Notify me: Updates about mytoken

Gabriel Zachmann, Marcus Hardt

Oct 2024

Recap mytoken

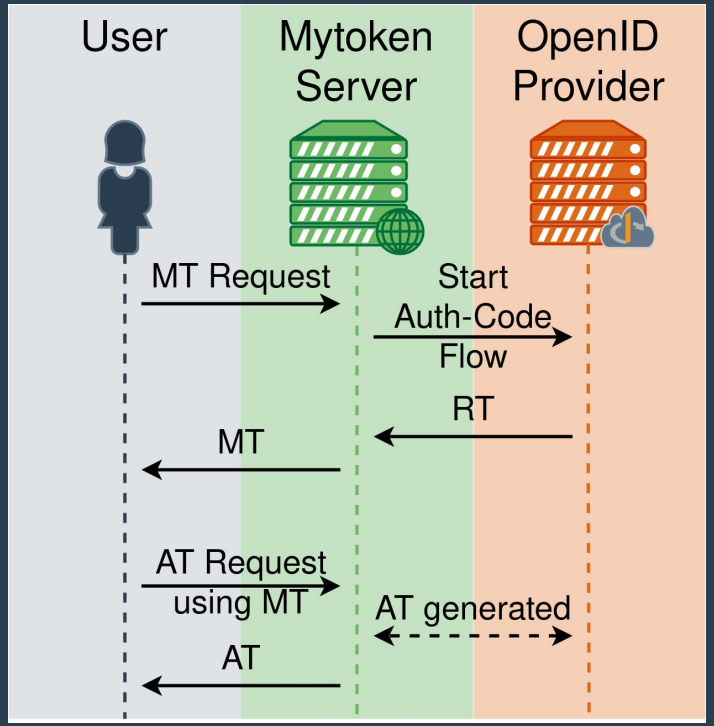
- Goal: Ensure availability of Access Tokens at any time
  - Allow short AT lifetime
  - **No user interaction**
  - On any remote machine (Bearer Tokens)
  - But secure
- Just like **oidc-agent**, but mostly server-side
  - (i.e. Refresh Token stored server-side)
  - Access protected via mytoken token (which is given to the user)
- **mytoken** tokens are essentially “full of policies”
  - Capabilities
  - Restrictions

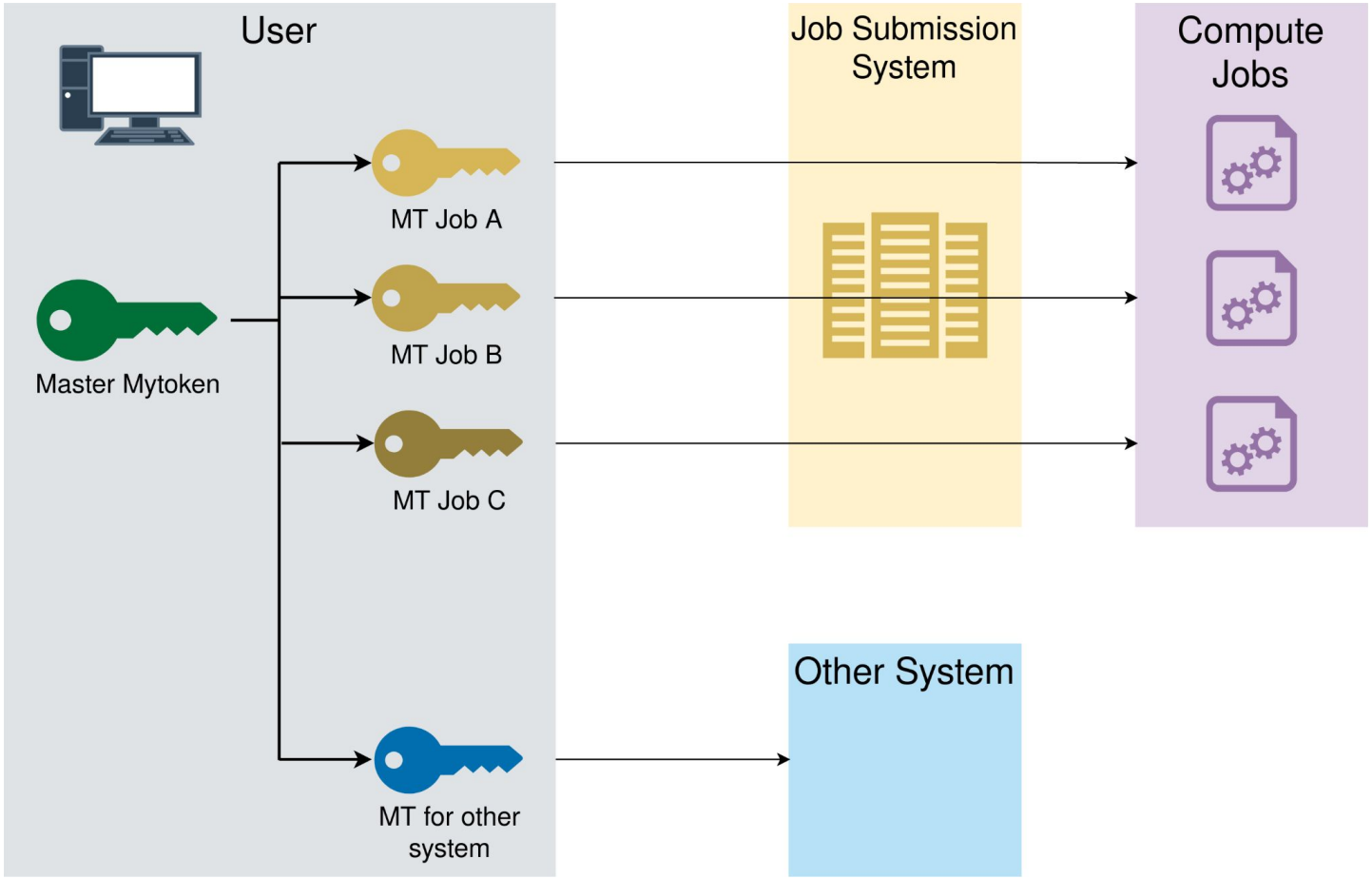
Basic Concept

- Similar concept to *myproxy* (i.e. secure storage of credentials)
- Mytoken can be used as a Bearer Token that can be passed around, e.g. to obtain ATs
- Mytokens can be restricted (e.g. IP, aud)

Mytoken can be created:

- From Authorization Code Flow
- From an existing Mytoken
- Via SSH





mytoken

Dedicated Mytoken for specific usage can be easily created from a Master Mytoken

Restrictions

- Using Bearer Mytokens as securely as possible
- Usage of each Mytoken can be restricted independently
- Very flexible approach
  - Different restriction dimensions (extensible)
  - Multiple privilege stages in one token possible

Restrictions

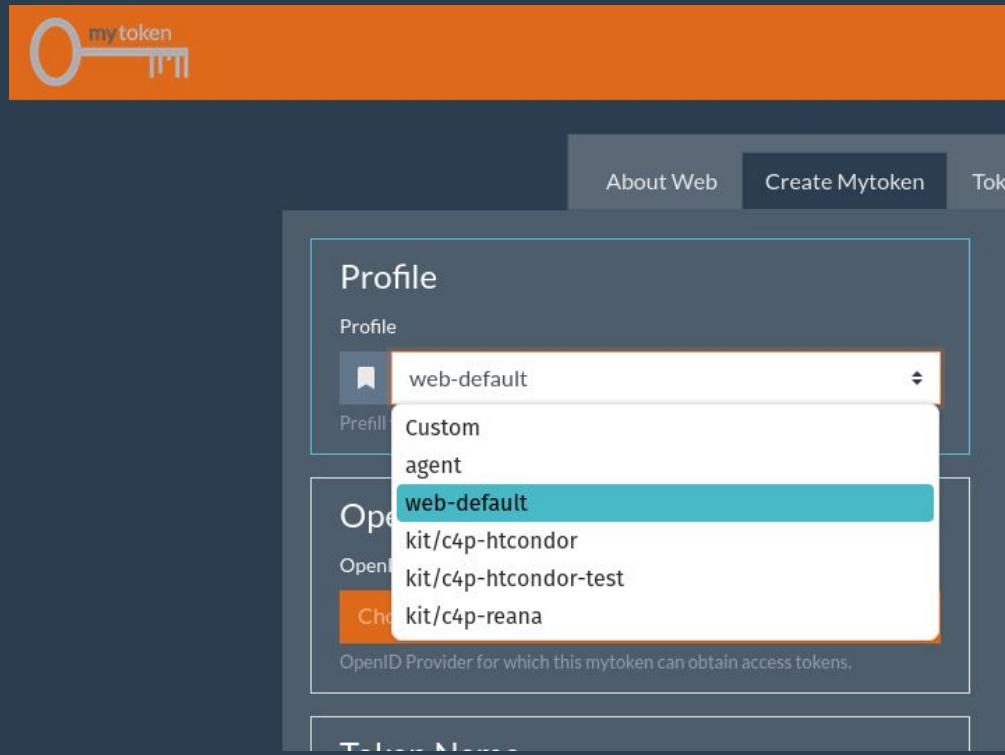
- Using Bearer Mytokens as securely as possible
- Usage of each Mytoken can be restricted independently
- Very flexible approach
  - Different restriction dimensions (extensible)
  - Multiple privilege stages in one token

- Time
  - **exp**: Only before this time
  - **nbf**: Only after this time
- Location
  - **ip**: Only from these IPs / Subnets
  - **geoip_allow**: Only from these countries
  - **geoip_disallow**: Not from these countries
- OIDC
  - **scope**: Only ATs with these scopes
  - **audience**: Only ATs with these audiences
- Usages
  - **usages_AT**: Only X ATs can be obtained
  - **usages_other**: Only X other actions can be performed

Updates

Updates - Profiles & Templates

- Pre-configured parameters
- Templates for
  - Restrictions
  - Capabilities
  - Rotation
- Profile for everything combined



Updates - Enforced Restrictions

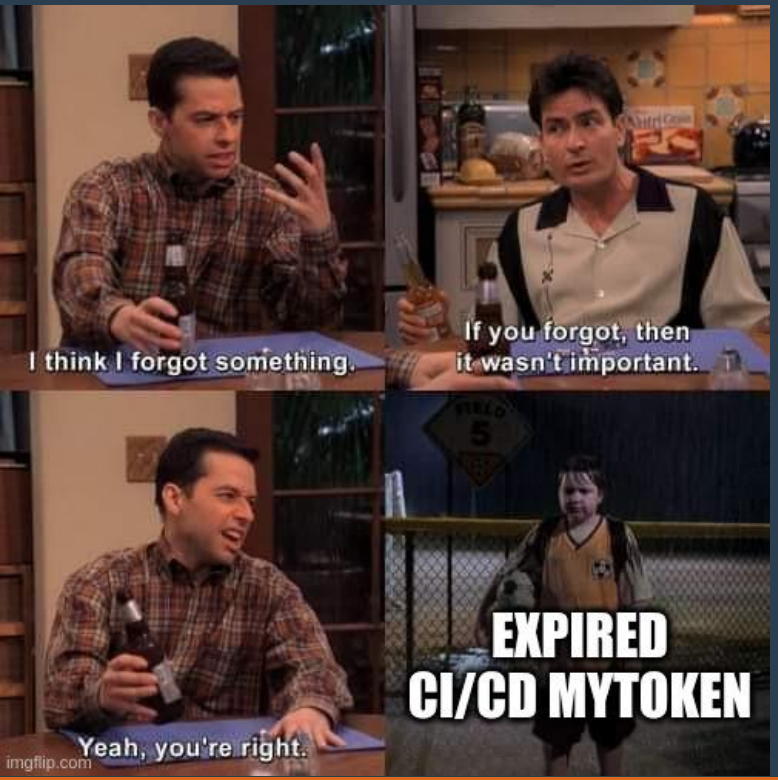
- Depending on **User Attributes** different *Restriction Templates* can be **enforced**
- Allows OP to have (some) control over which users can obtain less/more powerful mytokens

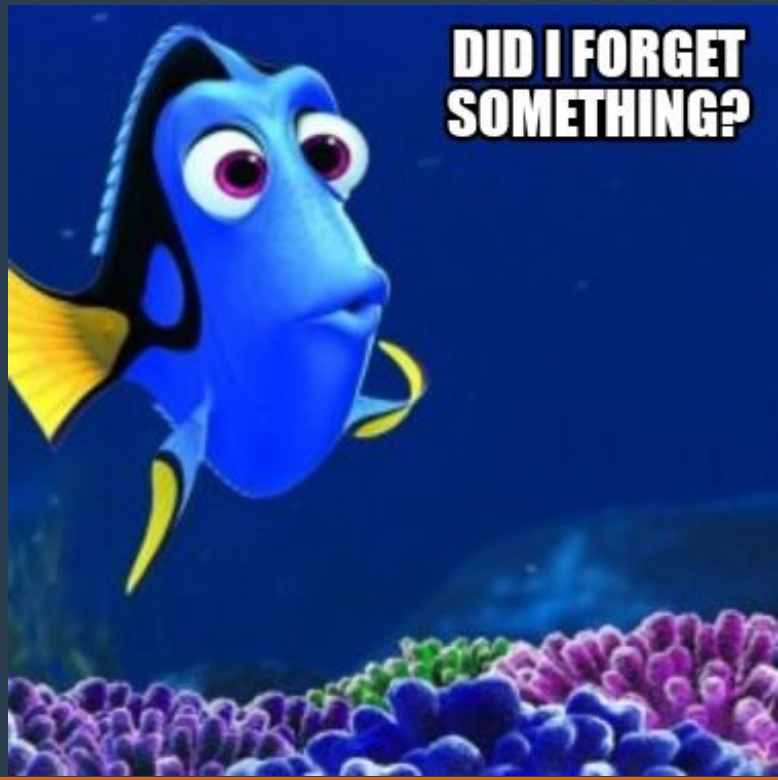
Idea:

- If users passed an online course they can obtain more powerful tokens

```
enforced_restrictions:
  claim_sources:
    userinfo: "eduperson_entitlement"
  forbid_on_default: true
  help_html_file: /mytoken/help.html
  default_template: web-default
  mapping:
    "urn:mytoken:super": super
    "urn:mytoken:advanced": advanced
    "urn:mytoken:base": base
```

Keep forgetting to renew your mytokens?





Updates - Notifications

- Add your important mytokens to your calendar and get reminders.
- Subscribe to email notifications.
  - Expiration
  - AT Creation
  - Subtoken Creation
  - Used to change settings
  - Security
    - Used from previously unknown IP
    - Blocked because of Capabilities
    - Blocked because of Restrictions
    - *Usage of a revoked token*
- User-wide (for all mytokens)
- For individual mytokens

DEMO

https://mytoken.data.kit.edu/

References

Demo Instance: https://mytoken.data.kit.edu

Production Instance: https://mytok.eu

Documentation: https://docs.mytok.eu

Contact: m-contact@lists.kit.edu

Github: https://github.com/oidc-mytoken

Backup Slides

```
{
  "ver": "0.7",
  "token_type": "mytoken",
  "iss": "https://mytoken.data.kit.edu/",
  "sub": "eeviiW0Jfoobarfoobarfoobarza9BcctBABF/mJyow=",
  "seq_no": 1,
  "name": "Demo Job",
  "aud": "https://mytoken.data.kit.edu/",
  "oidc_sub": "user@egi.eu",
  "oidc_iss": "https://aai.egi.eu/auth/realms/egi",
  "capabilities": [
    "AT",
    "tokeninfo"
  ],
  "exp": 1735400000,
  "nbf": 1734500000,
  "iat": 1727861635,
  "auth_time": 1727861635,
  "jti": "f5be2554-623b-4a84-becc-58937f827674",
```

```
  "restrictions": [
    {
      "nbf": 1734500000,
      "exp": 1734400000,
      "scope": "compute.create",
      "audience": [
        "fedcloud"
      ],
      "geoip_allow": [
        "BE"
      ]
    },
    {
      "nbf": 1734500000,
      "exp": 1734400000,
      "scope": "storage.read",
      "audience": [
        "storage-side"
      ]
    },
    {
      "nbf": 1735500000,
      "exp": 1735400000,
      "scope": "storage.write",
      "audience": [
        "storage-side"
      ]
    }
  ]
}
```