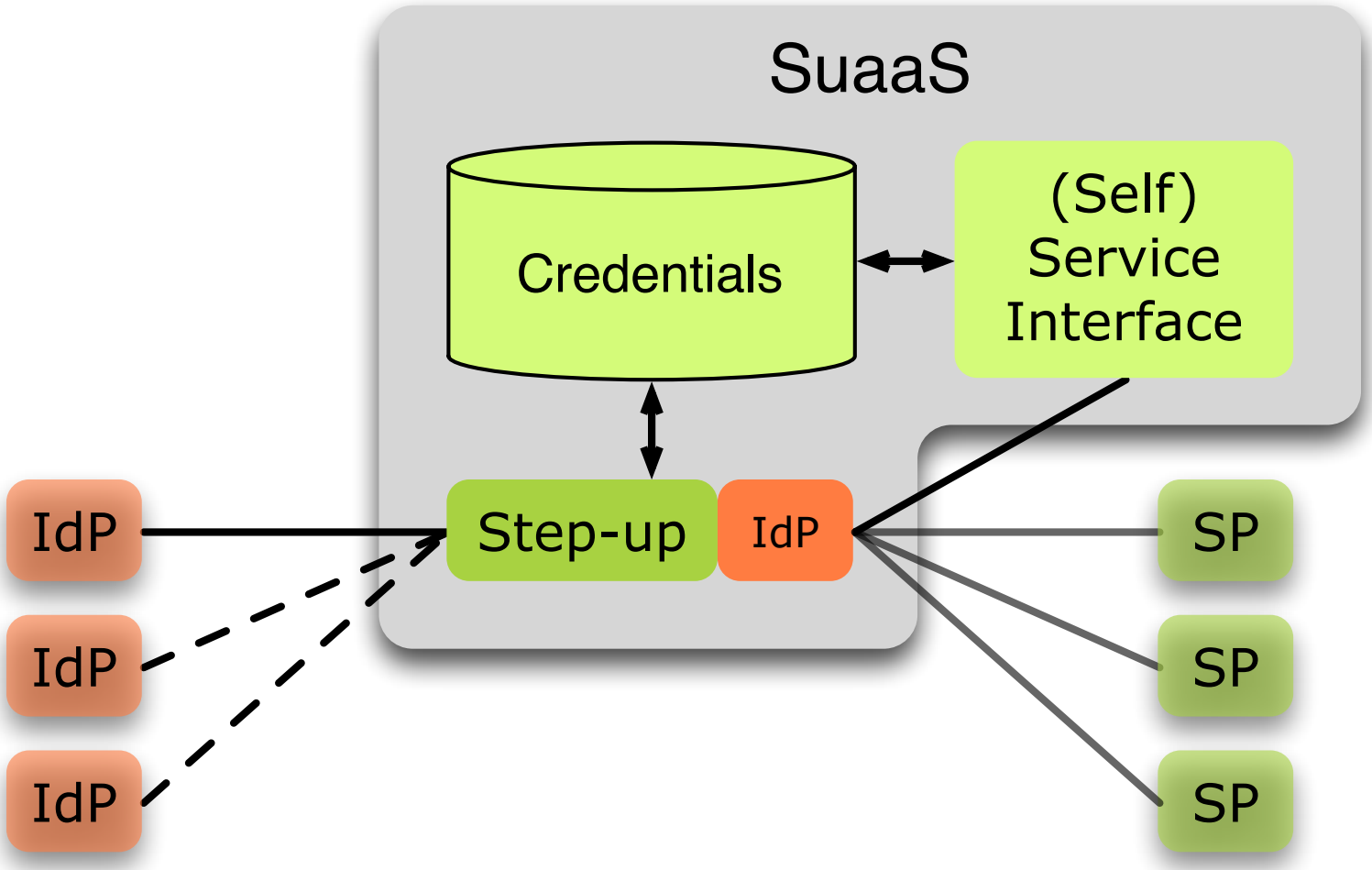
- Create new credential from
  - existing institutional authentication (SAML)
  - and Phone, Token



- Bind
  - Identity
  - to authentication



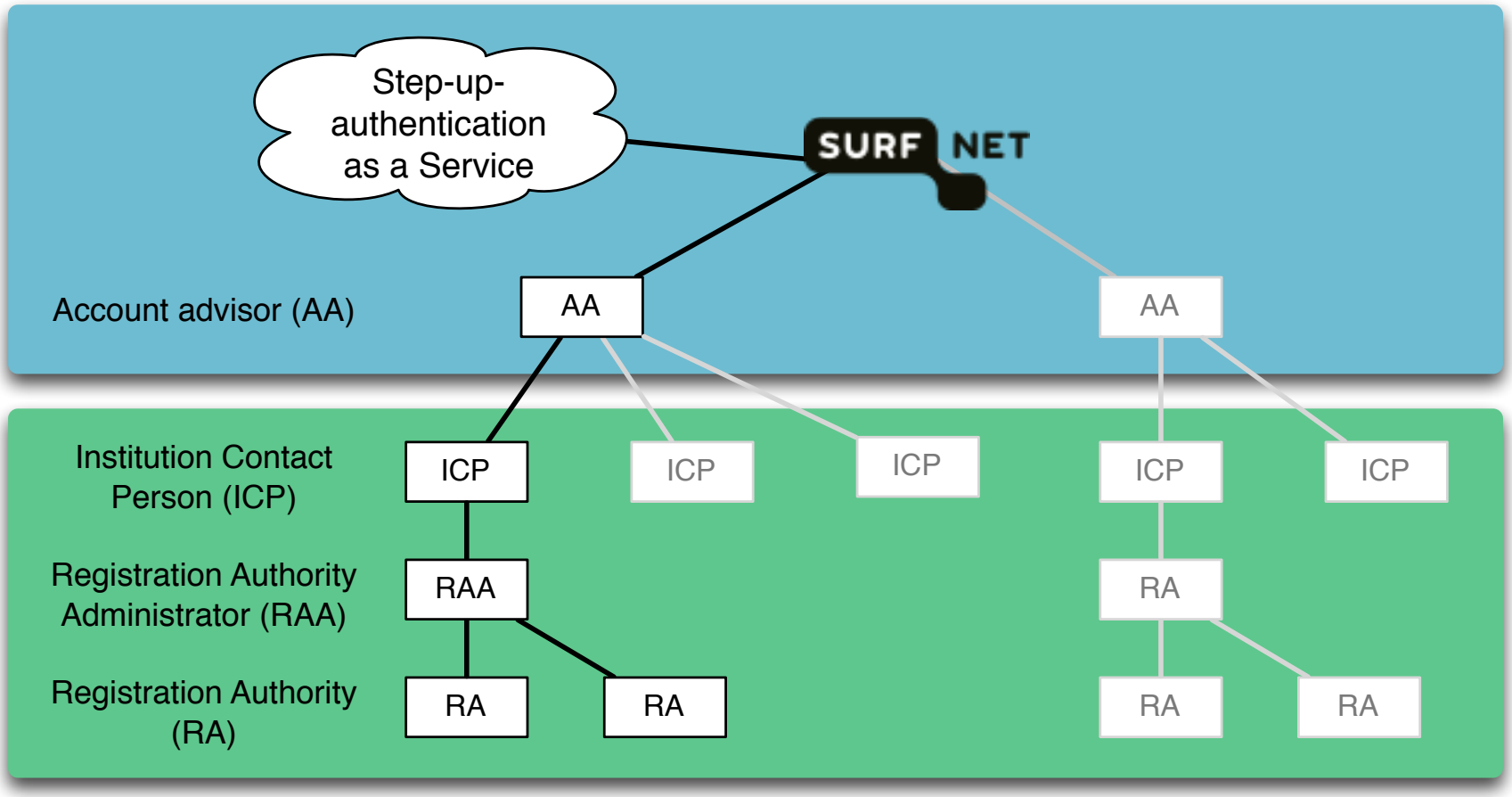
Architecture



Registration process

1. User self registration of token
   - (by invitation)
   - Binds token to institutional login
   - Results in a unique registration code
2. User visits a RA. Brings:
   - Registration code
   - Token
   - Identification
3. RA Verifies
   - Identification
   - User can authenticate using token

Registration Roles



Registration

- Why face-to-face registration?
  - Remote registration
    - Requires availability of trusted registries to validate name, address, ID numbers
      - E.g. Send registration letter to home address
  - In person registration
    - Seems more efficient ?!
    - Can meet requirements for LoA 4

Registration

- Optional face-to-face registration?
  - Use case: strong authentication only
- Implementation: skip vetting step
  - Requires additional controls

Next Steps

- Q2 2013 Pilot partners
- Q3 2013 Proof of concept
- Q4 2013 Production

Questions?
Remarks?

pieter.vandermeulen@surfnet.nl

http://nl.linkedin.com/in/pmeulen/