# Remote Vetting

## For SURFconext Strong Authentication

**Utrecht, December 2017**

**Version: 1.0**

About this publication

**Remote vetting for SURFconext Strong Authentication**

SURF

P.O. Box 19035

NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl

www.surf.nl/en

**Authors**

Bob Hulsebosch, Maarten Wegdam (Innovalor)

**Reviewers**

Pieter van der Meulen, Joost van Dijk, Peter Clijsters, Michiel Schok (SURFnet)

# Synopsis

SURFconext Strong Authentication is a service from SURFnet that introduces two-factor authentication to the SURFconext identity federation. SURFconext Strong Authentication uses a face-to-face identity vetting process. This deliverable provides an overview of solutions for remote vetting and assesses their suitability for SURFconext Strong Authentication based on a number of criteria (costs, user friendliness, assurance level, technical and organisational impact, controllability, coverage) and use cases (i.e. small user groups, remote users and bulk enrolment). The outcome of the assessment is that remote vetting solutions based on derived authentication via iDIN (the Dutch BankID) and mobile identification apps using NFC are most promising. These solutions best meet the criteria and the use cases envisioned in higher education and research. It is recommended to enhance SURFconext Strong Authentication with iDIN functionality to cater for derived authentication based vetting for Dutch users, and to develop a mobile app with NFC passport reader functionality for foreign users. Both these solutions allow for straight-through processing of vetted identities and subsequent activation of the second authentication factor and do not require any active involvement of a registration desk.

## Table of Content

# Management summary

## *Background and use cases*

SURFconext Strong Authentication (SCSA) allows users to obtain a second factor authentication token that provides additional identity assurance to their institutional username and password based account. In order to obtain a second factor token, users have to physically identify at a registration desk. This identity vetting process works fine for users that work at the institutional buildings; they can easily go to the registration desk and identify themselves. However, for users that do not work at the institutional buildings, getting a strong authentication token in this manner is problematic as it requires a lot of travelling. For Dutch and foreign users that work abroad it is almost impossible to get a token.

Moreover, setting up a registration desk is accompanied by costs: employees have to be available to identify the user, they have to be trained to do the identification properly and to know how to determine the authenticity of the shown identity document, evidence has to be archived, etc. If the number of users that require a strong authentication solution is limited, the costs of setting this up do not weigh against the benefits.

Finally, the current registration desk process does not scale for short term bulk enrolment of large amounts of users.

For these types of use cases, i.e., remote Dutch and foreign users, a limited number of users, and bulk enrolment, a number of alternative, remote vetting solutions have been assessed.

***Goal***
The main goal was to gather and assess possible solutions for remote/online vetting as part of SCSA. Remote vetting could imply online vetting, but other forms of remote vetting are also in scope. As a secondary goal, possible improvements to the current face-to-face vetting process were captured as well.

***Approach***
To achieve the goals of the project a number of activities were undertaken. During a kick-off meeting with SURFnet, the relevant use cases, assessment criteria and solutions for remote vetting were discussed. These aspects were further discussed and completed during interviews with institutions that make use of SCSA and are interested in remote vetting solutions. Interviews were conducted with several institutions that already make use of SCSA and have a registration desk or have valid use cases for remote identity vetting.

***Assessment criteria***
The following assessment criteria for remote vetting were identified:

1. **Easy to use by the user**: if the user experiences inconveniences during remote vetting he may cancel the process.
2. **Easy to organize by the institution**: it must be easy for the institution to enroll, deploy, initiate, or arrange a remote vetting solution.
3. **Limited impact on current SCSA service**: how easy can the remote vetting solution be integrated with the current SCSA service, what needs to be adapted technically or organisationally by SURFnet, is it a one-off (e.g. software improvement) or continuous (e.g. audit process) effort?
4. **Straight-through processing**: the possibility to vet for the user's identity in a fully automated manner without human interference. More automation means shorter vetting lead times and improves the user experience. It also provides more efficiency and less errors (e.g. due to typing errors when entering personal information).

5. **Sufficient penetration rate**: as many potential target users as possible must be able to go through a remote vetting process. Certain user groups may not be able to execute the remote vetting process because they lack certain functionality that is required for remote vetting (e.g. they use a smart phone without NFC or do not have a Dutch bank card).
6. **Sufficient level of authentication assurance**: the outcome of the remote vetting must provide sufficient assurance in the identity of the user (which on its turn will provide a higher authentication level of assurance). The SCSA service works at ISO29115 levels 2 and 3 depending on the authentication means (these levels roughly correspond to eIDAS Low and Substantial).
7. **Costs**: the costs of the solution are reasonable, with a particular focus on the vetting costs per user.
8. **Controllability/auditability**: the ability to control the remote vetting process in such a way that it is implemented by all institutions in an unambiguous manner including the ability to audit the process for accountability purposes.
9. **Future proof & maturity**: Is the solution future proof and does it have a sufficient maturity level?

***Solutions***

The following long-list of nine remote/online vetting solutions was established, based on desktop study, interviews and a workshop with stakeholders:

1. Physically at the door;
2. Live video chat;
3. Mobile app with picture of identity document and selfie;
4. Mobile app with NFC technology for reading the chip of the identity document and selfie;
5. Derived identity from strong authentication by iDIN, Idensys, or iDEAL;
6. Derived identity from strong authentication by national eID solutions via eIDAS;
7. Central registration desk;
8. Reuse of existing registration desks at other organizations like municipalities, banks, Chamber of Commerce, Certification Authorities or other education and research institutions;
9. Community-based vetting, i.e. let other users do the vetting.

***Assessment against criteria and use cases***
The scorecard below summarizes the criteria assessments of the various solutions for remote vetting. Green, yellow and red mean respectively 'meets', 'partially meets' or 'does not meet' the criteria. The points (respectively 5, 3 and 1) are used to provide an overall score for each solution.

| Requirement | Door | Video | App Optical | App NFC | Derived iDIN | Derived eIDAS | Central desk | Reuse desk | Com. based |
|---|---|---|---|---|---|---|---|---|---|
| Easy to use by user | 5 | 5 | 5 | 5 | 5 | 5 | 1 | 3 | 5 |
| Easy to organize by institution | 5 | 5 | 5 | 5 | 5 | 5 | 3 | 3 | 1 |
| Limited impact on SCSA service | 1 | 1 | 3 | 3 | 3 | 3 | 5 | 3 | 5 |
| Straight-through processing | 3 | 3 | 3 | 5 | 5 | 5 | 3 | 3 | 3 |
| High coverage / penetration rate | 1 | 5 | 5 | 3 | 3 | 1 | 1 | 3 | 5 |
| LoA 2/Low or 3/Subst. | 3 | 3 | 3 | 5 | 3 | 3 | 5 | 3 | 1 |
| Costs | 3 | 3 | 3 | 3 | 5 | 5 | 5 | 3 | 3 |
| Controllability / auditability | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 3 | 1 |
| Future proof & maturity | 5 | 3 | 3 | 5 | 5 | 3 | 5 | 3 | 1 |
| **Total score** | **31** | **33** | **35** | **39** | **39** | **35** | **33** | **27** | **25** |

The outcome of this assessment is that solutions based on derived authentication and mobile apps score best. For derived authentication, iDIN is the best choice as it offers a high national penetration level compared to Idensys, and provides more trustworthy personal data than iDEAL. As a remote vetting solution iDIN, however, struggles to achieve a level 3 assurance level since it is more susceptible to man-in-the-browser attacks. Consequently, compensating measures are required to achieve level 3. Moreover, mapping iDIN accounts to institutional account may be challenging since iDIN only provides initials and not full names. Looking at the mobile app solutions, the NFC-based app offers, compared to an optical-based app, more assurance and efficiency. However, lack of coverage of NFC-enabled mobile phones is a drawback (iOS devices currently do not support NFC). Because of the relatively large amount of actions required it is recommended to guide the user well through the whole vetting process to prevent them from dropping out.

The identified typical use cases add several additional requirements to the solutions: users may be limited in number but work at the institution's premises, they may be remote (abroad or do not work at institutional premises) or they need to be enrolled within a short period of time. Per use case the scorecard is as follows:

| Requirement | Door | Video | App Optical | App NFC | Derived iDIN | eIDAS | Central desk | Reuse desk | Com. based |
|---|---|---|---|---|---|---|---|---|---|
| Small amount of users (local) | 5 | 5 | 5 | 5 | 5 | 3 | 5 | 5 | 5 |
| Remote Dutch users | 3 | 5 | 5 | 5 | 5 | 1 | 3 | 3 | 5 |
| Remote foreign users (abroad) | 1 | 5 | 5 | 5 | 1 | 5 | 1 | 1 | 5 |
| Bulk enrolment of users | 1 | 3 | 5 | 5 | 5 | 3 | 1 | 1 | 1 |
| **Total score** | **10** | **18** | **20** | **20** | **16** | **12** | **10** | **10** | **16** |

For remote Dutch and foreign users that work abroad and large numbers of users any form of physical vetting is problematic. For foreign users, the iDIN derived identity solutions are also less optimal. The eIDAS solution could work for European citizens but is still too immature and lacks coverage. Video-based solutions score well for all user groups, but scale less for bulk scenarios. The mobile app based vetting solutions are to be preferred as these best facilitate all use cases.

***Conclusions and recommendations***

There is not one single best solution, therefore a combination of remote identity vetting solutions is needed to cater for the various use cases, serve all users, and to cover for fallback scenarios. It is recommended to extend the SCSA service with iDIN authentication functionality as the primary remote identity vetting solution and to develop a mobile NFC-based app for the vetting of users that do not have a Dutch bank account or are unwilling to use their personal bank account.
Proof-of-concepts of these solutions are needed to experiment with the technology, evaluate user experiences, gain knowledge on how to match/link accounts of users, and to integrate functionality with the current SCSA service.

Integrating iDIN in SCSA is not trivial. Attention has to be paid to the mapping of iDIN accounts to institutional accounts. This mapping is complicated by the fact that most iDIN accounts make use of initials whereas the institutional accounts make use of full first names. Additional information such as date of birth may be needed to assure that both accounts indeed belong to the same user, but currently the SCSA service does not have this information.

The iDIN solution suffers from a man-in-the-browser vulnerability that reduces the current assurance level for a SCSA YubiKey token from 3 to 2. Should SURFnet decide to implement iDIN for SCSA and to maintain the current physical RA-desk process for vetting, than two different levels of assurance exist for the same SCSA YubiKey token. It is recommended to take the type of vetting process into account prior to assigning the overall level to a token in the SCSA management portal.

The NFC-based app solution described includes selfie and interactive video/liveness detection functionality. This functionality is not required to achieve ISO29115 assurance level 2 or 3. If SCSA wants to be eHerkenning/Idensys or eIDAS compliant, the functionality is required to achieve level 3 or Substantial. It is up to SCSA to choose its level of assurance framework it wants to be compliant with. The choice is strategic and determines what functional identity features are required for the NFC-app.

A proof-of-concept allows for testing of user experiences with and without selfie and liveness detection and assessing the accuracy of biometric identification based on a selfie and identity document picture. During the research for remote vetting solutions, several potential improvements to the current SCSA face-to-face vetting process were identified. Improvements to consider that could contribute to an improvement of the assurance level and may make the process more compliant with other national or EU assurance frameworks could be:

- The Registration Authority should check if the identity document shown is not reported as being lost or stolen.
- The Registration Authority should check if the identity document shown is authentic, which requires training and/or tooling such as an app or scanner.
- Guarantee that the Registration Authority at the institutions is part of the ISMS and is included in internal or external security audits.

# 1. Introduction

## 1.1. Background

SURFconext Strong Authentication (SCSA) allows users to obtain a second factor authentication token that provides additional identity assurance to their institutional username and password based account[1]. It gives the users access to cloud-based services that are linked to SURFconext and require stronger forms of authentication than provided by their home institute. Users log in with their institution's account and, as an additional step, are then prompted to confirm their identity with the second factor authentication token. Currently, SCSA gives access to cloud services via three different types of authentication tokens: SMS, Tiqr (smartphone app) or YubiKey (USB hardware token).
Getting a valid token consists of two main processes:

1. A self-service registration process that allows the user to select a token;
2. A face-to-face identity vetting process at the registration desk of user's institution to activate the token.

To select a token, the user must first log in with their institutional account. After selection of the token, the user is prompted to confirm his identity with the selected token. In this way, there is a second layer of security.

In order to activate the token, the user must go through the identity vetting process by visiting his institution's registration desk to have an authorized employee, i.e. registration authority (RA), verify his identity. Subsequently, the RA will bind the selected token (SMS, Tiqr or YubiKey) to the institutional account of the user. This binding is based on the activation code the user has received during the registration process of SCSA. The user has to hand over the activation code to the RA and perform an authentication with the token to prove holder possession. The RA also registers the last six digits of the user's identity document for accountability purposes. After that the user's token will be activated and he can log in to any SURFconext federated service designated for strong authentication using a two-step login procedure.

This identity vetting process works fine for users that work at the institutional buildings; they can easily go to the registration desk and identity themselves. However, for users that do not work at the institutional buildings, getting a strong authentication token in this manner is problematic as it requires a lot of travelling. For users that work abroad it is almost impossible to get a token.
Moreover, setting up a registration desk is accompanied by costs: employees have to be available to identify the user, they have to be trained to do the identification properly and to know how to determine the authenticity of the shown identity document, evidence has to be archived, etc. If the number of users that require a strong authentication solution is limited, the costs of setting this up do not weigh against the benefits.

For these two use cases, i.e., remote users and a limited number of users, SCSA is looking for remote identity vetting solutions and has asked InnoValor to assess the possibilities.

## 1.2. Goal

The main goal of the assignment is to list and assess possible solutions for remote/online vetting as part of SCSA. Remote vetting may imply online vetting, but other forms of remote vetting are also in scope. As a secondary goal, possible improvements to the current face-to-face vetting process will also be captured in this report.

[1] For more information see https://www.surf.nl/diensten-en-producten/surfconext/wat-is-surfconext/surfconext-sterke-authenticatie/index.html or https://wiki.surfnet.nl/display/surfconextdev/SURFconext+Strong+Authentication.

## 1.3. Approach

To achieve the goals of the project a number of activities were undertaken. During a kick-off meeting with SURFnet, the relevant use cases, assessment criteria and solutions for remote vetting were discussed. These aspects were further discussed and completed during interviews with institutions that make use of SCSA and are interested in remote vetting solutions. Interviews were conducted with Inholland, HvA, StudieLink, Nikhef, Windesheim, and VUmc.

The first assessment of solutions for remote vetting were discussed during a midterm session at SURFnet. Most interviewed stakeholders and involved SURFnet project members were present at the session. The outcome of the session was incorporated in this final report on remote vetting for SCSA. This report was reviewed both by InnoValor and SURFnet.

## 1.4. Reading guide

Section 2 provides a description of the current vetting process and the assurance levels that can be achieved with SCSA. Section 3 describes the use cases for remote/online vetting and describes the requirements solutions will be assessed against. An overview of the solutions and their use case and requirements assessment is presented in Section 4.

# 2. Current situation

## 2.1. Strong authentication

The strength of the entire authentication system is usually expressed in terms of levels of assurance (LoA). The LoA specifies the degree of confidence in identifying a user to whom the credential was issued, i.e. the combination of the strength of the authentication solution used and the quality of the registration process (see Figure 1). The combination of the two – stronger authentication and identity registration – is basically what is needed in order to achieve true strong authentication.


**Figure 1: factors that determine the strength of the authentication.**

Strong authentication solutions are available and typically consist of two-factor solutions[2]. The registration process by which a physical person is linked to his/her digital identity information and to his/her authentication credential is critical to deter registration fraud. If this process results in a weak link of the person to either the credential or the identity, there can be little or no assurance that the person using that credential to authenticate and access services and information is who he/she claims to be. It could be anyone including impostors that impersonate a claimed identity, it could be multiple people over time, or even subscribers that were denied registration. If the linking is weak, even the most complete personal information and the strongest credential will not improve the assurance of identity.
The registration process is designed, to a greater or lesser degree depending on the assurance level, to ensure that the registration authority knows the true identity of the applicant. Specifically, the requirements include measures that:

- Increase proof in the identity of the user via verification against an official identity document, such as a passport, or other means, such as the assertion of the institutional identity provider about the user's identity. This process is also called identity vetting.
- Increase trust in the binding between the user's identity and his digital identity (e.g. institutional or bank account).
- Increase trust in the binding between the user and a second authentication credential or token.

This authentication triangle of binding is illustrated in Figure 2 below.
More information about strong authentication and identity registration and vetting can be found in SURFnet's report on "Step-up Authentication-as-a-Service - A study of the architecture and processes".[3]

[2] For an overview see e.g. Kuppinger Cole: Market Overview Strong Authentication, 2010, http://www.kuppingercole.com/report/srmo_stronauth_80310.
[3] See https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2012/rapport_step-up_authentication-as-a-service_architecture_and_procedures_final.pdf.

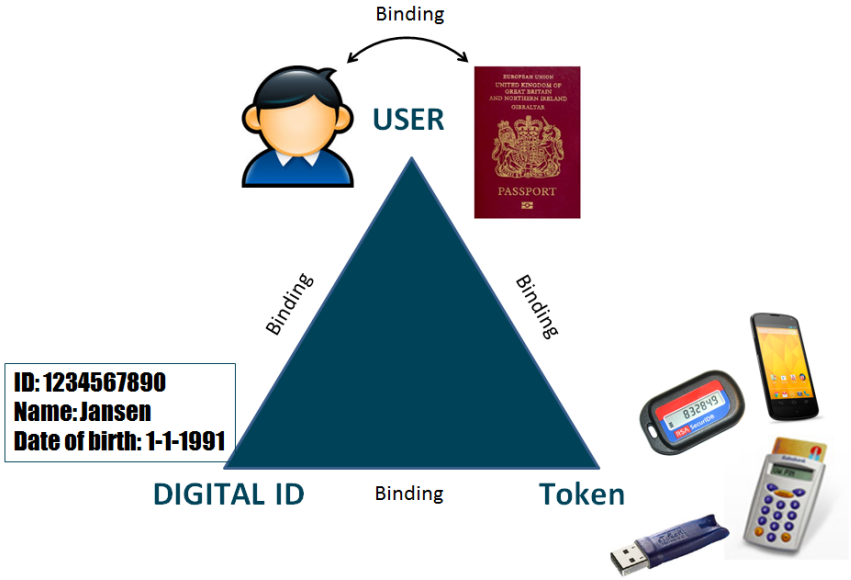


Figure 2: Binding triangle of user ID – digital ID – authentication tokens.

## 2.2. SCSA Vetting process

For SCSC, the above-described registration and vetting processes to establish the identity of the user and to link this identity to his authentication credentials has been implemented as follows:

1. The user logs in at SCSA self-service with his federated institution account. SCSA receives an authentication assertion from the institutional identity provider that contains the first and last name of the user and his email address.
2. The user selects a strong authentication token type (SMS, Tiqr, YubiKey, …) to register and does an authentication with it to prove that he owns the token.
3. The user receives an e-mail and is asked to click on the activation link.
4. The user receives an activation code via e-mail.
5. The user goes to the registration authority (RA) and hands over the activation code.
6. The RA logs in into the SCSA management portal and enters the activation code to find the corresponding token registration.
7. The RA asks the user to authenticate with the token to prove that he indeed owns the registered token.
8. The RA asks the user to show his identity document.
9. The RA checks the user's identity, i.e. compare the name of the user on the identity document with the name in the portal and compare the user's face with the picture on the identity document.
10. The RA enters the last 6 digits of the identity document number for accountability purposes.
11. The RA activates the token in the SCSA management portal, i.e. the binding the between the user's verified identity and his token is established. The user can now use the token as a second factor authentication credential.

Steps 1-4 constitute the self-service registration process; steps 5-9 constitute the identity vetting process. Step 10 is for audit/accountability purposes. These steps mimic the registration and physical vetting processes of e.g. authentication service providers in Idensys/eHerkenning such as Digidentity and KPN.

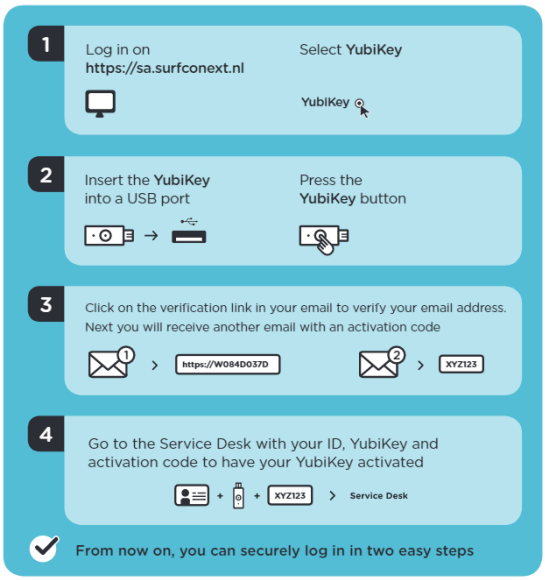


**Figure 3: Part of the current process for obtaining a YubiKey token.**

Each institute has one or a few RA Administrators (RAAs), who can assign the RA role to employees within their institute. RAs can only do the identity vetting for users from their own institute.
From the interview with one institution we learned that they have implemented a variant of the vetting process for users that somehow cannot physically visit the RA desk. For this institution this concerns about 150 users. For this user group the institution does vetting via mobile phone based video conferencing (other users cannot make use of this solution; they have to go to the RA desk). The process is as follows:

1. The manager of the user initiates the process by requesting a vetting at the RA (ICT service desk). The request includes the name of the user to be vetted and his phone number.
2. The RA contacts the user on his phone number and informs him about the vetting process.
3. The user is asked to provide the activation code.
4. The RA uses the activation code to lookup the registered token in the SCSA management portal.
5. The RA initiates a video channel with the user via an app on his mobile phone.
6. The RA verifies the user's identity; the user is asked to show his passport.
7. The RA registers the last 6 digits of the passport.
8. The RA activates the registered token after a successful identification.

The institution concerned is positive about this vetting solution. The mobile phone cameras are of sufficient quality and the users appreciate the fact that they do not have to visit the desk physically.

## 2.3. SCSA Use Cases

The interviews have learned that currently several institutions make use of SCSA for the following cases:

- Teachers of Inholland that need access to applications for evaluating student assignments or for developing tests/exams (about 500 – 1000 users).
- Remote desktop access for Inholland.
- Employees of VUmc that need remote access to health-related applications and data (about 6300 users).
- Researchers of University of Amsterdam and Amsterdam University of Applied Sciences access figshare.com.
- University of Amsterdam administration: datanose.nl, SAP

- Avans: Access for teachers.
- Windesheim: will make of SCSA in the near future for employees that need access to student information systems and to absence management systems.

On average a vetting takes about 5-10 minutes[4] and is typically executed by the service desk of the institution. Staff of the service desk is instructed/trained on how to do the vetting, i.e. there often is a procedure the staff member should follow.

## 2.4. SCSA Assurance levels

There are several international standards for identity assurance, like NIST (US)[5], eHerkenning/Idensys[6], eIDAS (Europe)[7] and ISO29115[8]. SURFconext Strong Authentication is based on ISO29115. The four levels of identity assurance commonly used are:

LoA 1 Little or no confidence in the asserted identity;
LoA 2 Some confidence in the asserted identity;
LoA 3 High confidence in the asserted identity;
LoA 4 Very high confidence in the asserted identity.

The different specifications elaborate on the meaning of these labels by specifying requirements for user identification and registration, authentication token management, authentication and operational security.
The SCSA service supports three levels of assurance:

LoA 1 Password authentication through SURFconext at the users institutional identity provider;
LoA 2 LoA 1 + SMS or Tiqr authentication;
LoA 3 LoA 1 + YubiKey (hardware token) authentication.

Though the vetting process is the same for all three solutions, the YubiKey token is considered more secure than the SMS or Tiqr solutions. Consequently it has been rated with a higher assurance level in SCSA context.
In terms of the more up to date and by most European countries adopted eIDAS framework for authentication assurance levels this roughly translates to level Low (= LoA 2) and Substantial (= LoA 3). This is a rough translation, since SCSA does not tick all the eIDAS boxes for particularly the Substantial level requirements. If SCSA wants to become eIDAS 2015/1502 compliant several improvements of SCSA are needed to obtain level Substantial. Potential areas of improvement are[9]:

- "*Steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents*" – the RA should check if the identity document showed is not reported as being lost or stolen.
- "*There is an effective information security management system for the management and control of information security risks. The information security management system adheres to proven standards or principles for the management and control of information security risks.*" – the RA at the institutions should be part of the ISMS, this is currently not clear/guaranteed.

[4] From interviews.
[5] NIST Special Publication 800-63-3 Digital Identity Guidelines, June 2017, see https://pages.nist.gov/800-63-3/sp800-63-3.html.
[6] Idensys/eHerkenning assurance levels framework, see https://afsprakenstelsel.etoegang.nl/display/as/Technische+specificaties+en+procedures+voor+uitgifte+van+authenticatiemiddelen.
[7] eIDAS Implementing Regulation (EU) 2015/1502 on assurance levels, 8 September 2015, see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002.
[8] ISO/IEC 29115:2013 Entity authentication assurance framework, see https://www.iso.org/standard/45138.html.
[9] From eIDAS Implementing Regulation (EU) 2015/1502 on assurance levels, 8 September 2015, see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002.

- "*The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil.*" – Are the RAs at the service desk sufficiently trained to identify the user correctly and to check the authenticity of the identity document shown?
- "*The existence of periodical independent internal or external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.*" – Is the institutional RA included in internal or external audits?

Some of these elements may need some attention in the current process. It will be interesting to see if some of these elements are addressed or implemented by remote vetting solutions.

# 3. Remote vetting background

## 3.1. Use cases for remote vetting

The three main use cases for remote vetting are

1. Education and research institutions that only have a limited number of users for strong authentication. For these institutions it is not worth the effort to setup a physical registration desk for identity vetting. They could benefit from remote vetting solutions.
2. Education and research institutions that have remote *Dutch* users for strong authentication. For these users it is not convenient to physical register at a desk at the institution.
3. Education and research institutions that have remote *foreign* users for strong authentication. For these users it is not convenient to physical register at a desk at the institution.

Specific examples of these generic use cases are:

- Foreign employees that need access to health data (VUmc; about 50 users – use case 3);
- Medical PhD students that do research at another medical center (VUmc; about 100 users – use case 2);
- Employees of institutions that have to get access to the Studielink management portal (StudieLink; about 5-10 employees per institution – use case 1 or 2 depending on who is offering the RA, i.e. the institution or StudieLink);
- An international group of researchers that need access to group-specific resources (Nikhef; relatively small and international research groups – use case 1, 2 and 3).
- Long-term sick employees that cannot come to the institution but are able to do some work at home (use case 1 and 2 typically).

The current physical registration process does not cater for bulk enrolment of SCSA users. It is too time consuming. If, however, remote vetting becomes a success, it is to be expected that more users will make use of the solution. So, a fourth scenario would be:

4. Bulk enrolment of SCSA users via remote vetting.

The potential risks of bulk enrolment via remote vetting are discussed in the next section.

## 3.2. Consequences and risks

The introduction of the remote vetting can have a cannibalizing effect on the current vetting process at the service desk. In principle this is acceptable if the assurance level for remote vetting is equivalent or better than its physical counterpart.

Remote vetting lowers the threshold for obtaining a strong authentication token. This creates the risk that many employees obtain a token, even if this is not needed from the institution's perspective. The institution then has to pay a potentially high(er) amount of costs. Measures are needed to allow the institution to control the costs of remote vetting for strong authentication. Such a measure is for instance whitelisting: the user gets a code of the institutions that allows him to obtain a strong authentication token. Only users that require a strong authentication token get such a code. Another control measure is to let the manager of the user initiate the vetting process, i.e. the user can only obtain a strong authentication token if the manager has given his approval towards the RA. This control is seen in the current implementation of remote vetting by one of the institutions (see section 2.2).

Furthermore, the user may try to attempt multiple times and via manipulation to obtain a token in the name of someone else. Mechanisms such as logging (of vetting processes) and delaying (after a number of attempts) should be in place to prevent such subversion of the vetting process.

## 3.3. Assessment criteria

Remote vetting solutions have to fulfil to a number of criteria. These criteria are derived from interviews and discussion sessions with SURFnet and stakeholder institutions.
Criteria for remote vetting are:

1. Easy to use by the user: if the user experiences inconveniences during remote vetting he may cancel the process. For instance, many users would like to be able to obtain a SCSA token outside office hours. Compared to the current practice, the ease of use of the solutions from a user perspective can be either better, equal or worse.
2. Easy to organize by the institution: it must be easy for the institution to enrol, deploy, initiate, or arrange a remote vetting solution. Compared to the current practice, the ease of use of the solutions from an institution perspective can be either better, equal or worse.
3. Limited impact on current SCSA service: how easily can the remote vetting solution be integrated with the current SCSA service, what needs to be adapted technically or organisationally by SURFnet, is it a one-off (e.g. software improvement) or continuous (e.g. audit process) effort? Solutions have no, limited or large impact on the current SCSA service provisioning.
4. Straight-through processing: the possibility to vet for the user's identity in a fully automated manner without human interference. More automation means shorter vetting lead times and improves the user experience. It also provides more efficiency, scalability and less errors (e.g. due to manual processing of personal information). For bulk enrolment scenario's this is very relevant. The automation capabilities of the vetting process are less, similar or better than the current situation offers.
5. Sufficient penetration rate: as many potential target users as possible must be able to go through a remote vetting process. Certain user groups may not be able to execute the remote vetting process because they lack certain functionality that is required for remote vetting (e.g. they use a phone that does not support NFC or do not have a Dutch bank card). The penetration rate is higher, equal or lower compared to what the existing SCSA solution for vetting.
6. Sufficient level of authentication assurance: the outcome of the remote vetting must provide sufficient assurance in the identity of the user (which on its turn will provide a higher authentication assurance). Solutions must achieve a level of assurance that at least correspond to LoA 2 and LoA 3 as used by SCSA.
7. Costs: the cost of the solution is reasonable. The current service desk costs are estimated to be about a minimum of 5 Euro per vetting[10]. User costs are also involved. However, these are more difficult to quantify as the costs for students are different than for employees. Therefore, the user's costs are taken into in the ease of use criterion above. There are other costs as well, such as development costs (only once), licensing costs (recurring), and technology/hardware costs. However, these costs are expected to be similar for all solutions. The focus therefore will be on the costs for vetting the user. Consequently, the costs assessment of remote vetting solutions will be rated as higher, similar or lower than 5 Euro. Specific, significant additional costs will be mentioned during the assessment if needed.
8. Controllability/auditability: the ability to control the remote vetting process in such a way that it is implemented by all institutions in an unambiguous manner including the ability to audit the process for accountability purposes. The controllability/auditability of remote vetting solutions is better, similar or worse than what SCSA currently offers.
9. Future proof: Is the solution future proof and does it have a sufficient maturity level?

[10] The costs are estimated as follows: on average it takes a service desk employee about 6 minutes to verify the user's identity and to activate the token. This employee costs the institution about 50 Euros per hour. So the costs of a single vetting amount to 5 Euro.

## 3.4. Existing Remote vetting solutions

Several remote vetting solutions exist. For illustration and benchmark purposes we briefly describe two most relevant solutions.

### 3.4.1. Idensys

The Dutch trust framework Idensys is exemplary for remote vetting as it allows for online vetting at assurance level Substantial (~LoA3 in terms of ISO29115). The best practice process for authentication service providers to implement in order to conform to Idensys LoA requirements is as follows:

1. User enters his personal information at the registration portal of the Idensys authentication service provider. The user already has an account at the authentication service provider with a username and password.
2. User makes 1-ct iDEAL transaction.
3. Idensys authentication service provider compares personal information obtained via iDEAL with the information entered by the user.
4. User installs mobile app and binds it to the registration session by scanning a QR-code that is generated by the registration portal.
5. App receives personal information and asks the user to check if the information is correct.
6. App asks the user to take a picture of the identity document or to scan the document with NFC.
7. App asks the user for a selfie.
8. App starts video session and gives random orders to the user (e.g. turn left, turn right, nod, smile, say specific words, etc.); this video challenge response is for liveness detection. The use of video is required for remote identification and replaces the physical identification process at the RA desk of the authentication service provider.
9. App sends information to the Idensys authentication service provider.
10. Idensys authentication service provider compares picture identity document with selfie.
11. Idensys authentication service provider checks if the user has followed the orders by checking the video.
12. Idensys authentication service provider activates the user's authentication token.

The process is depicted (in Dutch) in Figure 4 below[11].

[11] From https://afsprakenstelsel.etoegang.nl/download/attachments/21901233/Best%20practice%20registratie%20en%20verstrekking%20op%20afstand%20RFC2016.pdf?version=1&modificationDate=1470230581000&api=v2 (in Dutch).

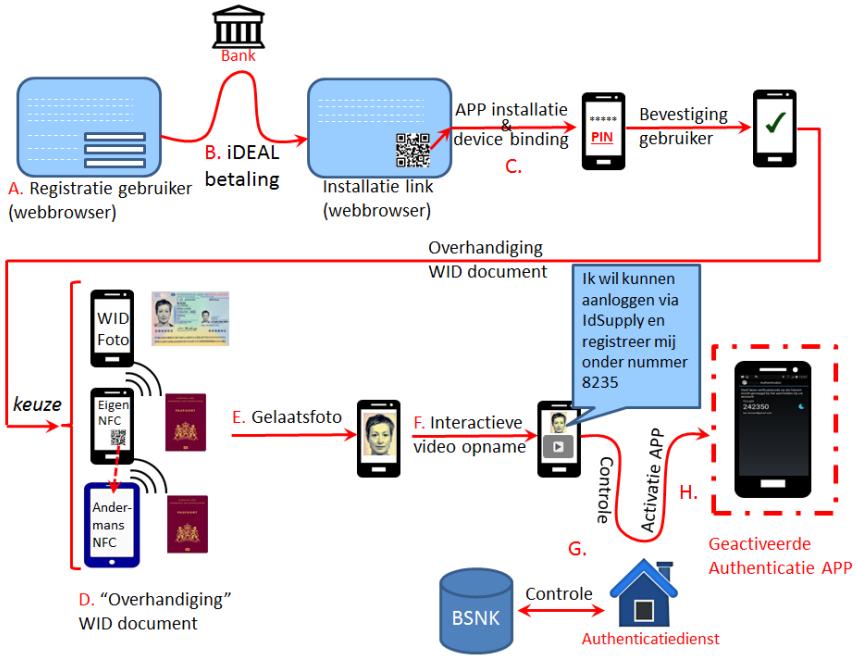


**Figure 4: Remote vetting in Idensys.**

It is foreseen that the eRecognition (eHerkenning) framework, for business-to-government authentication, will also accept this remote vetting process for the issuance of their authentication credentials.

### 3.4.2. DigiD Substantial

The Dutch national eID solution, DigiD, will be upgrade to eIDAS Substantial in the near future. The foreseen process for obtaining DigiD Substantial is as follows:

1. The user applies for a DigiD + SMS at www.digid.nl.
2. The user enters personal information (including social security number, name, date of birth and mobile phone number), generates a password, and obtains a challenge via SMS.
3. The user responds with the challenge. Now the mobile phone is connected to the user's identity.
4. An activation code is generated and sent to the user's home address that is obtained from the Dutch Municipal Personal Records Database (Basisregistratie Persoonsgegevens). The provide identity information is also verified against this database.
5. With the code, the user can activate DigiD + SMS.
6. The user visits www.digid.nl again to install the DigiD app.
7. The user downloads the app.
8. Prior to being able to use the app, the user has to login with DigiD + SMS at mijn.digid.nl.
9. Subsequently the user has to scan a QR-code from mijn.digid.nl with the mobile app.
10. The app generates a code that has to be entered at the website by the user.
11. The user is asked to generate a PIN-code. The app is now connected to the user's DigiD account.
12. To enhance the assurance level to Substantial the user has to login again at mijn.digid.nl with the DigiD app.
13. A QR-code needs to be scanned with the DigiD app and the user is asked for the PIN-code.
14. The user is asked to scan the chip of his passport with the mobile phone's NFC interface.
15. The via NFC obtained personal information is compared with the information in the Municipal Personal Records Database.

16. If the verification is successful, the assurance level of the DigiD app will be increased to Substantial.
17. The user can login with the DigiD app and PIN-code. Periodically the DigiD authentication server will ask to user to scan his/her passport with the mobile app via NFC.

An interesting observation is that the selfie and interactive video activities are omitted during the vetting process for the Dutch national eID, DigiD, at level Substantial. These omissions reduce the assurance that the presented identity document indeed belongs to the rightful user. The eIDAS implementing regulation 2015/1502 requires for identity proofing and verification the following: "*An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it.*" Taking into account the last part of this requirement, it is debatable whether DigiD Substantial is compliant to eIDAS Substantial. Does this requirement imply the use of a selfie and liveness detection or can it also be sufficiently implemented by e.g. sending an activation code to the user's validated home address? If the ISO29115 assurance framework is used as a reference, there is no proof of possession requirement: "*LoA3 meets the objectives of LoA1 and LoA2, as well as the objective of verifying the identity information through one or more authoritative sources, such as an external database. Identity verification shows that the identity is in use and links to the entity. However, there is no assurance that identity information is in the possession of the real or rightful owner of the identity*." So, even with the omission of the selfie and interactive video activities, the Idensys process could be rated as LoA3 in the context of ISO29115.

### 3.4.3. e-Science

The EUGridPMA, an international organisation that coordinates the trust fabric for e-Science authentication in Europe, has published an acceptable process for implementing remote vetting via video[12].
The reference process consists of the following steps:

1. The RA or trusted agent sends a registration form (that can be largely pre-filled beforehand, except for a nonce that will bind the video to the submitted documents) to the email address of record for the applicant.
2. The applicant sends a scan of the (representative elements of) photoID to the RA or trusted agent.
3. Start a video conference (with sufficient quality such as HD Skype or Facetime; this helps to better identify the user and to check the authenticity of the identity document to be shown) during which the applicant has to write down some unique information - provided in real-time during the conference - on the form and sign it visibly during the chat.
4. Request that the applicant scans this form and e-mails it from the same email account of record to the RA or trusted agent in real-time.
5. Request that the applicant holds up the same form with the permitted photo-ID next to the face of the applicant, of which the RA or trusted agent makes a screenshot for record and records the ID document serial number.
6. The RA or trusted agent will check that the form is correct, contains the nonce and - in an ongoing video conference - that the person is the one represented in the documents

In this manner, the RA or trusted agent will have validated the data, photo-ID, and a video nonce, with the screenshot as proof.
Also a number of compensating controls are mentioned:

- Identify authenticity of the photo-ID over video, e.g. by checking over video for holographic images, thickness, and reality, and e.g. by changing viewing angle.
- Check for liveness of the applicant (which may be implicit in writing the nonce).
- Use it to capture a biometric (which includes face or voice recording).

[12] European Policy Management Authority for Grid Authentication in e-Science, guidelines for remote vetting, see http://wiki.eugridpma.org/Main/VettingModelGuidelines.

- Capture real-time response to knowledge-based questions, from multiple categories, in order to demonstrate continuation of conversation.
- Verify a telephone number by sending a text message, which is visible on the video conference.
- Demonstrate control over a (social media) account that is known to be associated with the applicant.
- Demonstrate control over a contact address (phone, etc) which is verifiable from public trusted records.
- Device type and geolocation consistency.
- Awareness of the context behind the application and credential type ("why does this request come in?").
- Ensure the credentialing data has been submitted by the applicant.

# 4. Remote vetting solutions

## 4.1. Remote vetting building blocks

Remote identity vetting can be done in numerous ways. Key ingredients of the identity vetting process are:

- Establishment of the identity of the user, i.e. can the user proof his identity;
- Verification of the identity of the user, i.e. is the user proofing his identity indeed that user.

The establishment of the user's identity concerns evidence collection and validation and is typically based on the showing of an official, state issued identity document such as a passport of driving license. In a remote or online setting, this translates to the verification of a picture/copy of the identity document or the verification of the information that is obtained from the chip on the document via Near Field Communication (NFC) technology. Alternatively, the user can use an existing reliable digital identity to proof his identity. For instance by logging in with a bank account (iDIN), government controlled account (Idensys) or government issued account (eIDAS). The assumption here is that the identity of the user has been established during the issuing process of these accounts.
The verification of the user's identity, i.e. is the user who he claims to be, is the next step. The goal of identity verification is to confirm and establish a linkage between the claimed identity and the real-life existence of the subject presenting the evidence. This can also be done in various ways:

- By biometric comparison of a picture of the user's face (selfie) with the picture that was obtained from the identity document (copy or from the chip via NFC). Obviously, liveness detection is key here. The user must not be able to use someone else's picture/selfie.
- Via a live video session between the user and the RA; during the session the user has to show his identity document. This tackles the liveness detection issue but comes with video manipulation threats such as real-time morphing to manipulate the user's face or identity document during the video session.
- Face-to-face at a registration desk that needs to be visited by the user or that visits the user. The current practice but more practically implemented.

Useful remote vetting solutions can be created by combining several of these building blocks and embedding them in the authentication triangle of Figure 2. This report considers the following long-list of nine remote/online vetting solutions:

1. Physically at the door;
2. Live video chat;
3. Mobile app with picture of identity document and selfie;
4. Mobile app with NFC technology for reading the chip of the identity document and selfie;
5. Derived identity from strong authentication by iDIN, Idensys, or iDEAL;
6. Derived identity from strong authentication by national eID solutions via eIDAS;
7. Central registration desk;
8. Reuse of existing registration desks at other organizations like municipalities, banks, Chamber of Commerce, Certification Authorities or other education and research institutions;
9. Community-based vetting, i.e. let other users do the vetting.

The following sections describe them in more detail and assess to what extent they fulfil the assessment criteria of section 3.3. We base this on what we consider a typical implementation.

## 4.2. Physically at the door

In this case the registration desk comes to the user. Specially trained and equipped personnel of dedicated companies visit the user at home and determine his identity face to face. Companies that offer such services include amongst others AMP Group[13], Dynalogic[14], and PostNL[15].
Alternatively, the RA of the institution could visit the user at the door and do the identification. This solution, however, creates a lot of overhead for the RA (i.e. it is very time consuming) and does not work for institutions that do not have an RA.

**Figure 5: front door identity check (from PostNL promo video).**

How could it work:

1. The user logs in at SCSA service, selects a strong authentication token and uses it, enters his address information, and receives an activation code via e-mail.
2. The SCSA service communicates the user's registration information (name, address) to the company doing the identification at the door and requests for an identification.
3. An employee of the company goes to the user and checks his identity, i.e. the user has to show his identity document (e.g. passport or driving license).
4. The employee asks the user's activation code and six last digits of the identity document. Both are registered.
5. The employee returns the outcome of the identification (OK/Not OK) and the activation code and six digits to the RA of the SCSA service.
6. The RA enters the activation code in the management portal of the SCSA service and activates the token. The user is informed via an email. If the identification is negative the token will not be activated and the user will be informed about this. This process step could be executed manually or automatically.

Compared to trustworthiness of the current process, this remote vetting process only lacks a proof of possession check of the token (step 7 of the current process, see section 2.1). The added value of this check is that it provides extra certainty about the binding between the user and his token. However, its implementation in the 'physical at the door' solution, is rather complicated as it requires the employee of the identification company to have access to SCSA's management portal, i.e. it requires the employee of the identification company to become an RA in SCSA and to have credentials to log in at the management portal. Furthermore, the user will have to type in a one-time password (Tiqr, SMS) or insert his token (Yubikey) in a terminal from the employee of the identification company, which can be considered as facilitating phishing or may be perceived as such by the user.

[13] https://ampgroep.nl/identificeren/face-to-face-identificeren/.
[14] http://www.dynalogic.eu/nl/safeandsecure/id-verification-authentication/.
[15] https://www.postnl.nl/ontvangen/pakket-ontvangen/bezorging-pakketten/id-check-aan-de-deur/.

Omitting the extra proof of possession check will reduce the assurance level of the vetting process. An identity fraud scenario exists that exploits a vulnerability that is created by the omission. This scenario consists of a man-in-the-browser (MitB) of the user that tries to register a YubiKey token at the SCSA service. When the user has registered the YubiKey and is asked to do an authentication with it, the MitB replaces the user's YubiKey output with the output of his own YubiKey to the SCSA service. This attack vector is mitigated by the proof of ownership requirement at the physical RA-desk. However, without this requirement, the attacker could successfully link his own YubiKey to the identity account of the user (that, being a MitB, he has hacked too). Consequently, the MitB is able to login to critical/sensitive services that require a strong authentication token.

Particularly the YubiKey token solution is adversely affected by this possible MitB exploit as it is rated with LoA 3 assurance. But will the omission of the second proof-of-possession check reduce the YubiKey LoA from 3 to 2? The answer to this question is not trivial as the existing frameworks for LoA assessment are not very specific about MitB threats. Most concrete is the European eIDAS assurance framework. This framework states for assurance level Substantial (which is more or less equivalent to SCSA LoA3) that "The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms." (for level Low/LoA2 protection against an enhanced attack potential is required).

For this requirement, eIDAS reuses terminology from ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security" and ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation".[16] ISO/IEC 15408-1 defines "attack potential – measure of the effort to be expended in attacking a [mechanism], expressed in terms of an attacker's expertise, resources and motivation". For a moderate attack potential this translates to professional attackers (i.e. hackers with sufficient skills, time, expertise and capabilities). From these attackers, it is to be expected that they can successfully execute a MitB- attack. Consequently, the LoA of the proposed at the door vetting scenario drops from 3 to 2 for YubiKey as no MitB control measures are in place.

With compensating controls it is possible to increase the LoA to 3 again for YubiKey. Possible controls are:

- Notification: the user is notified, via a separate channel, about each login with the token. For each authentication he receives an email or SMS telling him he has logged in at a certain service provider. This allows the user to take action in case something is wrong. The drawback of the control is that it is very invasive for the user and costly for SCSA (costs of SMS-es for each login). For LoA4 solutions this notification requirement is mandatory in some frameworks (e.g. eHerkenning).
- Separate channels/platforms: force the user to make use of multiple separate out of band channels/platforms such as desktop and mobile phone. This way it is harder for the MitB attacker to compromise the registration and vetting process.
- Fraud detection: that monitors abnormal user behaviour. Monitoring strange authentication behaviour is challenging as it provides far less information than e.g. financial transactions that banks use to detect abnormal behaviour. One could for instance monitor IP-addresses.
- Passport scan: Ask the user to scan his passport with a Near Field Communication reader; the output contains personal identifiable information and will be communicated to the SCSA management portal for verification of the user's identity. A MitB must have access to the user's passport to successfully register and activate a token.

[16] The text of the standards is also freely available at www.commoncriteriaportal.org/cc, (CCPART1-3 being equivalent to ISO/IEC 15408 and CEM equivalent to ISO/IEC 18045).

Similar to asking the user to do an authentication at the door, implementing these compensating controls obviously is not trivial.

Note that also SMS authentication is affected by the MitB attack. The user has to enter his mobile phone number in the browser, this number may be adjusted by the attacker. The Tiqr solution requires more effort from the MitB attacker and seems less vulnerable. For LoA 2 solutions, however, the security measures against MitB are little, so these two solutions will keep their LoA 2 rating.
The assessment of the solution against the identified criteria is as follows:

| Criteria | Assessment | Score |
|---|---|---|
| Easy to use by user | Very easy. It does not require any traveling and may even be possible outside working hours (e.g. in the evening or during weekend). | Easy for the user. |
| Easy to organize by institution | Institutions do not need to setup an RA. | No hassle for the institution. |
| Limited impact on SCSA | The impact on the SCSA service is large. Name and address of the user are required and need to be processed by SCSA.<br>A company doing the identification at the door needs to be contracted and provisioned with the right information. The employee of the identification company needs to be instructed on what to do (check name, identity, get activation code, register last six digits identity document, etc.).<br>Furthermore, the outcome of the identification needs be communicated to a central RA for further automated or manual processing. | Large organisational impact; average technical impact on the SCSA service. |
| Straight-through processing | The RA needs to process the outcome of the identification at the door prior to activating the token. Initially, this will typically be a manual process as automating will require adjustments of the management portal of SCSA. | Similar automation level in terms of processing time and efficiency. Token activation may be automated. |
| Penetration rate / coverage | Only works nationally. Does not work for users that live abroad (use case 2) as it requires with a contract with a company that does identification at the door on an international scale. These companies do not exist. Alternatively, separate contracts with national companies have to be closed; this does not scale. | Does not work internationally. |
| Assurance level | Assurance levels 2/Low can be achieved with this solution. Level 3 / Substantial cannot be achieved for YubiKey without implementing additional security measures. | For YubiKey the LoA drops from 3 to 2 in the proposed scenario. |

| | | |
|---|---|---|
| Costs | About 12-18 Euro per identification[17]. For a small user-base this is doable; if the user-base becomes too large these costs may become a showstopper. | Significantly higher than currently, but not insurmountable. |
| Controllability/auditability | The company doing the identification at the door needs to be audited regularly. This can be arranged contractually (i.e. the right to audit). The output of the vetting at the door must be archived by the RA for accountability purposes. | |
| Future proof | Identification at the door services are offered by several private companies. Authentication service providers in Idensys and eHerkenning make use of these services for the issuance of their tokens. | |

## 4.3. live video chat

Identity vetting during a live video chat typically proceeds as follows: the user starts a video chat an employee of the institution or a dedicated company. The employee asks the user to show his identity document (i.e. passport or driving license), does an optical check of the authenticity of the document and identifies the user by comparing his face with the photo on the identity document. The employee must be trained to do this. Additional questions may be asked to verify information that was provided by the user during the registration process. Example of companies that offer video identification services are WebID Solutions[18] and AMP Group[19]. WebID Solutions is used by banks in Germany for customer enrolment. AMP Group's solution will be used by Idensys authentication providers. The RA of one research institution also makes use of video-based vetting.

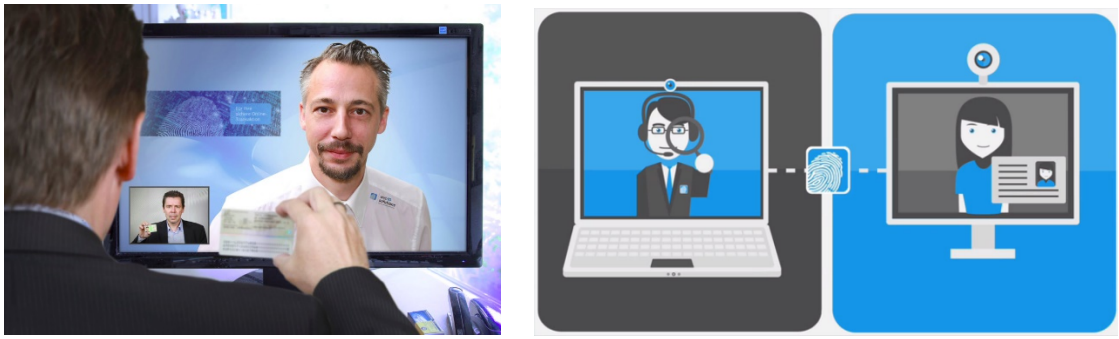

**Figure 6: Video identification (from WebID Solutions promo video).**

A leading standard for video identification is that of the German Federal Financial Supervisory Authority (BaFin). The standard describes the requirements a video identification solution has to adhere to. The standard has recently been updated and includes requirements for training of employees, premises the employees must be situated in, consent, security of the system, verification of identity documents, verification of the user's identity, video conditions, output, retention and

[17] Sources: BKR website https://www.bkr.nl/consumenten/opvragen-gegevens/bezorg-identificatiemethodes/ and letter Ministry of Interior to the government https://zoek.officielebekendmakingen.nl/kst-26643-352.html.
[18] https://www.webid-solutions.de/en/.
[19] https://ampgroep.nl/identificeren/identificeren-via-de-webcam/.

recording, and data protection.[20] For example, it is obligatory to record the entire identification process on video in order to be able to verify it at any time. Further requirements are the end-to-end encryption of the video identification and a solid visual inspection of at least three security features of the identity document (e.g. the holograms, the changeable laser image and the security printing on the identity document).

Given these requirements, it is not recommended to develop a proprietary video identification service for SCSA. The use of existing video identification services offered by professional companies is recommended. It is also recommended to let the video identification service only do the identification of the user and a separate RA do the activation of the token. The latter can be automated. Turning the video service into an RA requires customization of the service and is expected to come with high costs. There is one institution that combines SCSA with remote vetting via video and done by their own RA. Though the institution is positive about the solution, it turns out that, compared to physical identification, video-based identification comes with substantially more overhead. Particularly the scheduling of the video session consumes a lot of time. This confirms the conclusion that a specialised video service provider should do the identification and not the RA.

The BaFin update is a countermeasure to advanced video manipulations based on morphing technology. Research by the German Bundesamt für Sicherheit in der Informationstechnik shows that with state-of-the-art morphing technology video recordings of faces or identity documents can be real-time and accurately manipulated. An example is shown in Figure 7.

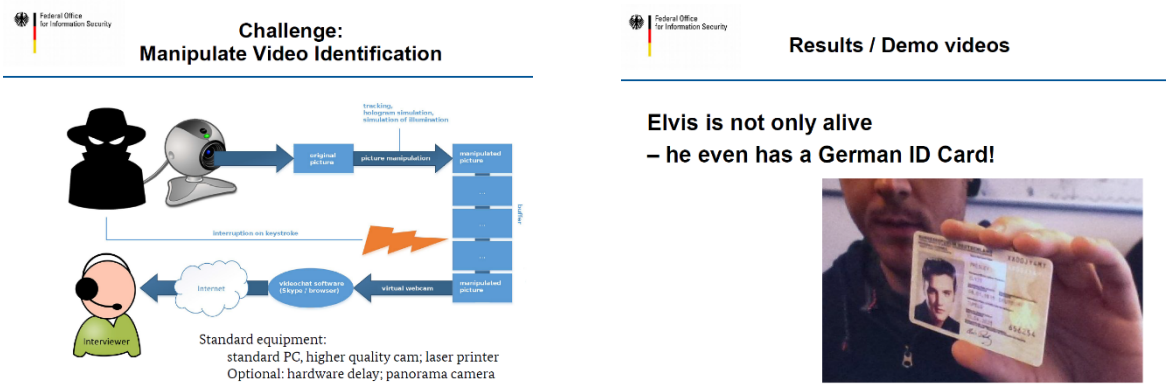


**Figure 7: German BSI research results on video manipulation of ID cards (from a presentation; slides are not publicly published).**

A test by CESNET, the e-infrastructure provider of the Czech Republic, between a few Certificate Authority admins, attempting to validate a regular national Czech identity card based on its security features, was not successful as the quality was too low to adequately assess them, and features like holograms and such were not part of the card anyway[21]. Based on this initial test (and even though remote vetting would be very welcome) this has not yet been proposed for adoption by CESNET.
The UK home office has examples of 'good looking' fake documents; this demonstrates how hard it is to optically distinguish an authentic identity document from a counterfeited one[22].
This is how it could work:

[20] BaFin requirements for video identification procedures, see https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/2017/rs_1703_gw_videoident_en.html.
[21] Source: http://wiki.eugridpma.org/Main/VettingModelGuidelines.
[22] UK Home Office Guidance on examining identity documents, 2016, see https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/536918/Guidance_on_examining_identity_documents_v._June_2016.pdf.

1. The user logs in at SCSA service, selects a strong authentication token and uses it, and receives an activation code via e-mail.
2. The SCSA service communicates the user's registration information (name and activation code) to the company doing the video identification.
3. The video identification service is started (could be done immediately after user registration).
4. The employee of the video identification service identifies the user and inspects the authenticity of the showed identity document.
5. The employee of the video identification service records the activation code and the last 6 digits of the identity document number (this is in line with the current process, instead of the last 6 digits the video identification service could store stills or video fragments for accountability purposes).
6. The employee of the video identification service reports the outcome of the identification and recorded evidence to the SCSA RA.
7. The SCSA RA processes the outcome, activates the token and informs the user.

Basically, this remote vetting *process* is similar to that of identification at the door. The assessment against the criteria, however, is somewhat different as can be seen in the table below.
Compared to the Idensys process (see section 3.4) the proposed process lacks the 1-ct iDEAL transaction. This process step, however, is replaced by the user login in with his institutional account. The assurance level of the institutional account is lower than that of the bank authentication for iDEAL. However, the purpose of this step is to obtain identity information that can be used for comparison with information obtained later on in the video process. The identity information provided by the institution's identity provider is considered to be as reliable as the information obtained via iDEAL. So, the proposed process provides identity assurance at level Substantial or LoA3.
Furthermore, the proposed process for video-based vetting lacks the second token-proof-of-possession check. This check could be added to the process but implies that the party doing the video-vetting has access to the SCSA management portal. For third parties this is cumbersome; for an institutional or a central RAs this is easy.

The assessment against the criteria is as follows:

| Criteria | Assessment | Score |
|---|---|---|
| Easy to use by user | Relatively easy. An overall video identification takes about 10 minutes time of the user[23]. Though this may seem a short time, the number of users that stop during the process is relatively high. However, compared to a visit at the RA this is more user friendly as it can be done 'from the couch' and at almost any time of the day. | |
| Easy to organize by institution | Only a central RA required, so no desks at each individual institution.<br>In case the institutional RA does the video-vetting: be aware that it typically takes more time than a physical vetting at the desk. There is more organisational overhead involved for video-vetting (e.g. scheduling, calling, explaining). | |
| Limited impact on SCSA service | Requires a contract with a company that does video identification. | Large impact. |

[23] Own experience with a video identification with WebID service.

| | | |
|---|---|---|
| | The video identification service needs to be informed about the user to be identified and the activation code he has.<br>The outcome of the video identification must be communicated to the RA of SCSA.<br>Evidence of the video identification need to be communicated as well and archived by the RA. Latter may come with privacy complications. | |
| Straight-through processing. | The RA needs to process the outcome of the identification. This is a manual activity and will lead to the activation of the token. The duration of the process is similar to that of the current solution. Automating it is possible but implies software changes in the SCSA service. | Process time is similar compared to the current process. |
| Penetration rate / coverage | Requires a video client and good internet connection, these are widely available. Users from all over the world can be vetted. | Works internationally. |
| Assurance level | The assurance level of video identification is negatively influenced by several factors:<br>1. Poor internet connection and illumination conditions may hamper the identification of the user.<br>2. Poor hardware for video and voice processing.<br>3. It is difficult to optically assess the authenticity of the showed identity document via a video connection.<br>4. Real time video morphing technology is advancing rapidly and allows the user to pretend to be someone else or to alter the identity document. The German Federal Office for Information Security did some experiments with morphing technology and concluded that video is not optimal for identity verification purposes.<br>Substantial/LoA 3 is the maximum level of assurance that can be achieved by video identification. For Yubikey, the second proof-of-possession check needs to be implemented. | OK, but requires some attention.<br><br>YubiKey LoA may drop to 2 if the second proof-of-possession step is not implemented. |
| Costs | About 15-20 Euro per video identification[24]. | Significantly higher than currently, but not insurmountable. |
| Controllability/auditability | The company doing the video identification needs to be controlled. This can be arranged contractually (i.e. the right to audit). Evidence of the video identification need to be recorded. | |
| Future proof | Video identification is used in the German financial sector. One Idensys/eHerkenning member will provide this solution in the near | |

[24] E.g. https://www.notarycam.com/pricing/.

| | | |
|---|---|---|
| | future. However, with the increasingly improving video manipulation technology, it is questionable of these services will continue to exist in the near future. Video manipulation countermeasures will likely have a negative influence on the vetting process (i.e. take more time, be more expensive, less user friendly, etc.). | |

## 4.4. Mobile app – optical + Selfie

This solution comprises a mobile app that allows the user to remotely vet his identity. After installing the app on the mobile phone, the user is asked to take a picture of his identity document. This picture is sent to the app owner company for further processing. This processing includes digitizing the information on the photo (name, birth data, gender, etc.) for further automatic processing, assessing the authenticity of the identity document based on the provided photo, and checking if the identity document is not registered as lost or stolen. Subsequently, the app asks the user to take a selfie. The selfie is compared to the picture on the photo of the identity document. Usually this is done manually by the RA. Upon a positive identification, the user's token is activated.

Compared to the vetting process for DigiD Substantial there are several differences. Where DigiD Substantial makes use of an activation code that is sent to the verified home address of the user, the optical app does not have this control feature (as reliable address information is difficult to obtain for non-government organisations). Instead the mobile optical app solution makes use of a selfie as a compensating measure. For obtaining the right level of assurance.

Particularly the authenticity check of the identity document is challenging for the mobile optical app solution. The uploaded picture of the document can be manipulated/photoshopped and it is hard to verify all of the identity document's optical security features from a picture.

To prevent users from using a selfie of someone else, some form of liveness detection has been built in. An example of a liveness detection solution is to ask the user to execute a random number of challenges during a video session (e.g. turn head left or right, nod, smile, eye blink or speak out a certain sentence). The employee checks if the user adequately responses to the challenges. Idensys participants such as Digidentity and Morpho/SecureIdentity make use of such video challenge-response solutions. An alternative solution for liveness detection is to use flashing colours during the video recording of the user, this is offered by iProov[25].

[25] https://www.iproov.com/

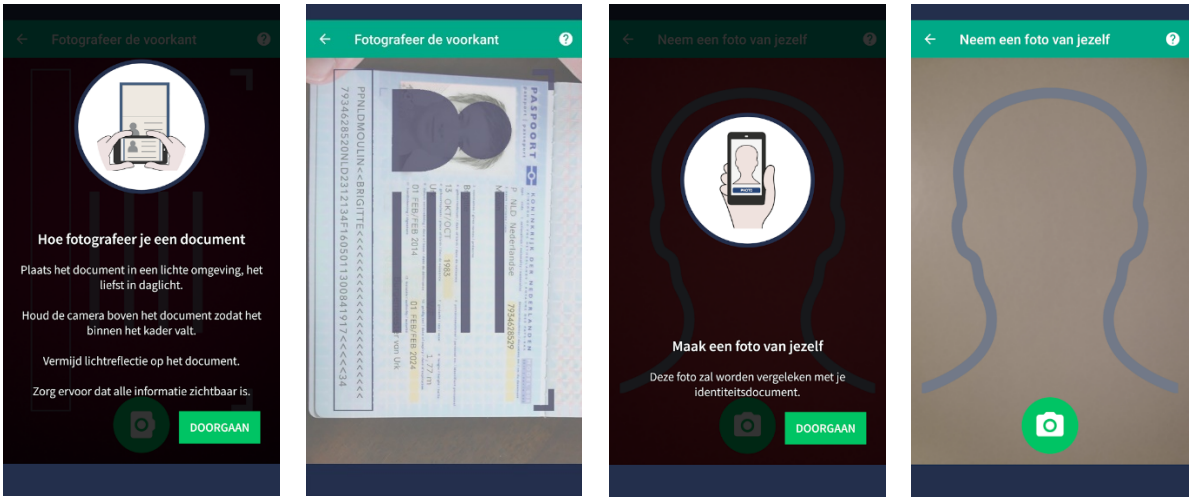


**Figure 8: Remote identification via mobile app (Digidentity pictures from Google Play app store).**

Sometimes a 1-ct iDEAL transaction is required to provide extra identity information, it allows the company to compare the user's name of the bank account with the name on the identity document. This is for instance the case for users that want to acquire an Idensys LoA 3 (substantial) authentication solution. Digidentity is a company that offers this solution[26]. As said before, the iDEAL transaction can in the SURFconext context be replaced by logging in with the federated institutional account.
This is how it could work:

1. The user logs in at SCSA service, selects a strong authentication token, enters his first and last name and receives an activation code via e-mail.
2. The SCSA service asks the user to install a mobile identification app. The app is bound to the user's web session via a QR-code that is generated by the SCSA service.
3. The newly installed app asks the user to take a picture of the identity document.
4. The app asks the user to take a selfie.
5. The app does liveness detection (e.g. via a video-challenge, flashing colours or otherwise).
6. The app asks the user to enter the activation code.
7. The app communicates the output to the SCSA service.
8. The RA of the SCSA processes the obtained output, informs the user that the identification was OK, and activates the token.

The processing in the last step includes a detailed inspection of the picture of the identity documents to check if it is authentic. The RA could do this, or he could outsource it to professional companies, such as IDchecker/Mitek[27]. These companies can also check if the identity document is not registered as stolen or lost. Furthermore, the RA (or company to which this is outsourced) must verify that if the user on the picture of the identity documents is the same user that took the selfie by comparing both pictures. This process is difficult to automate due to the low resolution of the identity document picture, i.e., there will be significant amounts of false rejects.

Despite the This solution offers sufficient protection against the MitB-attack as it makes use of a separate channel (i.e. the mobile phone) for the communication of the activation code that was obtained during registration. This code is now communicated via the mobile app and not the desktop's web browser.

[26] https://www.digidentity.eu/nl/home/#idensys.
[27] http://www.idchecker.nl/.

The criteria assessment is as follows:

| Criteria | Assessment | Score |
|---|---|---|
| Easy to use by user | Relatively easy. According to Digidentity, an overall identification takes about 15 minutes (including a 1-ct iDEAL transaction). Just like video identification this may take too long for a substantial group of users. Nevertheless it is far more convenient for a remote user to use than to visit a service desk. | Relatively friendly. Will the user be willing to install the app? It is important to guide the user well through the whole process of app-installation and identification. |
| Easy to organize by institution | Relatively easy to organize by the institution; no RA functionality is required at the service desk. | Easy for the institution. |
| Limited impact on SCSA service | Requires a mobile app that communicates its output (picture of identity document and selfie) to SCSA service for further manual validation/processing by a central RA. Less organisational impact compared to the video or door identification (e.g. no workflow instructions). | Adjustments of SCSA to communicate with an app. A central RA is required. |
| Straight-through processing | The RA must compare the picture of the identity document with the selfie. This is a manual activity. The duration of the process is similar to that of the current solution.<br>Potentially, the app could do face recognition with the selfie and photo on the identity document. It, however, is questionable if this will result in reliable outcomes, i.e. the false acceptance or rejection rate may be too high for sufficient assurance[28]. This is due to the fact that the photo on the identity document is small and of low resolution. Moreover, the quality of the camera of the mobile phone may also play a role. Manual inspection therefore is recommended for this solution.<br>Other aspects on the picture of the identity document like validity and name can also be processed automatically via Optical Character Recognition (OCR) but this too is not trivial. | Some manual effort still required. |
| Penetration rate / coverage | Anyone with a smartphone can do this. Could work internationally. | |
| Assurance level | The assurance level of video identification is negatively influenced by several factors:<br>1. It is easy to manipulate the picture of the identity document prior to sending it. | LoA 2 is the highest achievable assurance level. |

[28] Authentication assurance frameworks hardly address biometric authentication solutions. E.g. it is unclear what the false acceptance rate must be for a LoA4 solution. Only the recent NIST specification addresses the topic.

| | | |
|---|---|---|
| | 2. It is difficult to assess the authenticity of the identity document based on the picture.<br>3. The selfie can be faked easily.<br>4. Liveness detection via video challenge response is not always very reliable. | Note that Idensys rates this process with LoA3. |
| Costs | Similar as current situation as some manual RA involvement is required. | Similar costs. |
| Controllability/auditability | The mobile app guides the user through the vetting process in an unambiguous manner. The app should be pentested for security vulnerabilities (one of the requirements of the eRecognition/Idensys level of assurance framework). Evidence of the identification should be recorded and stored by the RA. | |
| Future proof | Mobile app based and optical identity vetting is deployed by Idensys authentication service provider Digidentity. For higher LoA's (3 and 4), this solution is not good enough. The biometrics part of this solution, i.e. face recognition, is expected to rise in popularity as an accepted authentication solution. | |

## 4.5. Mobile app – NFC + selfie

This solution is similar to the previous one. However, instead of taking a photo of the identity document the information in the chip of the document is read out via NFC technology. This has some advantages. Firstly, the information thus obtained is already digital and can be processed immediately. Secondly, the information is digitally signed and can be validated for authenticity. Thirdly, the chip itself can be challenged to check if it is not a clone. Finally, the app can automatically check if the identity document has not been registered as stolen or lost.
The information obtained from the chip also contains a picture of the user. The size and resolution of the picture is higher than the one on the document itself and allows for automatic comparison with the selfie. Companies that offer such a NFC solution include InnoValor Software (ReadID)[29] and Morpho[30].

**Figure 9: NFC scanning of identity document via mobile phone (from ReadID promo picture).**

[29] https://www.readid.com/.
[30] http://secureidentity.nl/.

NFC is not (yet) enabled for iPhone users[31]. These users will need to borrow an Android phone to do the NFC part of the vetting process. Moreover, not all Android phones are NFC-enabled. So coverage is an issue for this solution.
Globally, most passports have a chip that can be read via NFC (see Figure 10 below). In the Netherlands all passports have a chip, as do all identity cards.

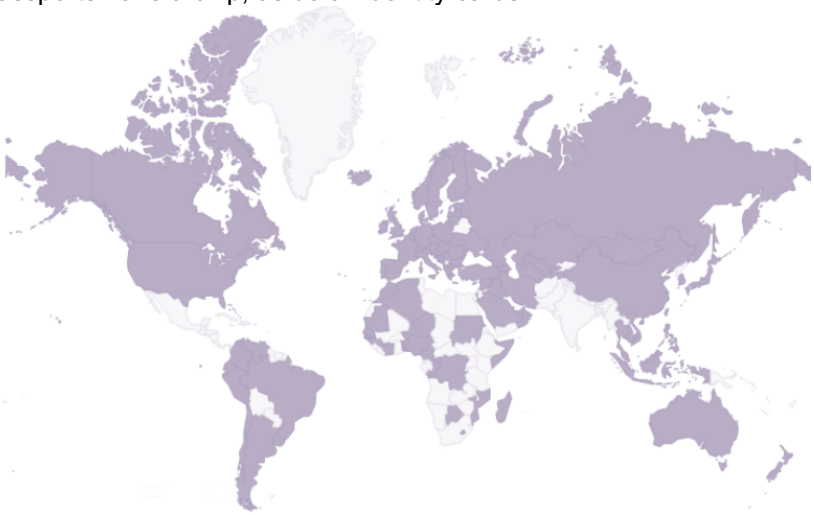

**Figure 10: Countries that have a chip on their passport that can be read with NFC technology.**

This is how it could work:

1. The user logs in at the SCSA service, selects a strong authentication token, and receives an activation code via e-mail.
2. The SCSA service asks the user to install a mobile identification app. The app is bound to the user's web session via a QR-code.
3. The app reads out the chip of the identity document via NFC.
4. The app asks the user to take a selfie[32].
5. The app does liveness detection (e.g. via a video-challenge, flashing colours or otherwise); this is an automatic process and does not involve any human interference.
6. The app asks the user to enter the activation code.
7. The app communicates the output to the SCSA service.
8. The SCSA service automatically processes the output of the app (i.e. biometric identification based on selfie and identity document picture, comparison of activation codes, comparison of names), informs the user that the identification was OK, and activates the token.

The last step can be conducted fully automatically and does not require any manual involvement of the RA, i.e. it allows for straight-through processing of an identity enrolment via SCSA.
The assessment against the criteria is as follows:

| Criteria | Assessment | Score |
|---|---|---|
| Easy to use by user | Relatively easy. According to ReadID, an overall identification takes about 5 minutes. This excludes the installation of the app. It is | For Android users. |

[31] As it stands today, NFC is used on the iPhone solely to transmit payment requests between a mobile device and a card reader. This is because Apple restricts how the chip is used at a system level within iOS. With the new Core NFC framework, however, Apple could let third-party developers make use of NFC in novel ways, or it could simply expand NFC functions beyond Apple Pay for use in its own apps and services.
[32] As an alternative to DigiD Subsantial's address check.

| | | |
|---|---|---|
| | recommended to properly guide the user through the whole process to prevent them from taking off prematurely. | |
| Easy to organize by institution | Relatively easy to organize by the institution as no local and physical RA is required anymore. | |
| Limited impact on SCSA service | Requires a mobile app that communicates its output (NFC scan of identity document and selfie) to the SCSA service for further validation. Likely, this can be done automatically by SCSA service (i.e. comparing NFC-obtained picture with selfie and do other checks). | Adjustments of SCSA to communicate with an app. No physical central RA required as processing can be done automatically. |
| Straight-through processing | STP is possible and may shorten the duration of the vetting process. | Can be done fully automated. |
| Penetration rate / coverage | Anyone with an NFC-enabled smartphone can do this. Currently this includes most Android devices[33]; the NFC interface of iPhones cannot be used at the moment. iPhone users could ask an Android user to use it for reading the chip via NFC. Could work internationally. A few non-Dutch users may be from countries with chip-less passports, or may not even have a passport. In the Netherlands all valid passports have a chip. | Does not work for iPhone users without adjustments. |
| Assurance level | Compared to optical solutions, the NFC solution provides more assurance regarding the authenticity of the identity document. It provides a higher resolution picture of the user that improves the identification assurance. Liveness detection is as good as for the optical solutions.<br><br>LoA 3/Substantial is the maximum level of assurance that can be achieved by mobile and NFC identification. Omitting any aspects such as liveness detection or the selfie-based biometric face identification will reduce the LoA to 2 / Low. These less elaborated variants of the NFC-based solution may lose assurance level reliability but may compensate this by gaining improved user experience/user friendliness.<br><br>MitB attacks are mitigated via the mobile app, so YubiKey keeps its LoA3 rating. | |
| Costs | About 5 Euro per NFC identification. | |

[33] About 60% of business users have an Android phone, see https://www.computerprofile.com/nl/analytics-papers-nl/apple-en-samsung-meest-voorkomende-zakelijke-smartphones-nederland (in Dutch).

| | | |
|---|---|---|
| Controllability/auditability | The mobile app guides the user through the vetting process in an unambiguous manner. The app must be pentested before it goes into production stage (is a eRecognition/Idensys requirement; the whole system that is used for authentication should be tested, but this is generally part of the ISO27001 certification which is another requirement). The app and/or RA must collect evidence of a successful identification. | |
| Future proof | Idensys member Morpho makes use of this technology. Also improvements of DigiD are NFC-based. It is expected that this technology will see an increasing uptake in the near future. Biometrics, the other part of this solution, is becoming more and more popular these days on mobile devices (due to Apple's TouchID). The technology is improving and becoming less intrusive to the user. | |

## 4.6. Derived identity – national

In the Netherlands there are several identity providers that offer authentication solutions with a substantial or high assurance level. Examples are iDIN and Idensys. The idea behind this solution is to let iDIN or Idensys vet for the identity of the user via an authentication with an iDIN or Idensys solution. After all, the iDIN or Idensys authentication service providers had to identify the user prior to issuing their authentication solution to him. This is called *derived* identity.
With derived identity, the user is asked to login with an iDIN or Idensys authentication solution at the SCSA service when he registers a token. The accompanying iDIN or Idensys authentication assertion contains sufficient information (e.g. first and last name and date of birth) to establish the identity of the user, i.e. the iDIN/Idensys asserted identity information is matched with the institutional IdP asserted identity information to establish the identity of the user.
Instead of iDIN or Idensys, the user can also be asked to make a 1-ct iDEAL transaction, as this also involves authentication with a bank solution. Since the iDEAL output consists of the initials and last name of the account holder, holders or delegate(s) this is a less reliable solution.


**Figure 11: Derived identity solutions.**

How could this work, with iDIN as example:

1. The user logs in at SCSA service, selects a strong authentication token, uses it, and receives an activation code via e-mail.
2. The SCSA service asks the user to login with iDIN.
3. The user logs in with iDIN.
4. SCSA obtains initials and last name from iDIN and compares them with the information provided by the home identity provider of the user (i.e. the institution).
5. SCSA asks the user to enter the activation code.
6. SCSA processes the entered code, activates the registered token and informs the user.

Compared to the current vetting process, this process lacks the registration of the last six digits of the identity document of the user for audit purposes. iDIN or Idensys simply cannot provide this

information. As an alternative, these solutions could provide, e.g., the date of birth of the user or his iDIN/Idensys pseudonym.

A drawback of iDIN is that it does not provide full first names but only initials. This may hamper the matching with the full names provided by the institutional identity provider. Additional information such as date of birth may help to increase the matching assurance. iDIN can provide such information. It is unclear if the institutional identity provider is able to assert for the user's birth date and if he is allowed to do so in this context (from a goal binding and/or subsidiarity, i.e. privacy, point of view).

A specific risk associated to using iDEAL for vetting purposes is that the owner of the account may have mandated another user to make financial transactions on his/her behalf. In that case, the mandated user may present himself as the owner of the account during the registration phase of a new authentication solution. For iDIN and Idensys this risk does not exist. An advantage of iDEAL is that it provides the bank account number of the user, for certain use cases this might be useful.

Note that, contrary to the current SCSA situation, the user has to show proof of possession of the registered token only once. Moreover, the whole process runs through the browser. So, the derived authentication solution is vulnerable to a MitB. This means that the YubiKey assurance level drops to LoA2 (unless additional measures are taken).

A big question is if users are willing to use their bank account credentials for obtaining a work-related strong authentication credential? User evaluation studies are contradictory with each other. A Panteia user evaluation study on the use of iDIN for public services shows that users in general do not experience the reuse of their bank credentials as an obstacle for getting access.[34] A SAMR study, on the other hand, concludes that users will be reluctant to use iDIN for public services and prefer DigiD instead[35]. It is unclear if users are willing to use iDIN for more private-oriented services such as SCSA.

The criteria assessment is as follows. We limit ourselves here to iDIN since this has a much higher penetration than Idensys and is more secure than iDEAL, since it provides the name (and other attributes) of the person logging in contrary to only bank account information.

| Criteria | Assessment | Score |
|---|---|---|
| Easy to use by user | Very easy. The user only has login with a strong, authentication credential he already possesses (e.g. his bankcard). | Are users willing to use their bank credentials for work-related activities? |
| Easy to organize by institution | Relatively easy to organize by the institution. A local and physical RA is not required anymore as the user's token can be automatically activated. | |
| Limited impact on SCSA service | Requires the user to login at the SCSA service with external strong authentication solutions. Extra functionality is required to perform automated matching of first and last names and the activation code. Matching may not be trivial as iDIN typically provides initials instead of full first name. | Name matching challenges may complicate things. Extra attributes may help to improve matching, but |

[34] "Gebruikerservaringen pilots publieke en private eID-middelen", Panteia, 2016, see https://zoek.officielebekendmakingen.nl/blg-780660.pdf.
[35] "Communicatieonderzoek elektronische identificatie (eID)", SAMR, 2017, see https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2017/05/29/communicatieonderzoek-eid/Rapportage+communicatieonderzoek+eID.pdf.

| | | |
|---|---|---|
| | | may come with privacy issues. |
| Straight-through processing | STP is possible and shortens the duration of the vetting process. | STP might be hampered by matching challenges (see above) and may need manual involvement (at least at the start). |
| Penetration rate / coverage | 86% of the Dutch have a bank authentication credential. This makes iDIN as a likely candidate for derived identity vetting. iDIN, however, only works for users with a Dutch bank account. This may exclude international users. | |
| Assurance level | With iDIN, is the maximum level of assurance that can be achieved is 2/Low. This is sufficient for the SMS and Tiqr SCSA solutions, but not for YubiKey. | |
| Costs | About 30 Eurocent for each iDIN identification. Depends on the amount of validated attributes that the chosen authentication solution has to assert for. Additional attributes beyond name, data of birth, address, and gender usually come with additional costs. | |
| Controllability/auditability | iDIN and Idensys authentication is highly controlled and governed by independent authorities. All other functionality is centralised and under the control of SURFnet. The iDIN/Idensys authentication assertion and matching output with the IdP-assertion could be archived for accountability purposes. | |
| Future proof | The 1-cent iDEAL transaction is used for several years already for identity proofing. Online banks such as Knab makes use of derived identity for the enrolment of new customers. | |

## 4.7. Derived identity – international (eIDAS)

International users typically will not have an iDIN or Idensys credential. They, however, can be authenticated with their own national eID solution via the eIDAS infrastructure. eIDAS allows for cross-border authentication in Europe[36]. Condition for this is that the SURFconext Strong Authentication service is connected to the eIDAS infrastructure. An eIDAS authentication assertion is of assurance level substantial or high and contains sufficient identity information of the user for vetting purposes. This is how it could work:

1. The user logs in at SCSA service, selects a strong authentication token, and receives an activation code via e-mail.
2. The SCSA service asks the user to login with eIDAS.
3. The user logs in with his national eID solution via eIDAS.

[36] https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification.

4. SCSA obtains first (full names typically) and last name from eIDAS and compares them with the informed provided by the user.
5. SCSA asks the user to enter the activation code.
6. SCSA processes the entered code, activates the registered token and informs the user.

The assessment against the relevant criteria:

| Criteria | Assessment | Score |
|---|---|---|
| Easy to use by user | Very easy. The user only has login with their national eID solution. | |
| Easy to organize by institution/SC | Relatively easy to organize by the institution. A physical RA is not required anymore; token activation can be automated. | |
| Limited impact on SCSA service | Requires the user to login at the SCSA service with external strong authentication solutions via eIDAS and automated matching of first and last names and activation code. | |
| Straight-through processing | STP is possible and shortens the duration of the vetting process. | |
| Penetration rate / coverage | Only works for EU member states that have notified their national eID solution and have indicated that it can be used by non-public service providers. The eIDAS regulation comes into effect in October 2018. It is expected that most European member states will have notified their national eID by then. For users outside of Europe, this does not work. | At least for the coming years penetration is likely quite low, and never outside EU. |
| Assurance level | With eIDAS potentially substantial or high can be achieved, these correspond to LoA 3 and 4 of ISO29115. LoA2 is largely out of scope for eIDAS: other EU member states do not have to accept national eID solutions with this assurance level; acceptance is based on a voluntary basis. The MitB attack scenario, however, reduces the eIDAS solution to LoA2. | |
| Costs | For free for public services, we assume here that SCSA will be considered such. If SCSA is considered a private service, it is currently unclear what the costs will be. | |
| Controllability/auditability | National eID solutions are peer-reviewed prior to notification and recognition under eIDAS legislation. This peer review includes the vetting process. | |
| Future proof | eIDAS is still very immature. Being a EU regulation it is expected to be future proof, unless it turns out to be a disaster. With the recent notification of Germany and the indication of other member states that they will also notify in the near future it is expected that eIDAS will slowly find traction in the coming years. | |

## 4.8. Central registration desk

Instead of setting up registration desks at each higher education and research institution, one or two central desks can be set up. This reduces the operational costs of the desks but requires the user to travel more. Likely candidates for central registration desks are SURFnet in Utrecht and UvA/VU or SURFsara in Amsterdam.

**Figure 12: Central registration desk.**

This solution marginally deviates from the current practice. The central RA could play a role in the processing of output information gathered at the door, video or mobile app identification solutions for remote vetting.

The assessment:

| Criteria | Assessment | Score |
|---|---|---|
| Easy to use by user | Not very easy. The user has to travel to the central desk. | |
| Easy to organize by institution | Convenient for most institutions. | |
| Limited impact on SCSA service | No impact on the service itself. The central desk(s) have to be catered for by one or more institutions or SURFnet. | |
| Straight-through processing | STP is not possible. The duration of the vetting process is similar to that of the current practice. | |
| Penetration rate / coverage | Relatively low. Does not work for users outside the Netherlands. | |
| Assurance level | Level 2/Low or 3/Substantial can be achieved. | |
| Costs | Cheaper than the current situation where every institution has to operate a desk. | |
| Controllability/auditability | Central vetting desks can be controlled relatively easy. Audit could be part of SURFaudit. | |
| Future proof | Registration desks are proven practice that will continue to exist. | |

## 4.9. Reuse of existing registration desks

Several companies still have a strong regional presence and could cater for vetting services. Examples are post offices of PostNL, banks, business offices of the Chamber of Commerce, telecom stores (such as Mediamarkt) and other RA-enabled institutions. For instance new customers for insurance company ASN can go to a regional PostNL desk for identification[37]. PostNL also identifies

[37] https://nieuws.asnbank.nl/asn-klanten-kunnen-voor-identificatie-naar-postnl.

customers of KPN that want to buy an Idensys credential[38]. From an organisational point of view, reuse of RA-desks that are already in place at several institutions is the most convenient; hiring an external desk requires much more contractual hassle.


**Figure 13: Reuse of existing registration desks.**

Two variants exist for this solution:

1. The registration desk is a full-blown RA. This implies that the desk employee has to have access to the SCSA management portal and knows how to work with it.
2. The registration desk only does identification and communicates the result to a central RA.

The first scenario is not very realistic as it has a huge impact on the existing registration desks and comes with significant SCSA access management overhead. The second scenario better suits the identification practices of the existing desks and is more realistic. How it could work is more or less similar to identification at the door.
The criteria assessment of the second scenario is as follows:

| Criteria | Assessment | Score |
|---|---|---|
| Easy to use by user | The user still has to travel to the registration desk, but less far. Does not work for international users however. | |
| Easy to organize by institution | Relatively easy to organise by the institution as no desk is required (except for the ones offering an RA-desk that can be reused by other institutions). | |
| Limited impact on SCSA service | A company offering physical registration desks has to be contracted. Less effort is required if another institution's RA-desk is used.<br>The outcome of the identity check somehow has to be communicated to the central RA of the SCSA service. There is no impact if another institution's desk is reused. | |
| Straight-through processing | STP is not possible. The duration of the vetting process is similar to that of the current practice. | |
| Penetration rate / coverage | Relatively high. Depends on the office density of the company contracted. | |
| Assurance level | Maximum LoA 2/Low can be achieved as the MitB attack is still possible. If the reused desk is also an RA then LoA 3/Substantial is possible. | |

[38] https://eid.kpn.com/content/uploads/docs/Persoonlijke-identificatie-voor-aanvraag-KPN-eID-op-een-PostNL-locatie.pdf.

| | | |
|---|---|---|
| Costs | Costs are expected to be high and in the order of 8 Euros[39]. Costs can be reduced if RA-desks at institutions are reused. | |
| Controllability/auditability | Controlling identity vetting at third party desks is more difficult to achieve. Reuse of existing registration desks at institutions is easier to achieve. | |
| Future proof | The density of registration desks is expected to decrease in the future due to online services. This can be seen in for instance the financial sector were banks continue to close their physical offices. | |

## 4.10. Community-based vetting

The community-based vetting solution establishes the identity of the user and the binding to his authentication solution via third party user attests. These third-party users are from the community or social network the user participates in, such as a research faculty or project team. For instance, if person A claims that user B is using a particular authentication solution, it could provide extra confidence for the service provider to allow access to resources with a higher authentication level of assurance (LoA). Person C could also claim to know B and his authentication mechanism thereby even further increasing the trust in the identity of B. In essence, this is a kind of "crowdsourcing of trust" in the identity of the user.
Particularly in the context of research groups or virtual organizations in which users know each other, such a community or web of trust based identity vetting could be executed in an efficient manner, without the need for registration desks. The research group manager could be the person the user has to go to for identification and activation of his second authentication factor. To increase the trustworthiness of the vetting it is desired to have multiple users/RAs from the community or web of trust vet for the user's identity. For the StudieLink use case, the institutional account managers/liaisons could do the identification of the employees that need access to the portal and communicate the outcome to StudieLink or the RA. In this case the liaisons form the web of trust for StudieLink.
An example of this solution is Pretty Good Privacy. Here PGP users sign each other's digital certificates during so-called signing parties. Web-of-trust based authentication has also been studied in the Géant 3+ WoT4LoA project[40].
The community or web of trust approach for vetting has its weaknesses. ENISA has summarized the possible threats such as the whitewashing attack, Sybil attack, impersonation and reputation theft, bootstrap issues and related to newcomers, extortion, denial-of-reputation, ballot stuffing and bad mouthing, collusion, repudiation of data and transaction, recommender dishonesty, privacy threats for voters and reputation owners, social threats such as discrimination or risk of herd behaviour, attacking of the underlying infrastructure and the exploitation of features of metrics used by the system to calculate the identity assurance[41]. These threats should be taken into account to evaluate usefulness of the community or web of trust based solutions for vetting purposes.
How could it work:

1. The user logs in at SCSA service, selects a strong authentication token and uses it, enters the email addresses of e.g. his manager or the institutional StudieLink liaison (or someone in his web of trust or community that is authoritative to vet for his identity), and receives an activation code via e-mail.

[39] Source: BKR website for identification at the post office, see https://www.bkr.nl/consumenten/opvragen-gegevens/bezorg-identificatiemethodes/.
[40] For more information see https://geant3plus.archive.geant.net/opencall/Authentication/Pages/WoT4LoA.aspx.
[41] Elisabetta Carrara and Giles Hogben, Reputation-based Systems: a security analysis, ENISA position paper, October 2007.

2. The SCSA service requests the user to go to his manager/liaison for identification.
3. The SCSA service emails the manager/liaison that the user will visit him for identification.
4. The manager/liaison physically identifies the user in his office, verifies the activation code, enters the six last digits of his identity document, asks the user to use the token, and activates the user's authentication token.

The assessment of the community-based vetting solutions against the criteria is as follows:

| Criteria | Assessment | Score |
|---|---|---|
| Easy to use by user | The user only has to find someone who is authorized and able to identify him. This can be his manager or liaison. Even for international users this could work. There may be a bootstrapping problem. | |
| Easy to organize by institution | Not that easy to organize. It requires the availability of managers/liaisons that are authorized to vet for the user's identity and that are capable of doing so. This implies that these managers/liaisons are trained and have credentials to access the management portal of SCSA. | |
| Limited impact on SCSA service | The impact is limited. | |
| Straight-through processing | STP is not possible. The duration of the vetting process is similar to that of the current practice. | |
| Penetration rate / coverage | Relatively high. Depends on the amount of authorized managers/liaisons. There is a bootstrap problem. | |
| Assurance level | It is difficult to determine the assurance level. The level is determined by the community. For a random service provider, however, this does not add any assurance. Unless, it is a community-specific service provider. Users from the community or web of trust do not always have the skills to properly identify a user, i.e. they are typically not trained for this. | |
| Costs | Costs are expected to be average. | |
| Controllability/auditability | Controlling identity vetting by third party users is difficult to achieve. Requires extensive logging and monitoring. One should check if the third party user doing the vetting is indeed member of the community. Is a single user doing the vetting sufficient? | |
| Future proof | Community or web of trust based vetting is hardly used in public or private settings. The technology and usability of the solution needs further improvement. In a closed setting (e.g. a virtual organisation or project team) the solution might be useful. | |

## 4.11. Summary

The scorecard below summarizes the criteria assessments of the various solutions for remote vetting.

| Requirement | Door | Video | App Optical | App NFC | Derived iDIN | Derived eIDAS | Central desk | Reuse desk | Com. based |
|---|---|---|---|---|---|---|---|---|---|
| Easy to use by user | 5 | 5 | 5 | 5 | 5 | 5 | 1 | 3 | 5 |
| Easy to organize by institution | 5 | 5 | 5 | 5 | 5 | 5 | 3 | 3 | 1 |
| Limited impact on SCSA service | 1 | 1 | 3 | 3 | 3 | 3 | 5 | 3 | 5 |
| Straight-through processing | 3 | 3 | 3 | 5 | 5 | 5 | 3 | 3 | 3 |
| High coverage / penetration rate | 1 | 5 | 5 | 3 | 3 | 1 | 1 | 3 | 5 |
| LoA 2/Low or 3/Subst. | 3 | 3 | 3 | 5 | 3 | 3 | 5 | 3 | 1 |
| Costs surpassable | 3 | 3 | 3 | 3 | 5 | 5 | 5 | 3 | 3 |
| Controllability / auditability | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 3 | 1 |
| Future proof / maturity | 5 | 3 | 3 | 5 | 5 | 3 | 5 | 3 | 1 |
| **Total score** | **31** | **33** | **35** | **39** | **39** | **35** | **33** | **27** | **25** |

The derived identity solution scores best, but only works on a national level. In the long term this derived identity solution can easily be extended with European coverage via eIDAS. Beyond Europe, other solutions have to be implemented. A mobile app with NFC functionality best fulfils this requirement and could be considered as an alternative for the derived identity solutions.
This outcome was more or less confirmed during a plenary feedback session with representatives from several institutions and SURFnet. When asked for a favourite solution, after a brief explanation of the solutions, the ranking was as follows (each representative was allowed to maximally vote 3 times and multiple votes per solution were allowed):

| Ranking | Solution | Votes |
|---|---|---|
| 1. | Derived – iDIN | 10 |
| 2. | App NFC | 10 |
| 3. | Reuse of (institutional) desks | 6 |
| 4. | Video | 3 |
| 5. | Community-based (via account managers) | 2 |
| 6. | Door | 0 |
| 7. | Derived – eIDAS | 0 |
| 8. | App Optical | 0 |
| 9 | Central desk | 0 |

There was discussion about the use of iDIN for SCSA. Users might be reluctant to use their private bank card for getting an institutional SCSA token. The mobile app was considered a more neutral

solution. On the other hand, the mobile app vetting process is more considerably more complicated. There is a risk that users will prematurely stop the process. Obviously good guidance is required for them to successfully complete the entire vetting process.

# 5. Use case assessment

The four typical use cases add several additional requirements to the solutions: users may be limited in number but work at the institution's premises, or they may be remote and Dutch or foreign (abroad or do not work at institutional premises) or they may come in big numbers.
The following sections assess the solutions against the use cases.

## 5.1. Use Case 1: Small amount of users (not necessarily remote)

This use case involves a small target group of users at an institution that does not have an RA for physical registration.

| Solution | Assessment | Verdict |
|---|---|---|
| Door | The door solution can easily facilitate vetting of a small user base. It is convenient for the user and the costs are controllable and surpassable as the number of users to be vetted is small. | |
| Video | The same holds for the video solution. | |
| App – optical | Users involved only have to install the app. | |
| App – NFC | Idem | |
| iDIN | It is expected that the majority of the users have a Dutch bank account and therefore can use iDIN. | |
| eIDAS | The added value of eIDAS for this user group is limited. | |
| Central desk | The target user group can easily go to a central RA for identity vetting. | |
| Reuse desk | Idem. | |
| Community based | A community based approach could provide a pragmatic solution to enable identity vetting for this user group. For instance, StudieLink liaisons at the institutions could verify the identity of the user and communicate the outcome to the StudieLink RA. | |

## 5.2. Use Case 2: remote Dutch users

This use case involves a relatively small target group of remote users that cannot visit the RA of the institution. Users will typically be Dutch researchers or employees that live and work in or outside the Netherlands.

| Solution | Assessment | Verdict |
|---|---|---|
| Door | The door solution does work for those working in the Netherlands. For those working abroad this use case is not supported. There are no companies that provide identification services at the door on an international level. These companies typically operate on a national level. This implies that SCSA has to close contracts with multiple companies and as such does not scale. | |
| Video | Video should work fine for remote Dutch users. | |
| App – optical | Idem. | |
| App – NFC | Idem. | |
| iDIN | Most Dutch users have a bank account and will be to make use of iDIN. | |

| | | |
|---|---|---|
| eIDAS | eIDAS is not useful for this user group. | |
| Central desk | Does not work for remote users living in the Netherlands, not for those abroad. | |
| Reuse desk | Idem. | |
| Community based | A community based approach could provide a pragmatic solution to enable identity vetting for this user group. | |

## 5.3. Use Case 3: remote foreign users

This use case involves a relatively small target group of remote users that cannot visit the RA of the institution. Users will typically be foreigners that live outside the Netherlands.

| Solution | Assessment | Verdict |
|---|---|---|
| Door | The door solution does not work for this use case. There are no companies that provide identification services at the door on an international level. These companies typically operate on a national level. This implies that SCSA has to close contracts with multiple companies and as such does not scale. | |
| Video | Video should work fine for remote users. | |
| App – optical | Idem. | |
| App – NFC | Idem. | |
| iDIN | Foreigners may not have a Dutch bank account. Consequently, they cannot make use of iDIN. For those who have a Dutch bank account (e.g. for receiving salary) this solution will work. | |
| eIDAS | eIDAS may be useful for this user group. The coverage of eIDAS is still low, but this aspect has already been taken into account for the assessment against the criteria. | |
| Central desk | Does not work for remote users living abroad. | |
| Reuse desk | Idem. | |
| Community based | A community based approach could provide a pragmatic solution to enable identity vetting for this user group. | |

## 5.4. Use Case 3: Bulk enrolment

This use case involves the identity vetting of large amounts of users via a remote solution.

| Solution | Assessment | Verdict |
|---|---|---|
| Door | Does not scale and comes with high costs. | |
| Video | May scale somewhat better but will come with high costs | |
| App – optical | Does scale and costs are surpassable. It is expected that a small group of users may abort the vetting process because of its complexity (app installation, picture of passport, selfie). These users will have to opt for an alternative vetting solution to get a strong authentication token. | |
| App – NFC | Idem. | |
| iDIN | Idem. | |
| eIDAS | Will be of limited use for the target user group. | |
| Central desk | Does not scale. | |
| Reuse desk | Idem. | |
| Community based | Does not scale. | |

## 5.5. Summary

Per use case the scorecard is as follows:

| Requirement | Door | Video | App Optical | App NFC | iDIN | eIDAS | Central desk | Reuse desk | Com. based |
|---|---|---|---|---|---|---|---|---|---|
| Small amount of users (local) | 5 | 5 | 5 | 5 | 5 | 3 | 5 | 5 | 5 |
| Remote Dutch users | 3 | 5 | 5 | 5 | 5 | 1 | 3 | 3 | 5 |
| Remote foreign users (abroad) | 1 | 5 | 5 | 5 | 1 | 5 | 1 | 1 | 5 |
| Bulk enrolment of users | 1 | 3 | 5 | 5 | 5 | 3 | 1 | 1 | 1 |
| **Total score** | **10** | **18** | **20** | **20** | **16** | **12** | **10** | **10** | **16** |

Obviously, for remote Dutch and foreign users that work abroad and large numbers of users any form of physical vetting is problematic. For foreign users, the iDIN derived identity solutions are also less optimal. The eIDAS solution could work for European citizens but is still too immature. Video-based solutions score well for all user groups, but scale less for bulk scenarios. The mobile app based vetting solutions are to be preferred as these best facilitate all use cases.
Combinations are possible to make individual solutions more efficient. For instance, the central RA that is required for video or front-door identification can also be used for physical vetting.
Combined with the criteria-based assessment outcomes, the ranking of the solutions is as follows:

| Ranking | Solution | Score |
|---|---|---|
| 1. | App NFC | 59 |
| 2. | App Optical | 55 |
| 3. | Derived – iDIN | 55 |
| 4. | Video | 51 |
| 5. | Derived – eIDAS | 47 |
| 6. | Central desk | 43 |
| 7. | Door & Community-based | 41 |
| 8. | Reuse of desks | 37 |

# 6. Conclusions and recommendations

Nine solutions for remote identity vetting that could be added to SURFconext strong authentication have been assessed to a number of generic criteria. The outcome of this assessment is that solutions based on derived authentication and mobile apps score best. For derived authentication, iDIN is the best choice as it offers a high national penetration level and is relatively cheap. iDIN struggles to achieve a sufficient assurance level and requires compensating measures to achieve level 3. Another weakness of iDIN is that it cannot be used by international users that do not have a Dutch bank account. Consequently, iDIN scores less in facilitating the use cases compared to the mobile app based solutions. Moreover, mapping iDIN accounts to institutional account may be challenging. Looking at the mobile app solutions, the NFC-based app offers, compared to an optical-based app, more assurance and efficiency. Lack of coverage of NFC-enabled mobile phones is a drawback. Because of the relatively large amount of actions required it is recommended to guide the user well through the whole vetting process. The app-solutions better facilitate the use cases.

Obviously, a combination of solutions is needed to cater for the various use cases, serve all users, and to cover for fallback scenarios. It is recommended to extend SURFconext Strong Authentication with iDIN authentication functionality as the primary remote identity vetting solution and to develop a mobile NFC-based app for the vetting of users that do not have a Dutch bank account. Proof-of-concepts of these solutions are needed to experiment with the technology, evaluate user experiences, gain knowledge on how to match/link accounts of users, and to integrate functionality with the current SCSA service.

The iDIN solution suffers from a man-in-the-browser vulnerability that reduces the current assurance level for a SCSA YubiKey token from 3 to 2. Should SURFnet decide to implement iDIN for SCSA and to maintain the current physical RA-desk process for vetting, then two different levels of assurance exist for the same SCSA YubiKey token. It is recommended to take the type of vetting process into account prior to assigning the overall level to a token in the SCSA management portal.

The NFC-based app solution described includes selfie and interactive video/liveness detection functionality. This functionality is not required to achieve ISO29115 assurance level 2 or 3. If SCSA wants to be eHerkenning/Idensys or eIDAS compliant, the functionality is required to achieve level 3 or Substantial. It is up to SCSA to choose its level of assurance framework it wants to be compliant with. The choice determines what functional identity features are required for the NFC-app.

During the research for remote vetting solutions a number aspects for potential improvement of the current SURFconext Strong Authentication face-to-face vetting process were identified. Possible improvements to increase the assurance level or to make the process more compliant with national or EU frameworks are:

- The Registration Authority should check if the identity document shown is not reported as being lost or stolen.
- The Registration Authority should check if the identity document shown is authentic, which requires training and/or tooling such as an app or scanner.
- Guarantee that the Registration Authority at the institutions is part of the ISMS and is included in internal or external security audits.