PAUL SCHERRER INSTITUT

PSI

Real-time workflow and application with high performance by cloud security enabled HPC for on-demand activity calculations for HIPA

Mei-Chih Chang, PSI

@hpc-ch forum on User-Centric View on HPC, 6 Oct. 2022

Vis-aS toolkit project

- A web-cloud application to calculate and visualize the amount of activated material after the final shutdown of the HIPA facility.

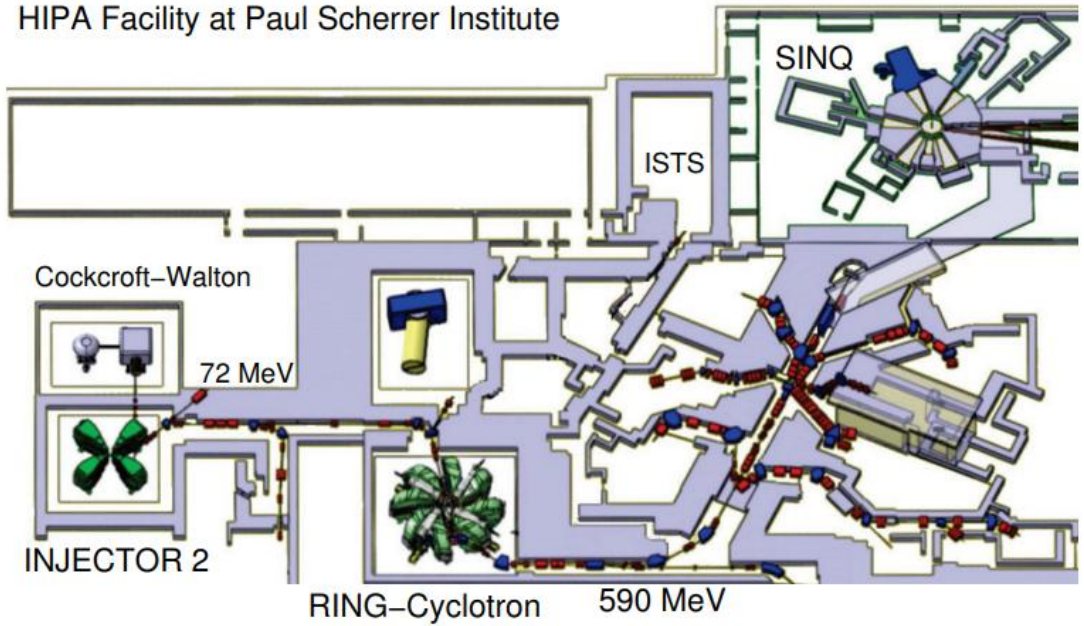
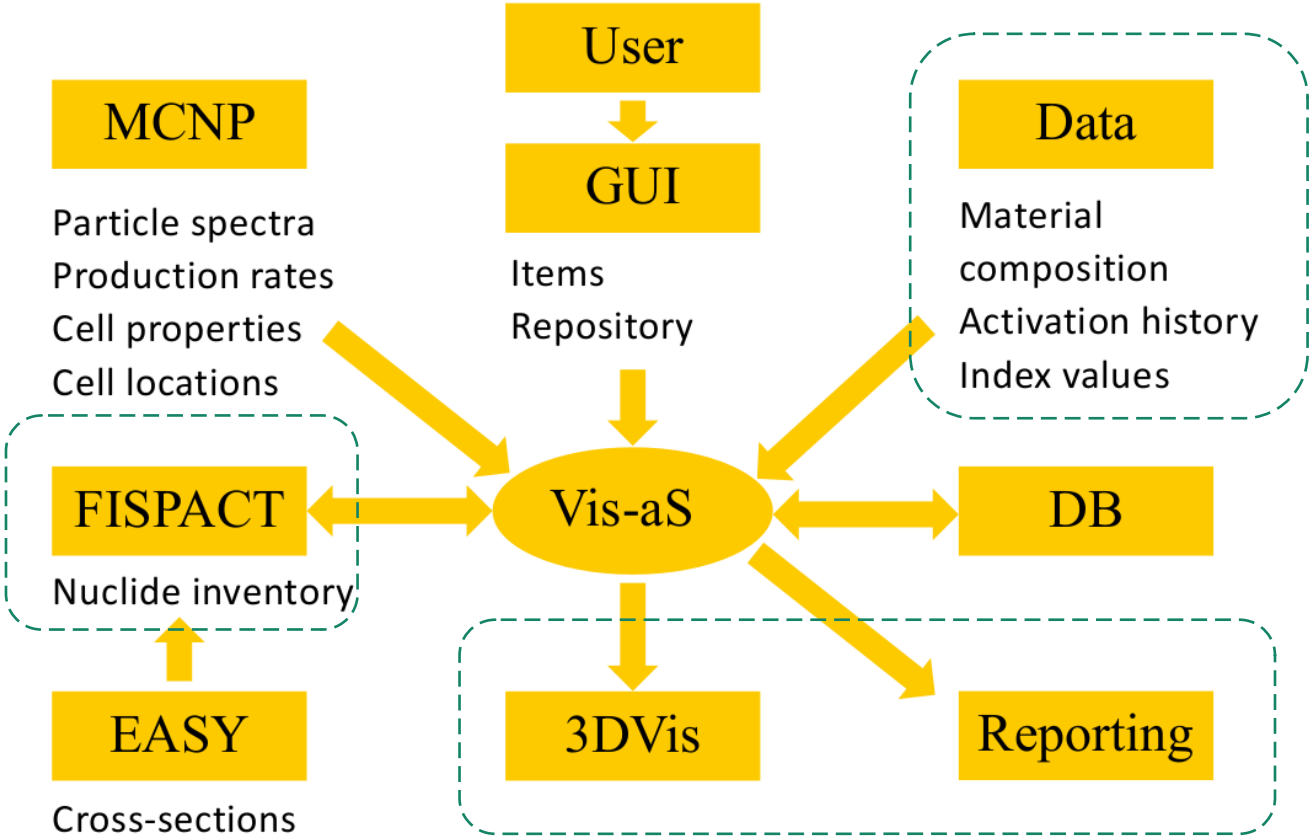


Figure from C. Baumgarten [1]

Diagram of the Vis-aS Framework



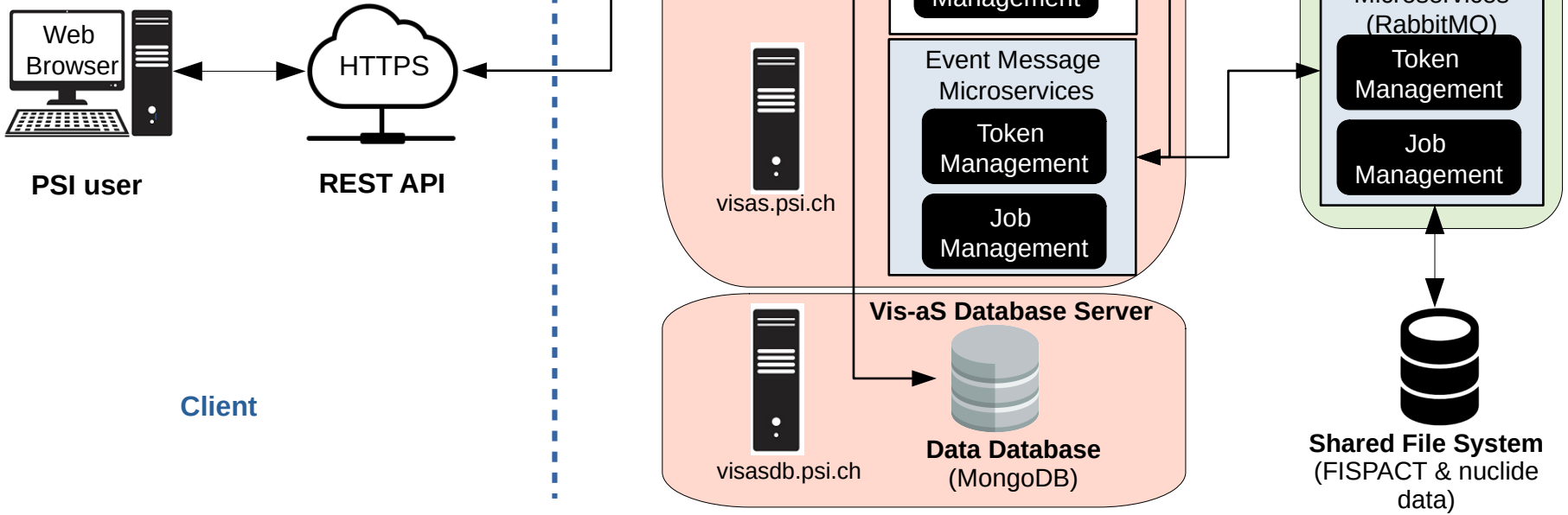
Vis-aS requirement & challenges

- Major Requirements
  - on-demand activity calculations
    - Real time workflow runs calculations on high performance HPC.
    - The HPC system for this project is Merlin HPC cluster with 23 nodes & 44 cores/per node.
  - Sensitive data is needed to be kept secure.

- Challenges
  - Real time workflow should run calculations secure specially cross the network on HPC.
  - Secure workflow should not reduce the overall performance on HPC.
  - Data should be kept secure.

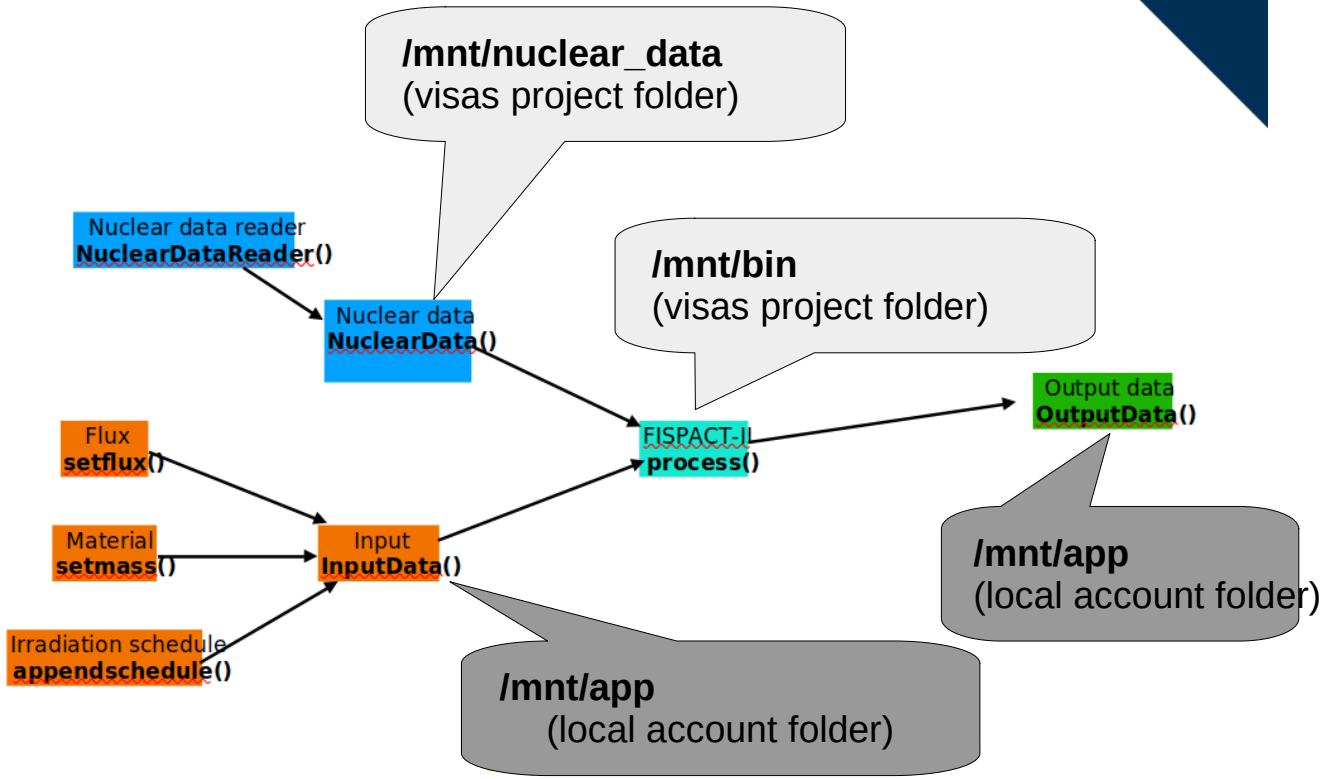
PAUL SCHERRER INSTITUT

Architectural Design

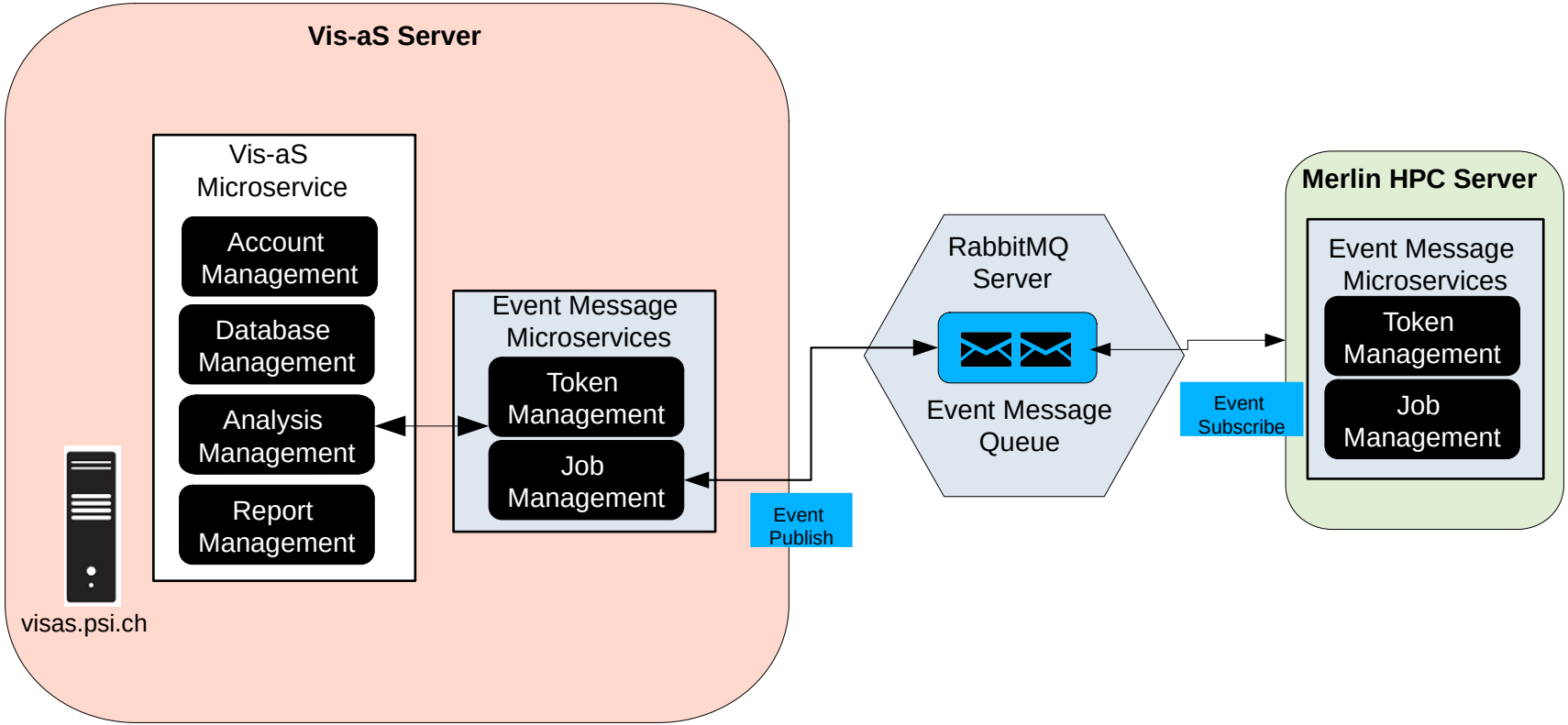


FISPACT API data flow

- Fispact program&library
- Nuclear data files
- **Input data files**
  - **(1)combine.i** – settings UI
  - **(2)files** – fixed
  - **(3)fluxes** – specturm database selec
- **Output files**
  - (1) **Combine.ou** saved in DB



Event Message based Micro-service (RabbitMQ)

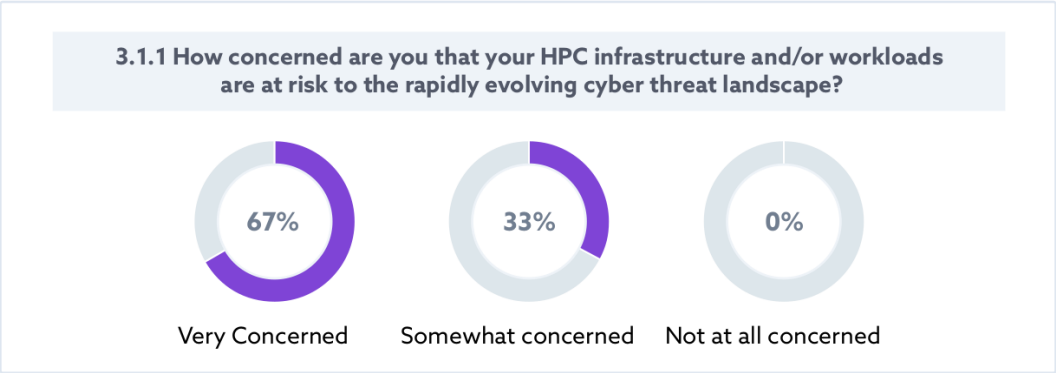


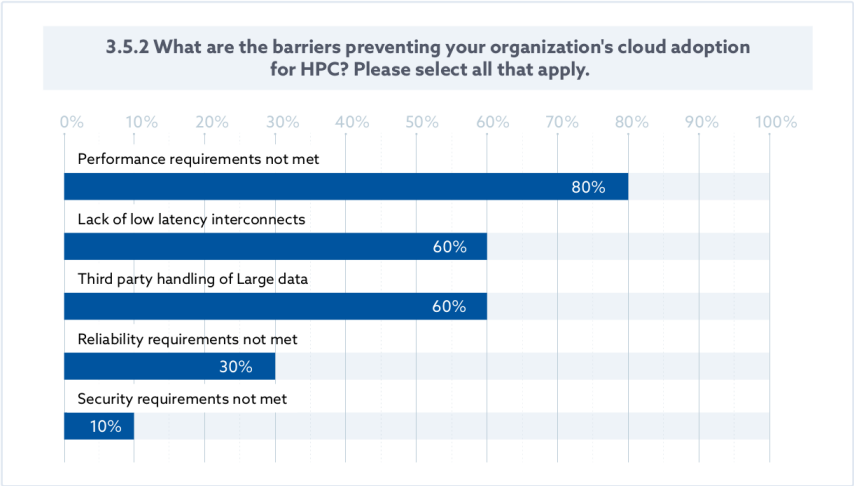
Cloud-based HPC’s security challenges

- Major Trends
  - The cloud is bringing supercomputing into the mainstream [2].
  - when cloud-based HPC is rapidly evolving, and so is security [3].

- Challenges
  - A survey [3] shows that 67% of respondents are “very concerned” about that their HPC infrastructure and workloads are at risk to the rapidly evolving cyber-threat landscape.
  - A dominating concern specific to the HPC sector impeding cloud adoption is performance trade-off (80%) [3].
  - Data privacy & security are other key factors for organizations deciding not to move to the cloud [4].

Cloud-based HPC's security challenges





Figures are from Cloud Security Alliance [4]

Our Contributions

- Improve the overall performance of workflow on HPC
  - Simplified TLS 1.3 handshake & record protocol to reduce the overhead of generations of tokens and improve the protection of replay attack.

- Support Data privacy & security
  - Different level of user accessibility and data tracking system to improve the data privacy.
  - Data is still kept even if the user deletes it.

Job Submission Workflow

I. **Handshake and record protocol setup**
II. Create user folder in Merlin (Utilities Queue)
III. Transfer file (Upload Queue) :
   - **combine.i & files & fluexes**
IV. Submit Job – sbatch file (Job Queue)
   - includes fispact & parse combine.out file
V. Transfer file (Download Queue)
   - **Parsed combine.out file**
VI. Save parsed .out in visas DB server (**Nuclide Inventory**)

Simplified TLS 1.3 Handshake & Record Protocol

- JWT Authentication token
  - The communication between Vis-aS and Merlin server needs the authentication token for Merlin server to verify the valid user request from Vis-aS server
  - Most of workflow protocol uses the short expired token to reduce the chance of token compromised
  - However, it will cause overhead token generations for a long job submission.
  - Therefore, Vis-aS proposes to use simplified TLS 1.3 handshake & Record protocol
    - Having a long expired token
    - Prevent the replay attack

Vis-aS's Simplified TLS Protocol

CLIENT
(Vis-aS)

SERVER
(Merlin)

Client Key Exchange Generation

Server Key Exchange Generation

Client Hello

- Nonce number
- Public key

Server Hello

- Nonce number
- Public key

Authentication

Encrypted user credential

Finished

Valid user?

Finished

Handshake Protocol

Record Protocol

Application Data

Nonce number with counter

Application Data

Valid request?

Simplified TLS 1.3 Handshake & Record Protocol

- Handshake Protocol
  - TLS 1.3 protocol is an improved version of TLS 1,2 with simpler handshake protocol.
  - It is good for a long time execution [5].
- Record Protocol
  - During the long time period of job submission workflow, the client (vis-as server) will send the nonce with counter number, therefore, they are used only once number.

Data Privacy & Security

- Three principles of data security
  - Data Confidentiality
    - Authentication
    - Access control: user has different level of role – power user & normal user
  - Data Integrity
    - Data version tracking system: when data is modified, the new version of data will be setup
  - Data Availability
    - Data is not deleted when the user deletes it. It will be kept in the database until the admin removes it forever.
    - Data can be recovered when some data was marked as lost/deleted.
- Data privacy: needs to improve in the next version

Short Demo

- User logins with different roles
- Importing data into database
  - Material, Spectrum, Activation History
- Create Item & Repo
- Run Repo
- Save nuclide inventory result to database

Team members of Vis-aS project

Vis-aS project is developed by Accelerator Operation and Development (ASA) and supported by Information Technology (AIT) and Radiation Safety and Security (ASI) as advisory.

- Project leader
  - Talanov Vadim, Dr. (ASA)
- Members
  - Chang Mei-Chih, Dr. (ASA)
  - Besana Maria Ilaria, Dr. (ASA)
- Advisory board
  - Kiselev Daniela, PD Dr. (ASA)
  - Walter Nick, Dr. (ASI)
  - Bücklers Thomas (AIT)
  - Solca Jan, Dr. (AIT)

References

[1] , “BEAM BASED CALIBRATION MEASUREMENTS AT THE PSI CYCLOTRON FACILITY,” Proceedings of Cyclotrons 2016, Zurich, Switzerland, 2020.
[2] J. Poort, “How Cloud-Based Supercomputing Is Changing R&D” Report: Harvard Business Review – Data Magement, Nov. 29, 2021.
[4J A. Howard, G. Sin Ong, “Survey Report - Security Practices in HPC & HPC Cloud” Report: Cloud Security Alliance, 2020.
[5J M. Fischlin, F. Günther, “Replay Attacks on Zero Round-Trip Time: The Case of the TLS 1.3 Handshake Candidates,” the proceedings of the 2nd IEEE European Symposium on Security and Privacy (EuroS&P 2017), Paris, France, 2017.

PAUL SCHERRER INSTITUT

PSI

Thank you