Automation of SP deployment

Public Sprint Demo

GN5-1 Trust & Identity Incubator

Alexandr Petrunin
Branko Marović
Niels van Dijk

23 January 2024

Activity description

This activity investigates a proxy approach to aggregate the services and potentially simplify the deployment and integration of tools. The Incubator will make an inventory of relevant services and discuss integration scenarios with stakeholders. The goal is to create proof of concept of at least one scenario and present it to federation operators.

It would be useful to enhance the level of support we provide to them with the aim of quickly being able to deploy an initial set of services, the ones which could de-facto start to attract users towards the newly deployed federation infrastructure and the federated IdPs.

The idea here is to propose a new cycle of T&I incubator task activities aimed at the following tasks:

1. ***Identifying an initial set of services*** we'd like to promote as SPs to the new identity federations. (e.g.: Wiki, Moodle, Joomla, eduMEET, Filesender, ..)
2. ***Design a solution for connecting to the services we'd like to deploy***, based on automation, possibly using containers, or automated deployment tools (which we should aim at making easy for early services deployers),
3. *Define both technical and strategic roadmaps* to ensure sustainability of these deployment solutions: how will they be upgraded/ported to new versions, which task, or permanent activity in the GN project, or the community could endorse the future work to keep the developed solution working also in future.

3 deployment models

- **SP proxy for new federations**
  -> easy connection to existing GÉANT services and commonly used SPs
  -> a clear and straightforward integration point for services

- **VO community SP proxy**
  -> simple integration for commonly used VO collaboration services

- **Institutional Service aggregation**
  -> integration point for on- and off-campus institutional services
  -> integrate federation, eduGAIN and guest identity access

SP proxy configuration

- Proxy configuration is very product specific
- Requires in depth knowledge of proxy product in use
- Proxy configuration:
  - deployment specific
  - connection specific

- Common Proxy Configuration Language proposal tries to simplify configuration and exchanging information of connected entities
  - https://github.com/surfnet-niels/cpcl

SP proxy configuration using CPCL

IN

```
---
in: # This side of the proxy recieves the credentials from the resource conf
  saml_idp: # A configuration for a SAML IdP
     name: "SURF bv"
     description: “Connect to the SURF Identity provider”
     entityid: "http://login.surf.nl/adfs/services/trust"
     metadata_url: "https://metadata.surfconext.nl/idps-metadata.xml"
processor:
    ...
out:
    ...
```

OUT

```
---
in:
    ...
processor:
    ...
out: # This side of the proxy sends the credentials from the resource config
  saml_sp: # A configuration for a SAML SP
     name: "InAcademia Affiliation Validation Service"
     description: “Connect to InAcademia”
     entityid: "https://inacademia.org/metadata/inacademia-simple-validation
     metadata_url: "https://inacademia.org/metadata/inacademia-simple-valida
```

Processing

```
pass # place incoming credential values in outgoing credential value
    in.foo
    in.bar
    out.foobar

passe # place incoming credential values in into outgoing credential val
    in.foo
    in.bar
    out.foobar

passo # place incoming credential value in preference of order into outg
    in.foo
    in.bar
    out.foobar

concat # Concatenate 1 or more incoming credentials using an optional se
    in.foo
    in.bar
    "stringvalue"
    out.foobar

split # Split an incoming credentials using the first occurance of the s
    in.foobar
    seperator
```

Candidate applications for SPs

- Web docs & collaboration: **DokuWiki**; alt. TWiki (MediaWiki, XWiki, Tiki Wiki (+forums), Gitit?)
- Content management: **WordPress**; alt. Joomla, Drupal
- Online office suite & collaboration: **ONLYOFFICE**; alt. Collabora Online
- Email server/agent: **Postfix**; alt. Exim, Sendmail
- Email client: **Roundcube**; alt. RainLoop, SquirrelMail, Horde, Mailpile
- Mailing lists: **Sympa**; alt. Mailman
- Learning management: **Moodle**; alt. Canvas LMS
- Video Conferencing & training: **eduMEET**,; alt. BigBlueButton
- File transfer: **FileSender**; alt. Nextcloud, ownCloud
- VPN: **eduVPN**; alt. OpenVPN

Other GN services to be provided as software, e.g., eduroam and eduGAIN-related?

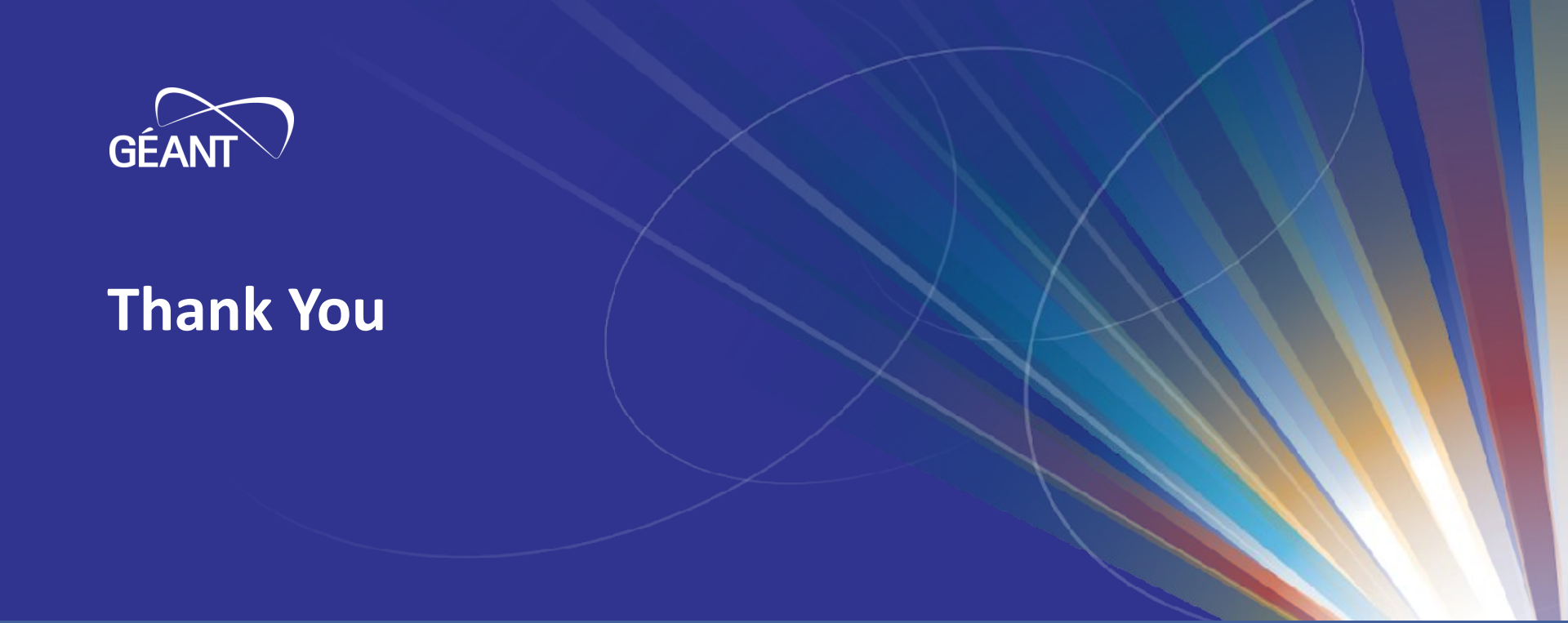
The final selection will depend on SAML/OIDC capabilities.

More at https://wiki.geant.org/display/GWP5/Proposed+applications

Work in progress

- Overview and demo of work in progress by

  Aleksandr Petrunin



Thank You

www.geant.org

Co-funded by
the European Union