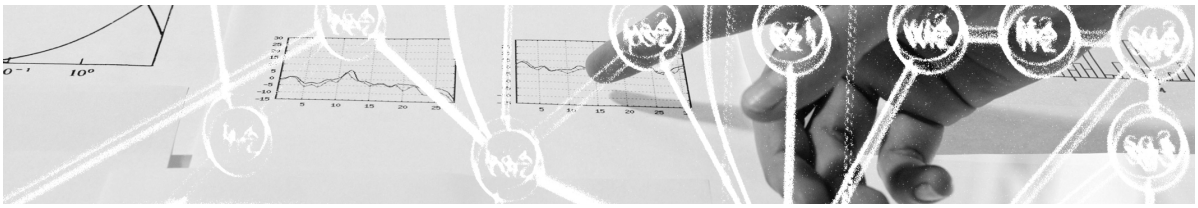
SWITCH
Serving Swiss Universities

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

Questionnaire

Identity Management Maturity Scan for SWITCHaai



Thomas Lenggenhager, SWITCH
Thomas Siegenthaler & Daniela Roesti, CSI Consulting AG

Version: V2.1
Created: 19. Aug. 2011
Last change: 13. Nov. 2011

SWITCH
Serving Swiss Universities

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

SWITCH
Serving Swiss Universities

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

Introduction

You are an operator of an Identity Provider (IdP)[1] in SWITCHaai. The identity management of your institution is an essential basis for its operation. The Service Providers (SP) which protect the access to their web applications trust the IdP and identity management of the particular Home Organization.

The maturity scan based on this questionnaire has a triple goal:

- Compare the maturity of your identity management to other Home Organizations
- Determine where you could improve your identity management
- Determine your maturity level as a mean to provide Service Providers (SP) an indication on the level of trust they can have towards your Home Organization.

In purpose to guarantee a professional IdP operating within SWITCHaai, SWITCH elaborated the document “Best Current Practices for operating a SWITCHaai Identity Provider”, which as well as other sources contributed to work out this questionnaire.

Scope

The scope of the identity management maturity scan for AAI is shown below in Figure 1. SWITCHaai is composed of central elements (components and processes), the IdP elements of each Home Organization and all SP elements of AAI Federation Members and Federation Partners. The maturity scan (shaded area) focuses on the IdP elements of the Home Organization and the identity management for all data sources it can access within the Home Organization.

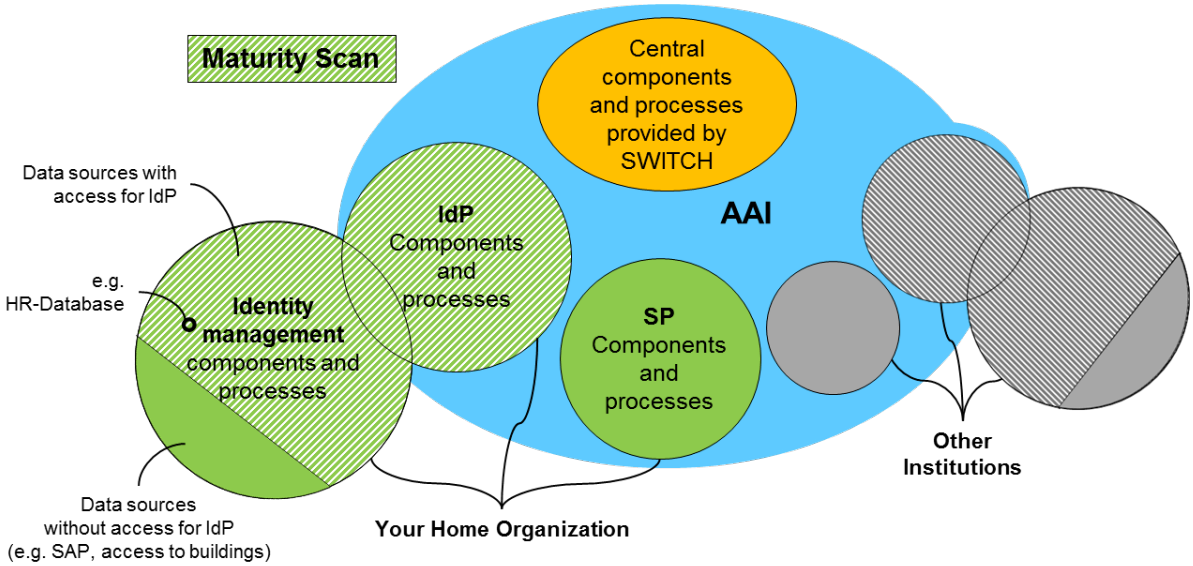


Figure 1: Scope of maturity scan

[1] The terminology of SWITCHaai understands the IdP (Identity Provider) as a software unit, which technically performs the authentication and makes a set of user attributes available to the SP (Service Provider) in the form of a SAML assertion.

SWITCH
Serving Swiss Universities

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

Questionnaire

Max. duration: 2.5 h

0 Preliminary questions

The purpose of the following preliminary questions is to facilitate the interviewing team's understanding of the organization and infrastructure of the interviewed representatives of the Home Organization. These answers are not evaluated in the maturity scan.

Max. duration: 15 min

1) Please explain your organization and IT-environment especially the organizational and technical elements that are involved into SWITCHaai.
2) Which are your most important applications that make use of SWITCHaai?
3) For which applications do you support other identity management solutions?
   What would the requirements be to integrate these applications into SWITCHaai?

1 Identity management and authentication

1.1 Identity management policy

1.1.1 Is an identity management policy defined (roles (IdM Service Manager and System administrator with their duties), and processes for the following topics: authorisation, authentication, provisioning, privacy, continuous improvement process)?
[Chapters 2.1.2 und 2.1.3 of BCP, SN]

1.1.2 Is the staffing (responsibilities and deputies) for the above-mentioned topics defined? [S001]

1.1.3 Is the reporting (including emergency reporting) and escalation to management defined (reports about e.g. availability, incidents, usage)? [S013, S058]

1.2 Data sources and unique identity

1.2.1 Does the Human Resources Department or student administration have knowledge of all person-related data sources (e.g. staff, student, further education, guests) and to what extent are these data sources integrated? [Chapter 2.1.1 of BCP]

1.2.2 Is the consistency of the identity data ensured?
(Are the consistency and perpetual aggregation (same keys on different sources) ensured, if user data is merged from different sources; is the user information stored in a single source (directory, database, etc.); is data accurate and complete; improvement possibilities) [S018, R019]

1.2.3 Is a swissEduPersonUniqueID never reassigned to another person? [R122]

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

1.3 Regulations and compliance

1.3.1 Are all valid regulations documented, do periodic supervisions on compliance take place? (Which federal, cantonal and organizational privacy and data protection regulations are relevant – are all of them applied; is the user informed of and required to consent to the release of personal information to a resource, is student/staff user information kept as long as the burden of proof for a specific delict requires it) [R008, R030, R033]

1.3.2 Do reviews and audits periodically take place?
(Internal reviews of processes and policies, intrusion test, technical audits, audits of processes and policies) [SN]

1.4 Identity lifecycle

1.4.1 Is a reliable identification for all identities guaranteed?
(Defined process, same quality for all identities; has every student/member of staff been identified with an AAI-enabled account by a photo from an official identity card or passport; is the initial credential distribution performed on a separate channel – for instance, sent by postal mail to the home postal address) [R002, R009]

1.4.2 Are changes applied according to the requirements?
(Defined process; is the user information updated within e.g. two weeks of being notified of the change; will a student/staff user account be disabled within e.g. 6 months after the person has left) [R004, R007]

1.4.3 Is a regular clean-up process implemented according to the requirements?
(To find expired or unused guest accounts, time limited accounts are triggered with an expiration date; do some persons have more than one account) [S005, R006]

1.5 Password policy

1.5.1 Is a policy including the password requirements published?
(Including the process of generating and resetting new passwords) [R020]

1.5.2 Is it required and enforced that the password has to have a minimum length? [R021, S022]

1.5.3 Are password requirements concerning complexity and lifecycle established?
(Mix of lower and upper case characters, digits and punctuation characters; common dictionary word prohibited; change at least once a year; reuse prohibited for e.g. at least 5 years; time delay after failed attempts) [S023-S027]

1.6 Strength of authentication

1.6.1 Are username/password transmitted by means of an encrypted channel? [R028]

1.6.2 Is a stronger authentication than username/password (e.g. X.509 user certificates, RSA Secure ID, Mobile ID) supported for all sensitive applications you have?
(E.g. those containing sensitive data like grades, financial or personal information)? [S029]

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

2 Identity service management

2.1 Availability

2.1.1 Does a service level description exist (e.g. max. 2h downtime during office hours, max. cumulative downtime e.g. 72 h p.a., existing communication concept)? [S036, S037]

2.1.2 Are scalability and availability technically assured?
(Standby system for manual failover; clustered setup and load balancer amongst IdP nodes; user sessions synchronized between clustered IdP nodes; no single point of failure) [S043-S047]

2.1.3 Are maintenance windows defined and maintained for standard system updates such as the installation of patches or new software releases?
(Documented; users are aware of; windows during off-peak hours; max. one per week; not exceeded in practice; maintenance only during the window) [S038-S042]

2.1.4 Is statistical data periodically reported concerning the quality of your Identity Management or IdP?
(Total number of authentications, number of distinct users, failed login attempts, number of accessed internal and external resources, released attributes, availability of IdP service; conclusions taken out of the report) [S059-S063]

2.2 Problem and emergency management

2.2.1 How and to which extent is help desk support provided to end users?
(Website, support contact point, opening hours, response time, password reset, issue tracking for reported problems, knowledge base for help desk personal, FAQ for users) [R048, S049-S055]

2.2.2 Is a disaster recovery procedure documented and tested twice a year?
(Do you also include a review of the Identity Provider Emergency Disabling Procedure (IdP Revocation) at least twice a year with staff in charge of operating the IdP? [S056, R057]

3 IdP host operation

3.1 Monitoring and alerting

3.1.1 Is monitoring of the network segment supported to which the IdP is connected?
(Same access path as user, test every 5 minutes, reachability/latency, port connectivity, respond to status request, test user login via IdP to SP) [R064, S065-S069]

3.1.2 Is monitoring and alerting of the host usage supported (time synchronization is running, monitor and alert if CPU >60%, memory >80%, disk usage >75%)? [R070, S071-S073]

3.1.3 Is monitoring of operating system logfiles done for errors or warnings (message, syslog, secure)? [R074, S075]

3.1.4 Is monitoring of webserver logfiles done for errors (access.log, error.log)? [R076]

3.1.5 Is monitoring of Java application container log files, IdP logfiles, data source log files done? [R077, S078]

3.1.6 Are automated alerting messages submitted to the IdP operator if errors occur? [R080]

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

3.2 Logging

3.2.1 Is it ensured and verified (how often) that only authorized staff members have access to the logfiles? [R083]

3.2.2 Is every access to personal data logged (e.g. actions concerning personal data sources)? [R084]

3.2.3 Is user identifying data anonymized (client IP address, username), when copies of logfiles leave the organization? [R088]

3.2.4 Are logfiles kept as long as the burden of proof for a specific delict (criminally liable) requires it and how long is this period? [R081, S082]

3.3 Backup and restore

3.3.1 Are a weekly full backup and a daily incremental backup performed? [S091, R092]

3.3.2 Are backups stored in an off-site and secure location? [S093]

3.3.3 Is the restore procedure tested at least twice a year and is it ensured that the procedure does not exceed 4 hours? [R016, S095]

3.4 Release management

3.4.1 Are critical updates of the IdP host operating system applied within 2 weeks and all the others within a month? [R110, S111]

3.4.2 Are critical updates of the IdP software applied within 2 weeks and all the others within a month? [R112, S113]

3.5 Documentation and training

3.5.1 Is documentation available for the IdP setup configuration (operating system, kernel version and installed package version, network address, host name, accessible ports, running services and their configuration location, cron jobs, log location and rotation schedule)? Is all the documentation regularly updated? [R014, R115]

3.5.2 Is documentation available for each attribute resolved by the IdP (data source, authoritative source, data steward); documentation with commands for starting and stopping the IdP together with test procedures to verify that the service started correctly; documentation with all IdP host and IdP software configuration changes? Is all the documentation regularly updated? [R014, S114, S116-S118]

3.5.3 Are further requirements and procedures for IdP host operation generally documented in operation manuals (monitoring, alerting, logging, security, backup and restore, release management, IdP configuration)? [x]

3.5.4 Is a procedure defined to educate the IdP administrators and is the staff trained? [S119]

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

4 IdP host security & configuration

4.1 Security

4.1.1 Does a security policy or security concept document exist which includes the IdP host? [x]

4.1.2 Are strong authentication methods (two-factor) used for management access on the IdP host (e.g. SSH with public key authentication, one time password, token or similar)? [R096]

4.1.3 Is management access to the IdP host restricted to specific network ranges and remote root logins prohibited? [R097, R098]

4.1.4 Is the root password changed regularly? [S099]

4.1.5 Are management accounts and permissions reviewed regularly (separations of duties: users have only the rights they need)? [S101]

4.1.6 Is the IdP host protected by firewall? [R102]

4.1.7 Is it ensured that front and backend channel HTTPS ports (usually 443 and 8443) are the only ports accessible from external networks? [S103]

4.1.8 Are the following requirements with respect to X.509 private keys fulfilled (private keys are only readable by the IdP process, creation of a new key pair after at most 3 years)? [R106, R107]

4.1.9 Does a process exist for revoking or removing compromised keys with respect to X.509 certificates? [R108]

4.2 IdP change management

4.2.1 Is a test system (staging system) operated which is equivalent to the productive system? [S141]

4.2.2 Is a version control system used to track the changes to the IdP configuration files? [S140]

4.3 IdP metadata and certificates

4.3.1 Is the required technical level of trust for metadata (SAML) ensured?
(SWITCHaai federation metadata is used as published by SWITCH; metadata is updated on an hourly/daily basis; SWITCHaai trust root is installed after the certificate fingerprint has been verified with SWITCH; signature of the metadata is verified against the SWITCHaai Metadata signing [MDS] certificate after each download; MDS-certificate and its chain is checked against the CRL) [R123, S124, R125-R127, S128]

4.4 IdP attribute resolving

4.4.1 Is the connection to the data source (LDAP, RDBMS) secured (e.g. TLS/SSL)? [R132]

4.4.2 Is it ensured that the IdP is not allowed to add, update or delete information in a data source unless the IdP is authoritative for that information? [R134]

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

4.5 Resource Registry

4.5.1 Is the IdP information in the SWITCHaai Resource Registry up to date (service locations, certificates, contacts) and verified at least twice a year? [R143, R144]

4.5.2 Is the attribute release and filter policy information within the SWITCHaai Resource Registry maintained and also validated at least twice a year?
(Does the default or specific attribute filter policy deny the release of information; are only those attributes released that are explicitly requested by the service provider) [R032, R135, S138]

5 Infrastructure

5.1 Server room environment & network

5.1.1 Is physical access control to the IdP host regulated, enforced and audited?
(Only entitled staff members have access; log entries for each access) [R145, S146]

5.1.2 Is physical security and electrical power for the IdP host ensured?
(Server room and server rack is used; fire-safe walls, windows and doors, IdP host hardware 1m above floor; room temperature and humidity are measured; uninterruptible power is applied) [R147, S148-S150, R151]

5.1.3 Is network connectivity of the IdP host guaranteed?
(IdP host(s) are connected to more than one LAN switch; IdP LAN has more than one connection to WAN) [S152]

5.2 Server hardware & software

5.2.1 Is spare hardware for the IdP host available or vendor support ensured?
(Identically configured IdP as stand-by or support contract with maximum supplier reaction time of one working day) [R154, S155]

5.2.2 Are the minimum requirements for IdP operating software fulfilled?
(Operating system for which security patches are provided through the vendor; distributor with long term support of at least 5 years; use of NTP) [S156, R157]

[XXXX] References to the "Best current practices" (BCP)

The above-mentioned numbers in brackets refer to the requirements and suggestions of the "Best current practices for operating a SWITCHaai Identity Provider", see: http://www.switch.ch/aai/bcp

[R000] Future revisions of the AAI Policy are expected to require compliance with these requirements for IdPs.

[S000] Suggestions reflect best common practices. Depending on the specific local environment, their implementation can be considered optional.

[x]: Intended to be integrated as a requirement in the next version of best current practices

[SN]: Adopted from the SURFnet Maturity Scan (2009)