# Using IRMA as an alternative to in person identity validation

Pieter van der Meulen – SURF

Peter Havekes - SURF

# Some context

- SURF – Cooperation of Dutch higher education and research institutions
- SURF has an identity federation – each institution manages it’s user’s identities
- SURFsecureID – A service for centrally adding a second authentication factor to the federated identities

# Concept SURFsecureID

Identity of user’s home institution

+

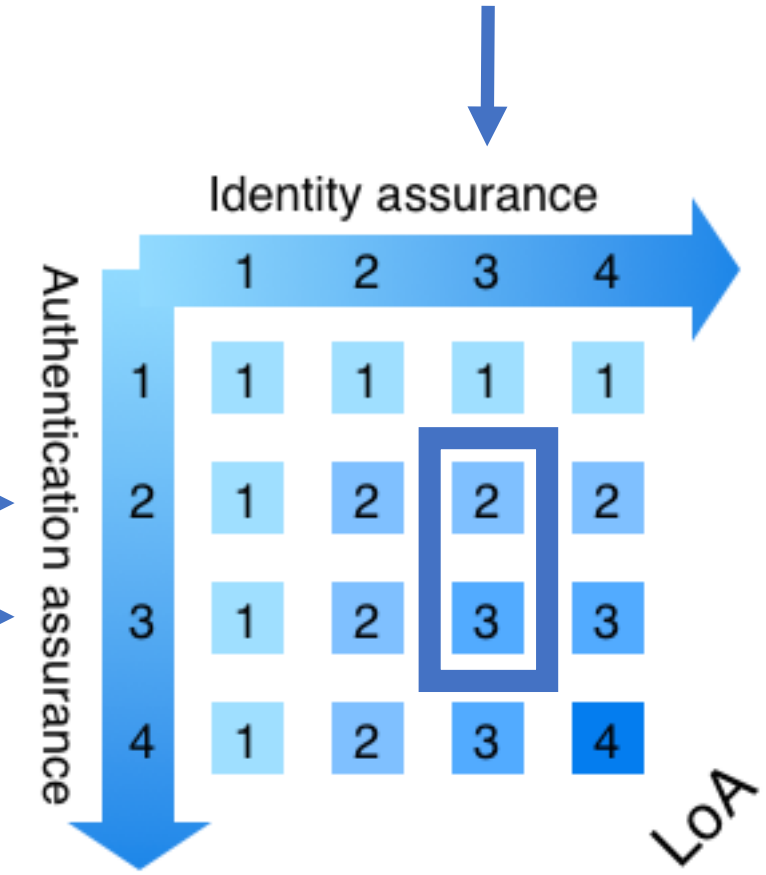
Centrally managed 2nd authentication factor

+

Face-2-face ID check

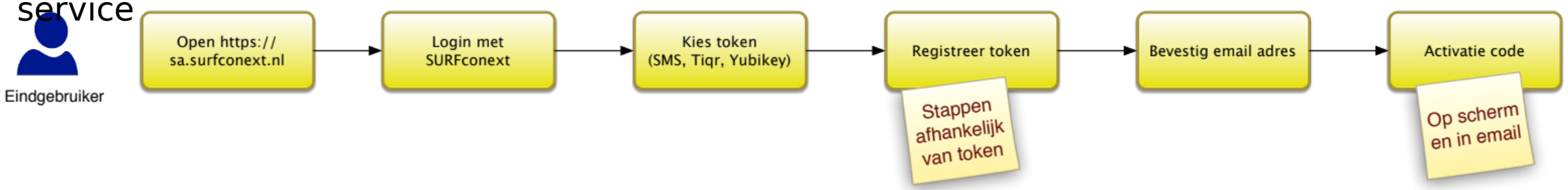
=

Higher Level of Assurance (LoA)

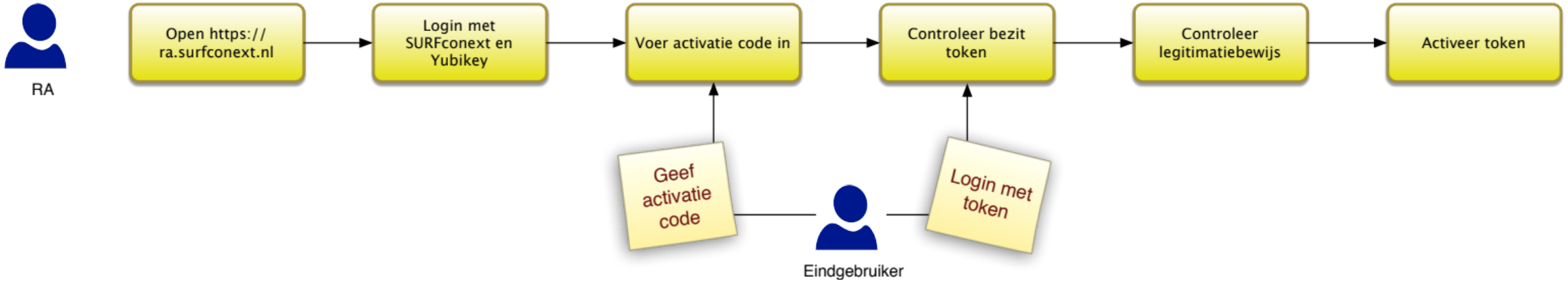


# 2nd authentication factor Registration flow

Self-service




Face-2-face



# Self-service everywhere

- Face-2-face proces works. But…
  - Costs
  - Logistics
  - Expectations

- Replace face-2-face vetting with self-service identity check based on another strong authentication method
  - IRMA (Gemeente, Bank)
  - RFID chip in identity document with face verification
  - iDIN

# Proof of concept (PoC) goals

- Questions
  - How do users experience the process?
  - How to match the Identity from the institution to the identity from IRMA/RFID/iDIN?
    - More complicated than a string compare
  - What false rejection and false acceptance rates can we expect?

# Creating the Proof of Concept (PoC)

- Good learning experience
  - Discussions with institutions
    - Expectations when dealing with identity documents
    - Gender issues
  - Making a production quality PoC with respect to privacy and security
    - PoC based in consent
    - IRMA realy simple to add
    - RFID and BSN
- Fork of production version of SURFsecureID

# Demo

- The Poc
  - https://selfservice.vetting-poc.surfconext.nl
- PoC help
  - https://wiki.surfnet.nl/display/SsID/SURFsecureID+Remote+Vetting+Proof-of-concept

- Optional: experience the PoC for yourself
  - If you have an account at a participating institution you can use that
  - Otherwise register a free eduID account at https://eduid.nl/

# PoC results (first round) 1/2

- Very high evaluation (8.5 out of 10)
  - But N=40 and bias

- Feedback:
  - Installing apps is a hassle
  - "I've no idea what I've just done :)”
  - Perfect for tech savvy users
  - Less hassle than the face-2-face process
  - Several users that could not use iDIN even if they had an account at participating bank. Notably Triodos.
  - Why do I have to pay? Confusing iDIN with bank transaction
  - Using the wrong app to scan the QR code˜

# PoC results (first round) 2/2

- Matching – mostly the expected issues
  - Roepnaam vs offical name – Maarten – Martinus
  - Missing or differently placed “tussenvoegsels”
  - Bank provides only initials, as expected
  - “Double” Last names like “janssen-de boer” not consistent

# Matching algorithm

- What is feasible?
  - Last name
    - Without voorvoegsel?
    - Allow partial match for double names?
  - First names
    - Match initials only
  - Birth date
    - Must match – should not be an issue. Formats are known.
  - Sex
    - Include in match or not?

# Risk of a false match

- Best attack I can think of:
  - Phish the password of some users at their home IdP
  - Find (Steal / buy) another “matching” identity
- Supporting more identification methods makes this attack worse

- How big is this risk?
- Other notable risks?
- What are possible mitigations?

# Next Steps

- More data
  - 2nd round Poc