

# Trust & Identity: What's next ?!

GN4-2 Project - Next Generation Trust & Identity Technology Development

## Maarten Kremers

Task Leader Trust & Identity Technology Development, GN4 Project

Technical Product Manager & Project manager T&I, SURFnet



Internet2 TechEx 2017, San Francisco, CA

16<sup>th</sup> October 2017

### Trust & Identity Operations

- eduGAIN
- eduPKI
- eduroam

### Trust & Identity Development

- eduGAIN Development – Federation and Campus
- eduGAIN Development – e-Research and Service Providers
- Trust & Identity Technology Development
- eduroam Service Development

OpenID Connect Federations

eduKEEP – Towards a User Driven Identity Federation

REFEDS Authentication profiles &  
Step-Up Service

eIDAS & eduGAIN



Overcome the organisation-centric identity model shortcomings

Identities are tightly coupled with role and affiliation

Poor support for dynamic and loose relationships

Identities bootstrapping

Multiple concurrent affiliations

## User-driven, persistent, privacy preserving, institutional backed identity (UPPII)

The user identity is created *outside* the organisation

The organisation *validates* the user identity

The organisation *link* the user identity  
to role and affiliation

and / or

The organisation *bootstrap* a local user account  
leveraging the external identity

Registration / Alumni /  
lifelong learners

One identity to rule them all  
To register, join another university, become an alumni

Researchers

One identity in concurrent projects with multiple  
affiliations and for all publication work  
(with help of ORCID and friends)

Teachers

One identity for interacting with their learners across  
multiple universities

Third Parties Services

Supports longer-term client-relationship.  
Offerings and conditions can be based  
on roles available at given time

SWITCH EduID  
(Switzerland)

Central user-centric IdP, enriching identities with attributes from Home Organisations

SUNET EduID  
(Sweden)

Central user-centric IdP to bootstrap identities at Home Organisations

GARR  
eGOV IDs, IdP/Proxy &  
Aas (Italy)

Considering to use an Idp/SP Proxy to link eGOV IDs to Home Organisations Attribute Authorities



Feature	SWITCH edu-ID	SUNET eduID	GARR IdP/SP Proxy
A- Target audience	R&E Community	R&E Community	R&E Community
B- A new identifier is provided	YES	YES	YES
B1- Identity suitable for AuthN	YES	YES	NO
B2- Long-term identity	YES	YES	YES *
B3- Persistent identifier	YES	YES	YES *
B4- Globally Unique Identifier	YES **	YES **	YES *
C- IdP acting on behalf of Home Organisation IdPs	YES	NO	YES

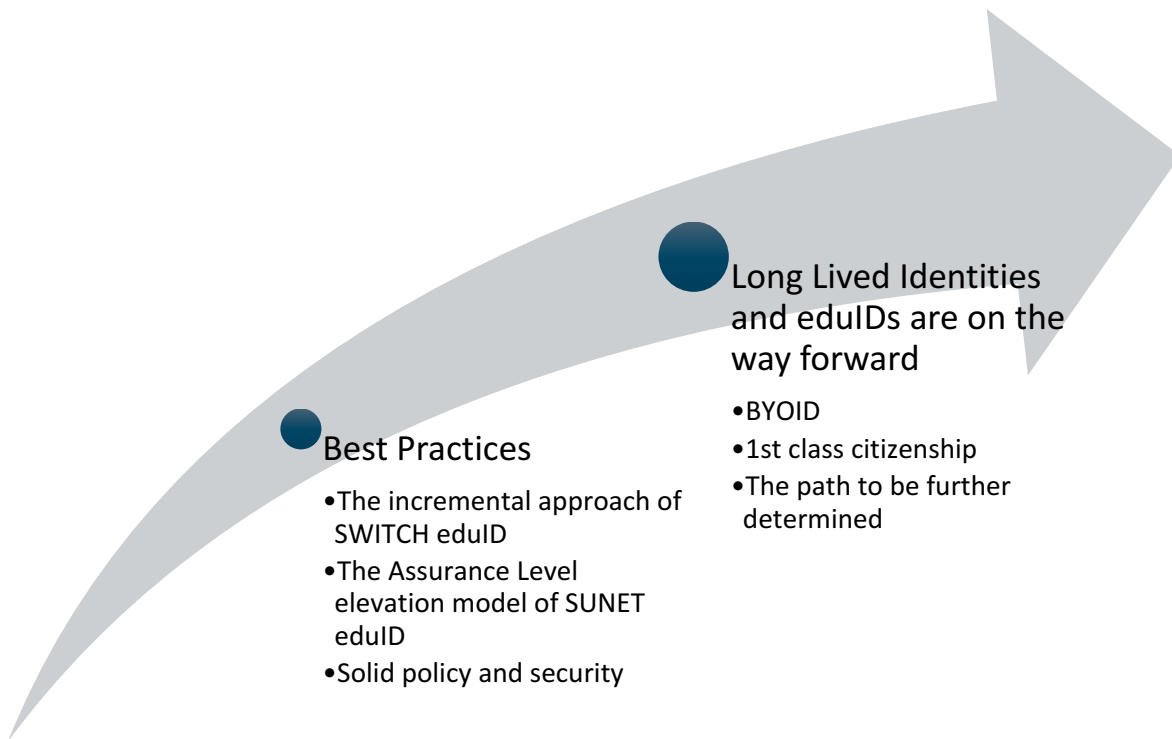
\* external dependency

\*\* confirmed identities

Feature	SWITCH edu-ID	SUNET eduID	GARR IdP/SP Proxy
D- Account Linking	YES	YES	YES
D1- Linked Account AuthN	NO	NO	YES
E- Self-asserted Identity	YES	YES	YES *
E1- Identity Assurance Elevation	YES	YES	YES
E2- VO-based vetting	NO	NO	YES
F- Attribute Aggregation at IdP	YES	NO	YES
G- Attribute Release Policy - Delegate Management to Home Organisations	YES	NO	YES *

\* external dependency

\*\* confirmed identities

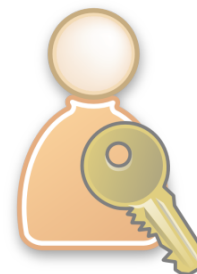


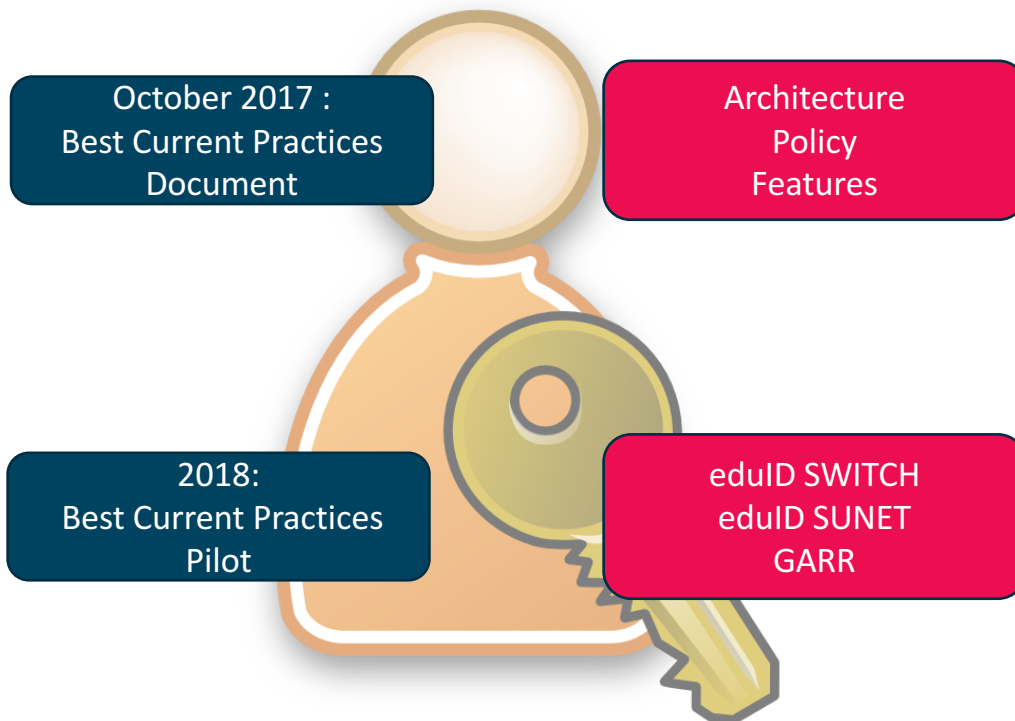
## Best Practices

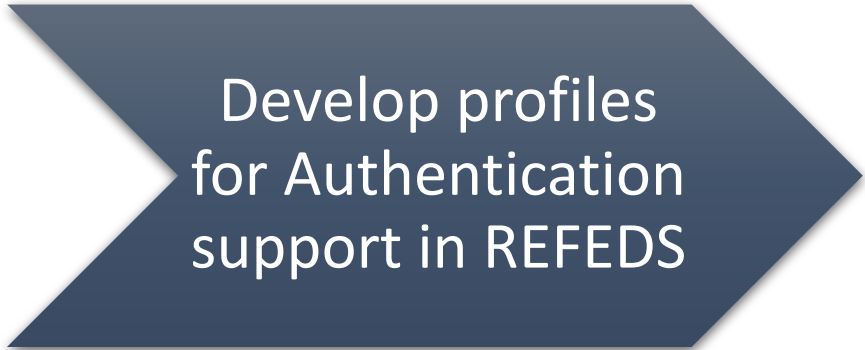
- The incremental approach of SWITCH eduID
- The Assurance Level elevation model of SUNET eduID
- Solid policy and security

## Long Lived Identities and eduIDs are on the way forward


- BYOID
- 1st class citizenship
- The path to be further determined



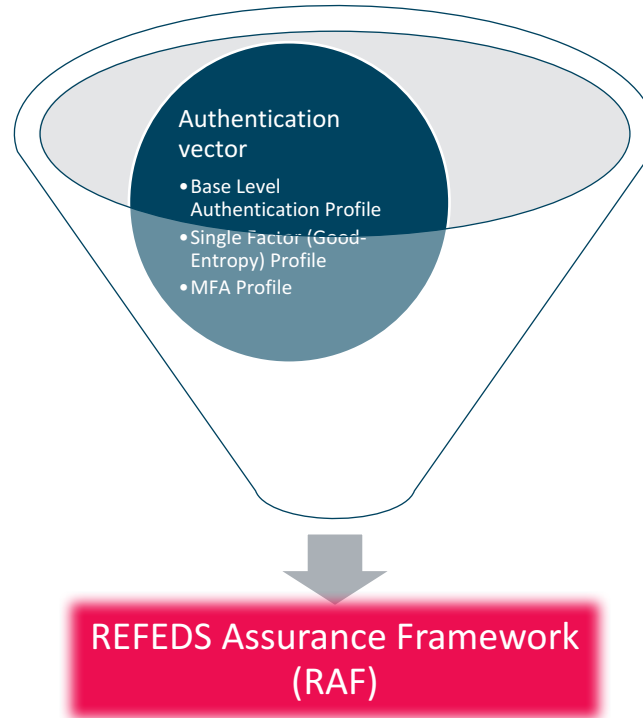




Develop profiles  
for Authentication  
support in REFEDS



Develop Step-up  
service



## Base Level Authentication Profile

- Base profile
- No explicit authentication requirements
- draft done, REFEDS consultation pending

## Single Factor (Good-Entropy) Profile

- Requirements for single factors
- BCP for password scenarios
- In progress

## MFA Profile

- Requirements for MFA
- Done

## Deliver Step-Up Service

Primary audience : Research Collaborations

Collaboration with AARC

- Use cases
- User / community requirements
- Architecture

In progress:

- Analyzing different approaches

Both Identity and Authentication Step-UP

Potential pilots (Autumns 2018)

Next Steps

- Timeline
- Testing scalability

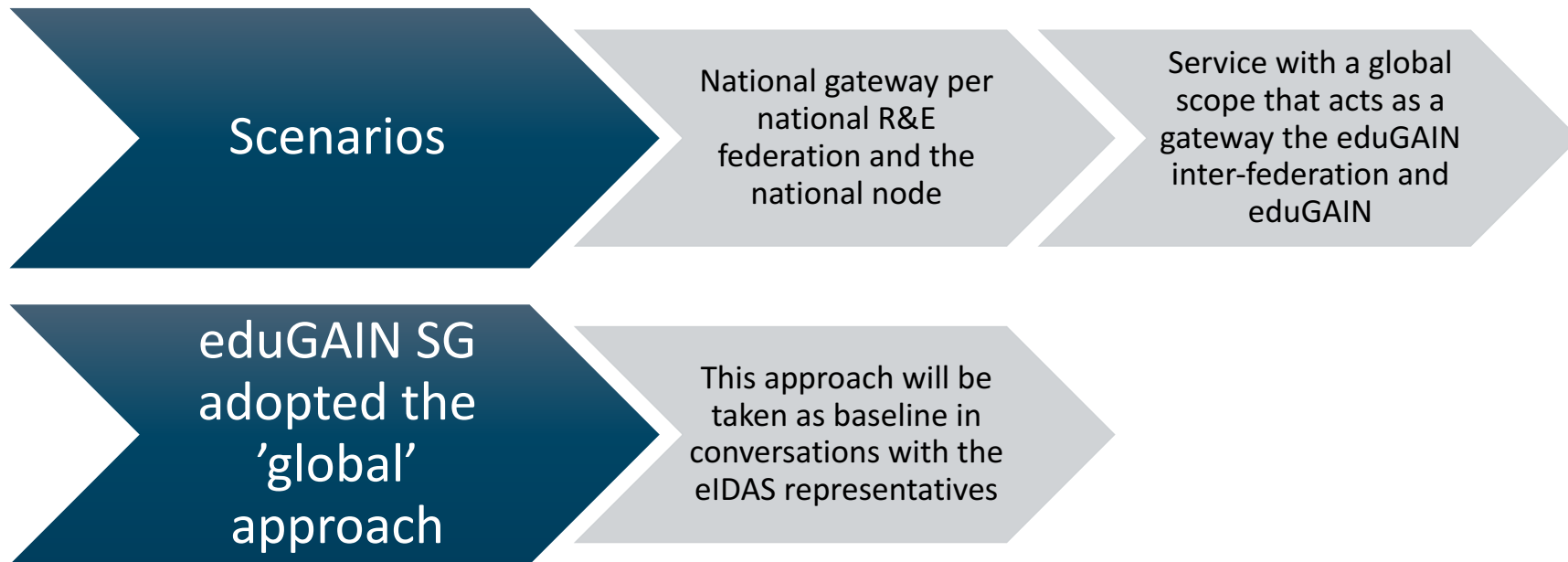


electronic Identification,  
Authentication and trust Services  
(Upcoming EU regulation)

Leverage the use of eGOV IDs for  
higher LoA in the R&E federations

Technical interoperability with  
build proxy, technical pilots done

Interoperability comparison  
between the frameworks



<https://wiki.geant.org/display/gn42jra3/Task+3%3A+Next+Generation+Trust+and+Identity+Technology+Development+-+TrustTech>



Thank you

[maarten.kremers@surfnet.nl](mailto:maarten.kremers@surfnet.nl)



Networks · Services · People  
[www.geant.org](http://www.geant.org)