Trust & Identity Incubator
WebAuthN

Ondřej Ernst

Sprint Demo, 07-30-2019

www.geant.org

Overview

WebAuthN
- SimpleSamlPHP WebAuthN
- Python version for Satosa

My tasks for the first demo have been:
- Create a testing environment for the WebAuthN
- Study the code in order to better understand it
- Add an attribute that determines whether to trigger the WebAuthN or not

Achievements

- The testing environment has been set
    - Debian 10
    - Apache/2.4.38
    - PHP 7.3.11
    - mariadb Ver 15.1 Distrib 10.3.18-MariaDB
    - SimpleSamlPHP v1.18.2
- I understand the code and other parts of the project better
- Attribute has been added
    - Compatible with the previous version

GÉANT

Authsource

```
$config = [
    'example-userpass' => [
        'exampleauth:UserPass',
        'student:s' => [
            'uid' => ['student'],
            'displayName' => ['jmeno'],
            'eduPersonAffiliation' => ['member', 'student'],
            'toggle' => ['true'],
        ],
    ],
```

🚀 Configuration

```
100 => ['class' => 'webauthn:WebAuthn',
        'store' => [
                   'webauthn:Database',
                   'database.dsn' => 'mysql:host=localhost;dbname=fido2',
                   'database.username' => 'webauthn',
                   'database.password' => 'password',
                   ],

        'attrib_username' => 'uid',
        'attrib_displayname' => 'displayName',
        'scope' => 'ip-78-128-251-71.flt.cloud.muni.cz',
        'request_tokenmodel' => true,
        'default_enable' => false,
        'force' => false,
        'attrib_toggle' => 'toggle',
        'use_database' => false,
        ],
```

Configuration

2FAEnabled	default_enable=true	default_enable=false
user not in DB	✓	✗
FIDO2Enabled in DB	✓	✓
FIDO2Disabled in DB	✗	✗

		force=false		force=true
	2FAEnabled	default_enable=true	default_enable=false	
use_database=true	user not in DB	✓	✗	
	FIDO2Enabled in DB	✓	✓	
	FIDO2Disabled in DB	✗	✗	
use_database=false	toggle not set or false	✓	✗	✗
	toggle true	✗	✓	✓

Status and next steps

☑ Testing environment

☑ Allow per-user authentication based on attributes

☐ Implement a standalone registration page

Thank you

Any questions?

www.geant.org