Swiss EduChain

Intermediate Master Thesis Presentation

Simon Müller, Vasileios Koukoutsas

02/12/2019

Agenda

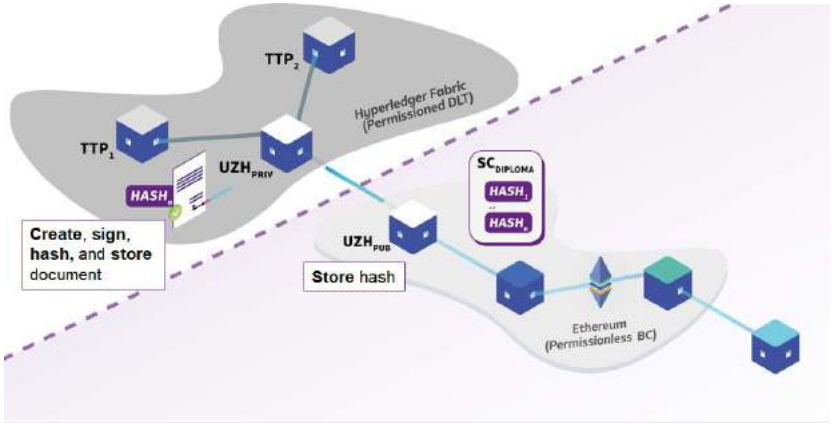
- Introduction (SM)
- Related Projects (SM)
- Requirements (VK)
- Swiss EduChain Architecture (SM/VK)
- Identity Management (VK)
- Diploma Verification (SM)
- Demo (VK/SM)

Motivation

- Fraud in academic diplomas on the rise
- Current issuance and verification process is manual
- Academia and private companies trying to solve the problem
- Public Blockchains for public verifiability:
  - Tamper-proof
  - Transparent
  - Decentralized

Swiss EduChain

- Digitize diploma issuance & verification
- Integrate with existing legacy systems
- Create a data-agnostic structure
- Extensibility of Swiss EduChain for credential verification (CV, work certificate etc.)



Source: EduChain – Proposal of Requirements and Architecture, Rodrigues et al. - 2019

Swiss EduChain Theses

Identity Management for a Blockchain-based Certificate Issuance	Design and Implementation of a Data-Agnostic Structure for Blockchain Proof-of-Existence
Vasileios Koukoutsas	Simon Müller

“Identity” ***“Verification”***

Related Diploma Verification Projects

	Verification via	**Requirements**	**Data types**	**Diploma Extensibility**
Blockcerts	Any blockchain	Blockcerts App	JSON	No
EduCTX	Ethereum	MetaMask	PDF	No
Block.co	Bitcoin	-	PDF	No
Swiss EduChain	Ethereum	Switch edu-ID Account	JSON	Yes

Requirements

1.3.1 Functional Requirements

Requirement	Description
RQ1	Only authorized UZH departments are allowed to issue diplomas
RQ2	Diploma data should be confidential to its recipients
RQ3	Process of issuing and verifying diplomas should abstract technical complexities
RQ4	Multiple diplomas should be processable in batch
RQ5	Verification capabilities should be accessible to any company
RQ6	Diplomas should be verified autonomously
RQ7	Graduates should receive their diplomas in a digital format

Requirement	Description
RQ8	Recipients should have a unique identification.
RQ9	Recipients should be the only ones that have the right to disclose issued credentials.
RQ10	Recipients account should persist over time and be independent of any association with an Issuing Organization.
RQ11	Registration needs identity verification.
RQ12	Issuers should be able to revoke diplomas.
RQ13	The governance model of the Swiss Educhain system must be defined.
RQ14	System allows for recipients to run their own nodes in the network ensuring data ownership is also physically restricted.
RQ15	Data owner is responsible for data backup. System should provide an option for a participants data to be exported.
RQ16	Issuing Organizations can hash the credentials individually or in batch.
RQ17	Multisig transactions should be possible.
RQ18	System processes data in a text-based format.
RQ19	Allow for identity details change (e.g. a recipient or an organization changes name).
RQ20	The process to onboard Issuing Organisations to the Swiss Educhain platform needs to be examined and defined.
RQ21	User accounts need to be associated with one or more Issuing Organizations.
RQ22	Issuing should create an unchangeable audit trail.

Table 1.2: Swiss EduChain Functional Requirements

1.3.2 Non-Functional Requirements

The Swiss Educhain system is intended to onboard a plethora of organizations such as Universities, Government departments and Employers of different sizes, in diverse jurisdictions and of varying technology maturity level. This creates the need for a system that fulfills these non-functional requirements:

Requirement	Description
RQ23	Easy to use from a user perspective, with a simple UX/UI and straightforward functionality.
RQ24	Easy to install, configure, deploy, operate, monitor and maintain from an System Administrator's perspective.
RQ25	Uses technologies that are freely available, popular, well-established and mature (important for security).
RQ26	Has as few as possible technology requirements and dependencies both in terms of hardware and software.
RQ27	Has as few as possible technology requirements and dependencies both in terms of hardware and software.
RQ28	Can be easily integrated with existing IT infrastructure and is cross-platform compatible.
RQ29	Is not dependent on state-of-the-art technologies such as Containers, Cloud etc.
RQ30	Can be extended to deploy nodes of the network to Mobile devices.
RQ31	Can be modularly enhanced by existing functionality.
RQ32	Data that are disclosed peer-to-peer should not be broadcasted.
RQ33	Ensures data integrity.
RQ34	All transactions in the system should be signed and the identity of any action initiator should be verifiable.
RQ35	Where possible quantum-resistant options for encryption should be preferred.
RQ36	High level Access Control must be defined for the different kind of identities participating in the system.
RQ37	System should support multiple issuing organizations.
RQ38	Verifier must be able to verify the diploma even when the private environment is not available.

Table 1.3: Swiss EduChain Non-Functional Requirements

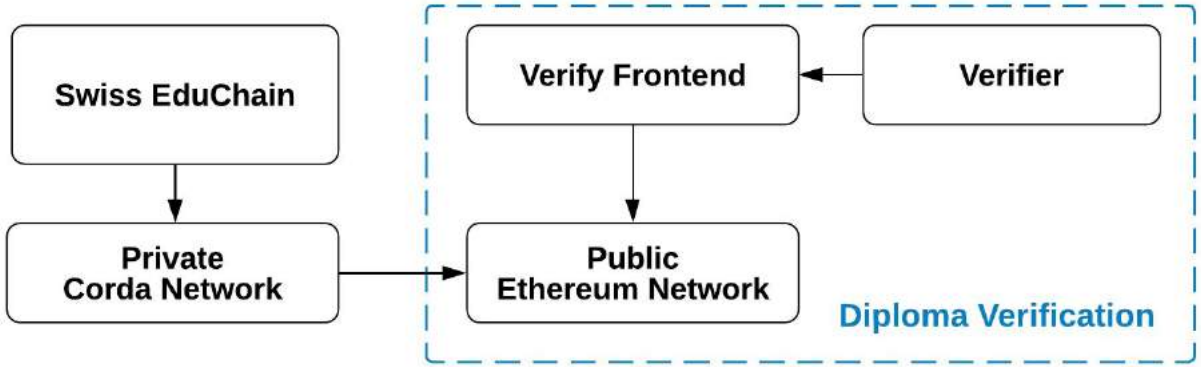
Identity Requirements

RQ2	Diploma data should be confidential to its recipients.
RQ10	Recipients account should persist over time and be independent of any association with an Issuing Organization.
RQ19	Allow for identity details change (e.g. a recipient or an organization changes name).
RQ21	User accounts need to be associated with one or more Issuing Organizations.

Verification Requirements

RQ5	Verification capabilities should be accessible to any company.
RQ12	Issuers should be able to revoke diplomas.
RQ22	Issuing should create an unchangeable audit trail.
RQ38	Verifier must be able to verify the diploma even when the private environment is not available.

Architecture so far



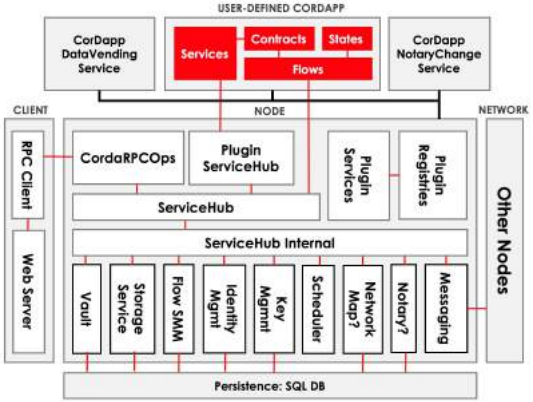
Why Corda?

- Data Disclosure on a “need-to-know” basis
- Non-verifying Notaries
  (no user data is disclosed to the Notary)
- Multiple consensus mechanisms for different actions under the same CordApp
- Open source and good documentation
- Written in Kotlin (compiles to Java bytecode)

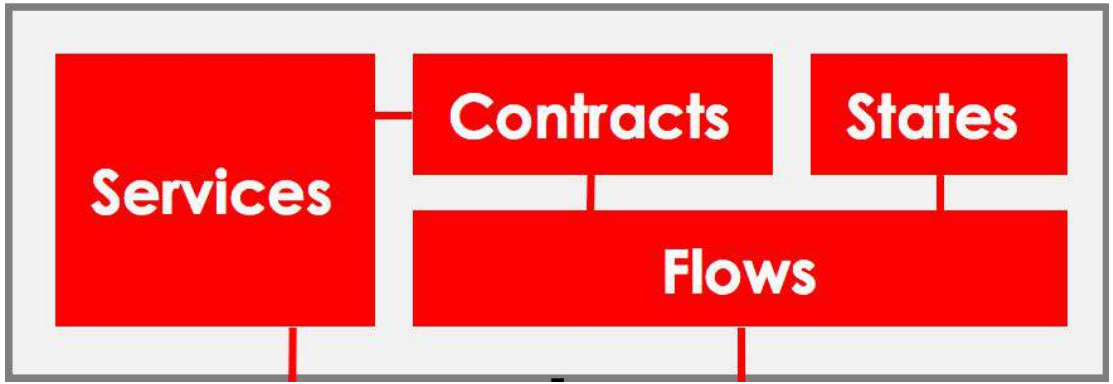
Source: https://www.coinwire.com/wp-content/uploads/r3com.png

How does Corda work?

Corda Platform



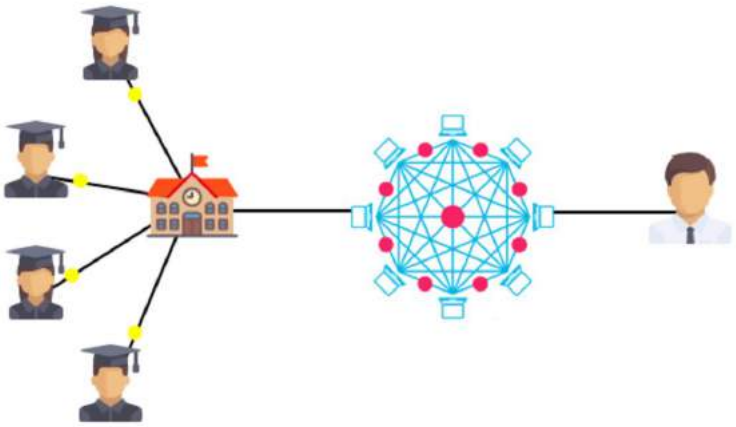
CorDapp



Source: R3 Corda Master Documentation - https://docs.corda.net/key-concepts-node.html

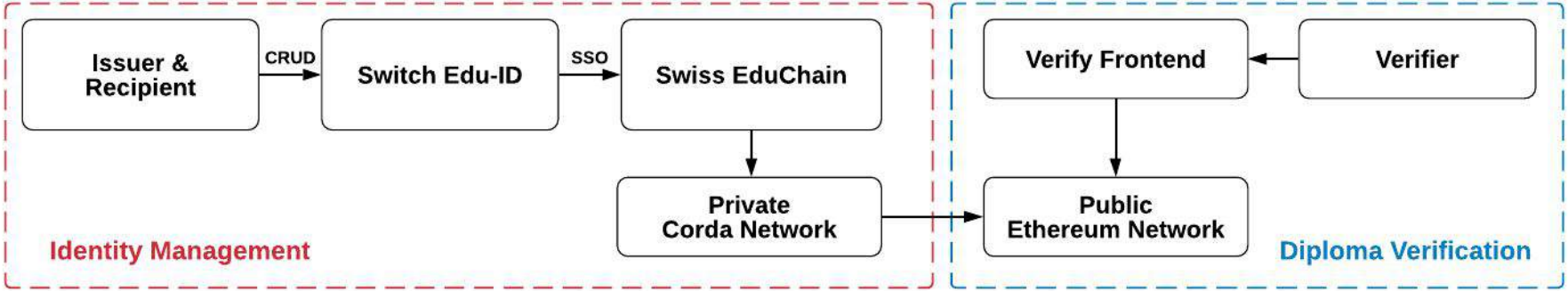
Why Ethereum?

- Widely used public blockchain
- Smart contract capabilities
- Adds transparency to the verification process
- Allows for anonymous verification



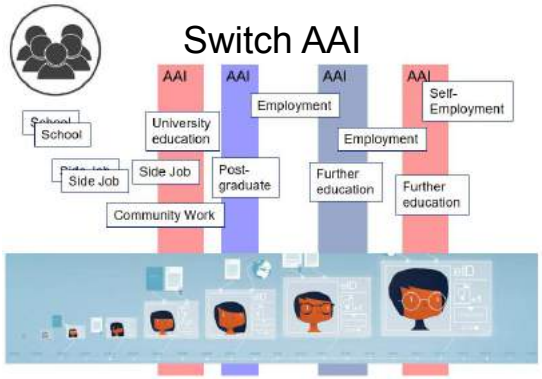
Source: http://www.certify.pk/

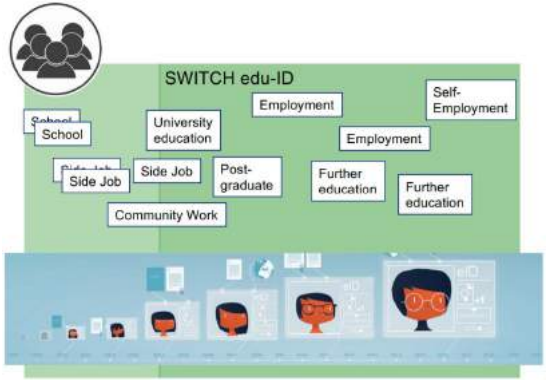
Identity Management



Switch edu-ID

- The evolution of SwitchAAI
- Digital identity for persistent use
- User-centric identity management
- Organization ↔ User Affiliation
- Single-Sign-On Integration





Source: https://www.switch.ch/edu-id/events/trid-wg-2019/

Why adopt edu-ID for Swiss EduChain?

- Already onboarded Users/Organizations
  (150000 users as of Nov. 1st 2019)
- Identity Integration/Standardization
- Account Lifecycle Management
- Affiliation Verification
- Access Control
  - Identification
  - Authentication (Multi-Factor)
  - Authorization (Attribute based)

Source: https://www.switch.ch/edu-id/events/trid-wg-2019/

Swiss EduChain as a Switch Service Provider (SP)

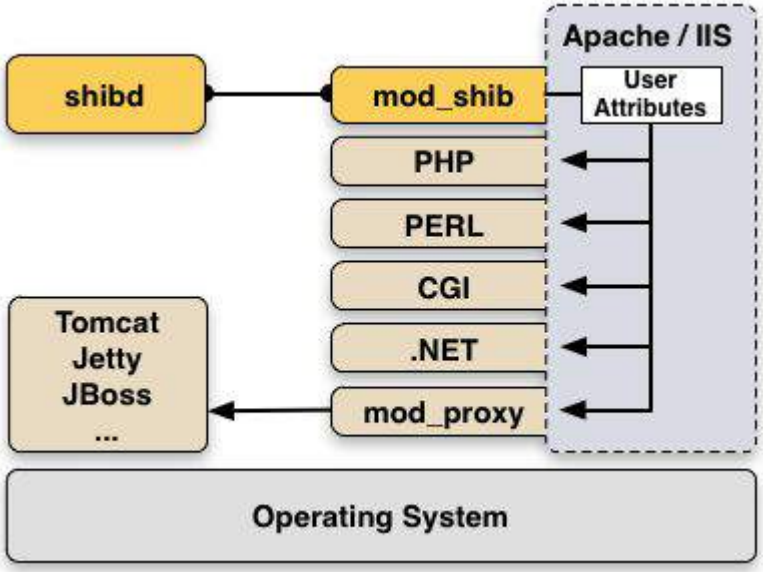
- Switch AAI Resource Registry
- Register as an SP under a specific Organization or under edu-ID (Switch)
- Web - SSO using Shibboleth (SAML)
- Currently deployed on the Testnet

Source: https://rr.aai.switch.ch/

Integration with Shibboleth

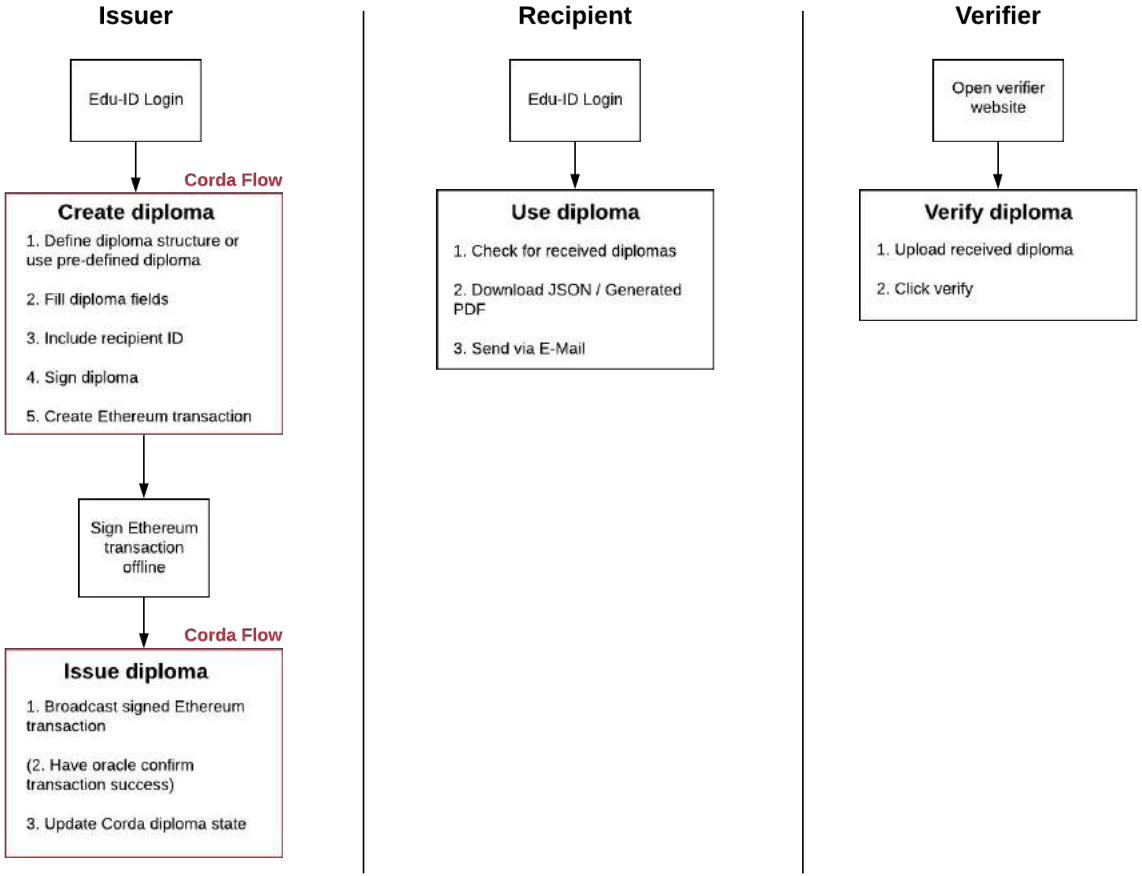
Software Requirements:

- WebServer
  (Apache HTTPD)
- Shibboleth Identity Provider
- Application Server
  (Spring Boot - Embedded Tomcat)



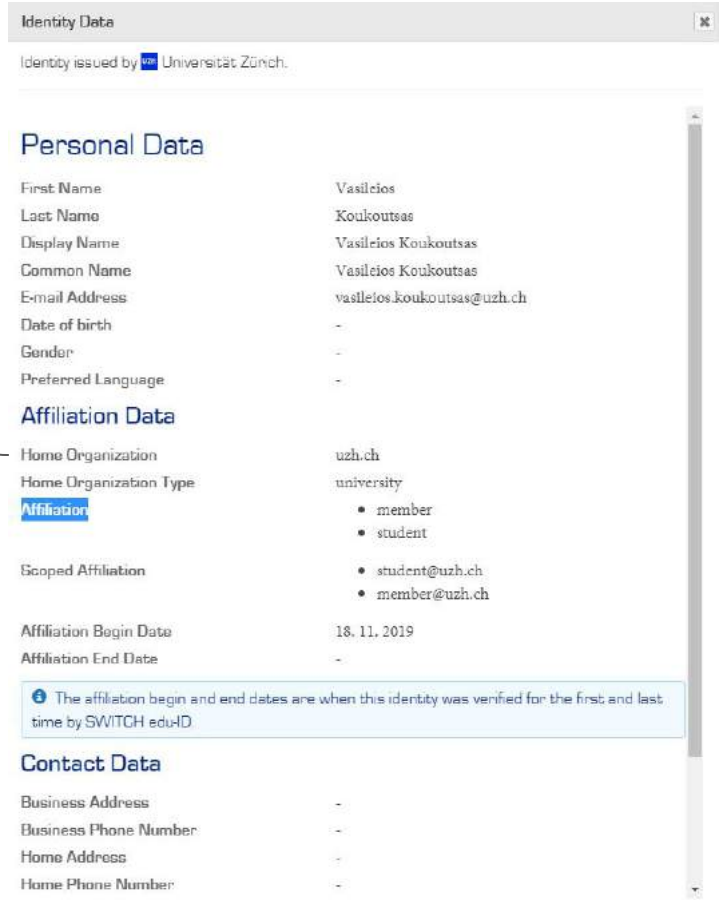
Source: https://www.switch.ch/aai/guides/sp/

Diploma verification



Demo

Organization Affiliation Attribute



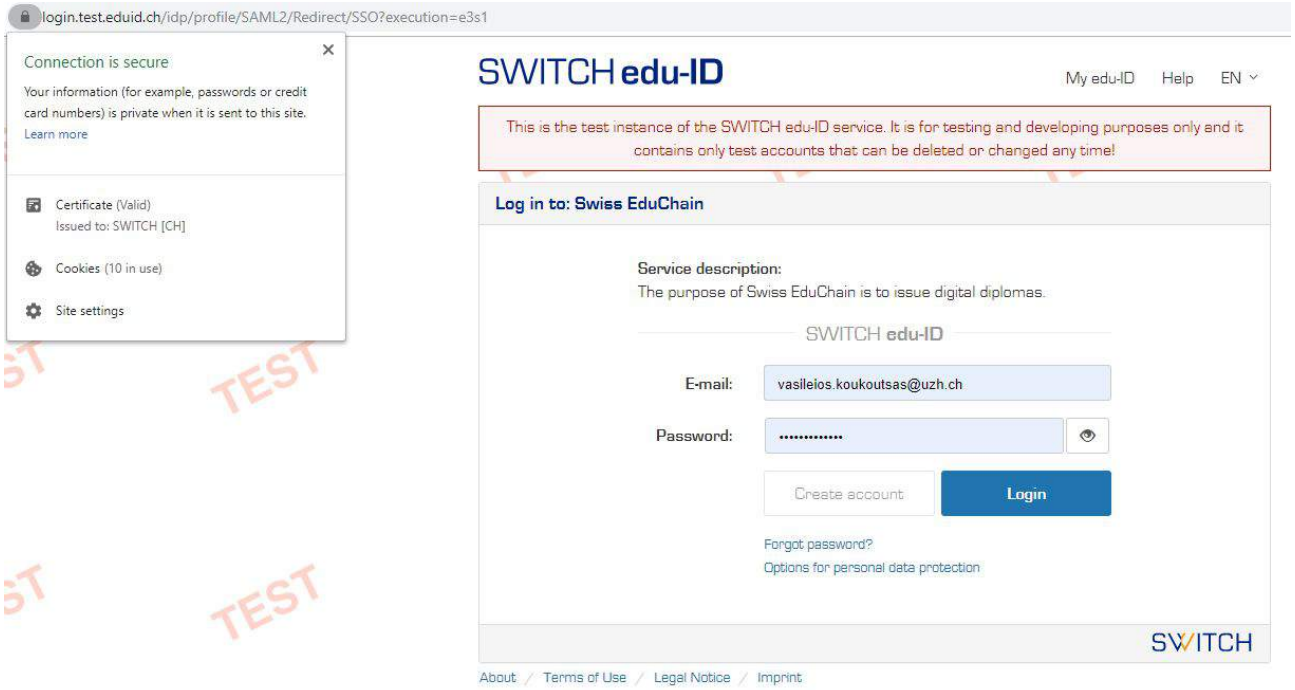
Swiss EduChain Relevant Values

Diploma Issuer	Diploma Receiver
faculty	student
staff	alum

DISCUSSION

Backup Slides

Redirect to edu-ID login page



SSO Session Attributes

Miscellaneous

Session Expiration (barring inactivity): 430 minute(s)
Client Address: 213.55.240.46
SSO Protocol: urn:oasis:names:tc:SAML:2.0:protocol
Identity Provider: https://test.eduid.ch/idp/shibboleth
Authentication Time: 2019-12-01T15:42:48.379Z
Authentication Context Class: urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Authentication Context Decl: (none)

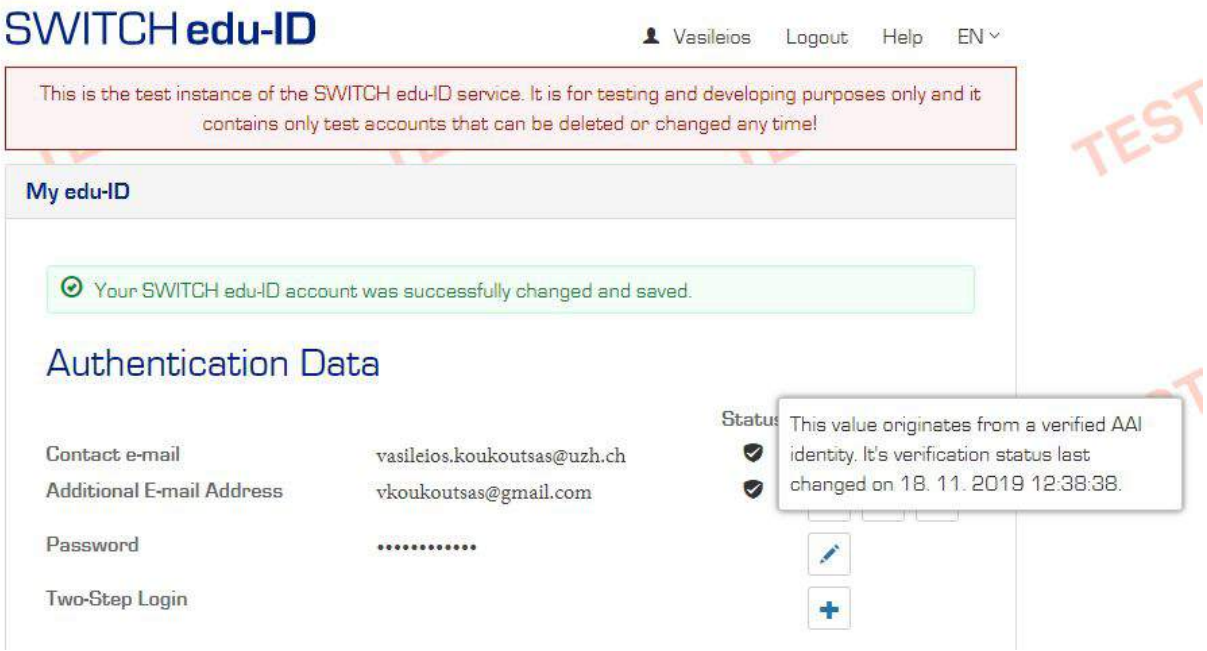
Attributes

Meta-displayName: SWITCH edu-ID [Test]
Meta-informationURL: https://projects.switch.ch/eduid/

SWITCH
edu-ID

Meta-largeLogo:
Meta-organizationURL: http://www.test.eduid.ch/
Meta-smallLogo: ID
affiliation: affiliate
cn: Vasileios Koukoutsas
displayName: Vasileios Koukoutsas
eduPersonUniqueId: 0000548154984554@test.eduid.ch
givenName: Vasileios
homeOrganization: test.eduid.ch
homeOrganizationType: others
mail: vasileios.koukoutsas@uzh.ch
persistent-id: https://test.eduid.ch/idp/shibboleth!https://educhain.csg.uzh.ch/shibboleth!NK8lncJ1X1tPONzrWYUSMY3JI5s=
principalName: 0000548154984554@test.eduid.ch
schacHomeOrganization: test.eduid.ch
schacHomeOrganizationType: urn:schac:homeOrganizationType:ch:others
scoped-affiliation: affiliate@test.eduid.ch
surname: Koukoutsas
uniqueID: 0000548154984554@test.eduid.ch

Verified attributes



Non-verified Attributes (User added)