Trust & Identity Meeting 2022

TRID Team
Zurich, May 18th 2022
Agenda

13:15 - 13:30  Introduction
13:30 - 14:00  SWITCH edu-ID
14:15 - 14:35  SWITCHpki & eduroam
14:35 - 14:45  Questions & Inspirations

🍎 Break 🍎

15:10 - 15:25  Innovation Project Blockchain
15:25 - 16:10  Self-Sovereign Identity / e-ID
16:10 - 16:30  Questions & Inspirations
16:30 - 16:45  Sum-Up & Closing

🍎 End 🍎
Main Goal: Secure & Stable Operations

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Uptime</th>
<th>May 17</th>
<th>May 16</th>
<th>May 15</th>
<th>May 14</th>
<th>May 13</th>
<th>May 12</th>
<th>May 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>APIs</td>
<td>98.98%</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Administration Portal</td>
<td>99.07%</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Attribute Aggregator</td>
<td>100%</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>My edu-ID</td>
<td>99.07%</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Resource Registry</td>
<td>100%</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>WAYF (Discovery Service)</td>
<td>100%</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>edu-ID Login</td>
<td>98.95%</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

Status & Registration: [https://status.eduid.ch/](https://status.eduid.ch/)
Incident: Rough overview

- **Duration:** approx. 9:00am – 10:20am, 16. May 2022
- **What happened? Analysis:** (in a nutshell*)
  - **Level:** Emergency Level
  - **Impact:** Partial outage of all IdP requests (AAI & SWITCH edu-ID)
  - **Component:** Global load balancer lost network connection
  - **Reason:** Network interface failure while hypervisor migration (from infrastructure provider)
- **Conclusions:** (not conclusive)
  - HA worked, but faulty load balancer did not disconnect (action in planning)
  - Improved coordination of key component maintenance
  - Decrease interdependency & increase HA (already on the roadmap)
  - Incident Management worked

*: We are conducting an in-depth analysis and final report this week
General Focus Topics

- **Responsibility** of providing secure & stable services
- **Security** as the key focus of all our services
- **Trust** as the main building block within our federation
- **Identity** as an integral part of the digital landscape
- **Integration** of features and needs on behalf of our community
- **Innovation** serving our community and the Swiss society
SWITCH edu-ID

700'000 registered users

SWITCHpki & eduroam

Blockchain

Self Sovereign Identity
Overview of Topics

- **Sprints**: Selection of Completed Topics
- **Community**: Overview of SWITCH edu-ID
- **Development**: Upcoming SWITCH edu-ID Tasks
- **Security**: Security Measures
- **Protocols**: OIDC & SAML
- **Exchange & Questions**: Certain Topics
Sprints: Selection of Completed Topics

- **Enhanced Availability**: Increased redundancy of critical components (IdP, LDAP, Postgres DB, API, My edu-ID) and automatic failover

- **Security**: Penetration Test 2021 for Web-GUI and APIs with external partner

- **Protocols**: Introduction of OpenID Connect

- **Upgrade**: IdP platform "containerized" as preparation to IdPv4 upgrade

- **Admin portal**: Read-only role for support staff
Community: Overview of SWITCH edu-ID

- **SWITCH edu-ID Adoption:**
  - **Recent:** USI, HEP-BEJUNE, FHNW, HES-SO, FFHS, USB (University Hospital Basel)
  - **Near future:** FH-HWZ, UniNE, USZ (University Hospital Zurich), EHSM, UZH
  - **Announced:** HSLU, ETHZ, HUG (University Hospital Geneva)

- **SLSP / Swisscovery**
  - **SLSkey:** ZB Zürich, ZHB Luzern, UB Basel

- **Transition to university:** Federation Bridge to edulog

- **Government:** CH-Login (eiam.admin.ch) with SWITCH edu-ID authentication
Dev: Upcoming SWITCH edu-ID Tasks 1/2

- Evaluation of mobile SWITCH edu-ID App
  - Passwordless authentication
  - Manage personal part of SWITCH edu-ID identity
  - Identity Check

- Operations: Continuous improvement of our HA service

- Interoperability with MS: architecture blueprint

- OIDC: Improve the support and management of SAML & OIDC clients

- Security Management (see next topic)
Dev: Upcoming SWITCH edu-ID Tasks 2/2

- **Linking**: New email-based method to integrate edu-ID at organizations (Jul’22)
Security: Part of our DNA

- **High Existing Standards:**
  - Security by design, High Isolation, Least Privilege, Penetration Tests, High Security Standards, Monitoring, Bruteforce Prevention etc…

- **Ongoing & Upcoming Topics Evaluated**
  - Measures to detect compromised accounts, Guide to help in the event of a compromise
  - Enhance cooperation with SWITCH CERT (e.g. Community SOC)
  - Implement further preventive measures (geo blocking, risk based measures, user detection)
Protocols: OIDC & SAML

- **SWITCH edu-ID supports OIDC**: ~100 clients have been registered
- **Aim**: harmonize management and functionality of SAML and OIDC clients
- **Differences**: not all attributes and no classic model supported in OIDC
- **Brand new feature**: OIDC client registration in Resource Registry

Resource Menu for 'New Resource'

To create a new Resource Description, first complete the section 'Basic Resource Information' and then the remaining sections.

Would you like to register a ○ **SAML resource** or an ○ **OpenID Connect resource**?
Connections: OIDC & SAML

Resource Menu for 'New Resource'

To create a new Resource Description, first complete the section 'Basic Resource Information' and then the remaining sections.

Would you like to register a **SAML resource** or an **OpenID Connect resource**?

- More than 100 clients have been registered since edu-ID has supported OIDC
- **New:** AAI Resource Registry allows registering and managing OIDC resources
  - Consistent management of SAML and OIDC clients
  - Same mechanisms for attribute release is used like for SAML
  - Differences: Not all attributes and no classic model supported in OIDC
  - Scopes not used for OIDC. Release policy decides what is released to client
 Worst you like to register a ☐ SAML resource or an ☐ OpenID Connect resource?

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Basic Resource Information</td>
<td>Incomplete</td>
</tr>
<tr>
<td>2.</td>
<td>Descriptive Information</td>
<td>Incomplete</td>
</tr>
<tr>
<td>3.</td>
<td>Contacts</td>
<td>Incomplete</td>
</tr>
<tr>
<td>4.</td>
<td>Service Locations</td>
<td>Incomplete</td>
</tr>
<tr>
<td>5.</td>
<td>Certificates and Credentials</td>
<td>Incomplete</td>
</tr>
<tr>
<td>6.</td>
<td>Requested Attributes and Claims</td>
<td>Incomplete</td>
</tr>
<tr>
<td>7.</td>
<td>Intended Audience and Interfederation</td>
<td>Incomplete</td>
</tr>
</tbody>
</table>
OIDC Registration

- OIDC clients/relying parties are in separate federations
  - But formally the belong to SWITCHaai federation
- Process to register OIDC clients is same as for SAML services
  - Approval by RRA administrators of same organisation or SWITCH
- Registrations/modifications don’t become active immediately
  - Clients in edu-ID OIDC *Test Federation* become active automatically (enabled from next week)
  - Clients in edu-ID OIDC *Prod Federation* become active automatically (enabled at end of June)
Questions & Inspirations
eduroam

• Rollover of eduroam CAT Profiles Root CA for SWITCHpki customers
  – Communications and preparations have been done, we’re in the transition phase now

• Managed SP pilot by GEANT
  – No need for your own Radius anymore, if you want to provide an eduroam Hotspot for Higher Education and Research users

• eduroam (IdP) Hosting at SWITCH
  – We operate the Radius for you and connect to your Directory via LDAPS
SWITCHpki - past

Jan 2019: Digicert acquired QuoVadis from WISEkey

Aug 2020: First vague announcement of replacement of the technical platform

Jun 2021: First SWITCHpki pilot customers on CertCentral

Aug 2021: General availability of CertCentral for SWITCHpki customers
SWITCHpki - present

• Server certificates on new platform only since End of April

• User (S/MIME) certificates can currently be issued on both platforms (prefer the new one, if possible)
Advantages of the new platform (Digicert CertCentral)

- **Automation**
  - Modern look & feel and UX
  - All approval and audit requirements integrated into the system
    - No need for separate document archive at Uni or SWITCH for new certs
    - Approval is done inside your Organisation, no need to contact SWITCH
  - Self-service and paperless on- and off-boarding of new users (also for administrators / RA admins)
- Self-service Organization and Domain Vetting
- Direct support by Digicert for all technical / process questions
- Support by SWITCH for pricing and billing
CertCentral UX

DigiCert CertCentral
Screenshots
Questions & Inspirations
Blockchain @ SWITCH

SWITCHverify

Dragonfly & Mantis

SSI Sandbox

Productive SWITCH Service

Productive Distributed Ledger

© 2022 SWITCH | 28
Dragonfly Blockchain

- Fast, Scalable and Secure
- Open to anyone (Public Blockchain)
- EVM Compatible (Ethereum Virtual Machine)
- Dragonfly Mainnet / Mantis Testnet
- Layer-2 Blockchain
Mantis Testnet

- Dashboard
- Block Explorer
- Faucet
- Validator Nodes
- RPC & Chains
- Link to Mainnet
- Link to Github
Dragonfly Mainnet

Dashboard
- Blockexplorer
- Validator Nodes
- RPC Endpoints & Chain
- MANTIS Testnet

Blocks
- Chain ID: 78281
- Symbol: DFLY
- Time: 5 seconds
- Transactions: 32502

Latest Blocks

Latest Transactions

This Blockexplorer is a tool for analyzing and inspecting EVM based blockchains.
SSI Sandbox (Self-Sovereign Identity)

- Hyperledger Indy
  - Tools, Libs, Reusable Components
  - Decentralized, digital Identities rooted on blockchain (DIDs)
  - Permissioned / Governed Blockchain

- Sandbox to experiment with SSI technology together with external partners.

- “One option” we work on is Hyperledger Indy

- Experiments with private distributed ledger technology
Further Links (Blockchain)

- SWITCHverify Service: https://verify.switch.ch/
- Dragonfly GitHub: https://github.com/hexapods
- Dragonfly Mainnet: https://dragonfly.switch.ch/
- Mantis Testnet: https://mantis.switch.ch/
- Hyperledger Indy: https://www.hyperledger.org/use/hyperledger-indy
Questions & Inspirations
Self Sovereign Identity
Self Sovereign Identity (SSI) & E-ID

• A bit of history and recent developments
• How does SSI fit into the picture?
• SSI & E-ID: our high-level goals and achievements:
  – Influencing the political process
  – Communication
  – Creating Facts in partnership
  – Stakeholder management
• Digital identity strategy of SWITCH
E-ID/SSI

• E-ID law rejected by popular vote March 2021
  – our interpretation: It’s a no to “this E-ID”, but “a better E-ID” might be ok

• Position of SWITCH
  – wants to offer access to a future E-ID by means of the edu-ID
  – wants to foster its values in a future E-ID: security/data protection, empowerment of users, innovation capability
  – willing to offer its identity-knowhow to the Swiss society
  – prepared to offer its services, if option arises

• SSI (Self-sovereign identities)
  – Currently being discussed as guiding principle for E-ID approach #2
  – SWITCH is assessing those principles also in the context of the edu-ID. See: https://www.switch.ch/stories/Bring-your-own-identity/
E-ID: Recent developments

- Sept ‘21: publication of the “Zielbild E-ID” / "Document de travail concernant le projet d’identité électronique (e-ID)"

- Oct ‘21: public consultation

- Dec ‘21: directional decision by federal council for SSI and “ambition level 3”
  https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-86465.html
  – Ambition levels: 1 = E-ID only, 2 = all e-Gov, 3 = public/private ecosystem

- Summer ‘22: New E-ID law expected for public consultation
Development of architecture

Account-based approach

Entity-based approach

Shift of Control

Privacy and security

User flexibility and control

Vendor-centric

IDP-centric

Entity-centric

© 2022 SWITCH | 40
ISSI eco-system

VC Verifiable Credentials

DID Decentralized Identifiers

Holder

Proof of Credentials

Issuer

Verifier

decentralized trust network

governance

technical scheme

framework

remuneration models

authority

rules of conduct

conditions of participation

data protection & privacy

© 2022 SWITCH | 41
The self-sovereign (ambition level 3) future

"Service Public", trust infrastructure regulated by the Confederation
Interaction of different sector ecosystems (examples)
SWITCH’s high-level goals with E-ID

• SWITCH is committed to support the emergence of a useful, secure and easy to use e-ID for the benefit of the Swiss society at large.

• SWITCH is committed to make the e-ID available to its community as part of the SWITCH edu-ID.

• SWITCH is committed to support international collaboration and mobility with the SWITCH edu-ID – regardless of the political weather conditions
Board-Retreat Apr’21: Action Clusters

- Politics
- Communication
- Creating facts in partnership
- Stakeholder management: cultivating exchange platforms
Achievements in since spring 2022 (1/2)

• Memberships
  – DIDAS https://www.didas.swiss/ (SSI expert group, no commercial focus): active member; starting May 2022 represented in the board
  – Digital Switzerland https://digitalswitzerland.com/: named experts, “shaper” in SSI Whitepaper & editor of “governance” chapter
  – IDunion https://idunion.org/ (German SSI implementation project): “Contributor” in German SSI implementation project, focus on diploma use cases
  – GÉANT: task lead “Distributed-Identities” in preparation for 2023-2024

• Politics/E-ID
  – Contribution to informal public consultation autumn 2021
  – Bi-weekly calls with BIT/OFIT to discuss progress in E-ID project
  – Ready to participate in upcoming review of new E-ID law in summer 2022
Achievements in since spring 2022 (2/2)

• Informal partnerships
  – HIN: education certificates in health sector
  – SBB/CFF: certificate of residency, education certificates

• Creating facts:
  – Support for ESI (European Student Identifier) in edu-ID (initiated by UZH)
  – Development started for edu-ID mobile app
  – Blockchain know-how building [https://dragonfly.switch.ch/dashboard](https://dragonfly.switch.ch/dashboard)
  – Master students at SWITCH in topics SSI (EPFL) and blockchain (ETHZ)
The journey across sector borders
User facing: SSI-Wallet

Personen ID / UID

Driver-license

FHNW Bachelor Diploma

ZHAW Master Diploma
Questions & Inspirations