

EduID Day 2020

Tuesday 3rd March 2020 & Wednesday 4th March 2020

Hosted by SURFnet in Utrecht, The Netherlands

Attendees	2
Agenda	2
Introduction	3
Presentations from participants	4
Collected Discussion Points	7
Discussion point 1: what is an eduID?	8
eduID characteristics	8
Duplicate eduID ?	8
User centric	8
Privacy	9
Role Government	9
Social Accounts	9
Attributes	9
Discussion point 2: what are use cases for eduID?	10
Use cases	10
Research Use Cases	10
Discussion point 3: used technology / architecture	11
Final remarks in closing rounds	12
Actions	13
Mailinglist	13
Possible topics for followup	13

Attendees

(In random order)

- Maarten Kremers, SURF
- Michiel Schok, SURF
- Wolfgang Pempe, DFN (online/video)
- Rolf Brugger, SWITCH
- Peter Havekes, SURF
- Bart Kerver, SURF
- Rene de Koster, ECCA
- Omo Oaiya, WACREN
- Miroslav Milinovic, SRCE
- Manne Miettinen, CSC
- Henri Mikkonen, CSC
- Michał Zimniewicz, PSNC
- Martin Božič, Arnes
- Pavel Sipos, Arnes
- Tomi Dolenc, Arnes
- Christoph Graf, SWITCH (online/video)
- José Manuel Macías Luna, RedIRIS (online/video)
- Licia Florio, Geant (online/video)
- Klaas Wierenga, Geant (online/video)

Excused in advance:

- Peter Clijsters, SURF

Agenda

Tuesday 3rd March 2020

12:00 - 13:00	Walk in and Lunch
13:00 - 13:20	Welcome and Introductions (Maarten Kremers & Michiel Schok)
13:20 - 13:30	Presentation SWITCH
13:30 - 13:40	Presentation CSC
13:40 - 13:50	Presentation ARNES
13:50 - 14:00	Presentation SRCE
14:00 - 14:10	Presentation DFN
14:10 - 14:20	Presentation PSNC
14:20 - 14:30	Presentation SURF
14:30 - 14:50	Coffee break
14:50 - 15:00	Presentation RedIRIS
15:00 - 15:10	Presentation WACREN
15:10 - 15:25	Presentation ECCA (Rene de Koster)
15:25 - 15:40	Presentation MyAcademicID (Licia Florio)
15:40 - 16:00	Determine Discussion topics
16:00 - 17:30	Discussion session 1
17:30	Drinks

Wednesday 4th March 2020

09:00 - 09:30	Walk in & Coffee
09:30 - 09:45	Recap of yesterday & update of topics
09:45 - 11:00	Discussion topic session 2

11:00 - 11:15	Coffee break
11:15 - 12:15	Discussion topic session 3
12:15 - 12:30	Wrap-up / Next steps
12:30 - 13:00	Lunch

Introduction

Welcome & introduction by Maarten Kremers

Presentation: [eduID Introduction](#)

Presentations from participants

The event started by having presentations on the national eduID initiatives. In advance we kindly requested to address the following topics:

- Status (concept/idea, exploration, proof of concept, pilot, pre-production, production)
- Which use cases in mind / are covered
- Relation to federation (eduID complimentary or replacement)
- Role and relationship towards educational Institutions (IdPs)
- Lifelong identity or restricted to (higher) educational period of time
- Plans to interfederate in future
- Identifier (if chosen, which one?)

Also MyAcademicID and ECCA have presented their projects, goals (etc.) and the relation to eduID in general.

SWITCH

Presenter: Rolf Brugger | Presentation: [SWITCH](#) | eduID website: <https://www.eduid.ch>

CSC

Presenter: Manne Miettinen | Presentation: [CSC](#)

ARNES

Presenters: Martin Božič and Pavel Šipoš | Presentation: [ARNES](#)

SRCE

Presenter: Miroslav Milinovic gave a presentation without slides of the developments.

A few highlights of the presentation:

The federation/AAI in Croatia also covers schools (besides higher education). There is one IDP for all schools, for higher education there are several IDPs. The central IDP is accepted as eIDAS IDP (level 1). Multi-factor authentication is being introduced, and a challenge/issue is the audit of a federation. There is no eduID initiative (yet), however SRCE recognizes use-cases like life long learning, collaboration and the need to solve user-provisioning / deprovisioning. Erasmus Program is being rolled out/developed in Croatia, therefore there's interest in identities that an eduID may/can deliver.

DFN

Presenter: Wolfgang Pempe | Presentation: [DFN](#) | eduID website:

<https://doku.tid.dfn.de/de:aai:eduid:start>

PSNC

Presenter: Michał Zimniewicz | Presentation: [PSNC](#)

SURF

Presenter: Maarten Kremers | Presentation: [SURF](#) | eduID website: <https://www.eduid.nl>

RedIRIS

Presenter: José Manuel Macías Luna | Presentation: [RedIRIS](#)

WACREN

Presenter: Omo Oaiya gave a presentation without slides of the developments.

A few highlights of the presentation:

WACREN has a hosted IdP solution: eduID.africa. The national infrastructure is still largely unexplored and therefore a kind of green field. They are searching for solutions and architectures in the form of blueprints. WACREN is exploring to go straight to/for a central solution - such as an hosted eduID - instead of IdP's per educational institution. WACREN therefore may benefit from the 'law of the inhibiting lead'.

ECCA

The European Campus Card Association (ECCA) is an independent, neutral, non profit organization in the field of Campus Cards and electronic ID for Higher Education Institutes.

Rene de Koster (Wageningen University and current president of ECCA) presented the work on which ECCA is currently working with funding from the Vietsch Foundation on a proposal for a Trusted Student Identification Framework. The project has realised a state-of-the-art report and conducted a market research survey. Based on these results together with to be held workshops the project will deliver a report on the recommendations for the development of a proposal for a trusted student eID framework.

Presentation: [ECCA](#) | website: [ECCA Trusted Student eID Framework](#)

MyAcademicID

Licia Florio (GEANT) presented the MyAcademicID project. The project aims to support the digitisation of the Erasmus programme by enabling electronic access to Erasmus services, enabling seamless mobility of students across borders and enabling secure and seamless electronic interactions between Higher Education Institutions (HEIs) with a “Login in Once Only” principle. Notably are the proposed proxy to bridge eduGAIN and eIDAS as well as the proposal for an identifier, the European Student Identifier based on the SCHAC PersonalUniqueCode

Presentation: [MyAcademicID](#) | website: <https://www.myacademic-id.eu/>

Collected Discussion Points

Based on the presentations the following (loosely undoubled) list of discussion points has been created. See the overview in [Collected Discussion Points](#).

	SWITCH	CSC	ARNES	SRCE	DFN	PSCN	SURF	RedIris	WACREN
Interoperability – international eduID scheme	x				x		x		
Used technology and architectures (also solutions)	x		x			x			x
Group management	x								
Lessons learned (experiences) from building eduID		x							x
What the users and service providers are doing and saying?		x							
What are use cases (Educational / Common) and services used?		x				x	x		
project management of transitioning to eduID and migration scenario's			x				x		
IdM solutions (attribute providers) in eduID (local AD & eduoam provisioning)			x						
provisioning / deprovisioning				x					
how to map identities (eduID and organisationID's)				x					
how to enable users to move between organisations				x					
ResearcherID – RID (see GoogleDoc) (Competing approach / Interoperability / Yet another Identifier)					x				
Idea's on MyacademicID								x	
Account-linking (f.e. ORCID) / how to connect link to national eID's								x	x

Based on the list and the score of the topics by the participants the following topics have been discussed:

1. What is an eduID?
2. What are use cases for eduID
3. Used technology / architecture
4. International scheme

Discussion point 1: what is an eduID?

eduID characteristics

- Lifelong
- User centric
- Linking to other identities (e.g. ORCID, other eduID's, bankID)
- Opens up extra use-cases
- Sector specific attributes are our unique proposition
- Separation of authentication (ie. webAuthN)

- One eduID per person, no duplicates allowed.

Duplicate eduID ?

- User must choose between identifiers in use
- Extra identifier is deactivated
- Service providers are informed of identifier deactivation and can migrate user to new identity
- Universities are driver of 'just one identifier'
- API where services can check if identifiers are deactivate
- SWITCH: process in place
- SWITCH: policy forbids multiple eduID-accounts per user

User centric

- Cannot trust
- Verification processes can raise level of assurance
 - E.g. link to an institution account
 - Or link to eIDAS (attributes)
- Vetting
- Users have to be active (link to other identities)
- Possibly identity created / attributes filled by Government, user is next
- Users are lazy - what motivates them to keep the identity up to date
 - And if they're dead? Who is going to tell us? Is there deprovisioning for eIDAS?
 - What's the use case for finding out if someone is dead?
- Recovery of identity – not solved yet
- Integrate into process of exit HEI (e.g. link to Google-account)
- Right to be forgotten – what to do if a user requests deletion?
- Bring you own authentication – WebAuthN –
- Support? How do you provide support to students (forgotten passwords, etc)
 - Communication / responsibility is organized at time of connecting university to eduID

Privacy

- SWITCH: eduID identifier – given to institutions if they need it for identity management.
- SWITCH: services get a persistent or an unique identifier.
- SWITCH: not very restrictive for unique identifiers
- SURF: only pseudonyms for services.
- SRCE: universal number (SSN) is used in many places in public sector
- CSC: would like to use 'national learner id', no solution for teachers

Role Government

- Can we trust the government?
 - Important role
 - Also for eIDAS
- But any system should be available without eIDAS account
- Not all NREs are equal / neutral / ...
- There is room for organizations that are trusted (e.g. by audits) to create id's. Could be NREs, could be others.
- Not every country has a national eID

Social Accounts

- Should we embrace them or do as if they don't exist?
- Some students want to separate 'fun accounts' (Instagram/tiktok) from serious work.

Attributes

- SWITCH: Introduced attributes for affiliation
- SWITCH: sync-protocols for attributes to institutions

Discussion point 2: what are use cases for eduID?

Use cases

- Vocational education
- Research projects with private partners
- Eduroam access for short durations (private users)
- “Roles” for “specific authorizations”
- In search of the Killing App
 - eduroam
 - National Library Platform (special access for some users)
 - File Sharing Platform (keep using after graduating)

Research Use Cases

- National Infrastructures – need for lifelong identifiers
- Frequent change of employers

Discussion point 3: Used technology / Architecture

Rolf presented the architecture of the SWITCH eduID. We took some additional time to discuss the data model. The model consists of three (main) parts. This allows for scalable quality (LoA) of the attributes within eduID.

- Personal/user part:
 - Data self created, under control by users
 - Fixed LoA of attributes

- Affiliations:
 - Data is created and controlled by universities
 - Data is interlinked at registration: IdM's of university and eduID
 - LoA of data is higher since it is checked and maintained by universities

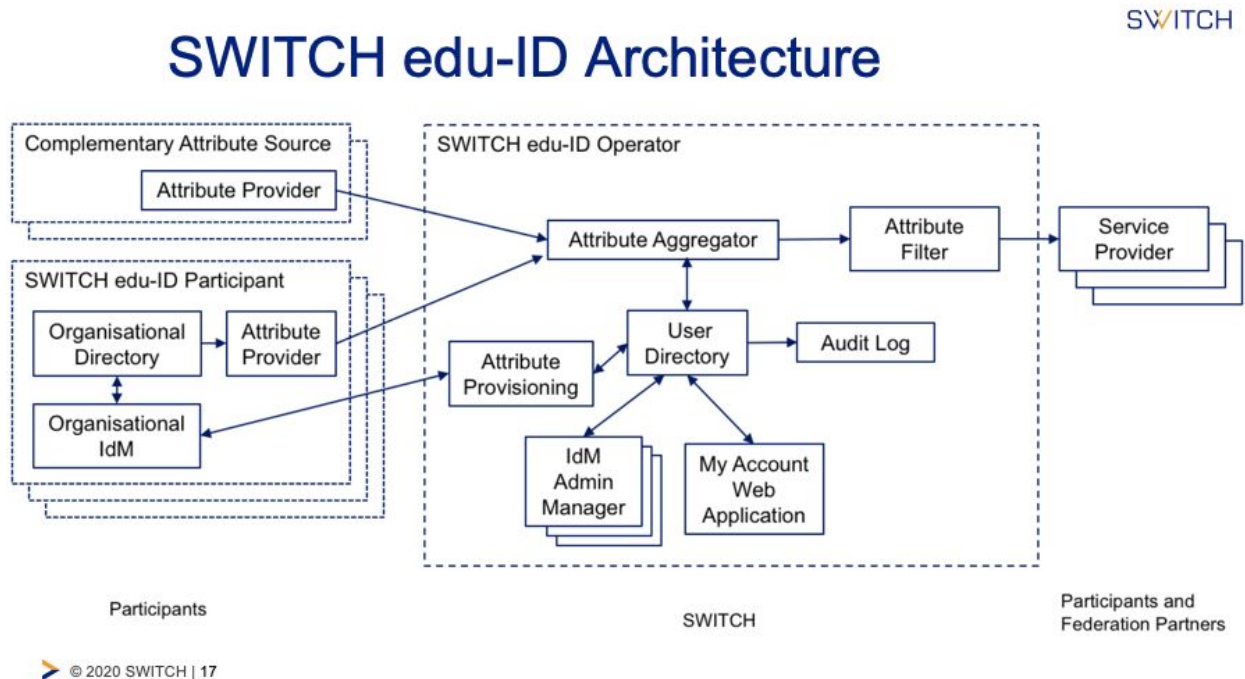
- Former affiliations
 - after graduation - or when a student temporarily leaves university - “current affiliation” moves to a list of previous affiliations (can be multiple).

- Group membership
 - Entitlements of users

- Data is under the control of both services and users

If a user has multiple affiliations, the user decides what affiliation (and therefore what profile) to use. This is at 'login time'. There are services/scenarios where all of the user attributes (so both profiles) are sent to a service provider. This feature can typically be used to merge accounts.

After we talked about the data model, Rolf explained the architecture and how the data is created and synchronized between the eduID-core and the eduID-participants.



SCIM is used as a protocol for exchange of attributes between universities and eduID.

Important is that participants implement a linking service within their own infrastructure that allows users to link their local identifier to an eduID identifier. The linking service typically asks for a local login (f.e. with AD) and an eduID login afterwards.

Services get a unique-ID of the user, the unique-UID is scoped on an organisation (eduID participant), the unique-ID is global for all service providers (in other words: every service provider gets the same identifier for a user). This solution is different from the Dutch eduID implementation where every service gets a different pseudo-ID for a user, letting the user in charge of the resolving of its identity.

Discussion point 4: International scheme

Due to the time, there was only a brief discussion on the international scheme.

It seems logical to proceed forward on the path of MyAcademisID as a solution for internationalisation despite a some downpoints that were mentioned: a significant part of the community is already behind this solution or is looking into it and it's really difficult matter to overcome (see the difficulties of eIDAS as an example).

Suggestion is not to try to go and fix this ourselves.

Final remarks in closing rounds

Tomi: question is what we can or should do to proceed forward. Possibly not so much driving own development, but copy existing solutions for our eduID?

Manne and Henri: we can reuse powerpoint slides that explain the concept of eduID. Gathered a lot of ideas. We will consider pushing eduID although we're aware of a lot of issues that need to be tackled (first?).

Miro: very useful to learn how other countries are working and how others handle things and that we can profit from both benefits and pitfalls. I see similar use-cases however its not yet clear how to move forward with eduID. Further discussions on architecture & internationalisation are important, let's continue on a mailing list.

Martin & Pavel: a lot of new things learned, ARNES has quite some infrastructure already in place to create an eduID especially because the infrastructure is in our own domain which makes it easy to make the push. For example a guest-IDP en HostedIDP could be a starting point.

Omo: besides what has been said before it was illuminating to see the challenges faced. I will continue to try and find blueprints. This network of people is great and may help us in further development.

Michał: The discussion based on the data model from Switch was interesting (personal data versus regulated data) and that it allows to differentiate meta-data. Challenge is to apply all of this to K12 and high-schools. It would be nice if there would be an (standard) architecture that we can rely on.

Rolf: I learned that Switzerland is ahead, but it is very useful to challenge ourselves: does it make sense what we are doing? Also good to get a feeling on how serious eduID is? If there's more interest in eduID, a suggestion to create a website with 'what is eduID', 'what are use cases', 'what architectures' and so on.

Michiel: It has been inspiring, good to get an impression on where others are. Concerning the road ahead: we stand on our own but must define how to proceed with TF-EDU. I'll discuss this with Klaas.

Klaas: first of all it has been inspiring, a lot of energy, good understanding and discussion. Secondly: all eduID-initiatives are national and I thought that there would not be much interest in international connections. It's good to see and hear that I was wrong and there actually is interest to explore cross country use-cases. Let's take that step and try to describe these use cases.

Wolfgang: it has been very instructive, it's good to know that we're not alone with questions.

Licia: besides all that has been said, I like to stay involved in further discussions with regards to the MyAcademicID.

Christoff: it's actually fun to be 'ahead of the pack', we will try and bring others closer to the pack!

Maarten: Very useful and inspiring session, good to learn from others on handling things and learning from other's use cases. Many thanks for being here and for your active participation.

Bart: as last on the table, not much to add to all of this, please consider to (re-) view all presentations since there's a lot of information on the different eduID-initiatives. We asked you to address specific topics in your presentation, this might help to get a quick overview on the status.

Actions

- Create a mailing list for further offline discussion (Maarten)

Mailinglist

A mailing list to continue the discussion is now available.

Information & Subscription: <https://lists.geant.org/sympa/info/eduid>

Mailing List: eduid@lists.geant.org