Campus IdP

Status and plans

Mario Reale, Davide Vaghetti

Consortium GARR

eduGAIN TownHall - Vienna - Tuesday,
February 21 2017

Agenda

- Goals
- PM1 to PM9 Achievements
- Product Roadmap
- Points still to be clarified
- Next steps

Goals

- **Develop a Campus IDP platform to support the deployment of Identity Providers at Campuses**
- **Pursue integration with current existing GEANT FaaS (“add the last mile..”)**
- **Start a pilot service and engage in the transition to production process with GEANT**
- **Exploit possible synergies/collaborations with Internet2 TIER project**

“Based on findings from AARC, TIER (Internet2) and NREN developments, ***develop a campus IdP extension to the FaaS service*** *for sites and regions who currently do not have the ability to* ***support or offer a cloud IdP-type of service to campuses***” *[Gn4.2 Description of Work - DoW]*

- Existing reference products to be taken into account :
  - Jagger [Resources Metadata Registry]
  - HSM, DS, MDA [FaaS components]
  - Cloud IDP [Some NRENs already offer a Cloud IdP solution to their customers]

Goals re-stated *(Translated from "DoW-ish")*

1. **Ease the deployment** of Campus IdP by Home Organizations
2. Leverage **automated installation and configuration** tools
3. Interface a Resource Registry to **handle (part of the) IdP configs through entity Metadata**
4. Support Federations in their role of **providers of Cloud based Campus IdP** service
   a. Exploit integration to private/hybrid cloud platforms
5. Interface existing **GEANT FaaS** components
6. **Re-use wherever possible** existing solutions (do not reinvent the wheel)
7. Be **as inclusive as possible** to satisfy community needs at large
   a. But avoid to produce a bits-and-pieces Frankenstein-like solution
   b. Foresee various service adoption options (toolkit, VM, container)

All you can eat menu for today
(People worked on IdPs before….)

GÉANT

ANSIBLE

puppet

LXC

ova

kubernetes

LXD

docker

openstack™

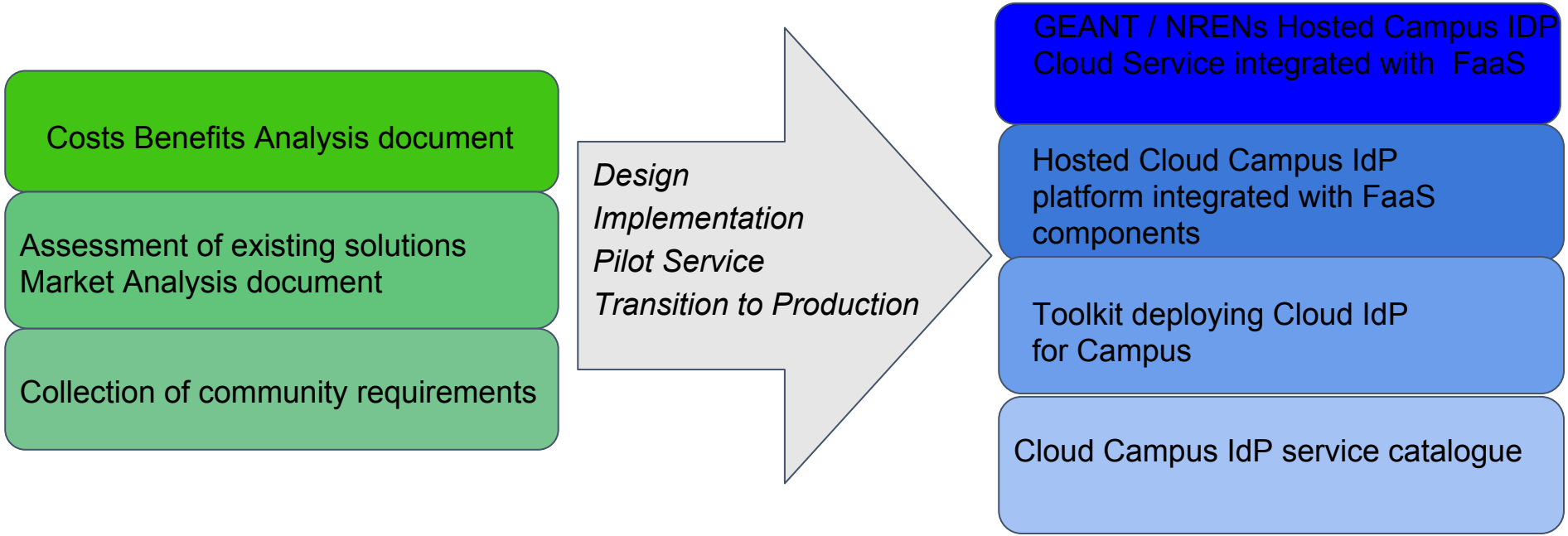
DOCKER COMPOSE

Achievements PM1-PM9 [1 / 3]

May 2016 to January 2017

1. Improve our **understanding of the community needs**: **GEANT Campus IDP NRENs Survey**
   a. Home Org IdP service deployment: High desire/Low skill 37.5% - Moderate desire/Cheap solution 18.75%
   b. Toolkit solution preference: Toolkit 45.45% - Cloud service model 27.27%
2. Assessment of the existing services within the GEANT community: **Market Analysis Deliverable** reporting on the existing solutions at some NRENs (under review by GEANT Technical editors)
   a. Federations with a Hosted/Cloud IdP solution: AMRES, CESNET, GARR, HEANET, JISC, RENATER, SWITCH
3. Agreement on **work plan** and on an **incremental approach** to product delivery to support Campus IdP
4. Organized our activities in 2 main teams: Architecture and Pilot
5. Setup of common working environment and tools
   a. GitHub public and private repository
      i. https://github.com/GEANT/CampusIdP
      ii. https://github.com/GEANT/ansible-shibboleth [PRIVATE !]
   b. Slack https://campusidp.slack.com
   c. Virtual Machines for test deployments (4 GEANT Okeanos, 4 GARR)

Incremental approach *to provide supporting services for Campus IdP*



Workplan

- Write **Market Analysis** with assessment of existing Cloud IdP solutions by NRENs [DONE]
- Design **Architecture** for an integrated solution: Campus IdP + FaaS [IN PROGRESS]
- Produce a **Costs-Benefits Analysis** [IN PROGRESS]
- Provide it to GEANT PLM Team
- **Refine** the architecture and **implements it**
- Start a **pilot service**
- **Review CBA** periodically
- Go through steps required by SA2 T1 **Services transition to production** procedures
    - Write all required Service Templates: SDP, Requirements, Documentation
    - Fill all required Service Templates

Achievements PM1-PM9 - *Architecture Team* [2 / 3]

May 2016 to January 2017

- Sketched (Still work in Progress!) an initial Draft Architecture Doc reporting (to be shared in few weeks)
  - Overall system components and their interaction
  - Detailed functionality to be provided for
    - Home Organization IdP admin
    - NRENs Federation Operators (FedOps)
  - Description of different architectural layers
- Initial brainstorming on API server implementation
- Defined high level schema for Configuration management directives - Client to API Server
- Started prototyping interfacing to Docker containers

Achievements PM1-PM9 - *Pilot Team* [3 / 3]

May 2016 to January 2017

- Hold team-internal code overview and hands-on demo on existing Ansible-based solutions to automate deployment and configuration:
  - CESNET - January 20, 2017 - Jan Oppolzer
  - GARR and RENATER planned for the next weeks

- Started prototyping with Docker-based Shibboleth IdP deployments:
  - First successful deployment few days ago (Janusz, HEANet)
  - On going tests by CESNET, GARR, AMRES
    - newly written dockerfile to build docker image
    - exploiting existing solutions on dockerhub and github

Architecture

Requirements for the Campus IdP platform

1. Due to spread in NRENs currently adopted technologies, be **as portable as possible** (independent of specific private cloud platform and infrastructure deployment model)
2. Security :
   a. Secure way to interface the LDAP/AD backend (LDAP+TLS, LDAPS - disable plain LDAP)
   b. Ensure **secure AuthZ approach towards MD-backend integration** (JSON Web Token or JWT)
3. Different levels of GUI management profiles:
   a. basic (all defaults)
   b. skilled manager (access to more advanced options)
4. Plug in Resource Registry - design a general solution for it
5. Integrates configuration management via Ansible
6. Provides:
   a. Ansible playbooks for deployment on Home Organization premises
   b. Pre-built Docker based IdP
   c. Automated spawning of IdPs on Openstack (container or VM)

Longer Term requirements to be addressed

- Provide High Availability for the IdP instances
- Consider integration with eduROAM GUI and a unique management interface for both

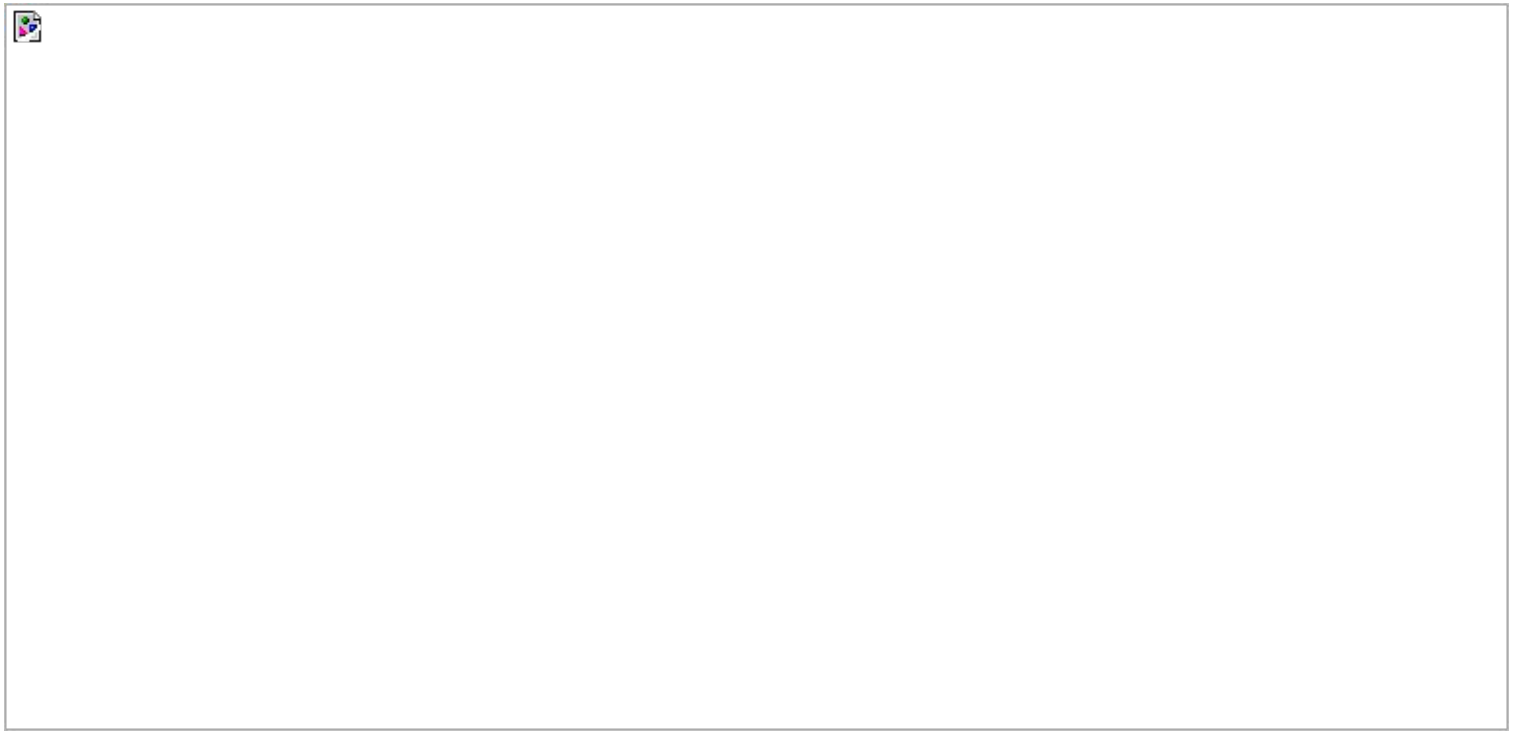
Achievements

Basic list of functionality

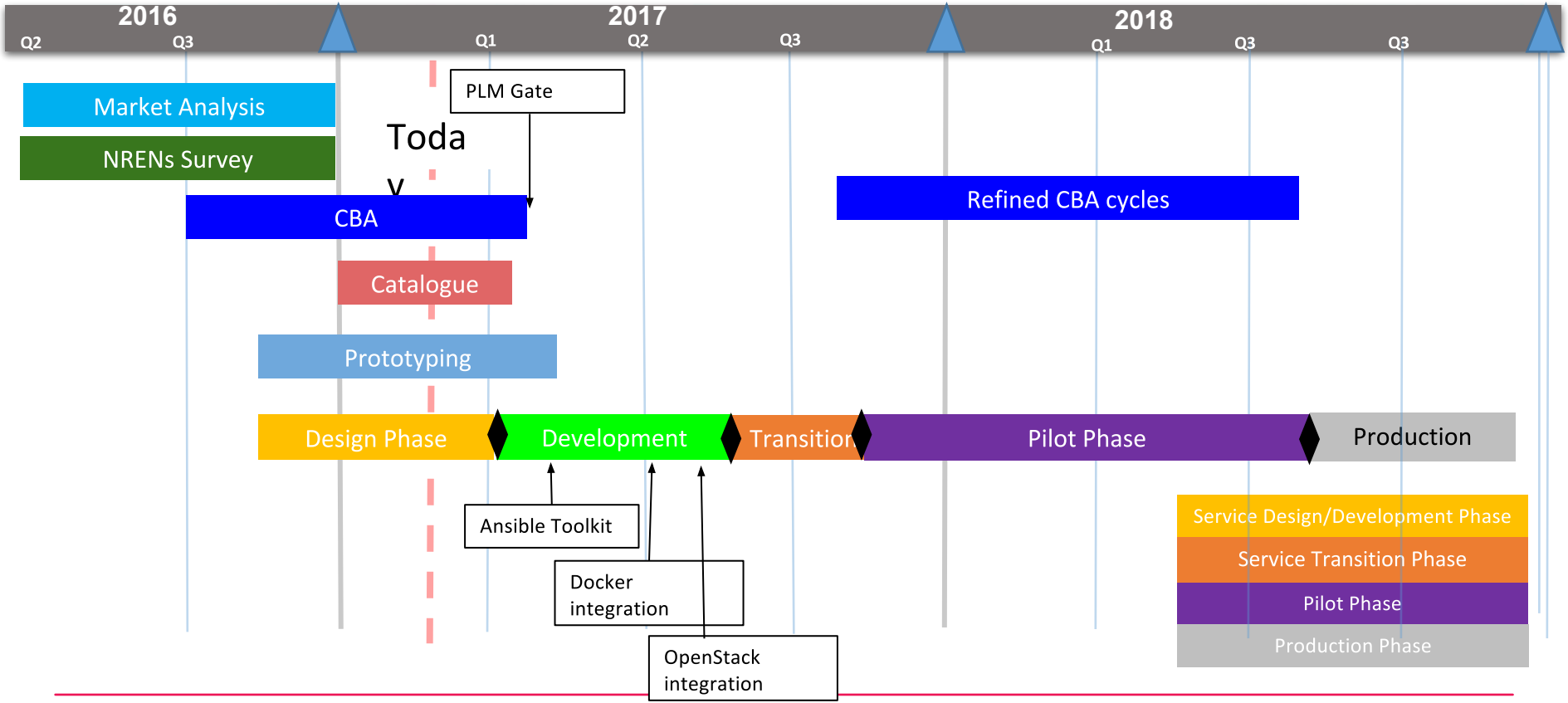
- Archive and management of the IdP metadata
- SAML SSO support to the Platform (registry) Service Provider
  - (.i.e.: the Platform itself will be a federation SP e.g. using FaaS)
- Configuration of the IdP instances
  - User/Authentication source (i.e. Directory)
  - Attributes mapping
  - Source of signed metadata
  - Locally defined attribute release policy and/or define remote attribute release policy (R&S and CoCo by default)
  - Customized login page
- Upload of required configuration files including public certificates
- Bulk configuration, patches, security updates management for all IdP instances through automation (Ansible)
- Build versioned docker template based on current configuration and upload to private docker repository
- Toolkit download (Ansible playbooks)
- Spawning of new IdP instances via Docker containers
- Spawning of new IdP instances on NREN Cloud Infrastructure

Achievements

Draft architecture



Campus IdP *Strawman* Roadmap

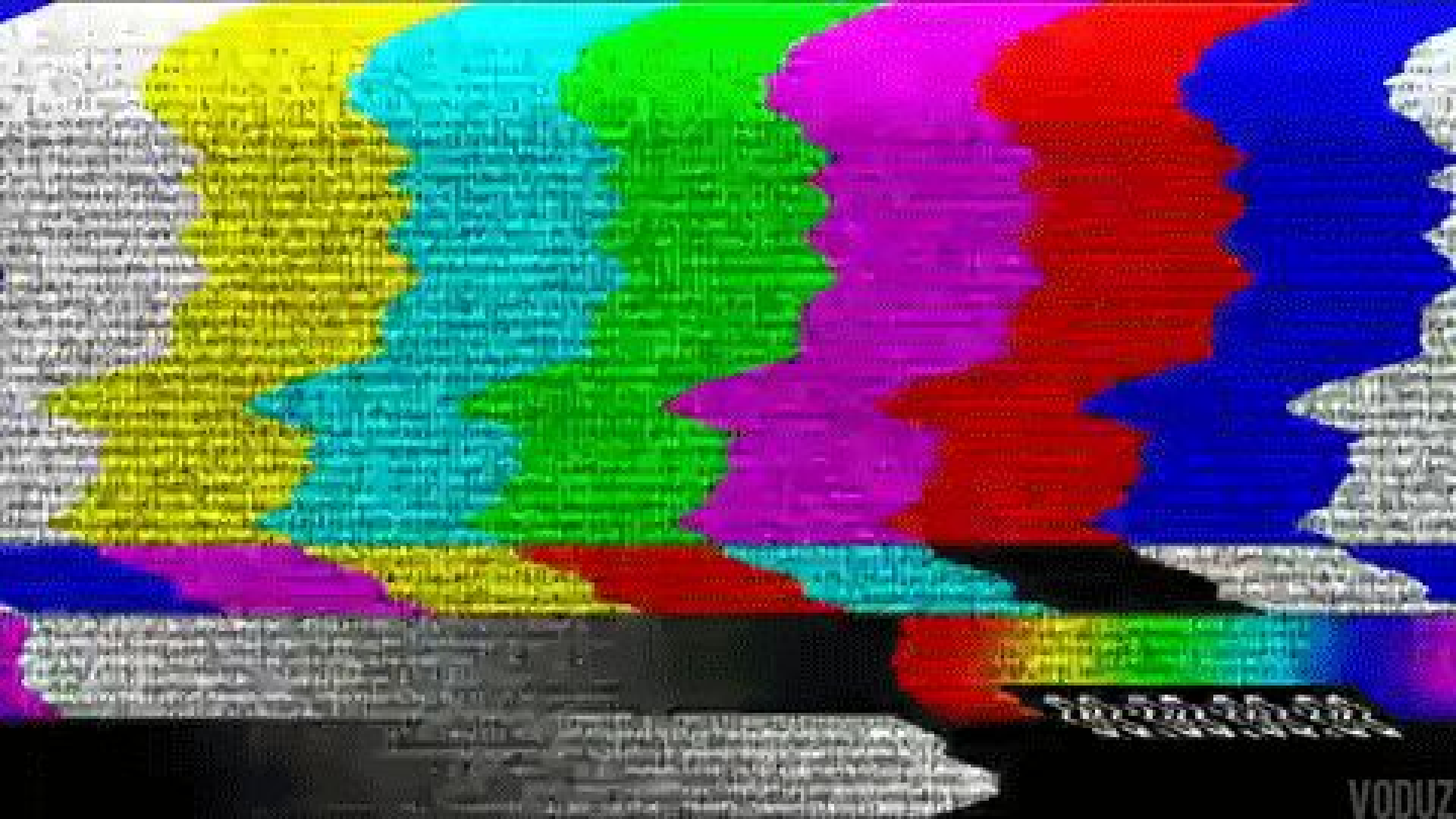


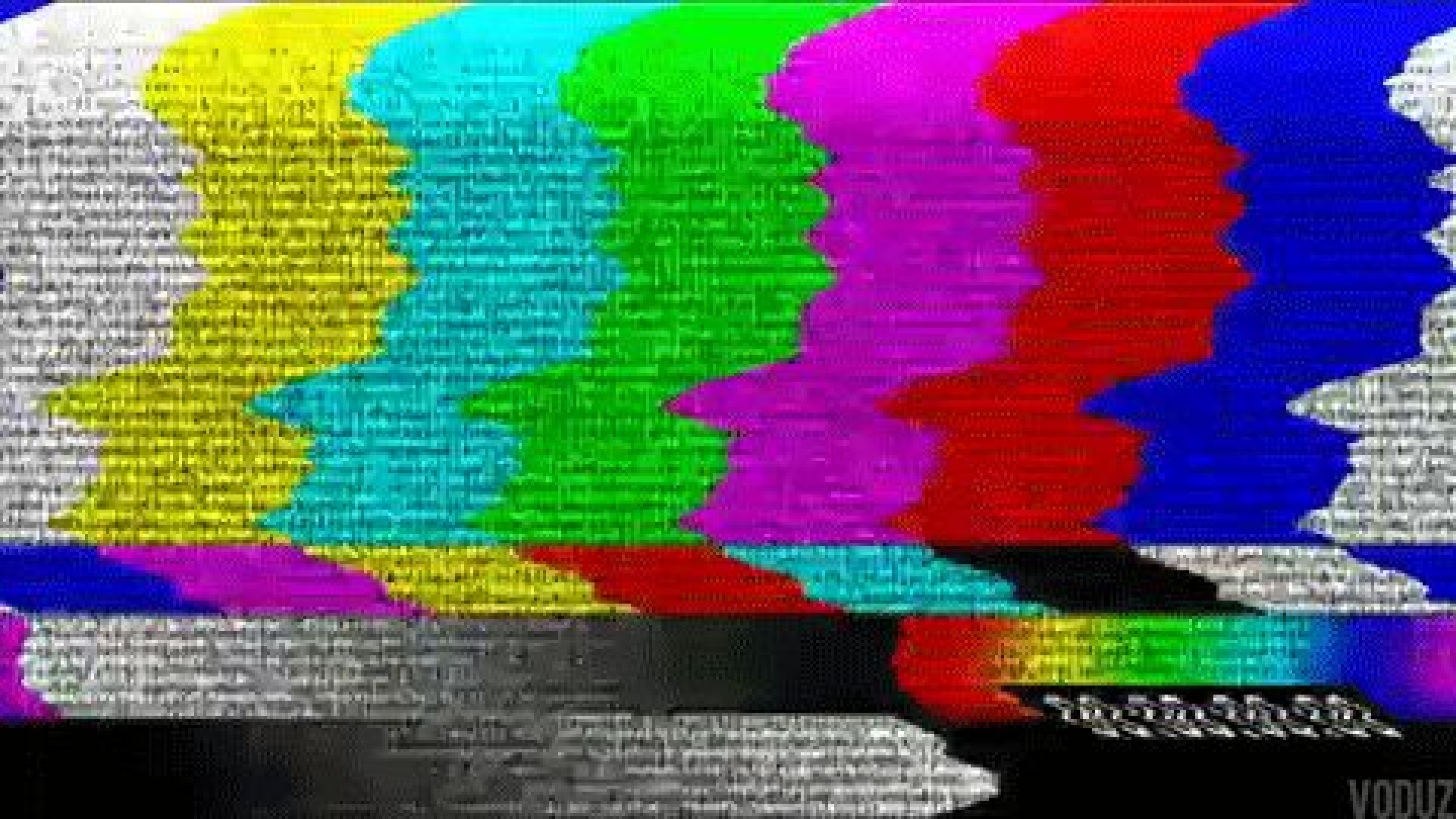
Docker related points still to be clarified by testing

- Practical feasibility overall
- Monolithic (1 IDP = 1 Docker container) vs Microservices (1 IDP = Many Docker) approach
- **Persistent data volumes - Full Separation of Application from Data layer**
- Private Docker Image Registry
- Openstack Docker
- Feasibility of implementation of advanced features (Docker Compose, Kubernetes)
- Integration with Openstack (nova-docker)

Next steps

1. Finalize the CBA document (two weeks from now)
2. Finalize the Catalogue of existing solutions - online
3. Complete architectural design for the Gn4.2 solution for IdP
   a. Finalize and share arch document
4. Converge to a common, unique, integrated solution for Ansible-based toolkit
5. Proceed with tests/piloting on spawning IDP instances on Docker
6. Develop API service for the Campus IDP Server component
7. Assess/Test Internet2 TIER work on deploying Campus IDP via VMs and Docker
8. Liaise with SA2


VODUZ


VODUZ

Thank you

mario.reale@garr.it
davide.vaghetti@garr.it

GÉANT

Networks · Services · People

www.geant.org

SPARE SLIDES

GEANT NREN Survey on Cloud IdP

- Survey on Cloud IdP circulated to the Fed Operators list - early October
- Aimed at better understanding the Campus IdP problem definition: Community Requirements, Potential for Cloud-based Campus IdP solutions
- Got 17 answers from the following NRENs:

  ARNES, CANARIE, CESNET, GARR, GRNET, GEANT, HEANet, Internet2, JANET,

  RedIRIS, RENATER, SURFnet, SWITCH

- **A relevant outcome:**

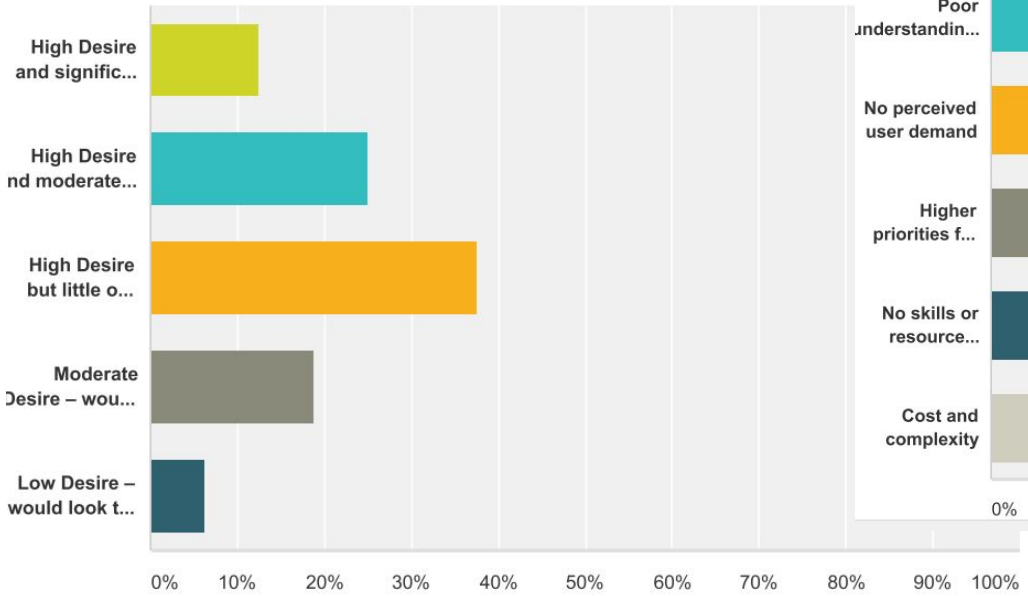
  there is high desire but little or none internal ability for institutions to deliver identity provider services to their users

  (~ 40 % of answers)

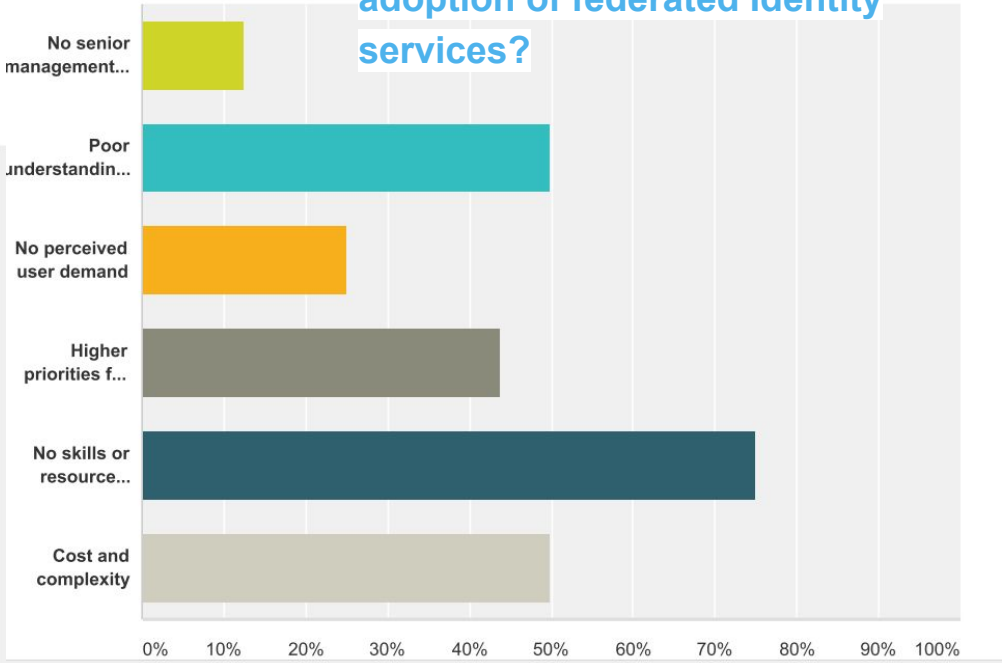
- Survey Still online on http://tinyurl.com/z33jond
- Detailed answers report available at http://tinyurl.com/zdr9gf5

Survey Results

Q2:What is the desire and ability of institutions to deliver Identity Provider services

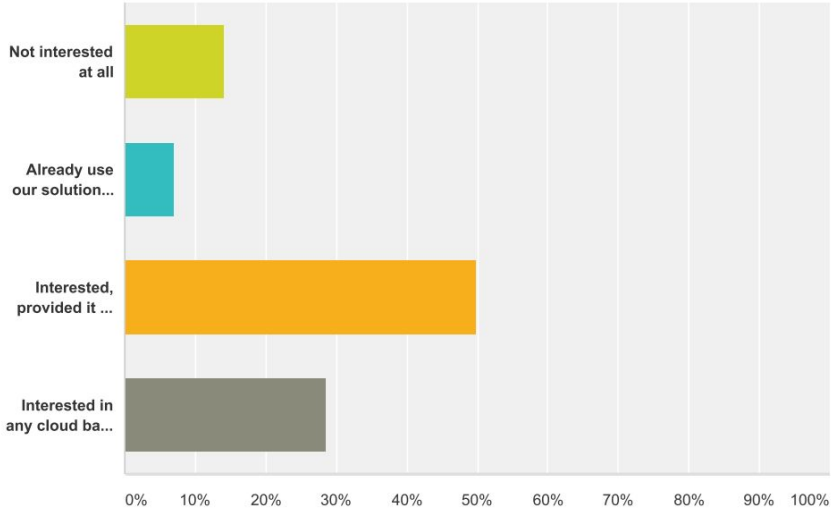


Q3:What are the main barriers to adoption of federated Identity services?

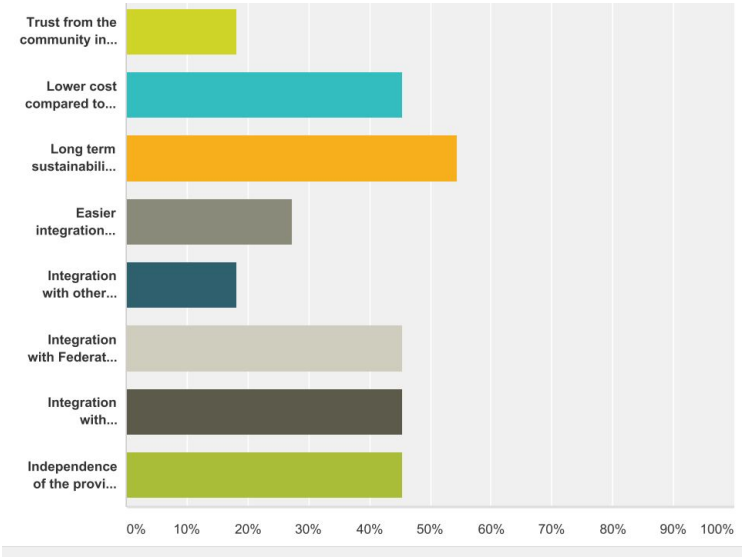


Survey Results

Q8: How interested would your individual institutions be in outsourcing the provisioning of a local IdP to a managed service provider?



Q11:Principle advantages of a GEANT provided and managed Cloud based solution for the IDP?



Market Analysis for Supporting Services for Campus IdPs Deliverable

D9.1 - Market Analysis for Supporting Services for Campus Identity Providers - due by end of December:

Deliverable needs to be completed in its overview of current Cloud IdP solutions by NRENs

Pending

- FInalize description of Cloud IDP offers by some NRENs (ARNES, JISC, HEANet, SWITCH...)
- Injection of outcome of Cloud IDPs NRENs survey
- Complete the use cases requirements for Campuses and Federations with and without FaaS
- GEANT role section

Currently in progress at

Delayed by 1 month due to need to define boundaries towards AARC activities on Cloud IdP

Example Feature List and Details

Release	Feature	Description	Benefit	Status
Release of Feature	Short Feature Tittle	Short description of the feature	A description of benefits of the feature	**Committed -** will be in this release **Planned** – is planned to be in this release but work required to move it to being **Committed** **Potential** – early stages of planning and more work to be done to move it to the **Planned** stage
V3.1	Security enhancements	Password pinning by securing a hash of private key using OTP fuses.	Improved security of private keys.	**Committed**