UNIL | Université de Lausanne

AAI Operations Committee

Multi-factor authentication for Shibboleth

Thoughts, experiences and questions

| le savoir vivant |

Etienne Dysli, Alexandre Roy

24.5.2011

Yubikey: what's this?

- Event-based OTP device
- USB keyboard
- One button
- No battery
- Supports OATH-HOTP
- Open-source software
- Online OTP validation service

yubico

the key to the cloud

http://www.yubico.com/yubikey

Multi-factor Login Handler

- Extension for the Shibboleth Identity Provider developed by Yubico
- Generic multi-factor, not limited to Yubikeys
- JAAS module to check the second factor
- LDAP patch submitted to Yubico Java client

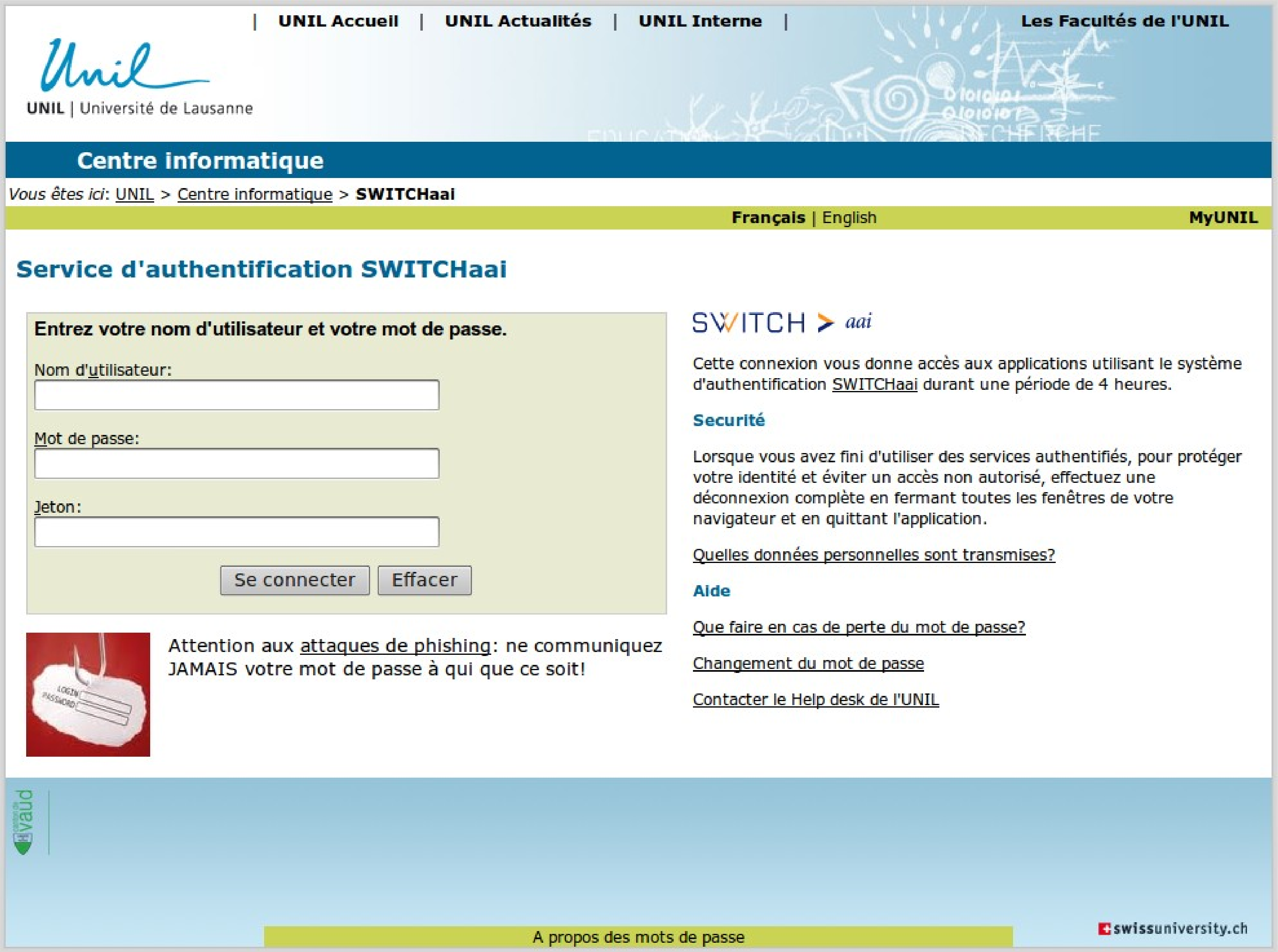
https://wiki.shibboleth.net/confluence/display/SHIB2/Multi+Factor+Login+Handler

https://github.com/Yubico/yubico-java-client/

Yubikey: Login Process (1)

- SP requests a particular authentication method:
  - urn:oasis:names:tc:SAML:2.0:ac:classes:Token
- IdP picks a LoginHandler configured for this method
  - Special login form
- IdP runs JAAS login modules for password and token

Yubikey: Login Process (2)



| UNIL Accueil | UNIL Actualités | UNIL Interne | Les Facultés de l'UNIL

UNIL | Université de Lausanne

Centre informatique

Vous êtes ici: UNIL > Centre informatique > **SWITCHaai**

Français | English **MyUNIL**

Service d'authentification SWITCHaai

Entrez votre nom d'utilisateur et votre mot de passe.

Nom d'utilisateur:

Mot de passe:

Jeton:

Se connecter | Effacer

Attention aux attaques de phishing: ne communiquez JAMAIS votre mot de passe à qui que ce soit!

SWITCH > aai

Cette connexion vous donne accès aux applications utilisant le système d'authentification SWITCHaai durant une période de 4 heures.

Securité

Lorsque vous avez fini d'utiliser des services authentifiés, pour protéger votre identité et éviter un accès non autorisé, effectuez une déconnexion complète en fermant toutes les fenêtres de votre navigateur et en quittant l'application.

Quelles données personnelles sont transmises?

Aide

Que faire en cas de perte du mot de passe?

Changement du mot de passe

Contacter le Help desk de l'UNIL

A propos des mots de passe

swissuniversity.ch

Yubikey: Questions

- Validation server: external (Yubico's) or internal?
  - rely on / maintain
  - new Yubikeys ready / load your seed
  - work with other websites / only yours
- Procedures? Registration, replacement, revocation
- Test with 10 users soon
  - Internal website of the Systems group

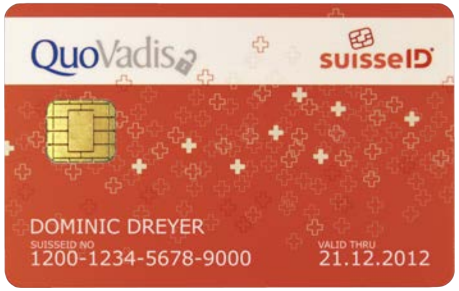
Using our CampusCard

- LEGIC RFID card sold by polyright
- Card ID in protected memory
- Needs:
  - USB reader with licensed LEGIC chip on every computer
  - Develop client software to import card ID into browser

⇨ too many ways to get it wrong

SuisseID: what's this?

- Smartcard PKI
  - Managed by CA, not you
  - Needs reader and client software
- SAML infrastructure
  - Fetch additional user attributes not present on certificate
  - Not Shibboleth
  - Poor documentation
  - No published metadata



http://develop.suisseid.ch/

SuisseID and Service Provider

- Authenticate on Shibboleth SP with a SuisseID
- Receive attributes from CA's IdP
- It works but...
  - Complex SP configuration
  - Foreign IdP, not yours nor SWITCHaai
- Huge thanks to Kaspar Brand (SWITCH) for helping me with configuration

SuisseID and Identity Provider

- Authenticate on Shibboleth IdP with a SuisseID
- X.509 Login Handler from SWITCH
- Classic SSL client certificate configuration
- It works but...
  - Certificate OR username/password, not both
  - Processes? certificate attributes?
  - No access to SuisseID additional attributes

https://wiki.shibboleth.net/confluence/display/SHIB2/X.509+Login+Handler

Further thoughts

- Our authentication system must be implemented for AAI login and SAP ABAP login.
- Support of devices without a USB port (smartphones, tablets, etc.)?
- SMS login: some users refuse to have a mobile phone.
- New AAA project (2012): collaboration, ideas?