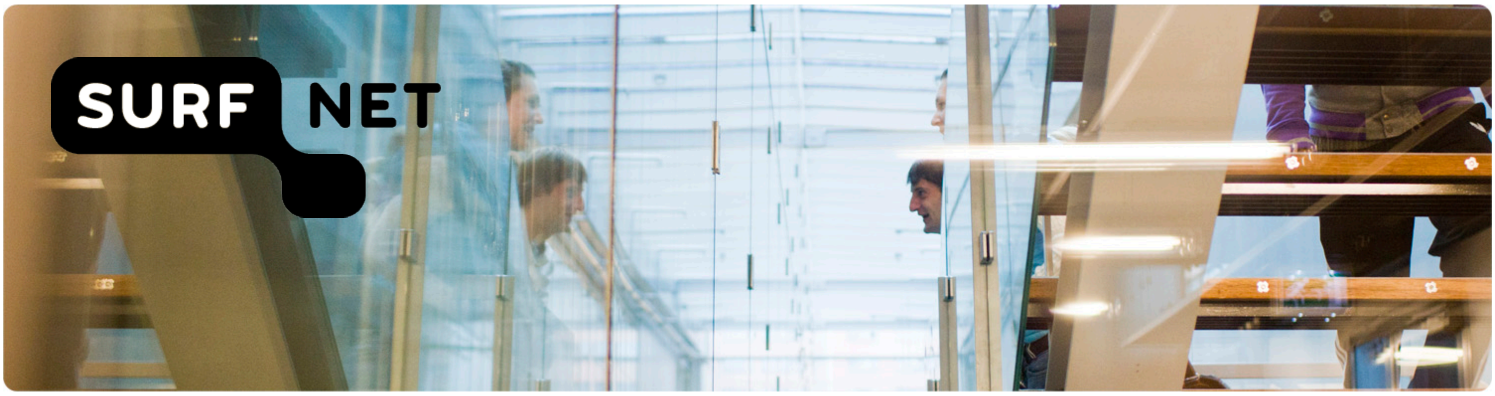


Step-up Authentication-as-a-Service

A study of the architecture and processes

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

Version: 1.0

Date: 14 November 2012

Radboudkwartier 273
3511 CK Utrecht
The Netherlands

PO Box 19035
3501 DA Utrecht

The Netherlands

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

Deutsche Bank 46 57 33 506

C of C Utrecht 30090777

VAT NL 0089.60.173.B01

Colophon

Programme line	: SURFworks
Part	: SI-Infra
Activity	: SII-12-19 Proofs of Concept
Deliverable	: Step-up Authentication-as-a-Service
Access rights	: Public
External party	: Novay

This project was made possible by the support of SURF, the collaborative organisation for higher education institutes and research institutes aimed at breakthrough innovations in ICT. More information on SURF is available on the website www.surf.nl.

Management Summary

The need for stronger forms of authentication is felt by Identity Providers (IdP) within the SURFconext federation. A business case analysis performed by SURFnet in Q2 2012 shows a clear need among SURFnet's constituency to address this need by introducing a service in the SURFconext environment that offers strong authentication on top of the existing identity hosted by a user's home institution. This report is a study of the architectural and procedural aspects of introducing such a service.

A number of current and near future use cases (described in Chapter 1) have emerged for which username/password is no longer sufficient. These use cases are in the areas of student information systems, administrative systems, and in collaborative research in which privacy sensitive and/or medical data is handled. The need for better authentication can be effectively addressed by introducing a SURFnet operated service (referred to as "SURFsure" in this report) offering technical and organisational assistance to the IdPs.

Handling different Levels of Assurance (LoA, the confidence relying parties can have in the authenticity of an identity) within a federation must be based on open and accepted standards. While some of these standards are still under development, it is already possible to make future-proof choices for standards defining the semantics and communication of the LoA. The SURFsure service architecture described in Chapter 2 supports the signaling of the LoA within the SURFconext federation while at the same time remaining loosely coupled to SURFconext.

LoA are based on the quality of registration and the quality of the second factor authentication token. It is fundamental that the meaning of the acquired LoA is precisely defined so that a higher level of confidence in a user's identity is justified. This means that the requirements for the registration process and the choice of tokens need to be precisely defined as well. The registration process (as defined in Chapter 3) therefore requires the user to appear in person at the registration authority's (RA) office, though the user is enabled to perform many of the mundane tasks through a self-service portal prior to appearing before the RA. The SURFsure service supports the RA and the user through portals, which are illustrated in the mockups in the Appendix.

1 Introduction

Over the past decade federated identity management has matured from a niche technology used by pioneering NRENs to a mainstream technology that is now used in all aspects of online business. It is increasingly more common to see cloud services (such as Google Apps, Salesforce.com and ADP) offering the possibility to authenticate using SAML-based federation technology.

Identity federations operated by NRENs have seen spectacular year-over-year growth figures, both in terms of number of services and identity providers (IdP) as well as in the number of authentications per day. For instance, SURFconext (and its federated authentication sub-component formerly known as SURFfederatie) has grown from hundreds of authentications per day in 2008 to figures approaching 100000 authentications per day in Q3 2012. The number of service providers (SP) and the diversity of services offered through federated access has also grown significantly over this period. With this growth comes the realisation both among federation operators as well as among service and identity providers that the ubiquitous username/password paradigm may not suffice anymore.

In the commercial arena, there is already an uptake of strong authentication. Historically, this was limited to financial institutions such as banks, but increasingly, "free" services in the social network arena are starting to adopt stronger forms of authentication (for instance Google[1], Dropbox[2], Facebook[3]). Identity federations are currently lagging behind in this field.

The classic paradigm for authentication systems identifies three factors as the cornerstones of authentication:

- Something you know (for example, a password or a PIN);
- Something you have (for example, a mobile phone or a token);
- Something you are (for example, a fingerprint or other biometric data).

Multi-factor authentication refers to the use of more than one of the factors listed above. Generally, the use of multiple factors results in a higher level of assurance (LoA) about the user.

Increasingly, service providers in NREN operated federations are offering services that deal with highly sensitive information (for instance privacy sensitive administrative, research, or medical data) and thus require the use of stronger authentication solutions. Multi-factor authentication solutions are needed but prohibitively expensive and complex for most identity providers. This report describes the design of a service facilitating the introduction of multi-factor authentication in an identity federation. Such a centrally operated service takes away barriers that would hinder introduction of multi-factor authentication at the individual IdP level. The report describes possible use-cases (in Chapter 1), the architectural obstacles and consequences of such an introduction (in Chapter 2), and procedural directives for the user registration process (in Chapter 3). It demonstrates, through mock-ups, what such a service might look like from the perspective of the registration authority (RA, responsible for approving new users), and of the user in the Appendix.

The goal of this service (referred to as SURFsure in the remainder of the report) is to combine the commonly used federated first factor (i.e. username/password) facilitated by the user's home institution with a second factor (e.g. a token). The result is that users are authenticated by at least two factors: something they know and something they have (see Figure 1). The second factor needs to be strongly bound to the user during a registration phase. The requirements for the registration process are also defined by the service. The fact that a user has been strongly bound to a token during registration and has proved possession of an authentication token during an online session must also be conveyed to the SP by the SURFsure service.

[1] See http://gmailblog.blogspot.nl/2011/02/advanced-sign-in-security-for-your.html.

[2] See https://blog.dropbox.com/index.php/another-layer-of-security-for-your-dropbox-account/.

[3] See http://blog.facebook.com/blog.php?post=10150153272607131.

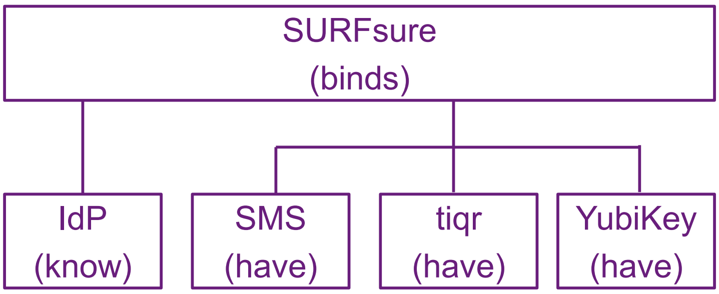


Figure 1 - SURFsure and authentication factors

1.1 Terminology list

The following technology-related terms are used in this report. The terms associated with the registration process are depicted in Figure 2.

- *Identification* is the process by which information about a person is gathered (also known as *Identity Vetting*) and used to provide some level of assurance that the person is who they claim to be.
- *Identity Proofing* is the process by which the physical person is verified and linked to his/her identity information. Identity Proofing is different from authentication, which is the process of someone identifying to a system as a previous identity that the system has interacted with (usually based on an authentication token). The distinction is important, because going through identity proofing each time someone wants to interact with a system would be overkill.
- *Credential* is something the user has access to (either “has” or “knows”) that can be used in an authentication protocol. A credential can be used to authenticate the user, but only if the credential has previously been bound to that user (see credentialing). Examples of credentials are username/password combinations, mobile phones (actually the SIM card inside the mobile phone), soft-tokens (such as certificates stored on the user’s PC) and physical tokens.
- *Credentialing* or *Registration* or *Identity Binding* is the process by which the user is linked to his/her credential and identity record.
- *Authentication* is the process of verifying that a claimed identity is genuine and based on valid credentials.
- *Registration Authority* is a trusted entity that establishes and vouches for the identity of a person.
- *LoA* (“Level of Assurance”) describes the degree of certainty that an individual is who he/she claims to be when he/she presents a digital credential. LoA is determined by the quality of the identity vetting, proofing and credentialing phase, and by the quality of the actual authentication process, including the quality/type of the authentication credential and robustness of the authentication mechanism. Various formalizations of the concept of LoA are described in Section 2.2.

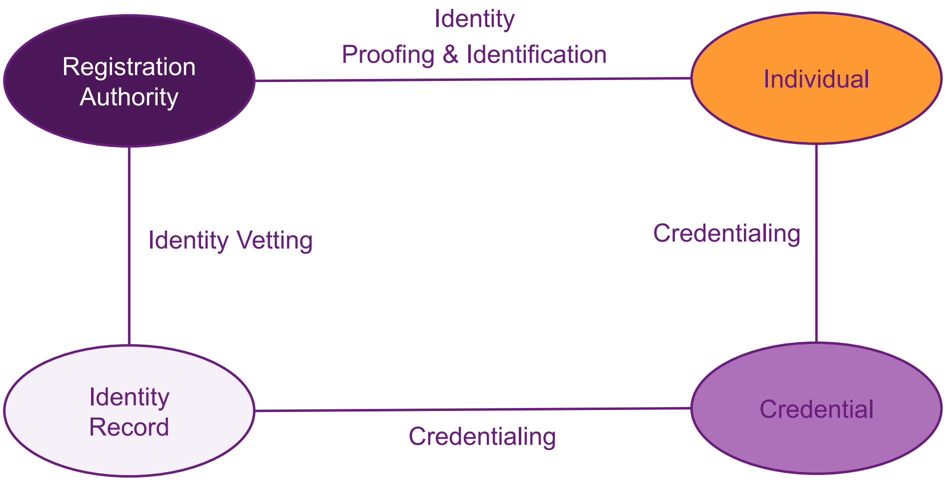


Figure 2 - Terminology used during registration

1.2 Use cases

In an earlier investigation [Ter Harst, Van Rijswijk 2012] SURFnet assessed the need for a service as described in this report among a large number of IdPs. The conclusion from that assessment was that many institutes feel a need to raise the level of assurance associated with authentication in the near future.

From the set of IdPs four were selected and representatives (from the IT department) were further interviewed to identify the precise needs (in terms of use cases), to get a feeling for what the registration procedure for users should be, and to see what potential problems are to be expected when introducing higher levels of assurance. The interviews focused on aspects of the institution (size and type of employee and/or student population, procedures in place for new employees, enrollment of user accounts in different IT systems), possible use cases for multi-factor authentication as foreseen by the institution (both internal and external SPs), and organisational aspects surrounding the role of registration authority (for instance, what department should take on this role).

1.2.1 Institute 1

IdP 1 is a private research institute with approximately 60 researchers focusing on open innovation. Some of the support systems (HR, CRM) are hosted by a (national) as-a-service provider, which does not support federated authentication. Mail and calendar are hosted at Google and are federatively accessible.

According to the persons interviewed at this IdP there is no real need for second factor authentication given the core business processes of this institute. At this point there are no federative use cases within SURFconext for which a higher LoA is needed. If second factor would need to be introduced, a relatively cheap solution based on smart phones (each member of the research staff has a company smart phone) would be the most likely solution.

Both IT and HR departments are small. User accounts for IT systems are created by the IT department (when asked by the HR department) in a central Active Directory, except for accounts for the externally hosted HR/CRM system (which is administrated directly by HR). This directory is also the source for attributes available through the federation.

Because of the small size of the institute itself registration procedures could be carried out by either department (HR or IT). The HR department is the most likely candidate as they perform the face-to-face enrolment of new employees.

1.2.2 Institute 2

IdP 2 is a scientific research institute with a number of smaller sub-institutes decentralised over different locations. The total size is around 600 persons. There is a central IT department, which serves the central organization and most of the sub-institutes; some of the larger sub-institutes have local IT support staff. The IT department has an Active Directory containing user attributes. The HR department is fully centralised. User accounts are created and maintained by the central IT department in an ad-hoc fashion based on “hierarchical” trust (if a new employee arrives his or her boss requests an account directly). The institute’s security officer is working on a new identity management strategy, which will look at processes and procedures for enrolment and thinks that SURFnet guidelines for enrolment could be an extra driver for this initiative.

Primary use cases for a second authentication factor would be VPN access for employees and admin access to sensitive systems. Note that for this internal use case the service to protect will likely not interface using SAML. Other, future, use cases that do use the federation are found in the area of research collaboration where some of the sub-institutes deal with very privacy sensitive data. Another possible use case is more fine-grained control of which users can use the institute’s licenses: specifically the SURFspot service was mentioned; each sub-institute has separate licenses, but not all of them have their own connection to the federation.

The IT department would, given the current situation, be the most logical place to act as a registration authority. A face-to-face enrollment process is seen as logical, the HR department already checks government issued identification when a new employee starts work.

Note that the IT department has already looked at using SMS (self-service attested mobile phone number, no company issued handsets) for password reset. They are aware that combining first factor reset via second factor means that the level of assurance decreases to first factor.

1.2.3 Institute 3

IdP 3 is a university for applied sciences (a college/school focusing on teaching, less on research). It consists of seven faculties divided over several clusters. There is a central IT department and a central HR department. The school has about 2500 staff, two thirds of which are teaching staff. In addition to that, approximately 800 teachers have a non-standard contract (they only teach a couple of classes) and are not hired via the central HR department but locally via one of the faculties. The school has about 45,000 students.

The IT department has implemented an identity management system (Oracle Waveset / Sun IdM) that serves all IT systems that staff and students can access.

The school is running a pilot with single sign-on and second factor authentication using a cloud based authentication provider (IP4Sure[4]), which uses SMS and/or a smart phone based OTP app (CryptoCard[5]). The solution consists of a network appliance. The cloud-based solution manifests itself to the user as a “bar” towards the bottom of web pages of the school’s web based IT systems. Second factor authentication is only available to employees in this pilot, not for students. Registration procedures (identity proofing) are not in the scope of the pilot.

The HR department is considered to be the logical entity to take on the role of registration authority and to facilitate face-to-face enrolment as they already have face-to-face contact with new employees.

The most prominent internal use case is the student information system (SIS, in this case Oracle’s Peoplesoft Campus Solutions), which has its own username/password, provisioned from the central IdM system. Students should not get write access to the SIS as that would lead to severe reputation damage to the institute. The school uses federative login for many services, but none of these constitute a business case for higher levels of assurance on their own.

1.2.4 Insitute 4

IdP 4 is one of the larger universities in the Netherlands, focusing on both education and scientific research. It consists of about 15 faculties, some 25,000 students, 5,000 staff of which 3,000 are involved in teaching and/or research and 2,000 support staff. There is a central IT department. The IT

[4] See http://www.ip4sure.com/.

[5] See http://www.cryptocard.com/.

department has implemented a central IdM system (based on Sun IdM). The university is running a program to restructure the HR department; one of the goals is to further centralize the university's HR department's back office.

Students are first identified when they enrol for a curriculum via the central "Studielink" service[6], for which students authenticate using DigiD[7] and which collects some attributes that are validated (by the Dutch government). An account within the university's IdM system is created instantly, yet with status "not yet registered". Students upload a photo for their student ID-card via a self-service website. The card is sent to the student's home address. There is also a non-regular path (not via Studielink) for students to apply, those will have to go through some extra menus and eventually end up in the same process.

Employee accounts are always created as the result of processes within the HR department. IT systems are only accessible using an account managed by the central IdM system. While there are no exceptions to that rule, the university sometimes has visitors that will need access at least to the network. The IT department is looking into the notion of guest users.

It seems reasonable that the role of registration authority should be assigned to the HR department. It should be noted that the representatives of this institute did not see the need for face-to-face registration or an RA.

The primary use case for stronger authentication at this institute is the Student Information System (SIS), to mitigate the risk of students altering their results. There are other controls (multiple professors look at the results, i.e., the "4 eyes principle") that minimize the impact of unauthorised access to this system, however the primary fear is reputation damage.

Another use case might be administrative users (HR, for example). The university has investigated the legal status of their username/password-based system for dealing with privacy sensitive employee records. While this is currently secure enough, handling privacy sensitive administrative data might be a second use case, but not on its own. A possible third use case could be access to sensitive data handled in higher management bodies (e.g. the Board of Regents). This data is made accessible through a web-based portal (a "virtual" file or record) and is sensitive from a strategic point of view.

(The IT department has introduced first factor password reset based on a self-service connected private email address: a reset link is sent to this non-institutional email address when a user forgets his or her password.)

1.3 Conclusion

That there is a need for second factor authentication is re-affirmed by the interviews. The primary use-cases are organisation-internal use cases. Student information systems (SIS) in the educational institutions form the primary use case. Most IdPs have introduced a central identity management system and strict processes to populate these systems with user accounts using data from HR departments and student administrations. The introduction of single logon makes it possible for teaching staff to perform tasks from different locations, this includes entering sensitive data such as student grades into the SIS based on the same credentials that they must use in less secure environments (a lab PC also accessible by students, let's say).

There are other use cases and even some federated (internal and external) use cases in the not-so-distant future. Collaboration using SURFconext is mentioned. License management for SURFspot is mentioned. Federated access, even to internal systems, is seen as an enabler. Making it technically easy to use second factor authentication through federated means could be a driver to introduce a second factor for use cases, which, on their own, do not have a business case.

[6] Studielink is a central enrolment system for higher education and is operated by SURF on behalf of the higher education community

[7] DigiD is an identity federation operated by the Dutch Government for the purpose if citizen to government authentication

Most institutes have recently implemented (or are planning to implement) processes for handling the registration of new employees (and, less relevant for the SURFsure service at this moment, students) at the HR department. The resulting identity data is being made available centrally within the institutes to systems managed by the IT department.

There are also institutes that are more sceptical. Smaller institutes may not see a use for second factor authentication at this point. Some institutes do see a use for multi-factor authentication for a small group of employees but do not see a use for a very formal form of (face-to-face) registration.

Table 1 below summarizes the results of the interviews:

	IdP 1	**IdP 2**	**IdP 3**	**IdP 4**
Type of organization	60 staff. SME. Heavy use of cloud for HR and IT.	600 staff including visitors. Collection of smaller institutes. IT dept creates accounts.	2500 staff. Temporary teaching staff. 42K students. Accounts only created as result of HR process.	25K, students and staff. Accounts only created as result of HR process.
IT infra type	ADFS 2.0	ADFS 2.0.	Sun IdM	Sun IdM
Use cases	None at this moment.	Internal and external. VPN, privacy sensitive data.	Internal: SIS.	Internal: SIS, administrative systems.
Who's the RA?	HR	IT	HR	No RA needed
Face-to-face?	Not relevant	Makes sense	Makes sense	Doesn't make sense
2nd factor needed?	No	Probably	Yes, already involved in pilot	Yes, waiting for conclusion of this study

Table 1 - Summary of interview results

2 Architecture

This chapter focuses on the architecture of the online authentication part of the proposed service. The processes associated with the registration phase are described in Chapter 3. Note that the proposed SURFsure service supports both phases (registration/identity proofing and authentication): the user and the registration authority interact with the service during registration, the user and the SP interact with the service during online authentication.

Identity assurance takes place in two successive phases:

1. **Identity proofing and registration**, in which the user's identity is ascertained by the Registration Authority (RA) (which is most likely co-located with the user's IdP).
2. **Online authentication**, in which the user shows (to an IdP) that he or she controls a number of authentication factors. The combined level of assurance of both registration and authentication factors (the token) is sent to the SP in the form of a LoA as part of the authentication assertion.

Figure 3 below shows these two phases. The user first goes through the registration process (shown on the left), and can then use the registered second factor during the online authentication process (shown on the right). The diagram is based on the E-Authentication Architectural Model in [NIST SP 800-63, page 19].

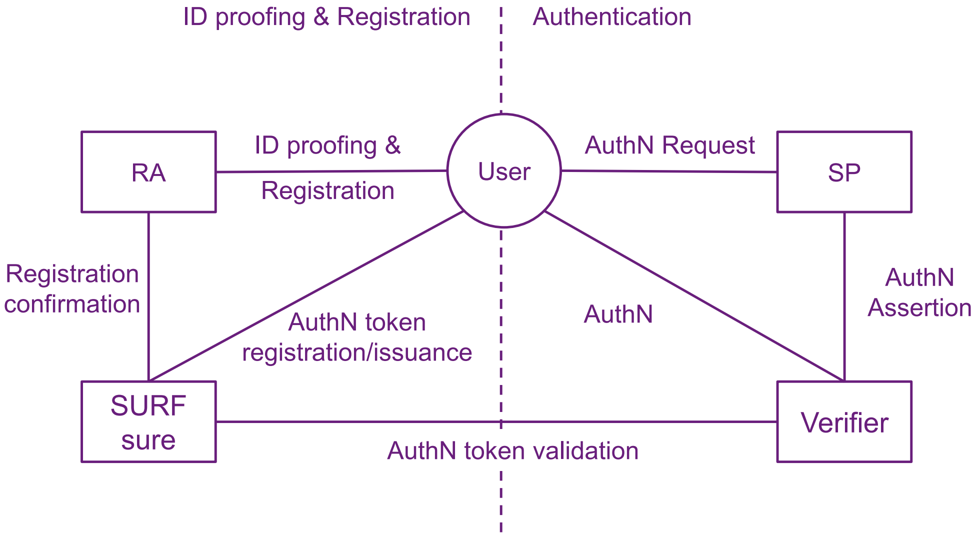


Figure 3 - a model for registration and authentication

It is assumed that SURFsure will initially support at least two different kind of second factor tokens in addition to username/password. It is also assumed that both types of token are bound to the user during face-to-face registration (so that the registration component of the LoA is high, meaning that the LoA that is signaled to the SP depends on the authentication token component only):

- A token that provides LoA2
- A token that provides LoA3

Note that different options for the precise semantics of LoAs are given in Section 2.3. The architectural questions that need to be answered are thus:

- How should the service be integrated within SURFconext?
- What LoA standard should be used?
- How should these different LoA be signaled from SURFsure to SP?

These questions are addressed in the sections below.

2.1 Location of the service

Independent of the choice of LoAs and standards to implement these, there are three options for positioning the SURFsure service within SURFconext.

- First, it might seem reasonable to make the IdP itself responsible for dealing with the second factor and integrate SURFsure with the IdP. After all, users are already forwarded to the IdP for first factor authentication, and locating the service centrally would be a break with the tradition that institutes authenticate their own users. However, the added value of a SURFnet hosted service with decentralised implementation of the second factor at the IdPs would be low in this case, as the IdP would need to integrate second factor validation logic in its own implementation. Moreover, there is a trend in which authentication (token) providers are moving to (cloud-based) managed service solutions which needs to be taken into account (all major authentication providers have as-a-service offerings, see e.g. Gartner's 2012 Magic Quadrant [Gartner 2012]).
- Second, to take away as much work from the IdP as possible, the service could be fully integrated in the federation hub, for instance as part of the SURFconext platform. Such a tight integration has many advantages, yet a drawback would be that the whole platform inherits all requirements (such as more stringent security controls) from the new service.
- Third, the service could be implemented as a transparent proxy, completely separated from the federation hub and the IdP. (In a sense, the service would be a new hub sitting next to the existing federation hub). In this architecture the security of the solution does not depend on the security of the SURFconext gateway.

The last option is the simplest to implement: It is relatively easy to build as part of the current hub-and-spoke federation setup of SURFconext, and since it is loosely coupled to the other building blocks it can be implemented so that it can be reused within other federations, thus enhancing the possibilities of international collaboration in implementing the service. The diagram below shows the SURFsure service based on the last option during a run of the authentication protocol. The service is situated between the federation hub ("SURFconext") and the SP.

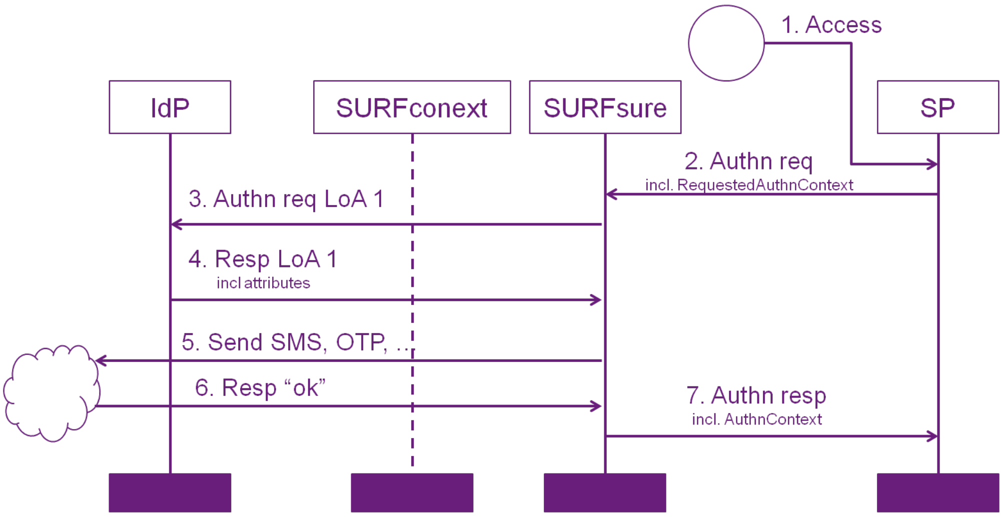


Figure 4 - SURFsure as a transparent proxy

Note that there are now two distinct IdPs from the point of view of the user: the home institution for the first factor; and SURFsure for the second factor (which in turn may redirect the requests to an authentication-as-a-service provider, perhaps a service that sends SMS messages to the user).

The flow given in the picture above is as follows:

1. User contacts SP and wants to access its service.
2. The SP starts SAML authentication as usual. The desired LoA is embedded in the authentication request as a RequestedAuthnContext filter conforming to [SAML 2.0 core, Section 3.3.2.2].
3. The authentication request first passes through SURFsure. The SURFsure service delivers the authentication request to SURFconext (which will deal with the first factor, so from the perspective of the SP there is only one IdP: SURFsure).
4. The (first factor) IdP (i.e., the user's home institution) checks the first factor (username/password), and releases an attribute assertion back to SURFconext. The response is received by SURFsure.
5. SURFsure now checks second factor authentication, which could, for instance, mean sending a request to an external authentication provider (e.g., an SMS service or similar) and redirecting the user to an appropriate internal or external web-based IdP (e.g., a form where the user can enter an OTP). The precise details depend on the second factor solution.
6. SURFsure receives a response from the authentication provider that second factor authentication succeeded.
7. SURFsure now embeds the appropriate LoA in the original authentication reponse, signs it, and redirects the user to the SP's landing page.

Variations are possible. One option would be for the SP to start with not providing an RequestedAuthnContext filter, and for SURFsure to give control back to the SP after first-factor authentication at the institute IdP, so that attributes issued by the IdP can be taken into account before determining an appropriate LoA to request. Such variations would make the service too complex at this point, and it is advisable to start out with a simple service first.

2.1.1 Single Sign On and Step-up Authentication

As a result of the selected transparent proxy setup step-up authentication and Single Sign-On (SSO) for second factor are easily implemented technically. If a user is authenticated using username/password only (as checked by the institute IdP) and attempts to access a service for which a higher LoA is necessary, the above flow will result in a user experience where the user is only asked to authenticate with the second-factor token. If the user has successfully accessed a service at a higher LoA and, later on within the same browser session, attempts to access another service of equal or lower LoA the above flow will result in a user experience where the user need not authenticate again.

Single sign-on for second factor, especially across different SPs may not be desirable or according to SURFnet policies. As SURFsure acts as the IdP for the SPs it can disable SSO if desirable.

2.2 Assurance level standards

NIST (the US National Institute for Standards and Technology) has defined four levels of assurance as a NIST special publication [Burr et al., NIST SP800-63]. The use of these levels dates back at least to 2003 [OBM 04 04]. The NIST publication focuses on the semi-precise meaning of the levels, and also on how to determine what level to use for what services (based on a risk analysis of the data handled by the service). Within the United States federal government ICAM plan (Identity, Credential, and Access Management, see [ICAM]) the LoA concept plays a central role. US-based federation InCommon translates these requirements into IdP profiles "Bronze" and "Silver" [InCommon, 2011].

Based on the four NIST levels, the 2009 STORK project studied the identity assurance problem in a European context. The situation in Europe was that many countries already had identity assurance levels in place and a direct translation between these levels was hard if not impossible. In deliverable D2.3 [STORK] the four NIST levels were adopted and more precise semantics are given for each level based on the different accepted registration processes and different government issued credentials as found in the field. The Dutch national eHerkenning (“eRecognition”) programme for business-to-government identification adopts the four STORK levels and specifies its own requirements on registration processes and token characteristics.

The four levels of identity assurance for electronic transactions requiring authentication 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 the registration phase, the authentication token management phase, and the online authentication phase, typically by using concrete examples.

It is expected that ISO will standardise the above four levels of identity assurance in ISO/IEC 29115 standard in 2012 [ISO/IEC 29115] (which coincides with ITU-T X.1254). From draft versions of this standard[8] the registration component requirements of the four levels have the following meaning:

- LoA1 – No requirements
- LoA2 – Information from an authoritative source
- LoA3 – Information from an authoritative source + verification
- LoA4 – Information from an authoritative source + verification + entity witnessed in person

LoA1 up till LoA3 may be verified either locally or remote. Only LoA4 must be verified locally (face-to-face).

The authentication token requirements of the four levels have the following meaning

- LoA1 – Only some minimal assurance is requested for the authentication mechanism.
- LoA2 – Like LoA1, but a secure authentication protocol shall be used. Controls shall be in place to reduce the effectiveness of eavesdropper and online guessing attacks. Controls shall be in place to protect against attacks on stored credentials.
- LoA3 – Like LoA2, but any secret information exchanged in authentication protocols shall be cryptographically protected.
- LoA4 – Like LoA3, but tamper-resistant hardware devices for the storage of all secret or private cryptographic keys shall be used. Sensitive data included in authentication protocols shall be cryptographically protected.

2.3 How to signal an assurance level to the SP

There are a number of options for signalling the acquired LoA between IdPs, SPs, and the SURFsure service. It stands to reason that the federation opts for a *standards based* approach compatible with the authentication standard already in use. Below is a list of relevant standards for signalling level of assurance information.

2.3.1 SAML 2.0 authentication context

The SURFconext gateway is moving towards a 100% SAML 2.0 only federation in that the authentication process is supported by an architecture based on SAML 2.0 [SAML 2.0 core, SAML 2.0

[8] At time of writing available from: https://www.oasis-open.org/committees/download.php/44751/285-17Attach1.pdf.

profiles]. SAML authentication assertions are Boolean valued: authentication succeeded or failed, still the SAML standard has supported the concept of an authentication context since SAML 2.0 which can be used to include additional information about the quality of aspects of the authentication process.

An authentication context can also be part of an authentication *request* (as per [SAML 2.0 core]). The authentication context element then acts as a filter to indicate to the IdP what the SP expects in terms of allowable authentication contexts.

The authentication context is a comprehensive XML fragment that is part of SAML attribute assertions containing sections describing characteristics of:

- the identification (identity proofing) process,
- the technical protection (how the “secret” is secured),
- the operational protection (e.g., security audits, records archival),
- the authentication method (e.g., a password versus a smart card),
- and governing agreements (e.g., liability constraints and contractual obligations).

This leads to a very complex structure, as is illustrated by the diagram below, which shows the XML schema for SAML 2.0 contexts:

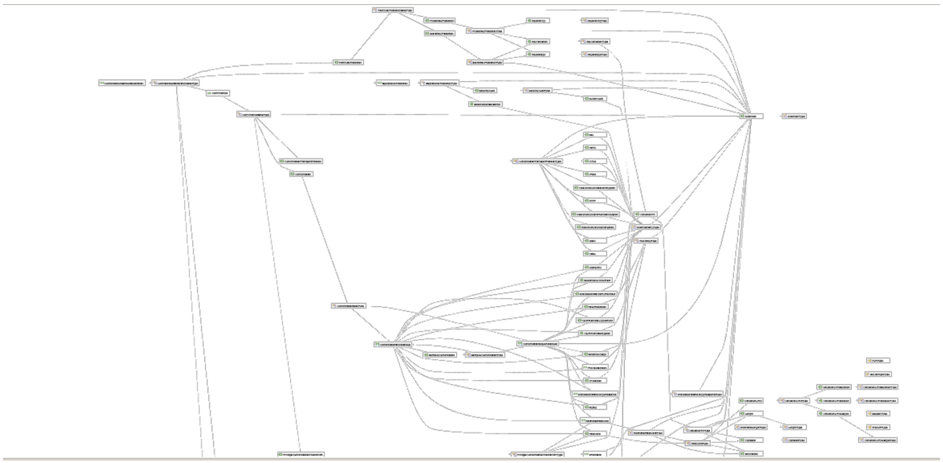


Figure 5 - Graphical representation of the SAML 2.0 authentication context XSD schema

The diagram in Figure 5 (the reader is not supposed to be able to make out the details) shows the many choices that must be made to create a concrete authentication context instance. Note that there are many, many options for each section describing an aspect of authentication, and most, if not all, option lists also contain the possibility for an extension reference value.

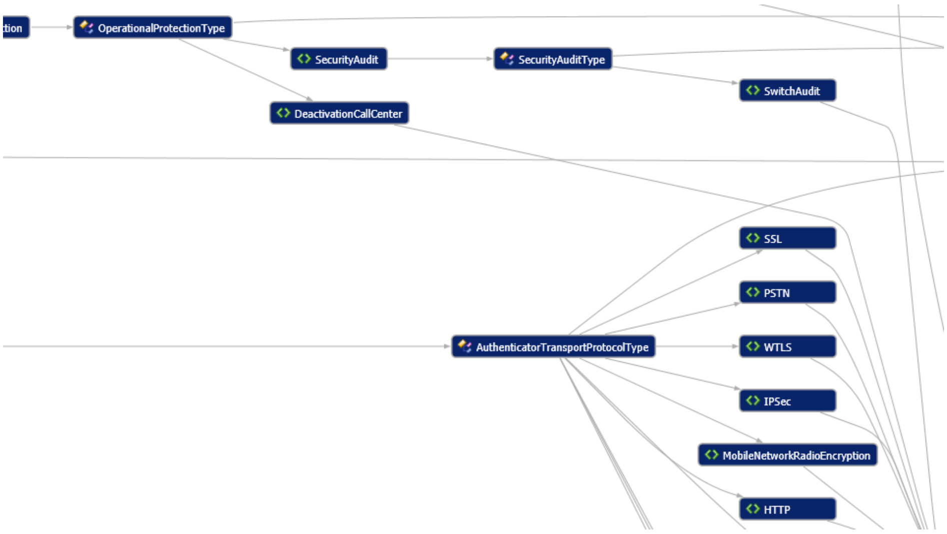


Figure 6 - SAML 2.0 authenticaiton context, detail

Figure 6 shows a fragment of the graph in Figure 5, containing some audit aspects (part of the operational protection section) and some aspects of the communication channel by which credentials are sent from the user's client to the authentication provider (part of the authentication method section).

A lot of standardized information fits in an authentication context. Needless to say, for the SP determining whether a given concrete authentication context is appropriate for the service can be very challenging. The standard, as such, is too broad to be useful in practice. This was recognized by the authors of the standard and consequently Authentication Context Classes (Section 2.3.2) were introduced.

2.3.2 SAML 2.0 authentication context class references

The authors of the SAML 2.0 authentication context specification realized that it is difficult to apply such a broad standard. They introduced authentication context *classes* that correspond with typical authentication tokens and processes applied in practice. For instance, the standard lists authentication context classes for: authenticating users based on IP address, Kerberos ticket, mobile device, phone line (caller line identification), password (over insecure and over secure transport), previous session, and PKI (software, smart card). These authentication context classes can be viewed as pre-determined authentication contexts. A unique identifier (taking the form of a URI) is associated with a class. This means that a relying party does not need to interpret the sections listed above, but can base its determination of the level of identity assurance on this identifier alone.

Examples of context class references are used in Dutch eGovernment framework *eHerkenning*. The eHerkenning specification [eHerkenning - Koppelvlakspecificatie HM-MR] (version 1.5), while claiming to use the four STORK levels, technically uses four levels represented by context class references. The identifiers used (the URNs below) should be viewed as constants whose meaning is re-defined in [eHerkenning – betrouwbaarheidsniveau's].

eHerkenning level	SAML2 AuthnContextClassRef element
1	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
2	urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered
3	urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
4	urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI

Table 2 - Context classes for LoA's in eHerkenning

Another example of a context class for challenge-response based tokens can be found on the OASIS web site[9].

2.3.3 Level encoded as an attribute

Since a LoA is simply a piece of information originating at the IdP and destined for the SP, it can be transmitted as an attribute value (in SAML 2.0 or other languages). This is, of course, from a technical standpoint the easiest solution. The drawback is that IdP and SP need to make sure they use the same attribute name and set of possible values. Several solutions have taken this route. Below is a sample from ProtectNetwork's website[10]:

```
<AttributeRule Name="http://protectnetwork.org/pn/loa" Header="Shib-PN-LOA" Alias="LOA">
  <SiteRule Name="pnidm">
    <Value>LOA-1</Value>
    <Value>LOA-2</Value>
  </SiteRule>
</AttributeRule>
```

A possible route to gain some standardisation is to use registered identifiers (URIs, for example) for possible attribute values: The Internet2 project has an eduPersonAssurance draft specification[11] in which values for LoA are encoded. There is a draft RFC for an IANA register for LoA style URIs [Johansson, 2012].

2.3.4 SAML 2.0 identity assurance profiles (drafts)

Several years have passed since the SAML 2.0 standard was finalized. Several attempts at standardising the embedding of identity assurance information have been mounted since then:

The sstc-saml-loa-authncontext-profile-draft-01 (draft) [Lockhart et al., 2008] limits the authentication context class reference. The LoA is signaled to the SP using an identifier such as "urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:*x*" for *x* in { 1, 2, 3, 4 }. The profile limits the possible contents of authentication classes so that it can only refer to a policy document (a URL that holds a PDF of NIST SP800-63) that describes the levels, no further characteristics of the authentication solution are described.

The SAML v2.0 Identity Assurance Profiles 1.0 [Morgan et al. 2010] describes the same Authentication Context reference based solution except that the context is even further restricted to include only a GoverningAgreements section, which points to LoA frameworks (allowing a couple, usually 4, concrete URNs). The standard contains a step-by-step procedure to setup level of assurance in SAML 2.0:

Therefore, to define class schemas for a set of LOA:

1. *Define a* URI *for each LOA.*
2. *Determine a* URL *to an appropriate document (or section) for each LOA (this may be, but does not have to be, the same as the URI in the previous step).*
3. *Create an* XML *schema for each LOA:*
    a. *The schema should redefine the base authentication context types schema* (saml-schema-authn-context-types-2.0.xsd) *as per the class schemas in the SAML Authentication Context specification.*

[9] See https://wiki.oasis-open.org/security/TextChallengeResponse.

[10] See http://www.protectnetwork.org/support/policies/level-of-assurance.

[11] See https://spaces.internet2.edu/display/macedir/eduPersonAssurance+Draft+Specification.

b. *The schema's target namespace should be the URI from step 1.*

c. *The schema should restrict the* **AuthnContextDeclarationBaseType** *complex type so that only a single* <GoverningAgreements> *element, with no other children, is allowed.*

d. *The value of the* governingAgreementRef *should be fixed to point to the corresponding URL from step 2.*

(Cited from [Morgan et al. 2010], Section 2.1)

The latter profile is a committee draft, meaning that it is very close the eventual final version.

2.3.5 OpenId Connect, OAuth 2.0 and other non-SAML protocols

The OpenId Connect specification (which is still in draft at the time of writing of this report) [OpenId Connect] allows the inclusion of an Authentication Context Class Reference (abbreviated to "acr" in the specification). OpenId Connect also mentions several LoAs with concrete values "0", "1", "2", "3", and "4" while referring to [ISO/IEC 29115] for the latter four values and the IANA [Johansson, 2012] registry mentioned in the previous section. OpenId Connect is the latest version of OpenId and is based on OAuth 2.0.

Previous versions of OpenId (at least since 1.0) included the possibility of an optional extension known as PAPE[12] (Provider Authentication Policy Extension), that describes how to include NIST style LoAs as part of an authentication request and response.

2.4 Conclusion

For a first version of the SURFsure service a good location for implementing the SURFsure service would be as a transparent proxy separate from the federation hub as indicated in Figure 4. Other locations and/or configurations are possible but result in a solution that is more complex to build and maintain.

It is recommended that four levels of LoA are used in accordance with NIST, STORK, and the upcoming ISO standard. The best candidate for signaling LoA information from the SP to SURFsure and back (in terms of standards compliance) would be to use:

- The SAML 2.0 Authentication Context class reference
- Based on the SAML 2.0 Identity Assurance Profiles 1.0 (2010) spec (once it is final)
- Using internationally used identifiers (URNs) possibly using the IANA registry described in [Johansson, LoA Registry].

There is no need for the IdP to change anything, it will be responsible for first-factor authentication and attribute issuing. An SP that does not need higher LoAs also does not need to change anything. SPs that do require higher LoAs will need to add a RequestedAuthnContext element to the SAML authentication request and will need to be able to parse and interpret the resulting AuthnContext that SURFsure adds to the response. Most SAML 2.0 implementation software libraries (such as SimpleSAMLPHP and Shibboleth) support authentication contexts.

[12] See http://openid.net/specs/openid-provider-authentication-policy-extension-1_0.html.

3 Identity registration and authentication guidelines

The 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 users that deny ever having registered. 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 (RA) knows the true identity of the applicant. Specifically, the requirements include measures to ensure that:

1. A person with the applicant's claimed attributes exists, and those attributes are sufficient to uniquely identify a single person;
2. The applicant whose token is registered is in fact the person who is entitled to use the identity;

There are two general categories of threats to the registration process:

- Impersonation of a claimed identity – An applicant claims an incorrect identity, supporting the claim with a specific set of attributes created over time or by presenting false credentials.
- Compromise or malfeasance of the infrastructure – Lack or poor implementation of security measures and policies undermine the reliability of the registration.

This report concentrates on addressing the impersonation threat. Infrastructure threats are addressed by normal computer security controls (e.g., separation of duties, record keeping, independent audits, etc.) and are outside the scope of this document.

Registration fraud can be deterred by making it more difficult to accomplish or by increasing the likelihood of detection. During the registration process methods should be employed to determine that a person with the claimed identity exists, and that the applicant is in fact the person who is entitled to that identity. As the level of assurance increases, the methods employed provide increasing resistance to casual, systematic and insider impersonation.

3.1 In person or remote registration

Different registration processes and mechanisms applied to identity vetting, proofing and credentialing result in different registration assurance levels. An applicant may appear in person to register, or the applicant may register remotely.

Remote registration is limited to Levels 1 through 3 and is more vulnerable to threats and technically complex to achieve. Remote registration relies on the availability of trusted sources to cross-reference and validate the provided assertions such as name, home address, age, social security number (BSN), and photo. Examples of such sources are the institution's HR system or the government/municipal administration (in The Netherlands: *Gemeentelijke BasisAdministratie,* GBA). Consultation of the latter source is restricted by legislation and not available for step-up authentication purposes; the HR system on the other hand could be used as an alternative source. Typically, after a successful validation, a registration activation code is sent to the applicant's home address. This is cumbersome and expensive.

Therefore, in person registration seems the most efficient option. In case the user is somehow not able to register in person, video conferencing tools such as Skype could be used. In this case the user identifies him/herself via the videoconference and shows his/her passport or other valid photo-ID to the registrar. The use of video conferencing tools for identification, however, has several drawbacks: it introduces scheduling overhead and it makes it harder to detect a forged ID. Other – less attractive and/or appropriate – alternatives (such as use of physical address, email & mobile phone, use of bank account) are discussed in [Hulsebosch, 2011].

Different circumstances may translate to different requirements. There are use cases in which a second factor authentication token without a strict registration process makes sense: Google, for example, offers second factor authentication to its users in the form of an SMS service and a smart phone OTP app, but has no face-to-face registration processes in place. The difference between this "Google use case" and the use cases identified in Chapter 1 is that Google users are protecting their own account (from, say, snooping governments) as opposed to the educational institute's student information system use case where the IdP is protecting its organisational assets. To put it differently: in the "Google" use case, the user is protecting himself, whereas in the use cases identified in Chapter 1 the institution is protecting itself (or its reputation). In the latter case, there is a strong need to be able to determine that a service provider (e.g. a student information system) is dealing with a legitimate user, thus necessitating a stringent identity proofing process during user registration (i.e. a face-to-face process) described below.

3.2 Registration Process

Users and registration authorities shall follow an identity vetting, proofing, credentialing, and registration process that meets the requirements defined below when issuing two-factor authentication:

1. The user needs a LoA 2 or 3 authentication credential (token) and goes to the SURFsure website.
2. The user is asked to authenticate. Since SURFsure is part of SURFconext, the user can use his institutional username and password combination for this purpose.
3. After successful authentication, the user is presented a number of LoA 2 and 3 authentication solutions. Possible solutions are e.g. tiqr, SMS-OTP, and Yubikey.
4. The user selects one of the solutions.
5. SURFsure initiates an authentication session with the selected solution. E.g. in case of SMS-OTP the user is asked to enter his mobile phone number and OTP challenge that is sent to him via SMS. Note that each solution may have its own authentication procedure. For instance, the selection of tiqr may involve downloading and installation operations prior to continuing with the SURFsure registration.
6. After successful authentication with the selected solution an e-mail containing an activation link is sent to the user. The user is asked to click on the link to confirm and prove that he/she is the owner of the token. This step proves that the user has access to the e-mail address that has been provided by the IdP and forms an additional validation of the user's identity. Moreover, the user can detect it if someone else attempts to request a token in his or her name.
7. After activation, SURFsure shows the user a registration form that contains personal information obtained from the IdP and possible authentication solution specific information such as a telephone number. The form also contains a unique registration code. The registration code should have enough entropy to prevent a guessing attack (an attacker should not be obtain the valid code via trial-and-error by generating codes), yet short enough to be written down by the user[13]. The form is sent to the user's e-mail address. It is also possible to print the form if the user has access to a nearby printer. Additionally, SURFsure submits a second factor registration request entry to the RA of the user's institution.
8. Subsequently, the user is asked to go to the RA of the institution to complete the registration process. For that purpose the user is requested to be able to show the e-mail (e.g. via his/her mobile phone) or printed form in combination with a valid photo-ID (e.g. driving license, passport, student card, employee card). SURFsure has access to a list of RAs for each

[13] The authors recommend a length of 8 characters from [0-9A-Ba-b].

institution to be able to provide the user with all the required information (e.g. what building and room the RA is at the university).

9. At the RA desk, the user gives the registration form or shows the e-mail to the RA. The RA logs in to SURFsure and enters the registration code. Note that the RA has to log in with a LoA that is equal to or higher than the LoA of the authentication solution selected by the user. Otherwise the RA cannot execute the registration.
10. In registering the user, the RA must verify the IdP-provided information against other trusted sources. SURFsure shows the registration request including some personal information of the applicant obtained from the IdP (i.e. the user's first and last name and e-mail address). The registrar verifies this information against the information in the valid photo-ID, i.e. he inspects the photo-ID (is it valid), checks if the photo matches the applicant and if the first and last name on the ID corresponds to those provided by SURFsure[14]. Note that the RA is, in principle, able to perform additional checks based on other local trusted identity sources during registration. E.g. local HR sources could be used for validation of day of birth or social security number. This is not part of the requirements for SURFsure, however.
11. The user shows he or she controls the second factor by performing an authentication using the RA's workstation. The RA oversees the authentication attempt and can tell whether it was successful.
12. Having successfully identified the user, the RA confirms the registration and binds the second factor authentication solution to the user's federated account credentials; if this is not the case the registration is rejected.
13. The user can now use step-up or strong authentication to access services.

The identity registration and proofing process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a credential without the cooperation of another authorised person (that is to say: an RA may never enrol him/herself). Ultimately, the first RA for any organisation is enrolled by SURFnet, for instance by their account manager at SURFnet.

3.3 RA self service

The registration process described above identifies several RA-specific functionalities that can be handled via self-service by the RA:

1. Selection of the set of preferred second factor authentication solutions from a long list provided by SURFsure.
2. Specification of the location of the RA helpdesk to direct the user to.
3. Registration and deregistration of users.
4. Customization of the registration form according to the institutional policy including logos ("branding").
5. Delegation of RA rights to other users within the organization (not all RAs have delegation power, see Section 3.4 below)

The long list of authentication tokens referred to in item 1 as provided by SURFnet contains tokens and solutions (e.g. SMS-OTP, Yubikey, etc.) from different vendors with different characteristics (and therefore with a different LoA). The processes for admission of new types of tokens and the

[14] Note that the LoA of the verified attributes increases as well as a consequence of this registration process. This may be useful for advanced attribute-based authorisation solutions that require trustworthy attributes. Currently storing LoAs for attributes at the IdP is out of scope for SURFsure, however.

procedures for determining an appropriate LoA for each token type are out of scope of the current report.

3.4 RA selection

Potential RA candidates are ICPs (“Instellings Contact Persoon”, the point of contact for SURFnet’s account management department) and/or members of the HR or IT departments. Note that an RA is required to use a strong authentication solution to access the SURFsure portal. A representative of SURFnet (for instance the account manager for the institute in question) must validate the strength of the authentication solution during physical presence with the delegated RA of the institute.

There are two classes of RA. Normal RAs have access to all of the functionalities described above, but lack delegation power. Super-RAs are, in addition, able to delegate RA power to other users within the institute. The initial RA appointed by the SURFnet representative is a super-RA.

Such delegation functionality must take into account that during delegation degradation of authentication LoA is prevented. What has to be done first is that a potential delegate RA registers his/her second factor via SURFsure (as a common user would do for a LoA 3 factor). Subsequently, the authorized RA selects the delegate RA’s user identity in the SURFsure RA registry by entering his/her e-mail address. Deregistration of delegate RAs occurs via a similar process. All delegation registration and deregistration activities must be logged.

3.5 Classification of authentication solutions in SURFsure

The quality of the authentication process provides, in combination with the registration process, a measure for the LoA of the authentication solutions that are available via SURFsure. SURFnet selects suitable authentication solution providers for SURFsure and assigns an authentication LoA to them based on the NIST/STORK/eHerkenning frameworks described in Section 2.2.

When selecting authentication service providers the following aspects should be considered:

- Ease of use and registration for users;
- Ease of implementation in SURFsure;
- Credentials that the community commonly has;
- (Ongoing) Costs of the solution;
- How well the solution meets SURF and SURFnet’s criteria for open technology.

Furthermore, the SPs should be aware of the LoA concept and have guidelines to determine the LoA that best suits their service offering(s). eHerkenning, the Dutch governmental e-recognition framework, provides such guidelines for SPs [Handreiking]. It may be advisable to define a similar guideline document more specific to SURFnet’s constituency.

Further elaboration of these aspects in the context of higher education and research is beyond the scope of this work.

3.6 Audit / logging / retention

Audit log files must be generated for all events relating to access, security and activities (e.g. configuration management) of SURFsure. Where possible, the security audit logs shall be automatically collected.

At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event.
- The date and time the event occurred.
- A success or failure indicator.

- The identity of the entity that triggered the event.

Audit logs shall be retained on-site for at least two months in addition to being retained in the manner described below. The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing. Procedures must be implemented to ensure that only authorised personnel can archive or delete security audit data. Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access). Security audit data shall be moved to a safe, secure storage location separate from the location where the data was generated. Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit log shall be sent off-site on a monthly basis.

The RA must maintain a record of the registration (including revocation). The NIST standard [NIST SP 800-63] specifies a minimum record retention period for registration data for LoA 2 credentials of seven years and six months beyond the expiration or revocation (whichever is later) of the credential. InCommon requires a retention period of at least 180 days [InCommon IAP]. Retention periods for SURFsure will have to be further specified.

3.7 Step-up authentication revocation and re-issuance

Processes should be in place to handle revocation of lost, stolen, or compromised SURFsure authentication solutions. Revocation should preferably take place within 72 hours after the incident.

These processes can either be triggered by the user (in case of a stolen or lost token), by the RA (during e.g. deprovisioning) or SURFnet (in case of a compromised token).

The user can log in with his/her federated account credentials (i.e. username/password) to SURFsure to deregister the binding between his federated account and the second factor authentication solution. The RA will be notified and SURFsure will log the action.

The RA may deregister the binding between a user's account and the second factor authentication solution in case the user has left the institution. The user will be notified via email.

SURFsure (SURFnet) will be authorised to remove an authentication solution in case of compromise (e.g. Diginotar type of incidents). The authentication solution provider must be informed as well as the users of the removed authentication solution. SURFnet will only take this extreme measure after careful deliberation with the security officer and account management given the blocking effect such a measure will have on (some) users of the service.

3.8 Password resets with the second factor

In some situations a second authentication factor is used, not to provide additional identity assurance, but as a communication channel to the user to perform password reset. For example, an IdP which knows a user's mobile phone number can send that user an SMS text message with a new password when the user (through some self-service portal) indicates that he or she forgot the original password. A second authentication factor should ***never*** be used for password reset in situations where it is also used for additional identity assurance in the context of SURFsure as this degrades the security of the whole to single factor authentication.

3.9 Impact on infrastructure

The LoAs described by NIST and STORK primarily focus on the robustness of the authentication. The robustness of the technical infrastructure is mostly beyond their scope. It is assumed that proper measures are in place to prevent potential authentication protocol threats such as eavesdropping, man-in-the-middle, replaying, and hijacking. Attacks are not limited to the authentication protocol itself. Other attacks include the use of malicious code to compromise authentication tokens, insider threats to compromise authentication tokens, social engineering to get a subscriber to reveal his password to the attacker, "shoulder-surfing", fooling claimants into using an insecure protocol, when they think that they are using a secure protocol, or intentionally denying ever having registerd by subscribers who deliberately compromise their tokens.

Other types of threats are (SAML) assertion related such as modification, disclosure, repudiation, reuse, or redirect. Countermeasures should be in place to prevent these attacks as well. It goes too far to describe for each LoA the amount and strength of the required countermeasures. Most of these countermeasures are addressed in the information security policy of the stakeholders. NIST 800-63-1 also gives some guidelines. The most important ones are the use of digital signatures to sign assertions with and the use of SSL/TLS to secure the communication channel. Both control measures are required to fulfil the requirements for LoA2 and LoA3 and are already in place in SURFconext. NIST SP 800-63-1 recommends the CSP (i.e. SURFsure) for LoA2 to “employ appropriately tailored security controls from the low baseline of security controls defined in [NIST SP 800-53] and to ensure that the minimum assurance requirements associated with the low baseline are satisfied”. For LoA3 security controls from the moderate baseline of security controls are required.

3.10 Attribute LoA

Several attributes provided by the IdP of the institution will be validated during registration and identification. These attributes include first and last name and e-mail address. An LoA could be assigned to these attributes. In attribute-based access control scenario’s, information about the reliability of these attributes could be beneficial for SPs to make their authorisation more reliable.

There are, however, a number of arguments against doing this:

- Mixing attributes with different LoA’s is complex;
- There is no suitable way to express differing LoA’s for attributes in SAML assertions;
- The registration process will become more complex as attribute validation will need to be explicitly included.

Because the benefits do not outweigh the added complexity, SURFsure should therefore solely focus on authentication LoA.

4 Conclusions

4.1 Use cases

Based on interviews with IT staff representing the institutes of research and higher education, with respect to use cases and the need for a service like SURFsure, the following can be concluded:

1. That there is a need for multi-factor authentication was already apparent from the business case analysis, the interviews reemphasize this. The current project is followed with interest. Institutions are working on defining identity management policies. Use cases where multi-factor authentication plays a role are being studied by the institutions. In fact, some of the institutes are already piloting solutions of third party authentication providers.
2. The primary use case is formed by internal systems such as Student Information Systems (SIS) and HR and other administrative systems. These systems should only be accessed by particular members of staff (e.g., teaching resp. administrative staff) and the institutes want to make sure that access by other individuals is made as difficult as reasonably possible. Note that an institute's internal systems do, in principle, not rely on federative authentication. This may change as software vendors start supporting federation standards (for example because of cloud based offerings).
3. There are other use cases on the horizon. Some of these are internal and deal with sensitive information being made accessible to select groups within the institution (teaching staff, policy makers, managers, administrators). Others involve collaboration (SURFconext) between researchers from different institutions working on (privacy) sensitive data.
4. Not all institutions currently have a solid business case for introducing multi-factor authentication on their own, which means that cost is important and the service already raises the security level significantly if relatively affordable tokens are used (SMS, YubiKey, mobile app OTP generators such as tiqr). Also, making it easier to address a variety of use cases (e.g. through uniform interfaces) helps to make the business case for multi-factor authentication for these institutes. SURFnet offering a SURFsure service might just make the difference.

4.2 Architecture and standards

With respect to architecture the following can be concluded:

1. The easiest way to implement the initial version of the service is as a transparent proxy near the SP-bound border of the federation hub. Authentication requests can then be examined by this service at the point of entry and forwarded, by way of the federation hub, to the first-factor IdP and second-factor authentication provider. The response can be enriched with the combined authentication result, the attributes as issued by the first-factor IdP and level-of-assurance information by the service at the point of exit. No changes to the IdP are required. Changes to the SP are minimal.
2. The 2010 "Authentication context id assurance profile" by OASIS should be adopted. The identifiers (URIs) that are used should preferably be those that are internationally used for conveying level-of-assurance information. If it is more opportune to use federation specific definitions for the level-of-assurance, these levels should at least be well defined and registered centrally, for instance in accordance with RFC 6711 [Johansson 2012].

It is recommended that the initial version of the SURFsure service is kept as simple as possible, and that more advanced features are added iteratively in future versions.

4.3 Registration Process and Registration Authority

It is recommended that the registration process be structured as follows (in accordance with the description in Chapter 3 and the mockups in the Appendix).

1. The user registration process proceeds in two steps. First, a self registration portal is accessed by the user (using first-factor login). This portal enables the user to select a type of second-factor token (from a list of SURFsure and IdP selected tokens), and to prove that the user already owns an instance of that token type. The result of this is an 8-digit registration code that is to be written down (or printed) by the user.
2. The user is to appear, in person, at the registration authority's (RA) desk and present the registration code, a valid passport or identity card and the second-factor token. The RA accesses the administrative portal of the service (using first- and second-factor login), verifies that the passport or identity card belong to the user, verifies that the name attributes as issued federatively by the IdP match with what is written in the passport. The user also shows to the RA that he or she can authenticate using the second factor.
3. The RA is vetted (i.e., issued a second-factor token) itself, initially, in a bootstrap procedure where SURFnet acts as a central RA. Once vetted, the initial (super-)RA can delegate his/her powers to other sub-RA staff members within the institute.
4. All steps taken by the RA and other events related to the SURFsure service are logged, and logs are kept for an appropriate amount of time.

These requirements are taken as input for implementing the self-service and the RA portal, but it is also recommended that SURFnet clearly *communicate* these requirements (and the rationale behind the requirements) to the institutes. The meaning of the resulting level of assurance in assertions sent around between the participants in the federation is dependent on the quality of the registration processes as implemented at the institutes.

It is also recommended that SURFnet define procedures for admission of new token types and assessment of appropriate LoA for token types.

References

Burr, B., Polk, T., Dodson, D., *Electronic Authentication Guideline, NIST Special Publication 800-63 version 1.0.2, April 2006*

Cantor, Kemp, Philpott, Maler, *Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005*

eHerkenning, *Koppelvlakspecificatie HM-MR v1.5, Juli 2012*

eHerkenning, *Betrouwbaarheidsniveau's, September 2010*

Forum Standaardisatie, *Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten – handreiking voor overheidsorganisaties, http://www.forumstandaardisatie.nl/fileadmin/os/publicaties/HR_Betrouwbaarheidsniveaus_WEB.pdf,* 2012

Gartner, *Magic Quadrant User Authentication, ID: G00227026, available (at the time of writing, for instance) from http://www.clico.pl/rozwiazania/producenci/safenet/MagicQuadrantforUserAuthentication_2012.pdf, 2010*

Hulsebosch R. J., et al., *D2.3 Quality Assurance Levels van het STORK project, https://www.eid-stork.eu/dmdocuments/public/D2.3_final._1.pdf, 2010*

Hulsebosch R. J., *Step-up Authentication-as-a-Service, SURFconext Adoption*, 2011

ITU / ISO, *Information technology – Security techniques – Entity authentication assurance framework, ITU-T Recommendation X.1254 / International Standard ISO/IEC DIS 29115 – Draft, 2011-11-xx*, To Appear (in 2012)

Johansson, L., *An IANAregistry for Level of Assurance (LoA) Profiles, http://tools.ietf.org/html/draft-johansson-loa-registry-06 , May 4, 2012*

Kemp, Cantor, Mishra, Philpott, Maler, *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005*

Lockhart, Campbell, *Level of Assurance Authentication Context Profiles for SAML 2.0, Working Draft 01, 01 July 2008*

Morgan, R.L., Madsen P., Cantor, S., *SAML V2.0 Identity Assurance Profiles 1.0 (Committee Draft)*, November 2010

Morgan, R.L., et al., *InCommon Identity Assurance Profiles Bronze and Silver*, http://www.incommon.org/docs/assurance/IAP.pdf, May 2011

NIST, *Special Publication 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations*, August 2009 (errata May 2010)

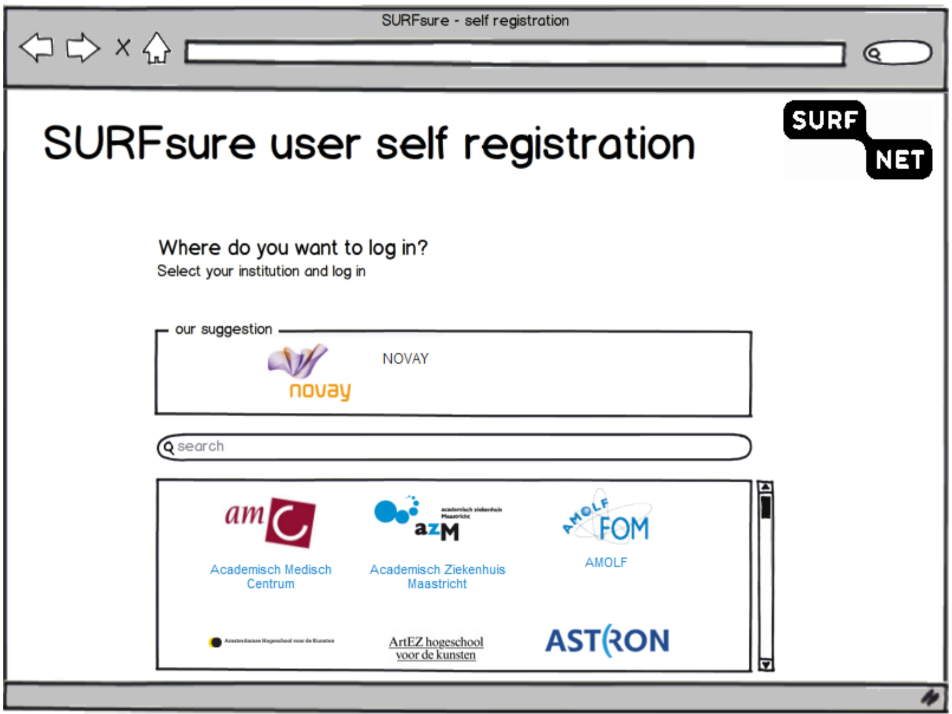
NIST, *Special Publication 800-63, Version 1.0.2, Electronic Authentication Guideline*, available from http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf, 2006

Ter Harst, Van Rijswijk, *Step-up-authentication-as-a-service business case - SI Infra 2012 - Collaboration Infrastructure Wiki*, June 2012

Appendix – Mockups

The wireframe mockups in this Appendix give an impression of what the self-service portal could look like. The mockups in this appendix and the next one are in part inspired by earlier mock-ups by Roland van Rijswijk - Deij, the existing WAYF flow as implemented by a number of SURFnet services, and the UnitedId.org proof-of-concept service.

General mockups for the user self registration portal

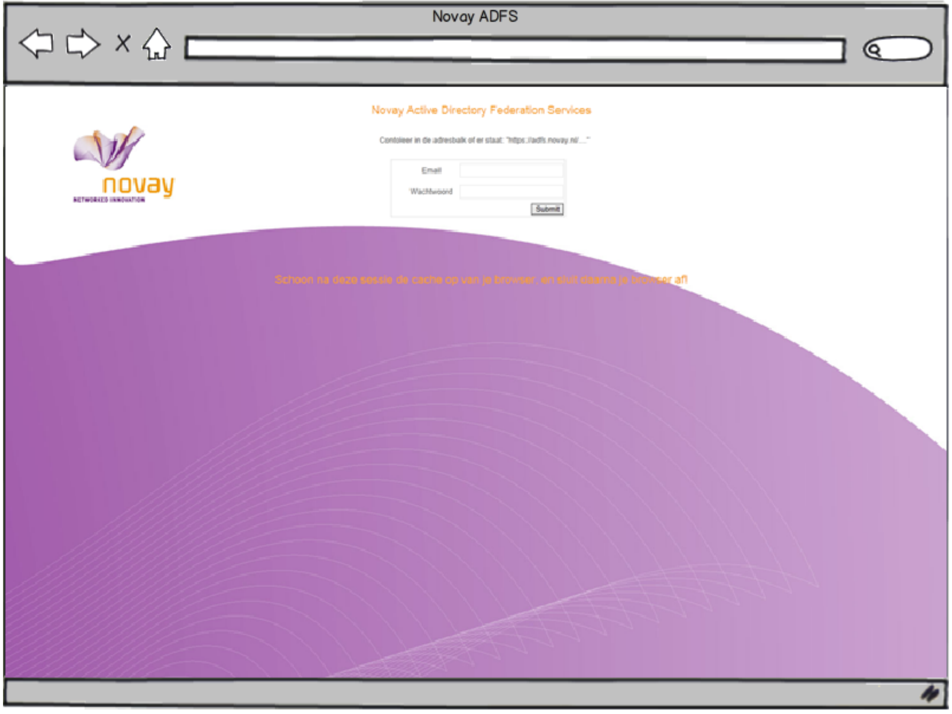


SURFsure - self registration

SURFsure user self registration

Where do you want to log in?
Select your institution and log in

our suggestion
NOVAY
search
Academisch Medisch Centrum
Academisch Ziekenhuis Maastricht
AMOLF
ArtEZ hogeschool voor de kunsten
ASTRON



Novay ADFS

Novay Active Directory Federation Services

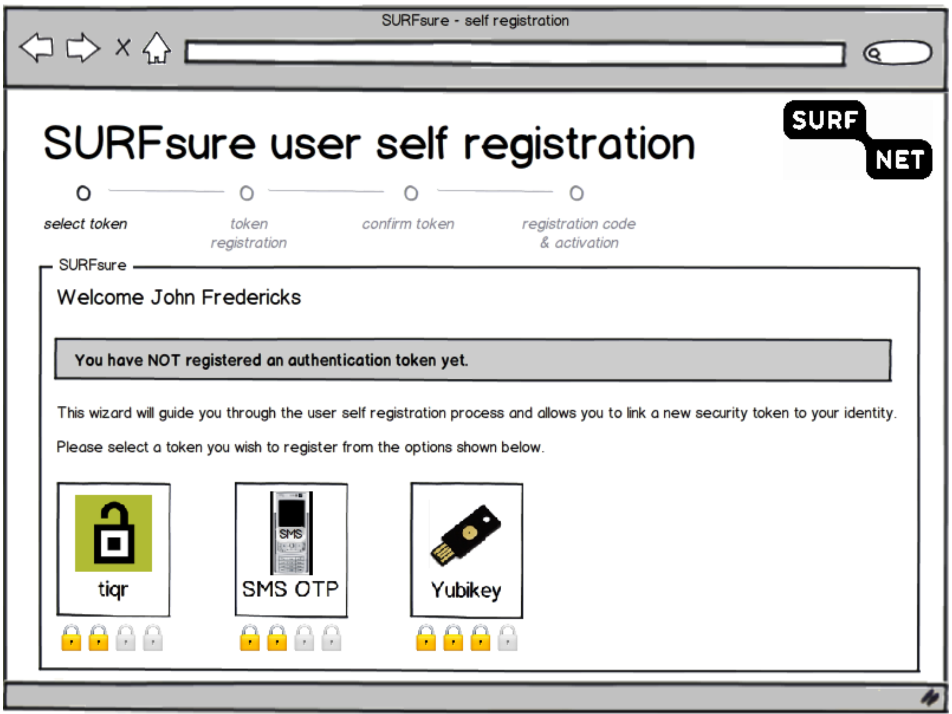
Contoleer in de adresbalk of er staat: "https://adfs.novay.nl/...."

Email

Wachtwoord

Submit

Schoon na deze sessie de cache op van je browser, en sluit daarna je browser af!



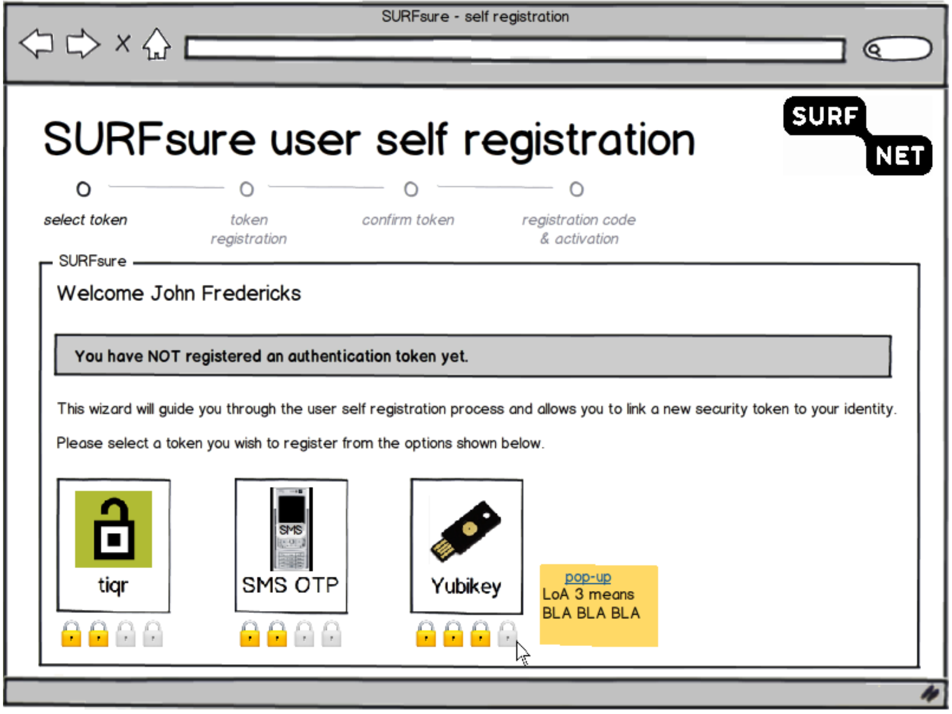
SURFsure user self registration

Welcome John Fredericks

You have NOT registered an authentication token yet.

This wizard will guide you through the user self registration process and allows you to link a new security token to your identity.

Please select a token you wish to register from the options shown below.



SURFsure user self registration

Welcome John Fredericks

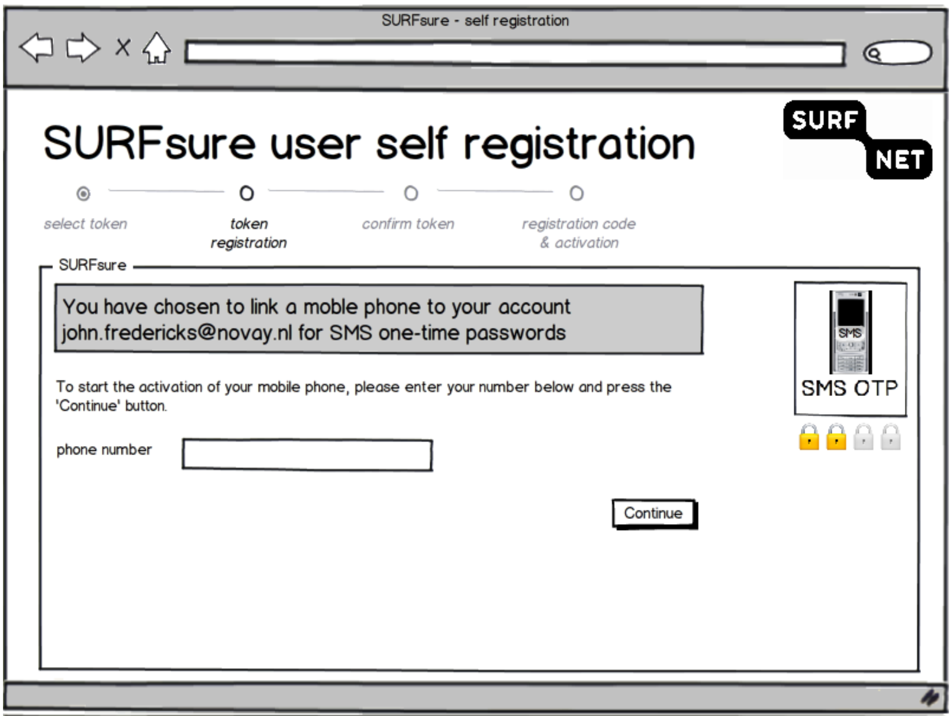
You have NOT registered an authentication token yet.

This wizard will guide you through the user self registration process and allows you to link a new security token to your identity.

Please select a token you wish to register from the options shown below.

LoA 3 means
BLA BLA BLA

Mockups for self registration of SMS OTP



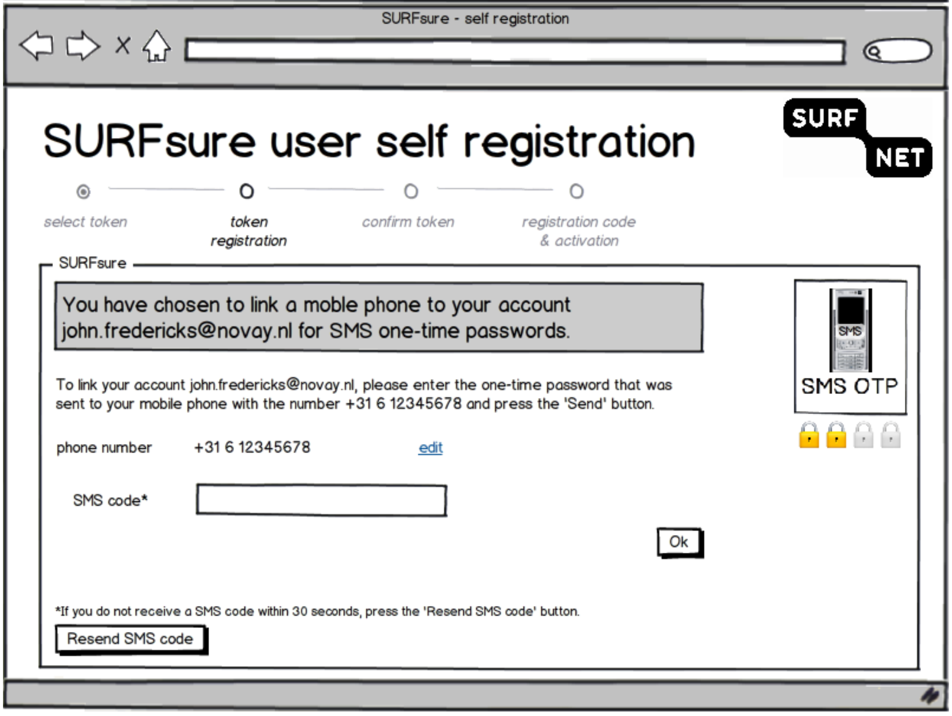
SURFsure user self registration

SURFsure

You have chosen to link a moble phone to your account john.fredericks@novay.nl for SMS one-time passwords

To start the activation of your mobile phone, please enter your number below and press the 'Continue' button.

phone number



SURFsure user self registration

SURFsure

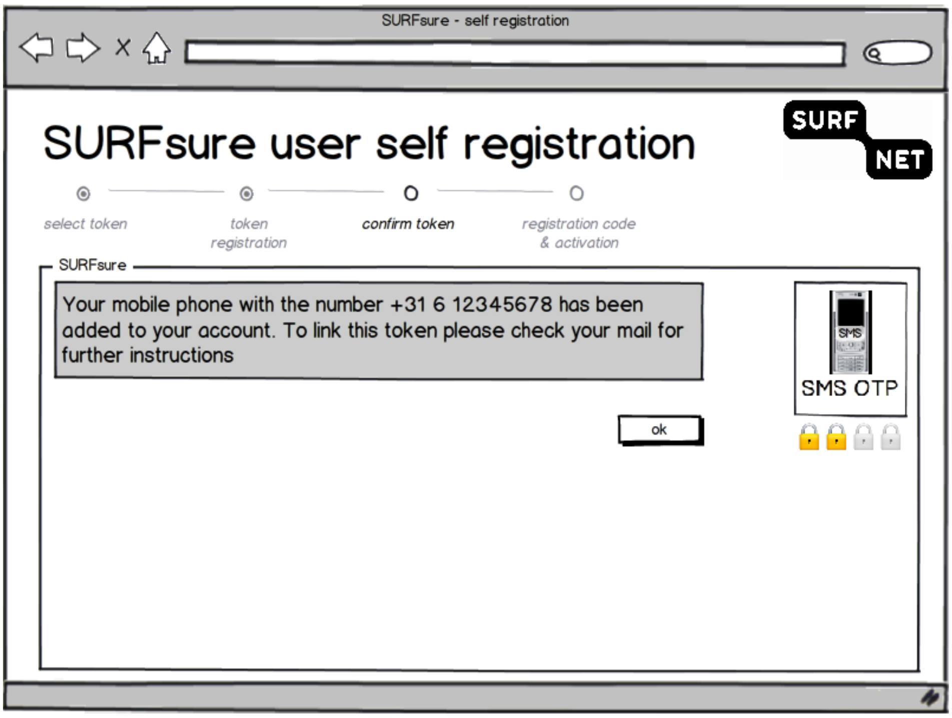
You have chosen to link a moble phone to your account john.fredericks@novay.nl for SMS one-time passwords.

To link your account john.fredericks@novay.nl, please enter the one-time password that was sent to your mobile phone with the number +31 6 12345678 and press the 'Send' button.

phone number +31 6 12345678

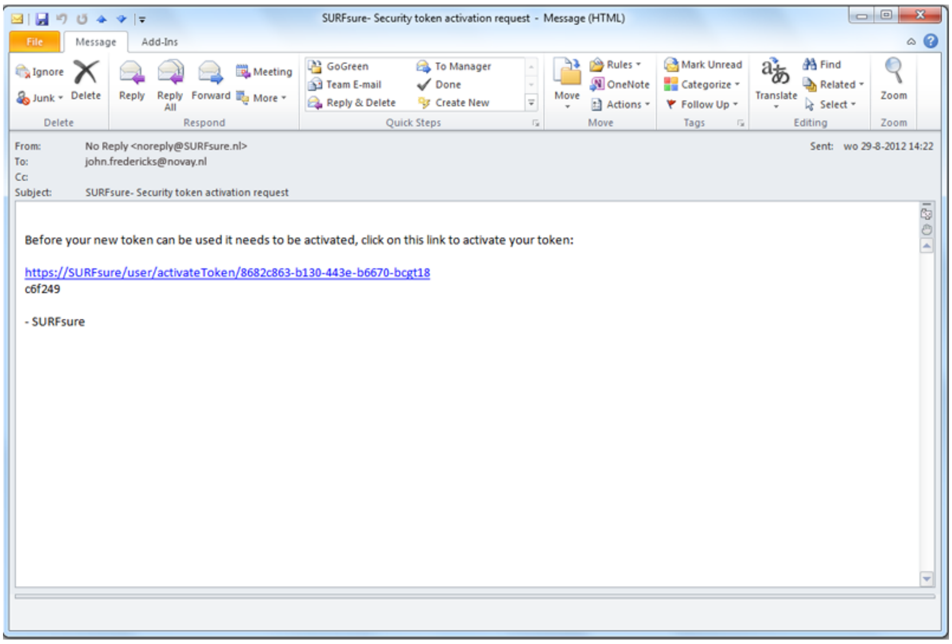
SMS code*

*If you do not receive a SMS code within 30 seconds, press the 'Resend SMS code' button.



SURFsure user self registration

Your mobile phone with the number +31 6 12345678 has been added to your account. To link this token please check your mail for further instructions

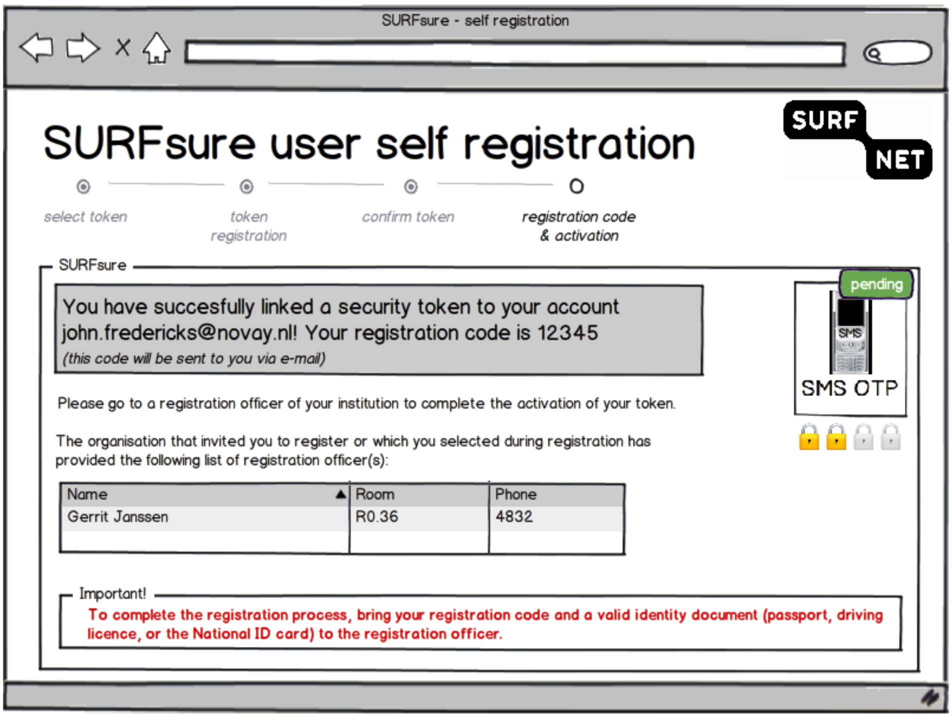


From: No Reply <noreply@SURFsure.nl>
To: john.fredericks@novay.nl
Cc:
Subject: SURFsure- Security token activation request
Sent: wo 29-8-2012 14:22

Before your new token can be used it needs to be activated, click on this link to activate your token:

https://SURFsure/user/activateToken/8682c863-b130-443e-b6670-bcgt18
c6f249

- SURFsure



SURFsure - self registration

SURFsure user self registration

You have succesfully linked a security token to your account john.fredericks@novay.nl! Your registration code is 12345

(this code will be sent to you via e-mail)

Please go to a registration officer of your institution to complete the activation of your token.

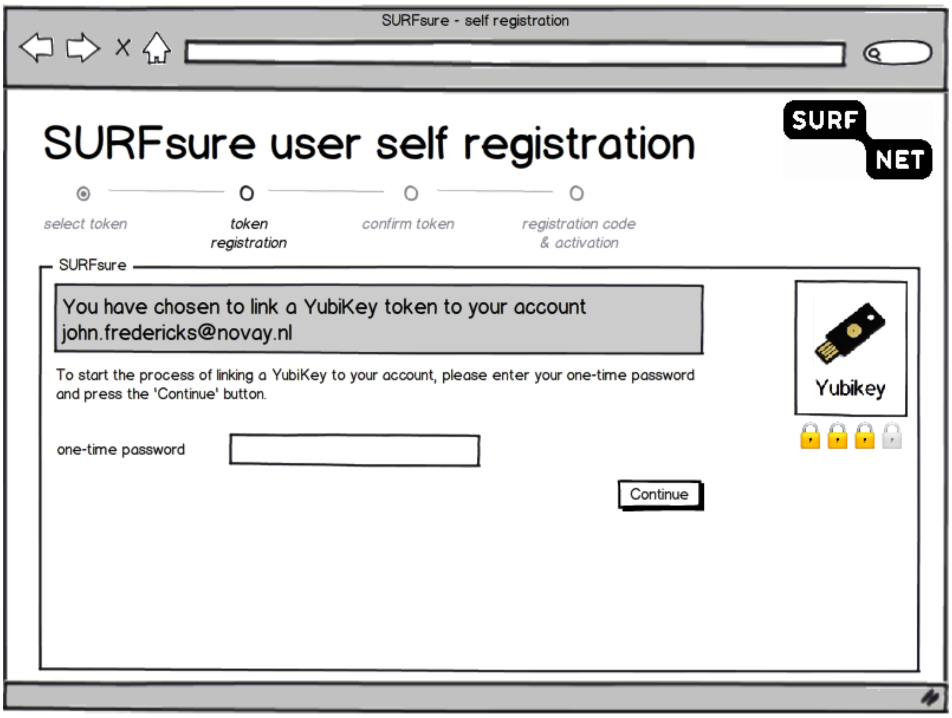
The organisation that invited you to register or which you selected during registration has provided the following list of registration officer(s):

Name ▲	Room	Phone
Gerrit Janssen	R0.36	4832

Important!

To complete the registration process, bring your registration code and a valid identity document (passport, driving licence, or the National ID card) to the registration officer.

Mockups of user self registration for Yubikey



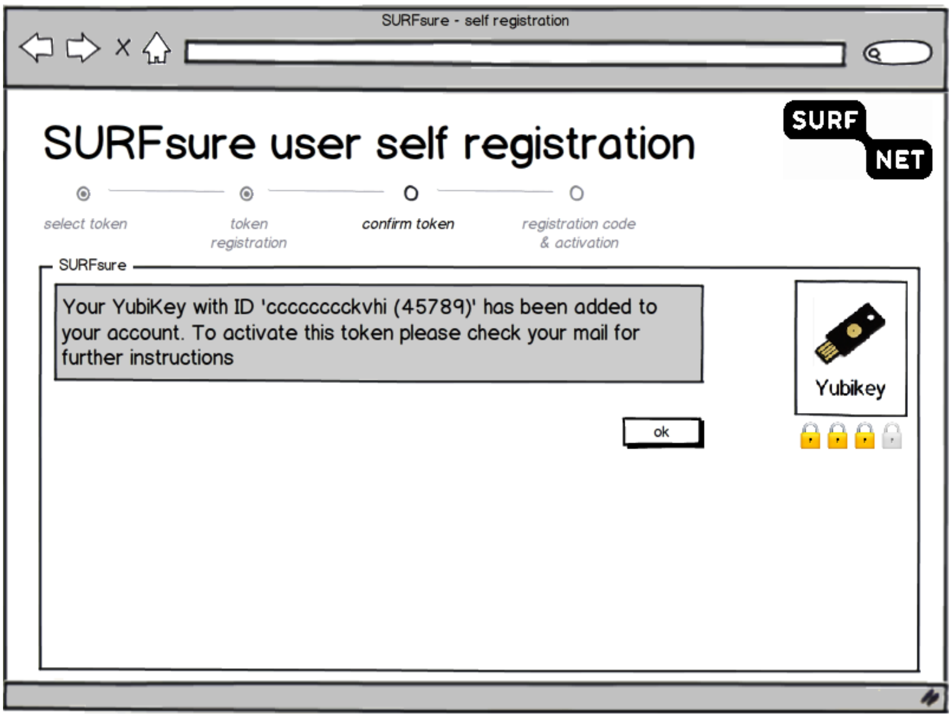
SURFsure - self registration

SURFsure user self registration

You have chosen to link a YubiKey token to your account john.fredericks@novay.nl

To start the process of linking a YubiKey to your account, please enter your one-time password and press the 'Continue' button.

one-time password

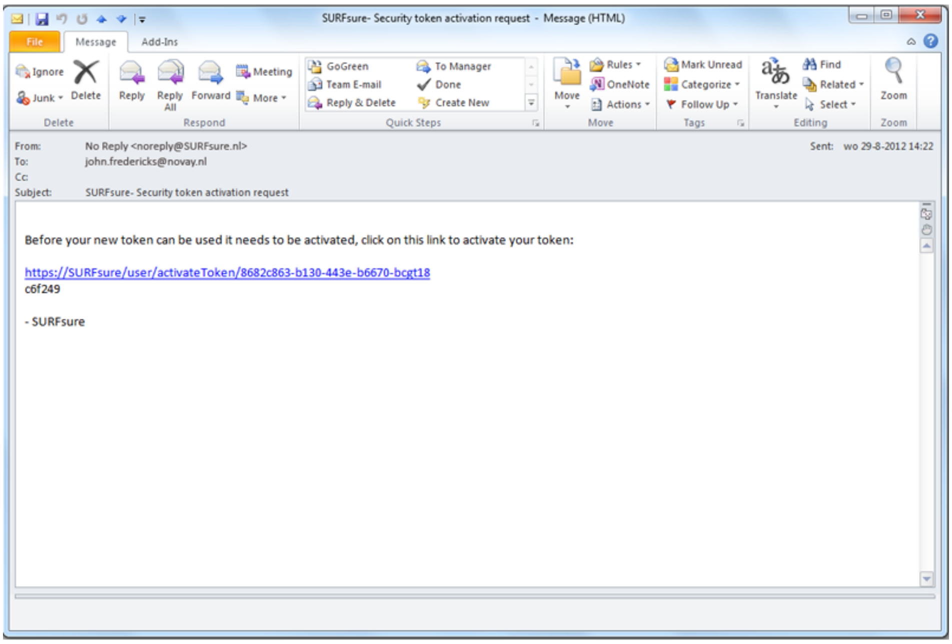


SURFsure - self registration

SURFsure user self registration

Your YubiKey with ID 'cccccccckvhi (45789)' has been added to your account. To activate this token please check your mail for further instructions

ok



SURFsure- Security token activation request - Message (HTML)

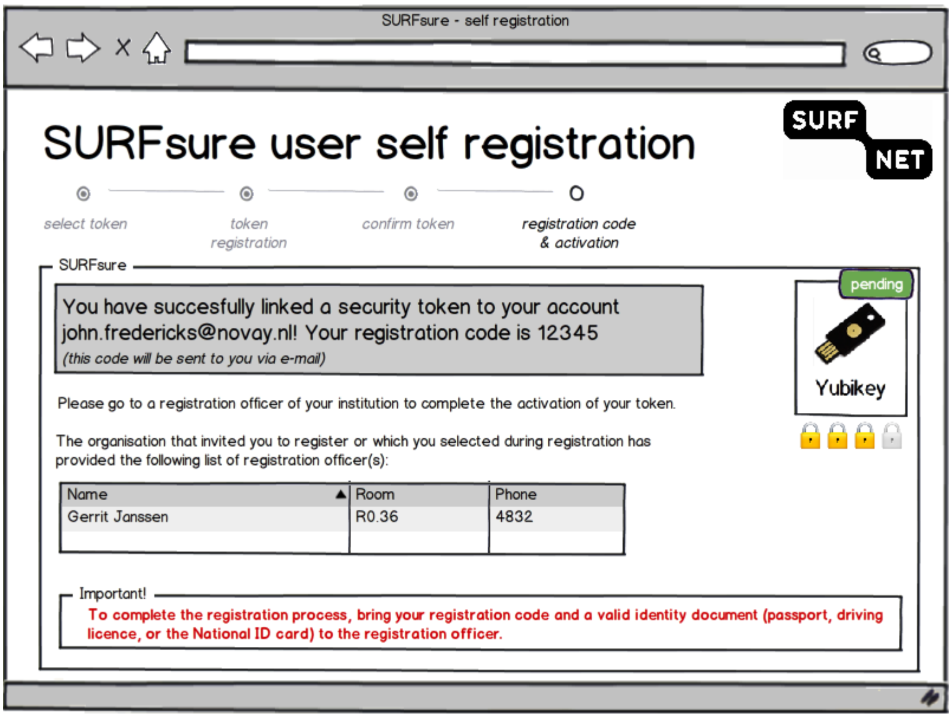
From: No Reply <noreply@SURFsure.nl>
To: john.fredericks@novay.nl
Cc:
Subject: SURFsure- Security token activation request

Sent: wo 29-8-2012 14:22

Before your new token can be used it needs to be activated, click on this link to activate your token:

https://SURFsure/user/activateToken/8682c863-b130-443e-b6670-bcgt18
c6f249

- SURFsure



SURFsure - self registration

SURFsure user self registration

SURFsure

You have succesfully linked a security token to your account john.fredericks@novay.nl! Your registration code is 12345

(this code will be sent to you via e-mail)

Please go to a registration officer of your institution to complete the activation of your token.

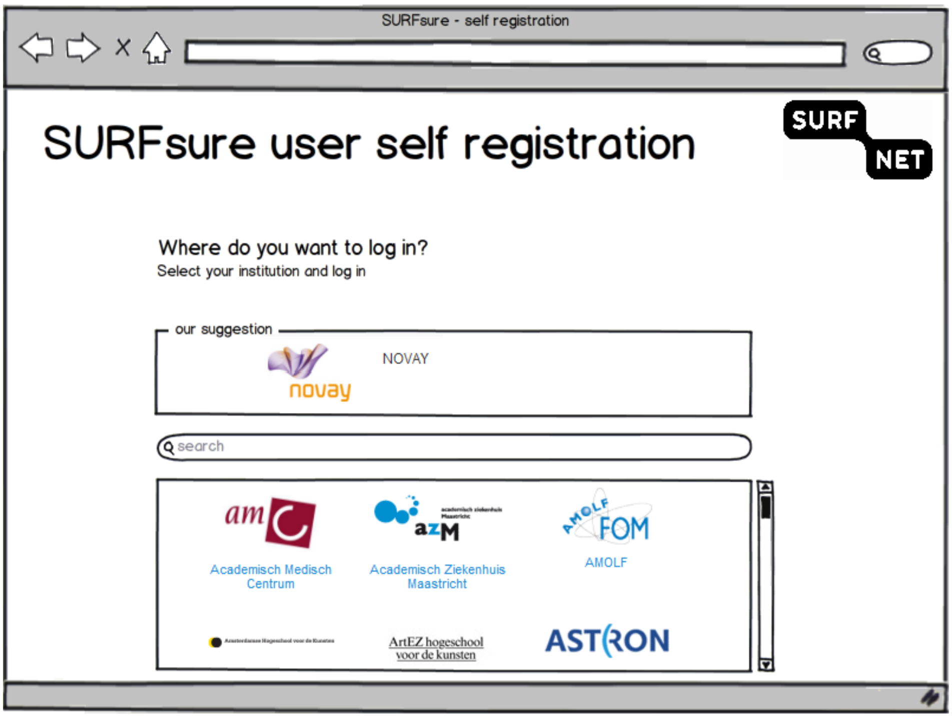
The organisation that invited you to register or which you selected during registration has provided the following list of registration officer(s):

Name ▲	Room	Phone
Gerrit Janssen	R0.36	4832

Important!

To complete the registration process, bring your registration code and a valid identity document (passport, driving licence, or the National ID card) to the registration officer.

Mockups of user self management (removing registration)



SURFsure - self registration

SURFsure user self registration

Where do you want to log in?

Select your institution and log in

our suggestion

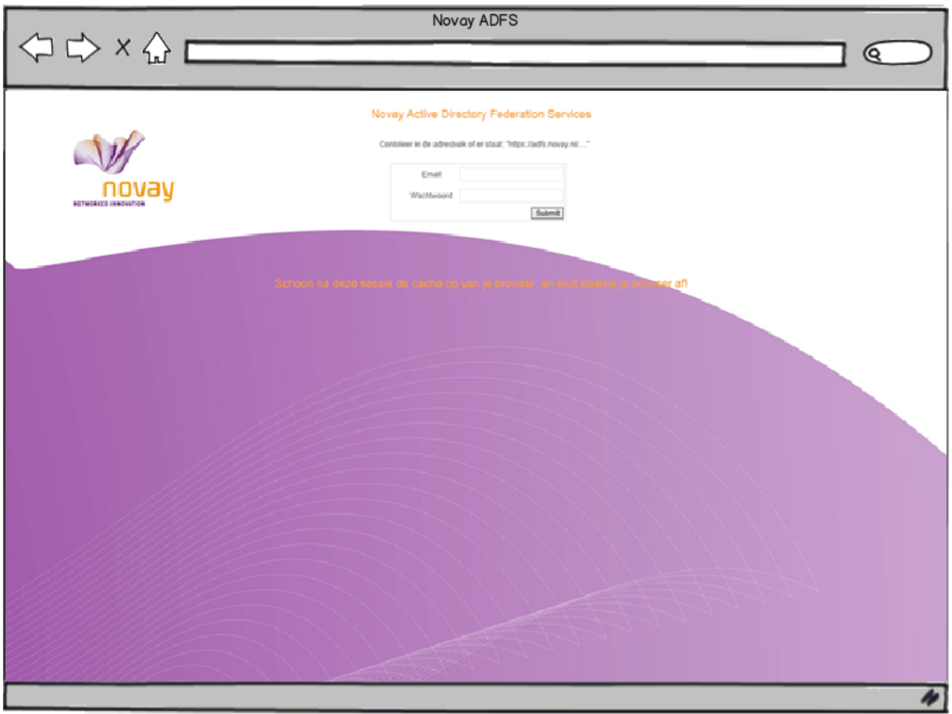
NOVAY

search

Academisch Medisch Centrum

Academisch Ziekenhuis Maastricht

AMOLF



Novay Active Directory Federation Services

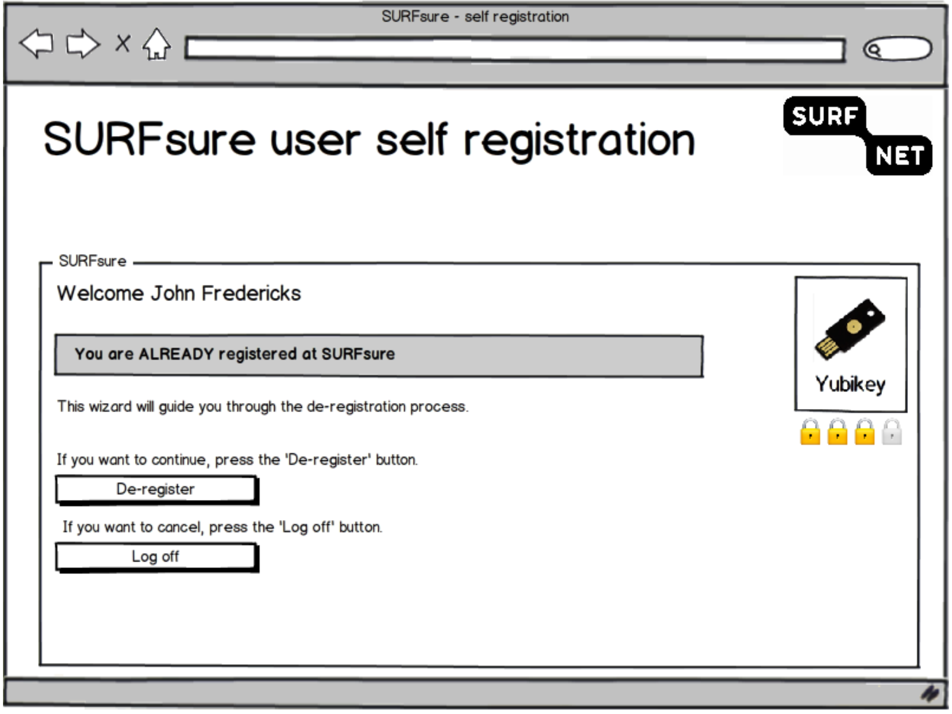
Contoleer in de adresbalk of er staat: "https://adfs.novay.nl/....."

Email

Wachtwoord

Submit

Schoon na deze sessie de cache op van je browser, en sluit daarna je browser af!



SURFsure user self registration

SURFsure

Welcome John Fredericks

You are ALREADY registered at SURFsure

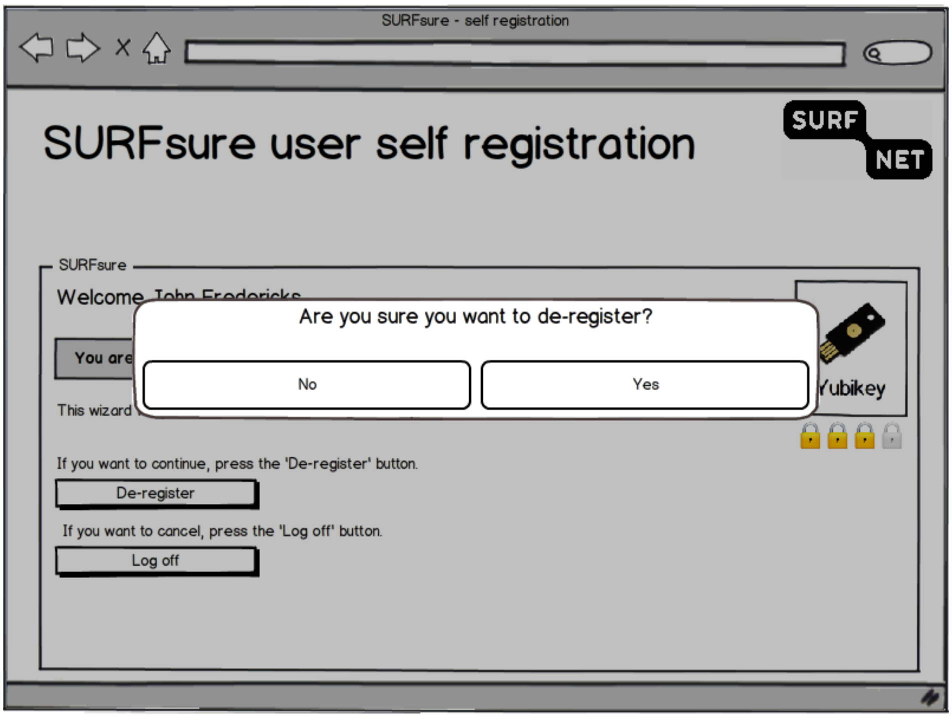
This wizard will guide you through the de-registration process.

If you want to continue, press the 'De-register' button.

De-register

If you want to cancel, press the 'Log off' button.

Log off



SURFsure - self registration

SURFsure user self registration

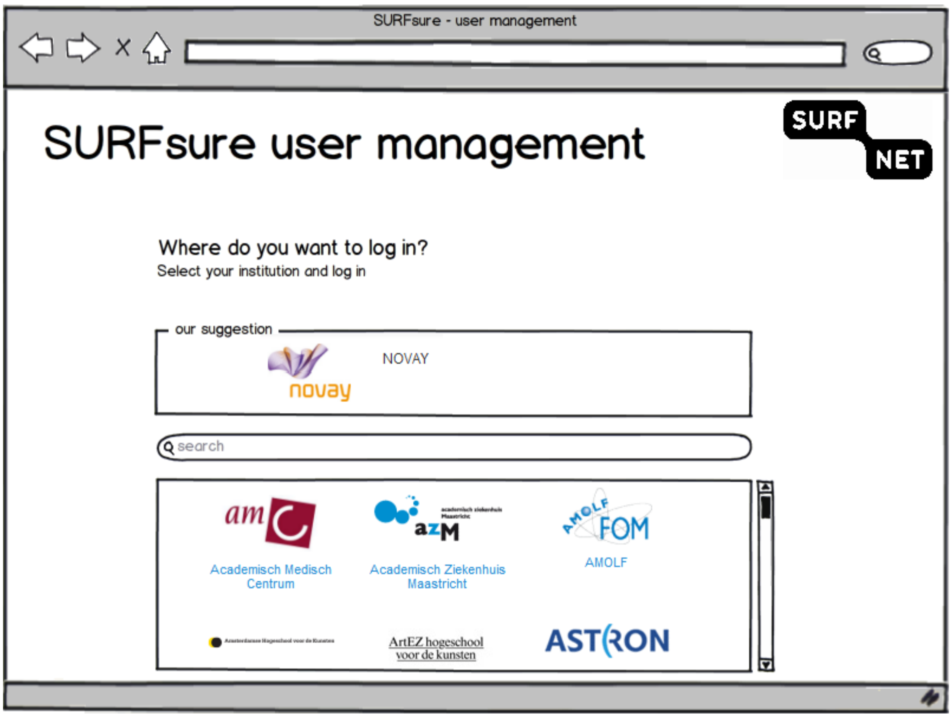
Welcome John Fredericks

Are you sure you want to de-register?

If you want to continue, press the 'De-register' button.

If you want to cancel, press the 'Log off' button.

General mockups of user management by the RA



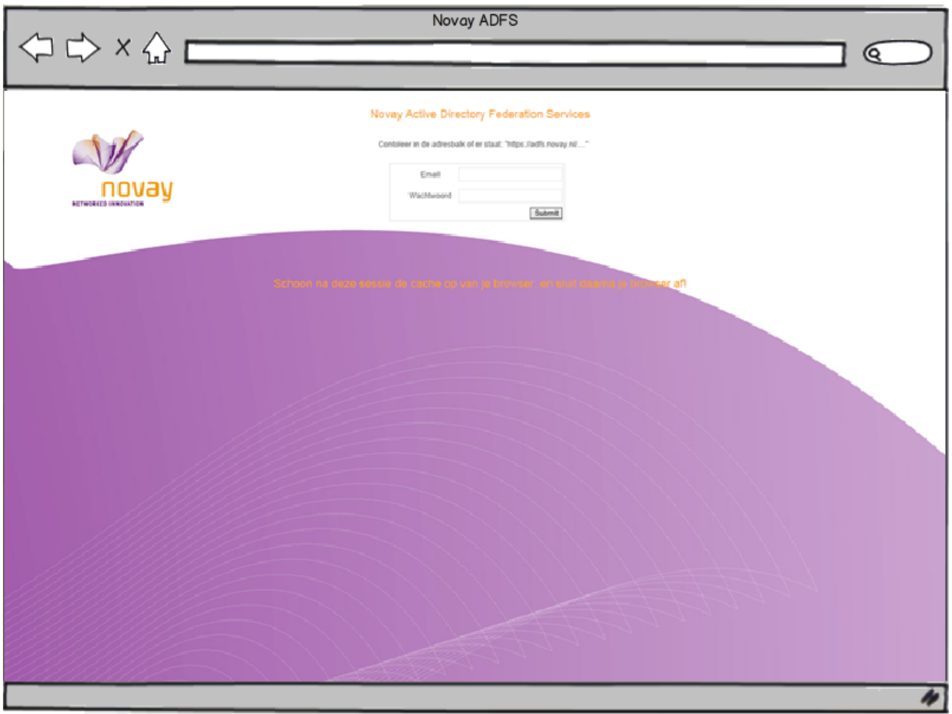
SURFsure - user management

SURFsure user management

Where do you want to log in?

Select your institution and log in

SURF NET
our suggestion
novay
NOVAY
search
amc
Academisch Medisch Centrum
azM
Academisch Ziekenhuis Maastricht
AMOLF FOM
AMOLF
ArtEZ hogeschool voor de kunsten
ASTRON



Novay ADFS

Novay Active Directory Federation Services

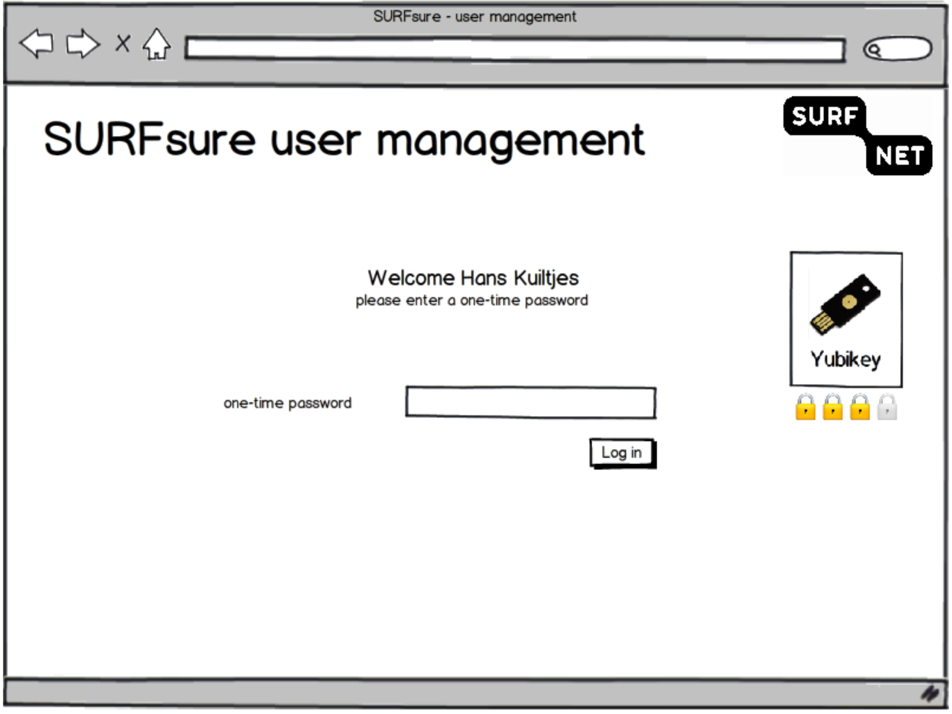
Contoleer in de adresbalk of er staat: "https://adfs.novay.nl/...."

Email

Wachtwoord

Submit

Schoon na deze sessie de cache op van je browser, en sluit daarna je browser af!



SURFsure - user management

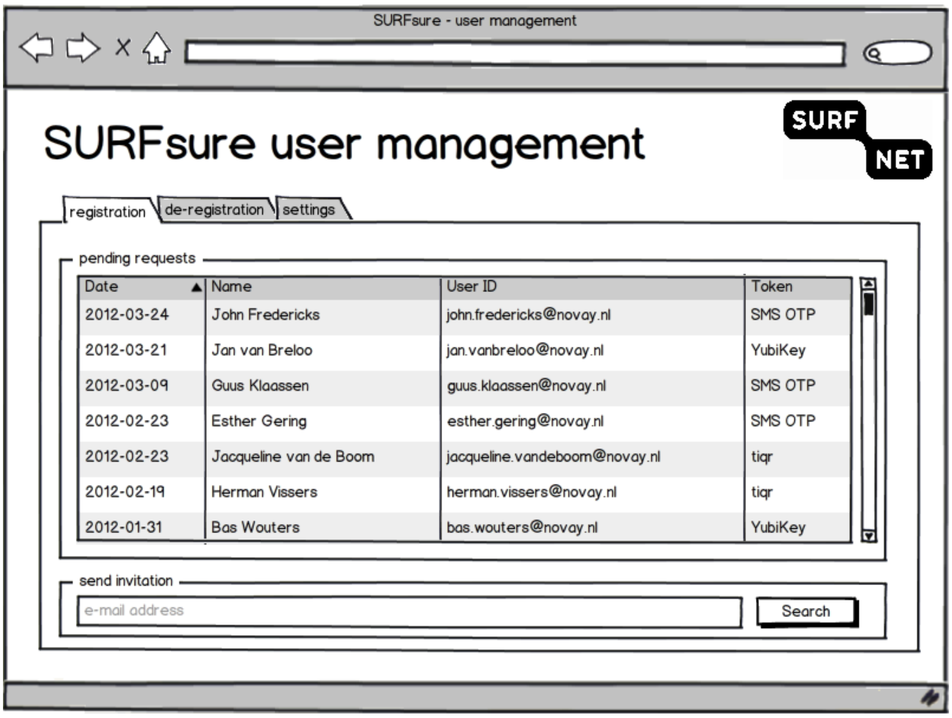
SURFsure user management

Welcome Hans Kuiltjes

please enter a one-time password

one-time password

Log in



SURFsure - user management

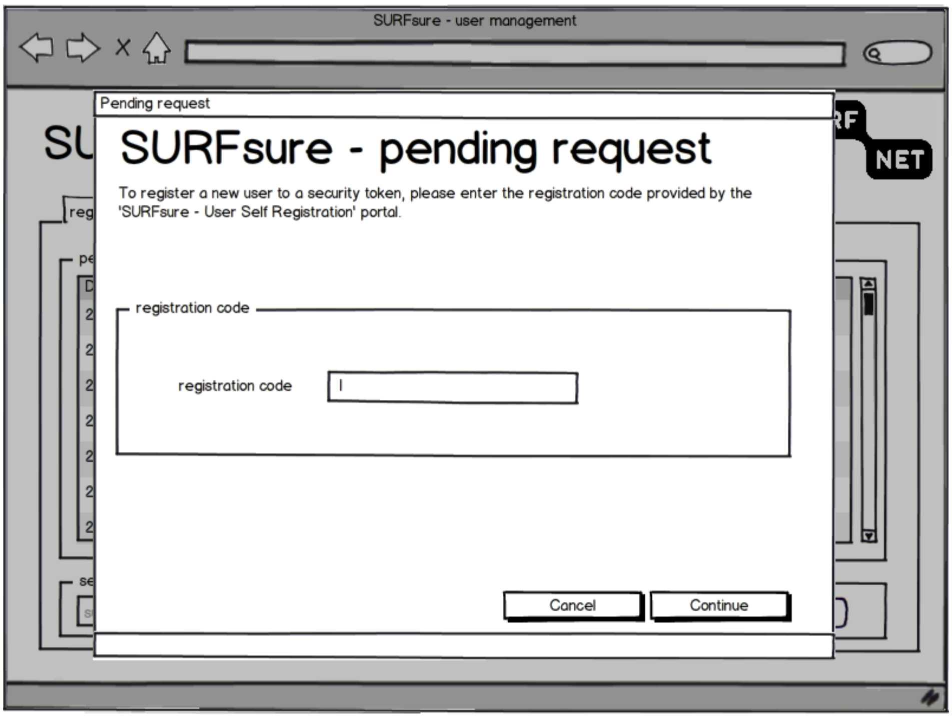
SURFsure user management

pending requests

Date ▲	Name	User ID	Token
2012-03-24	John Fredericks	john.fredericks@novay.nl	SMS OTP
2012-03-21	Jan van Breloo	jan.vanbreloo@novay.nl	YubiKey
2012-03-09	Guus Klaassen	guus.klaassen@novay.nl	SMS OTP
2012-02-23	Esther Gering	esther.gering@novay.nl	SMS OTP
2012-02-23	Jacqueline van de Boom	jacqueline.vandeboom@novay.nl	tiqr
2012-02-19	Herman Vissers	herman.vissers@novay.nl	tiqr
2012-01-31	Bas Wouters	bas.wouters@novay.nl	YubiKey

send invitation

Mockups for handling pending registration requests by the RA



SURFsure - user management

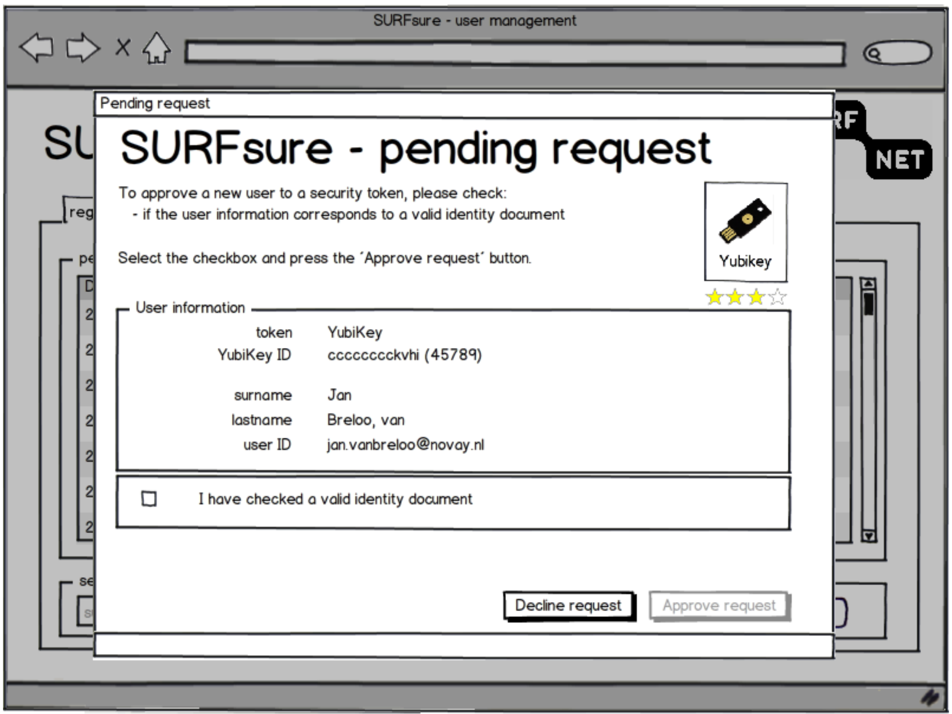
Pending request

SURFsure - pending request

To register a new user to a security token, please enter the registration code provided by the 'SURFsure - User Self Registration' portal.

registration code

registration code: I



SURFsure - user management

Pending request

SURFsure - pending request

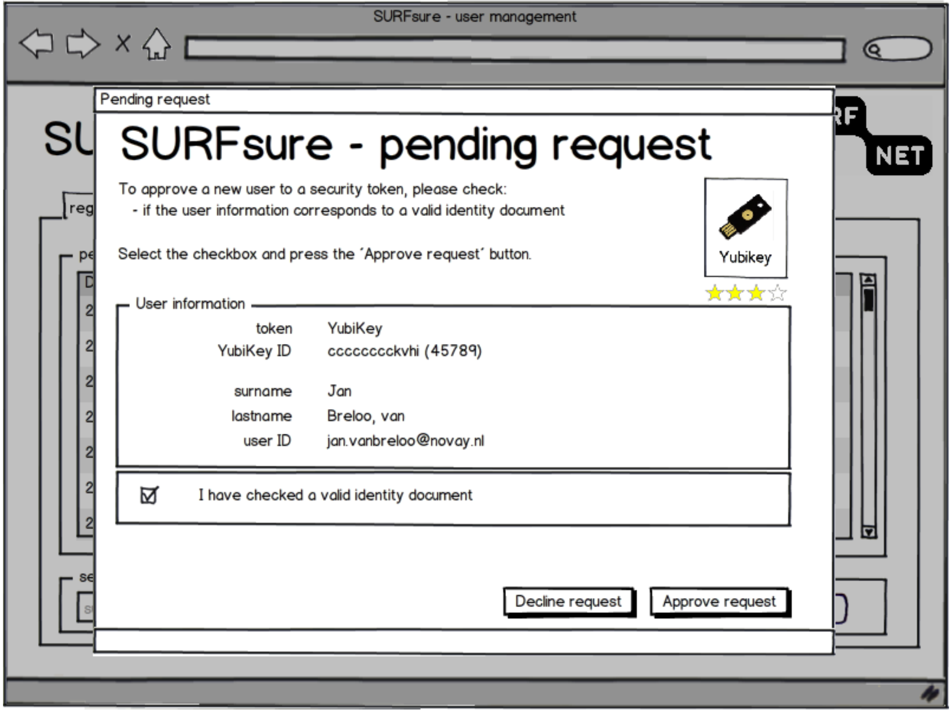
To approve a new user to a security token, please check:
- if the user information corresponds to a valid identity document

Select the checkbox and press the ´Approve request´ button.

User information

token	YubiKey
YubiKey ID	cccccccckvhi (45789)
surname	Jan
lastname	Breloo, van
user ID	jan.vanbreloo@novay.nl

□ I have checked a valid identity document



SURFsure - user management

Pending request

SURFsure - pending request

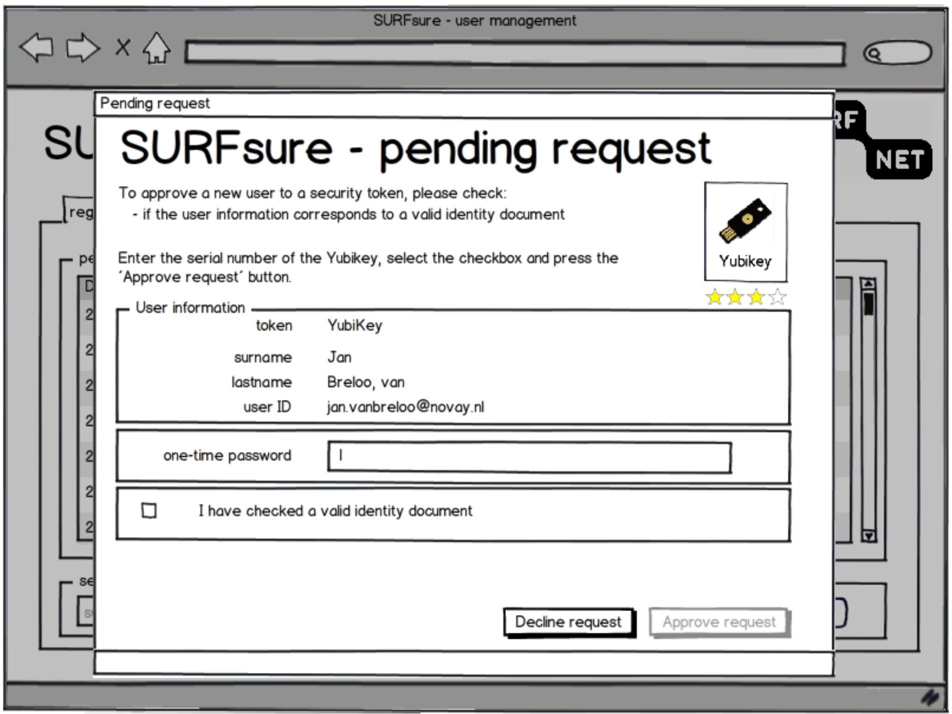
To approve a new user to a security token, please check:
- if the user information corresponds to a valid identity document

Select the checkbox and press the ´Approve request´ button.

User information

token	YubiKey
YubiKey ID	cccccccckvhi (45789)
surname	Jan
lastname	Breloo, van
user ID	jan.vanbreloo@novay.nl

☑ I have checked a valid identity document



SURFsure - pending request

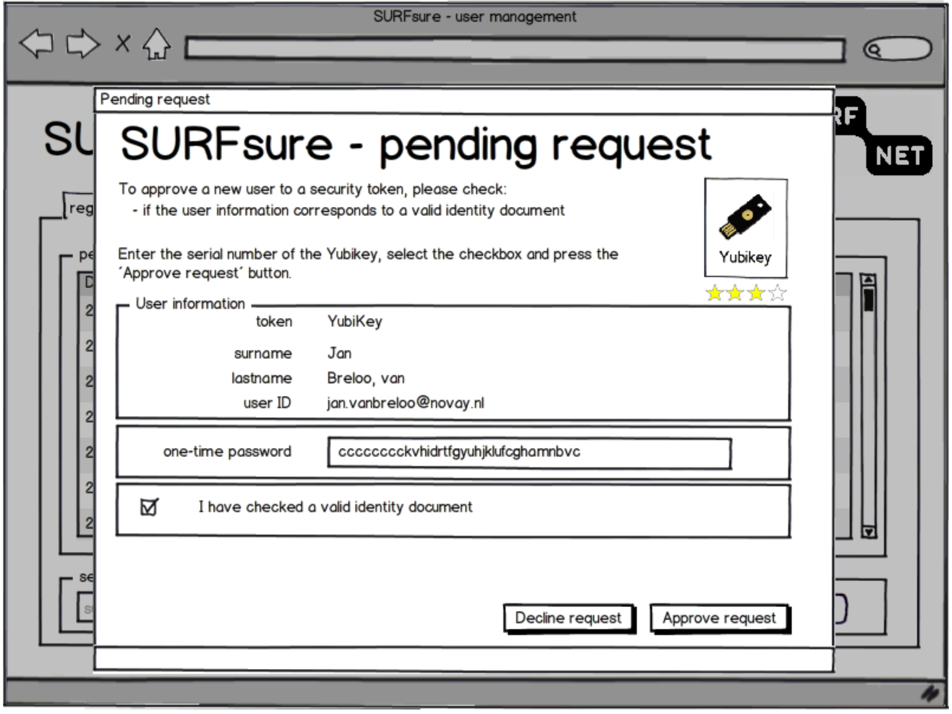
To approve a new user to a security token, please check:
- if the user information corresponds to a valid identity document

Enter the serial number of the Yubikey, select the checkbox and press the ´Approve request´ button.

User information

token	YubiKey
surname	Jan
lastname	Breloo, van
user ID	jan.vanbreloo@novay.nl
one-time password	I

☐ I have checked a valid identity document



SURFsure - pending request

To approve a new user to a security token, please check:
- if the user information corresponds to a valid identity document

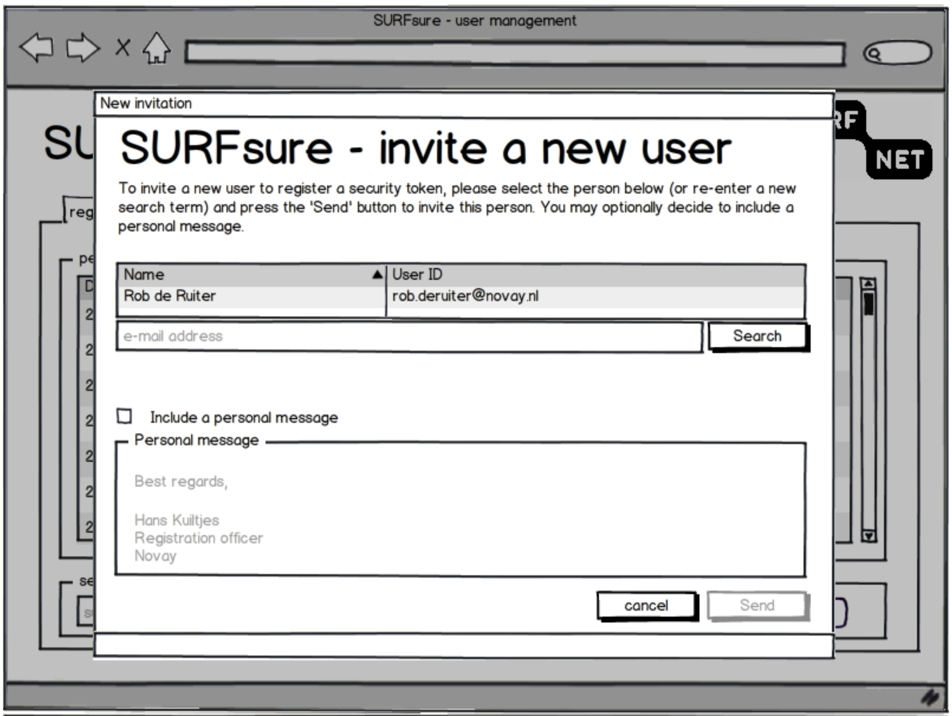
Enter the serial number of the Yubikey, select the checkbox and press the ´Approve request´ button.

User information

token	YubiKey
surname	Jan
lastname	Breloo, van
user ID	jan.vanbreloo@novay.nl
one-time password	cccccccckvhidrtfgyuhjklufcghamnbvc

☑ I have checked a valid identity document

Mockups for inviting new users



SURFsure - invite a new user

To invite a new user to register a security token, please select the person below (or re-enter a new search term) and press the 'Send' button to invite this person. You may optionally decide to include a personal message.

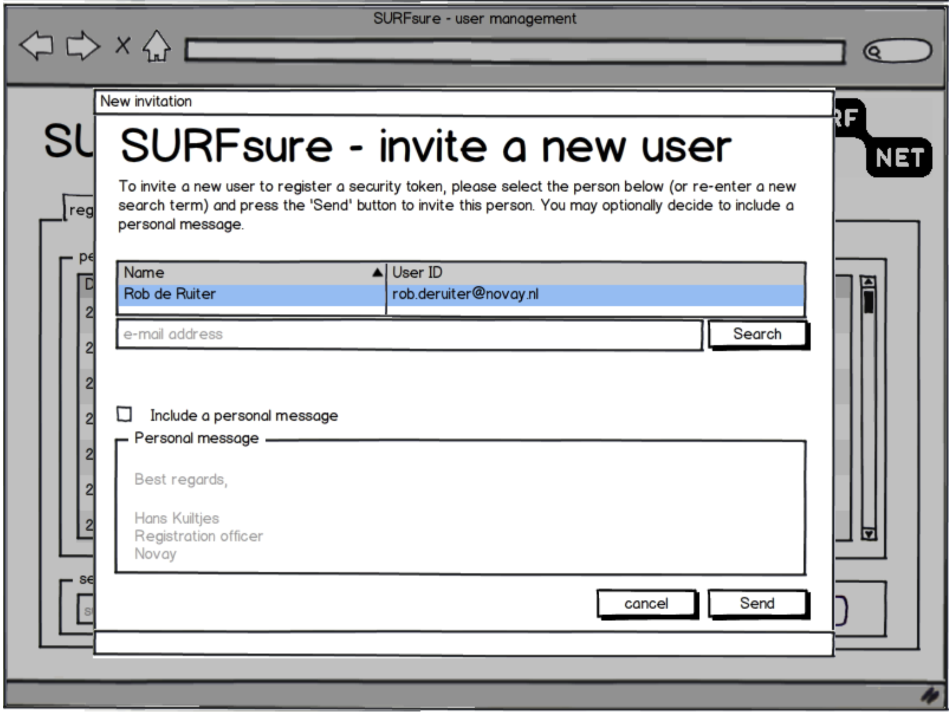
Name ▲	User ID
Rob de Ruiter	rob.deruiter@novay.nl

□ Include a personal message

Personal message

Best regards,

Hans Kuiltjes
Registration officer
Novay



SURFsure - invite a new user

To invite a new user to register a security token, please select the person below (or re-enter a new search term) and press the 'Send' button to invite this person. You may optionally decide to include a personal message.

Name ▲	User ID
Rob de Ruiter	rob.deruiter@novay.nl

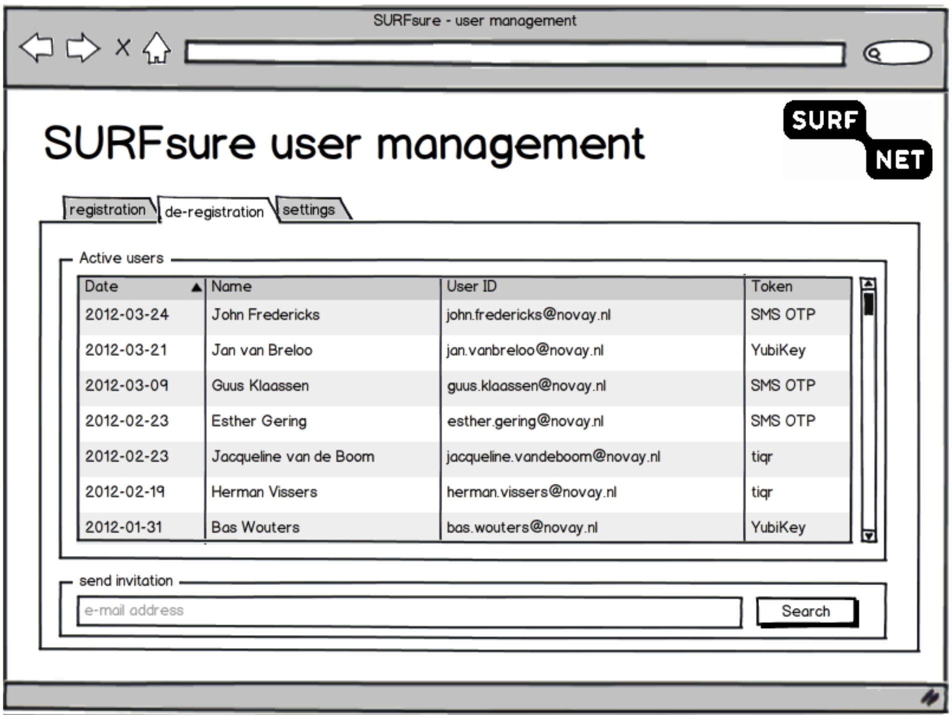
□ Include a personal message

Personal message

Best regards,

Hans Kuiltjes
Registration officer
Novay

Mockups for user deregistration by the RA



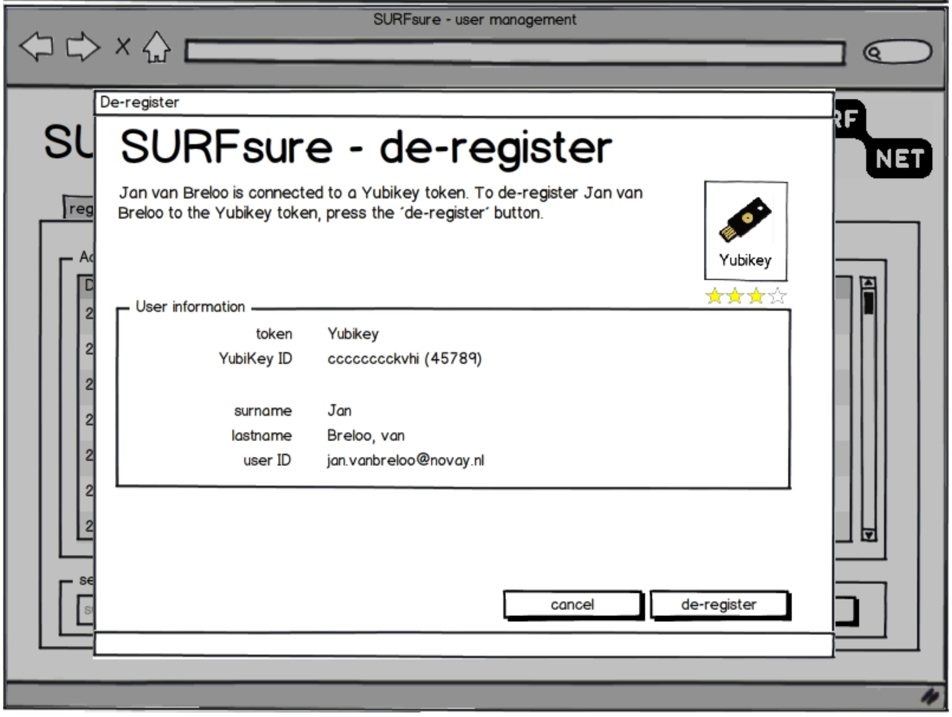
SURFsure user management

Active users

Date ▲	Name	User ID	Token
2012-03-24	John Fredericks	john.fredericks@novay.nl	SMS OTP
2012-03-21	Jan van Breloo	jan.vanbreloo@novay.nl	YubiKey
2012-03-09	Guus Klaassen	guus.klaassen@novay.nl	SMS OTP
2012-02-23	Esther Gering	esther.gering@novay.nl	SMS OTP
2012-02-23	Jacqueline van de Boom	jacqueline.vandeboom@novay.nl	tiqr
2012-02-19	Herman Vissers	herman.vissers@novay.nl	tiqr
2012-01-31	Bas Wouters	bas.wouters@novay.nl	YubiKey

send invitation

e-mail address



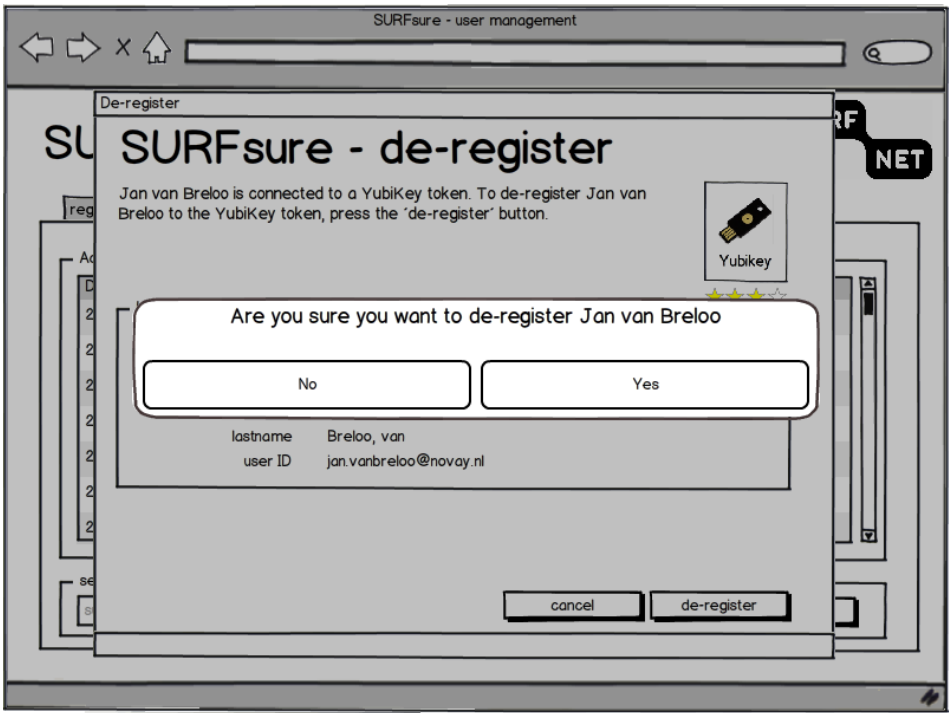
SURFsure - de-register

Jan van Breloo is connected to a Yubikey token. To de-register Jan van Breloo to the Yubikey token, press the ´de-register´ button.

User information

token Yubikey
YubiKey ID cccccccckvhi (45789)

surname Jan
lastname Breloo, van
user ID jan.vanbreloo@novay.nl

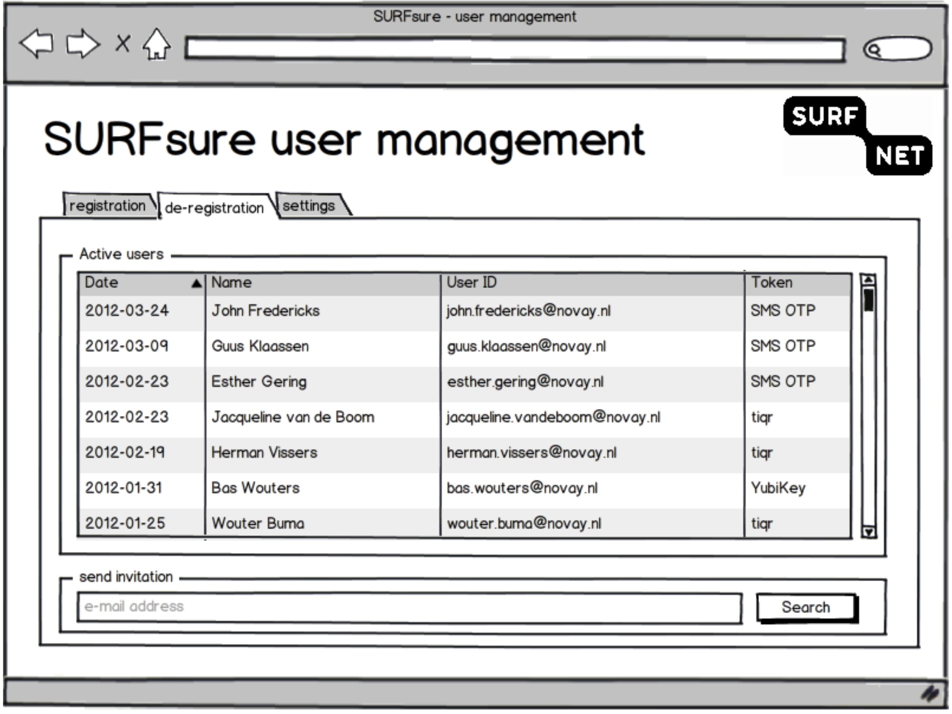


SURFsure - de-register

Jan van Breloo is connected to a YubiKey token. To de-register Jan van Breloo to the YubiKey token, press the 'de-register' button.

Are you sure you want to de-register Jan van Breloo

lastname Breloo, van
user ID jan.vanbreloo@novay.nl



SURFsure user management

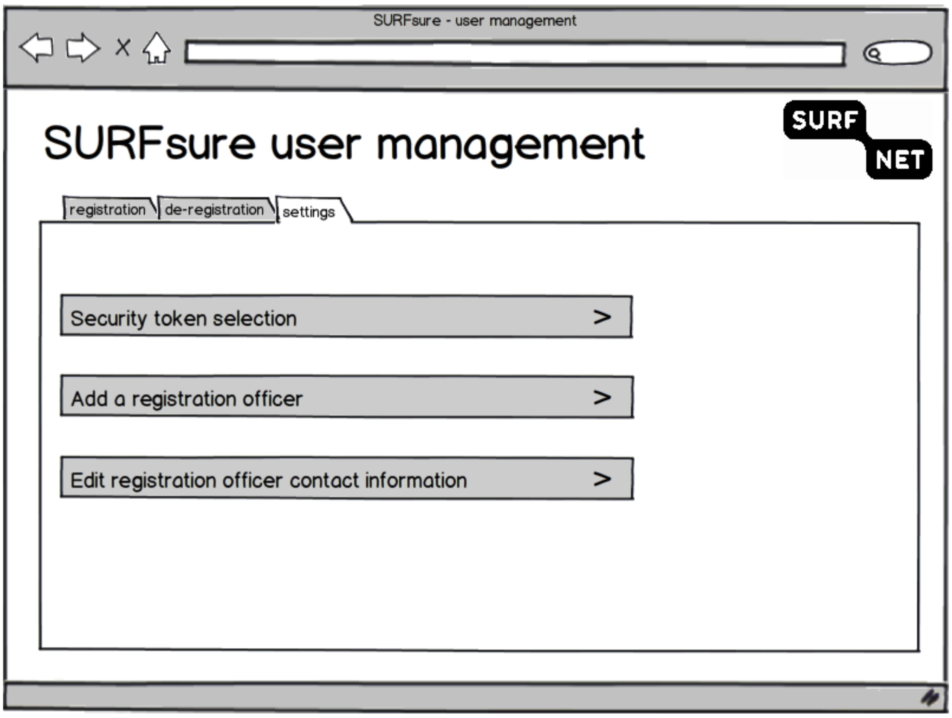
Active users

Date	Name	User ID	Token
2012-03-24	John Fredericks	john.fredericks@novay.nl	SMS OTP
2012-03-09	Guus Klaassen	guus.klaassen@novay.nl	SMS OTP
2012-02-23	Esther Gering	esther.gering@novay.nl	SMS OTP
2012-02-23	Jacqueline van de Boom	jacqueline.vandeboom@novay.nl	tiqr
2012-02-19	Herman Vissers	herman.vissers@novay.nl	tiqr
2012-01-31	Bas Wouters	bas.wouters@novay.nl	YubiKey
2012-01-25	Wouter Buma	wouter.buma@novay.nl	tiqr

send invitation

e-mail address

Mockups for the settings panel



SURFsure - user management
SURFsure user management
SURF
NET
registration
de-registration
settings
Security token selection >
Add a registration officer >
Edit registration officer contact information >