GÉANT
Networks • Services • People

# Cryptech HSM

Activity kick-off, 19.02.2019

Public

www.geant.org

# Agenda

- Introduction
- The A-Team
- About Cryptech HSM
- Activity goals
- Tools
- Next steps

# The A-Team

| Name | Role | Subject |
|---|---|---|
| Brook Schofield | Magnum | Activity lead 1/2 |
| Leif Johansson | P.I. | Activity lead 2/2 |
| Niels van Dijk | Mentor | Advise |
| Michael Schmidt | Scrum Master | Process support |
| Branko Marovic | Team Member | ? |
| Alan Lewis | Team Member | ? |

# About HSM

- Hardware Security Module (HSM)
  - A HSM is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing.
  - Commercial offerings are very expensive
  - Most GÈANT T&I services rely on cryptographic keys
- Cryptech HSM
  - Open-source hardware cryptographic engine that can be built by anyone from public hardware specifications and open-source firmware
  - First implementations available to test GÈANT use cases
  - Very new, chance to influence as early adopter
- https://cryptech.is
- https://docs.google.com/document/d/1DwpIEqxXAdj7h1Ec2-aaX7JYN_EG7lVOHU3fW5Igt6s/edit?pli=1#heading=h.4l7dmzp9v58s

# Activity goals

- Investige Cryptech HSM modules
- Gather community use cases
- Match requirements and identify improvements
- Identify interfaces to other services
- Examine opportunities for HSM as a service

# Tools

- Action items in Trello (https://trello.com/b/386wEkfc)
- Source Code in GitHub (https://github.com/GEANT)
- Documentation in Confluence (https://wiki.geant.org/x/D3JwBg)
- Communication
  - Informal via Slack (cryptech-hsm)
  - Formal via mailing list (hsm-incubator@list.geant.org)

# Next Steps

- Finalise project description (Brook, Leif)
- Deep dive Cryptech HSM (Brook, Branko, Alan)
- Prepare the Activity Backlog (Brook, Leif, Michael)
- Scrum training & sprint planning (05./06.03)

TRUST & IDENTITY INCUBATOR

GÉANT
Networks • Services • People

# Thank you

Any questions?

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 3 project (GN4-3).
The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation
programme under Grant Agreement No. 856726 (GN4-3).