

# WebAuthN (TIM)

Sprint demo #6 (Final) – 30<sup>th</sup> June 2020

**Ondrej Ernst, Pavel Brousek**

Q2 2020

Public

[www.geant.org](http://www.geant.org)





# Aims and Objectives

- enable major parts of the T&I community to use state-of-the-art multi-factor authentication
- contribute to the SimpleSAMLphp WebAuthN module
- develop a new custom module for SATOSA



# What did we do?

- contribution to the SimpleSAMLphp WebAuthN module
  - Standalone registration page ([#30](#))
  - Toggle MFA based on user attribute ([#28](#))
  - UI improvement ([#29](#))



# What did we do?

- develop a new custom module for SATOSA
  - microservice for SATOSA
    - triggers WebAuthN
      - enable/disable per service provider
      - handles REFEDS MFA profile
  - flask WebAuthN module
    - performs WebAuthN authentication
    - token management (during login)
    - temporarily disable MFA



# How did we do it?

- contribution to the SimpleSAMLphp WebAuthN module
  - a. find bugs, possible improvements and new features
    - GitHub issues
    - code inspection
    - test deployment
  - b. prioritize
  - c. code
  - d. submit PR to upstream repository



# How did we do it?

- develop a new custom module for SATOSA

- a. design

- similar to SimpleSAMLphp WebAuthN module
    - SATOSA limitations (no GUI)

- b. technologies

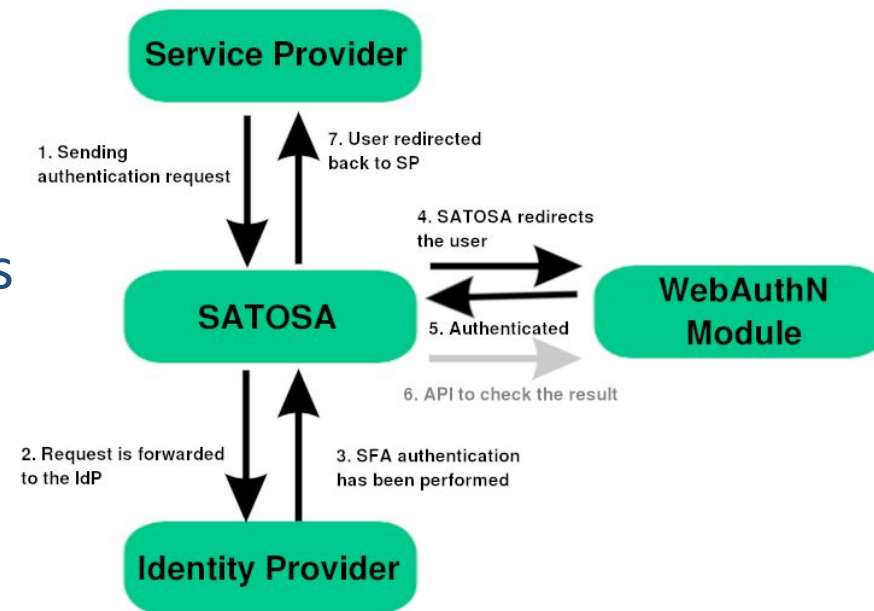
- both parts in Python

- c. implement fundamental features

- WebAuthN authorization
    - token management

- d. improve

- nicer user interface
    - more configuration options





# What was achieved

- contribution to the SimpleSAMLphp WebAuthN module
  - accepted (merged) by SSP developers
- WebAuthN for SATOSA
  - ready for use
  - published on GitHub
  - eduTEAMS are interested



# Demo

- videos





# What did we learn?

- SimpleSAMLphp WebAuthN module
  - quite mature and ready for most use cases
- WebAuthN for SATOSA
  - separate module (forced by SATOSA design)
    - proxies/IdPs may share WebAuthN server
    - can be used by other software than SATOSA
- advanced token management
  - out of scope for a WebAuthN module
  - privacyIDEA might be a solution



## How do I find out more?

- SimpleSAMLphp WebAuthN module:  
<https://github.com/simplesamlphp/simplesamlphp-module-webauthn>
- (SATOSA) WebAuthN module:  
<https://github.com/CESNET/satosa-module-webauthn/>
- satosa-microservice-webauthn:  
<https://github.com/CESNET/satosa-microservice-webauthn/>



# Looking ahead

- WebAuthN module
  - offered to eduTEAMS
  - allow multiple proxies to share the module
  - standalone registration
  - different token storage (e.g. IMS)
- token management
  - manage tokens for all authentication methods



# Thank you

[www.geant.org](http://www.geant.org)



© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).  
The research leading to these results has received funding from  
the European Union's Horizon 2020 research and innovation  
programme under Grant Agreement No. 731122 (GN4-2).