



SWITCH

The Swiss Education & Research Network

Assurance Levels

Lukas Haemmerle
haemmerle@switch.ch



SWITCH as organization asserts:

“The person giving the presentation right now in front of you is a staff member and his name is Lukas Haemmerle”

- What do we actually know about a user identity?
- How much to trust the asserted identity?

Today there is no explicit level of assurance for SWITCHaai identities

- Is the authenticated user who he claims to be?

All SWITCHaai users today are authenticated with login name and password

- Is this secure enough for all applications?

Identity Assurance Levels

- Describe the “degree of **confidence in a user’s asserted identity**”
- Policy describes levels (processes, requirements, ...)
- Usually expressed in numbers, e.g. 1 - 4 (NIST, EU IDA)

Multi-Factor Authentication

- Enhance **confidence in authentication** and thus also trust in asserted identity
- Usually required for higher assurance levels

- **Assurance levels and multi-factor authentication open new opportunities for more sensitive applications**
 - Federated applications as well as internally used applications
 - More and more such applications will use AAI
- **AAI authentication methods can be extended and improved**
 - For a subgroup of users and specific applications

Applications developers shouldn't have to care themselves about quality of user identities and secure authentication

1. How individuals are initially **identified**, including **required proofs** of identity and the identification process.
2. How the credential is **uniquely linked** to the individual, including how the credential is issued.
3. The level of **security** afforded to the **credential**

Requirements

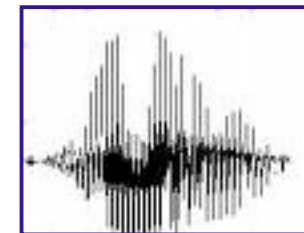
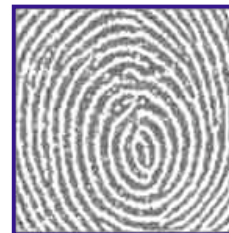
- Registration procedure
 - Basis for identity proofing
 - Credential delivery
 - Authentication session validity
 - Credential validity
 - Financial Liability
- **Authentication security**

Factor is something you

- know (e.g. login name and password)
 - May be asked (social engineering, phishing)
- have (e.g. tally sheet, hardware token)
 - May be stolen and/or duplicated
- are (e.g. fingerprint)
 - May be replicated

Username: haemmer
Password:
Login

1-20	21-40
<input checked="" type="checkbox"/> BFEAL	<input type="checkbox"/> MCUC
<input checked="" type="checkbox"/> BFGG	<input type="checkbox"/> BUOC
<input checked="" type="checkbox"/> CQSC	<input type="checkbox"/> NRSB
<input checked="" type="checkbox"/> NUSK	<input type="checkbox"/> TRIV
<input checked="" type="checkbox"/> HRSZ	<input type="checkbox"/> UXTV
<input checked="" type="checkbox"/> BKST	<input type="checkbox"/> SLDL
<input checked="" type="checkbox"/> PUVV	<input type="checkbox"/> SKZV
<input checked="" type="checkbox"/> FJFB	<input type="checkbox"/> NZWS
<input type="checkbox"/> VTSD	<input type="checkbox"/> SPTL
<input type="checkbox"/> HAZJ	<input type="checkbox"/> CZVA



The more factors are combined,
the more secure the authentication

Assurance Levels

- Draft policy for assurance levels
- For SWITCH internal pilot levels: “Silver” and “Gold”
- Gold level only for small sub group of staff
 - RA administrators, grid project staff and some others

Use cases

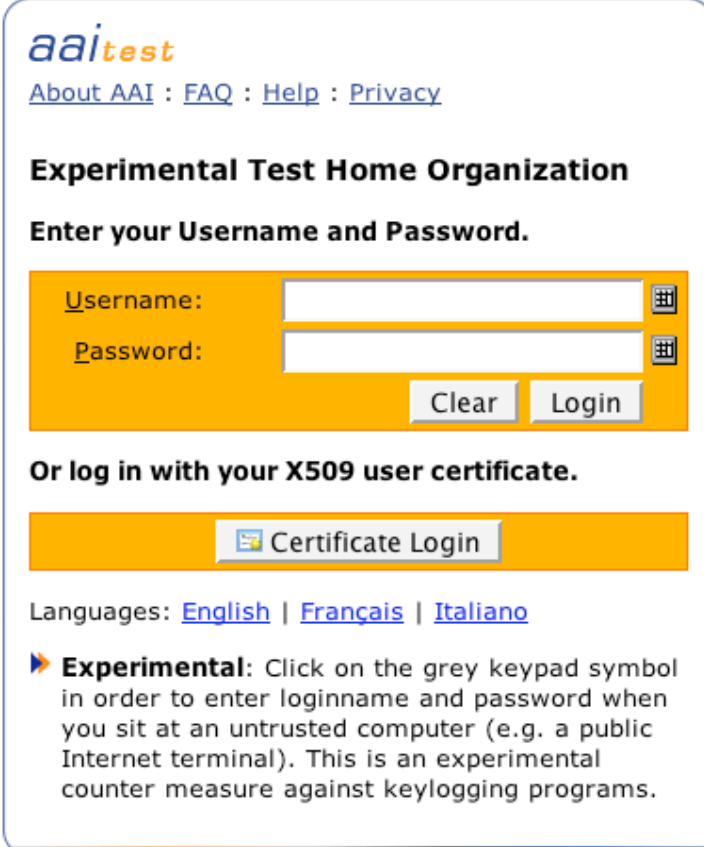
- Short-lived certificate service
- Foundation council documents
- Certificate RA services and documents
- CustomX (address management)
- Certain intranet areas

Setup

- CAS 3.0.5 dual login
- LDAP and x509 authentication
- X.509 certificates must match email address in LDAP repository
- Virtual keypad (against key-loggers)

Outlook

- Switch to production status
- SMS Token authentication
- Shibboleth 2.0 and AuthenticationContext



The screenshot shows the 'aai test' login interface. At the top, it has the 'aai test' logo and navigation links for 'About AAI', 'FAQ', 'Help', and 'Privacy'. Below this is the heading 'Experimental Test Home Organization' and the instruction 'Enter your Username and Password.'. There are two input fields: 'Username:' and 'Password:', each with a grey keypad icon on the right. Below the fields are 'Clear' and 'Login' buttons. Underneath, it says 'Or log in with your X509 user certificate.' and features a 'Certificate Login' button with a certificate icon. At the bottom, there are language links for 'English', 'Français', and 'Italiano'. A note with a blue arrow icon states: 'Experimental: Click on the grey keypad symbol in order to enter loginname and password when you sit at an untrusted computer (e.g. a public Internet terminal). This is an experimental counter measure against keylogging programs.'

Q & A

 <http://www.switch.ch/aai>

aai@switch.ch

Example for Assurance Level Policy

This could be a specification for levels of assurance.

	Level 1 (Bronze)	Level 2 (Silver)	Level 3 (Gold)
Registration	Remote, In-Person	Remote, In-Person	In-Person
Identity Proofing	Nothing	Valid (copy of) Government document	Valid Passport, ID
Credential delivery	Email, post mail, personally	Post mail, personally	In-Person
Authentication security	Login/Password or better	Login/Password or better	At least two-factor authentication
Financial liability	CHF 100.-	CHF 1'000.-	CHF 10'000.-

Shibboleth 1.3

- Assurance levels can be implemented with an additional attribute
- Two-factor authentication can be done with CAS 3.x

Shibboleth 2 and Assurance Levels

- SP will be able to require a certain assurance level/authN method
- SAML2 AuthenticationContext classes and declarations
- No final specification yet what will be supported by Shibboleth 2

Shibboleth 2 and Authentication

- Due to AuthenticationContext and Single-Sign Logout, the authentication system must be closer to Shibboleth
- An authentication system will be included in Shibboleth 2