Distributed Vetting for SFA - demo#3

Team Omega

Goals

This project investigates:

- investigate together with research communities how the token registration can be scaled for scenarios where participants are distributed over EU and beyond

Preparatory work

- Report document
  - Secondary research: literature
  - Primary research: Interviewees
- Requirements specification
  - Use cases
  - Scope

Possibilities to investigate

- **Physically at the door**
- **Live video chat**
- **Mobile app with picture of identity document and selfie / NFC technology for ID document**
- **Derived identity from strong authentication by iDIN, Idensys, or iDEAL; eID solutions via eIDAS;**
- **Central registration desk;**
- **Reuse of existing registration desks at other organizations like municipalities, banks, Chamber of Commerce, Certification Authorities or other education and research institutions;**
- **Community-based vetting, i.e. let other users do the vetting.**
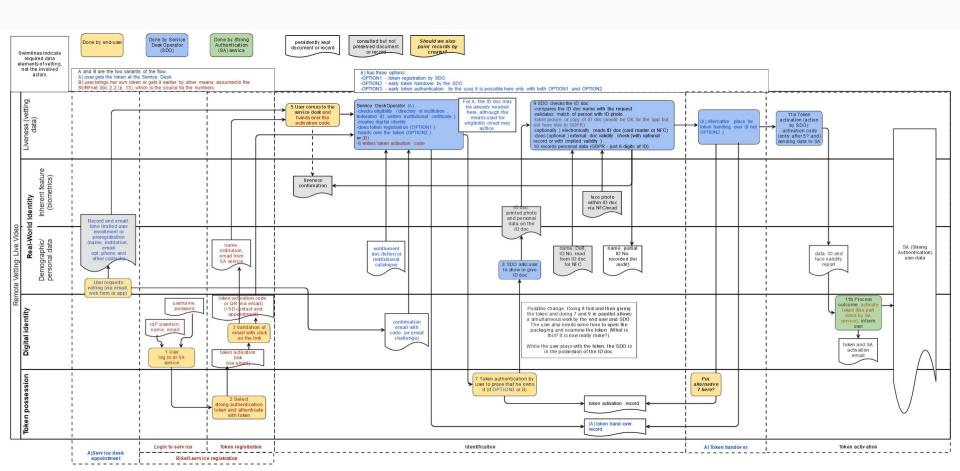
Progress

- Done
  - Building blocks definition / Investigation structure
  - Consolidation of various documents to one report document
- In Progress
  - apps testing, flow testing
  - report document
  - DV-MFA table to discuss with research communities

Example of analysis: A registration desk flow in BPMN-like notation as described in SURFnet report "Remote Vetting" chap. 4.8-9

Legend boxes:
- Done by end-user
- Done by Service Desk Operator (SDO)
- Done by Strong Authentication (SA) service
- persistently kept document or record
- consulted but not preserved document or record
- *Should we also paint records by creams?*

Swimlines indicate required data elements of vetting, not the involved actors.

A and B are the two variants of the flow
A) user gets the token at the Service Desk
B) user brings her own token or gets it earlier by other means, assumed in the SURFnet doc 2.2 (p. 13), which is the source for the numbers.

A) has three options:
-OPTION1 - token registration by SDO
-OPTION2 - early token handover by the SDO
-OPTION3 - early token authentication by the user it is possible here only with both OPTION1 and OPTION2

Swimlanes (left side, top to bottom):

Liveness (vetting data)

Inherent feature (biometrics)

Real-World Identity

Demographic/ personal data

Remote Vetting: Live Video

Digital identity

Token possession

Process elements:

5 User comes to the service desk and hands over the activation code

Service DeskOperator (A):
-checks eligibility (directory of institution, federated ID, written institutional certificate)
-creates digital identity
-does token registration (OPTION1)
-hands over the token (OPTION2)
or (B):
-6 enters token activation code

For A, the ID doc may be already needed here, although the means used for eligibility check may suffice.

9 SDO checks the ID doc
-compares the ID doc name with the request
-validates match of person with ID photo
-takes picture or copy of ID doc (would be OK for the app but not here due to GDPR)
-(optionally) electronically reads ID doc (card reader or NFC)
-does (optional) external doc validity check (with optional record or with implied validity)
10 records personal data (GDPR - just 6 digits of ID)

(A) Alternative place for token handing over (if not OPTION2)

11a Token activation (action by SDO)
-activation code (entry after 5? and) sending data to SA

liveness confirmation

face photo within ID doc via NFC/read

ID doc printed photo and personal data on the ID doc

Record and email: time limited user enrollment or preregistration (name, institution, email opt. phone and other contacts)

name, institution, email from SA service

entitlement doc (letter) or institutional catalogue

name, DoB, ID No. read from ID doc for NFC

name, partial ID No. recorded (for audit)

data, ID and face validity report

SA (Strong Authentication) user data

User requests vetting (via email, web form or app)

8 SDO asks user to show or give ID doc

username, password

token activation code or QR (via email) (+SD contact and appointment)

Possible change: Doing 8 first and then giving the token and doing 7 and 9 in parallel allows a simultaneous work by the end user and SDO. The user also needs some time to open the packaging and examine the token (What is this? It is now really mine?).

While the user plays with the token, the SDO is in the possession of the ID doc.

11b Process outcome, activate token (the part done by SA service), inform user

IdP assertion: name, email

3 Validation of email with click on the link

confirmation email with code (or email challenge)

token and SA activation email

1 User log in at SA service

token activation link (via email)

7 Token authentication by user to prove that he owns it (if OPTION3 or B)

Put alternative 7 here?

2 Select strong authentication token and authenticate with token

token activation record

(A) token hand-over record

Bottom labels:

A) Service desk appointment

Login to service

Token registration

B) Self-service registration

Identification

A) Token handover

Token activation

Leftover

- actual interviews
- try more-more-more solutions
- trials with user communities
- finish up reports

Thank you!