AAI evolution

A. Forti

GridPP42

23 April 2019

Beyond X509

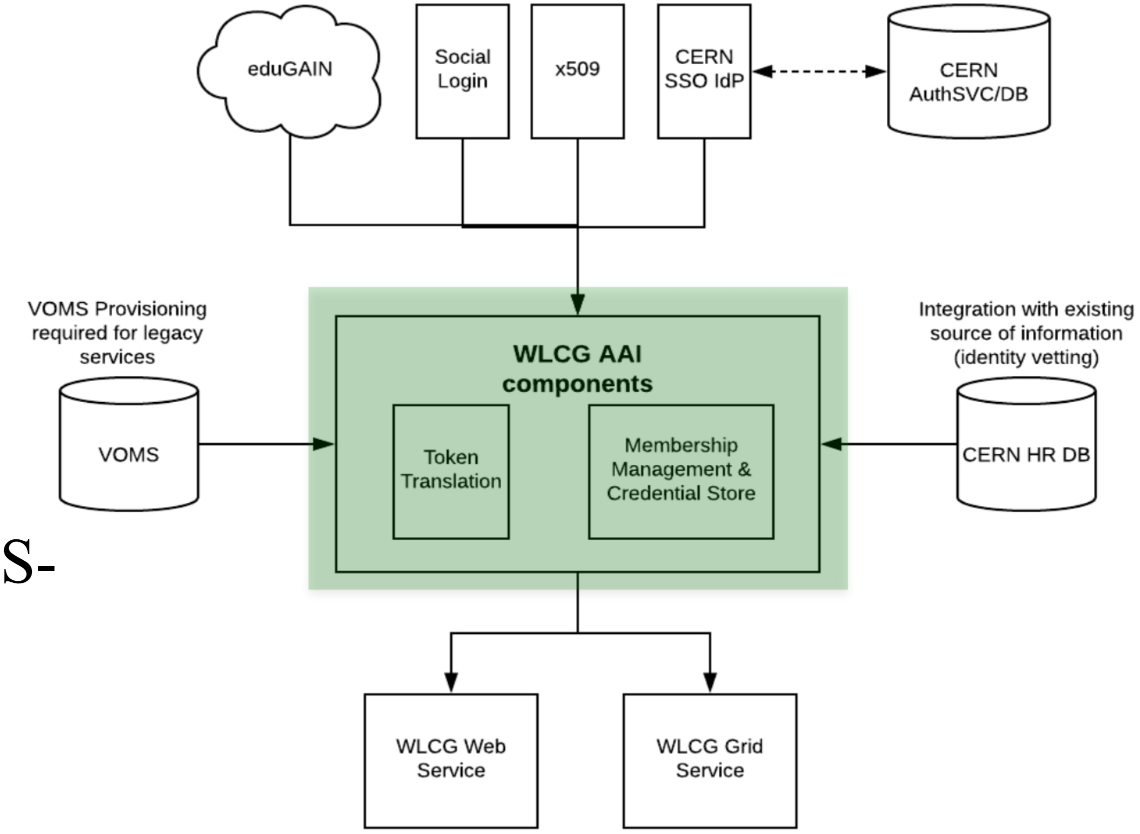
- Evolution towards federated identities
  - Same authentication for different authentication managements
- Evolution of AAI in the rest of the world
  - Oauth third party authorization protocol
    - Looks new to us but ~12 years old
- WLCG Authz WG recommend a common strategy
  - Remove the need for users to manage x509 certificates
  - Replace VOMS-Admin
  - Devise tokens schema
- Proof of concept (DOMA)
  - Enabling token based authorisation

Current limitations

- Usability
  - X.509 certificates are difficult to handle for users
  - VOMS does not work in browsers
- Inflexible authentication
  - Only one authentication mechanism supported: X.509 certificates
  - Hard to integrate identity federations
- Authorization tightly bound to authentication mechanism
  - VOMS attributes are inherently linked to an X.509 certificate subject
- Home grown solution
  - Developed our own standard, ad-hoc libraries and central services
    - Very difficult to integrate with new type of services

Evolution

- Multiple authentication mechanisms
- Persistent, VO-scoped user identifier
- Exposes identity information, attributes and capabilities to services
- Integrates with existing VOMS-aware services
- Supports Web and non-Web access, delegation and token renewal


eduGAIN
Social Login
x509
CERN SSO IdP
CERN AuthSVC/DB
VOMS Provisioning required for legacy services
VOMS
WLCG AAI components
Token Translation
Membership Management & Credential Store
Integration with existing source of information (identity vetting)
CERN HR DB
WLCG Web Service
WLCG Grid Service

WLCG AuthZ WG

Evolution (2)

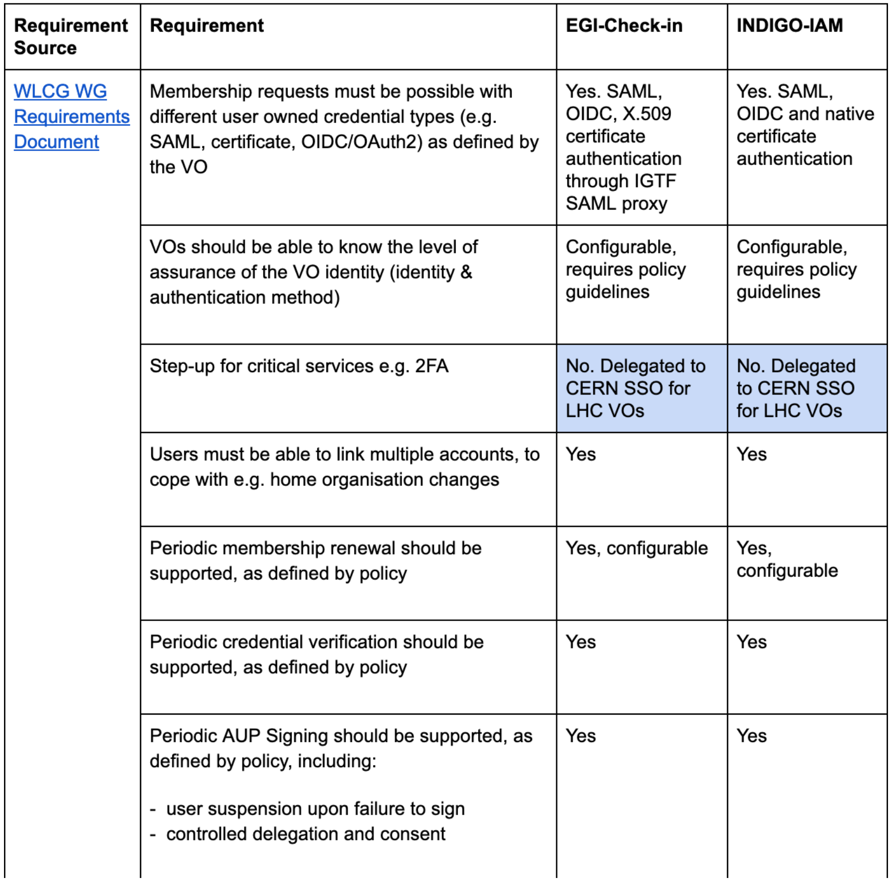
- Legacy VOMS aware services will be supported
  - token → VOMS proxy translation service
- New services better integrated with Oauth2.0 type of authorization can also be supported
  - Openstack
  - Kubernetes
  - Jupyterhub
  - …..
- Some grid services Authentication will be integrated with CERN HR DB
  - Not all the components re-usable by other communities

Another difference

- VOMS is identity/role based authorization
  - The proxy brings information about attribute ownership (e.g., groups/role membership), the service maps these attributes to a local authorization policy.
  - Policy managed at service level (agreed with the VO)
- Token have capability based authorization:
  - The token brings information about which actions should be authorized at a service, the service needs to understand these capabilities and honor them.
  - The authorization policy is managed at the VO level

Two solutions

- Two sw stacks identified as candidates
  - EGI Check-in
  - Indigo IAM
- Both satisfy 90% of the list of 22 requirements
- Both will be supported in the future.
- Initial tests with EGI Check-in not straightforward.
  - Haven't tried with indigo IAM

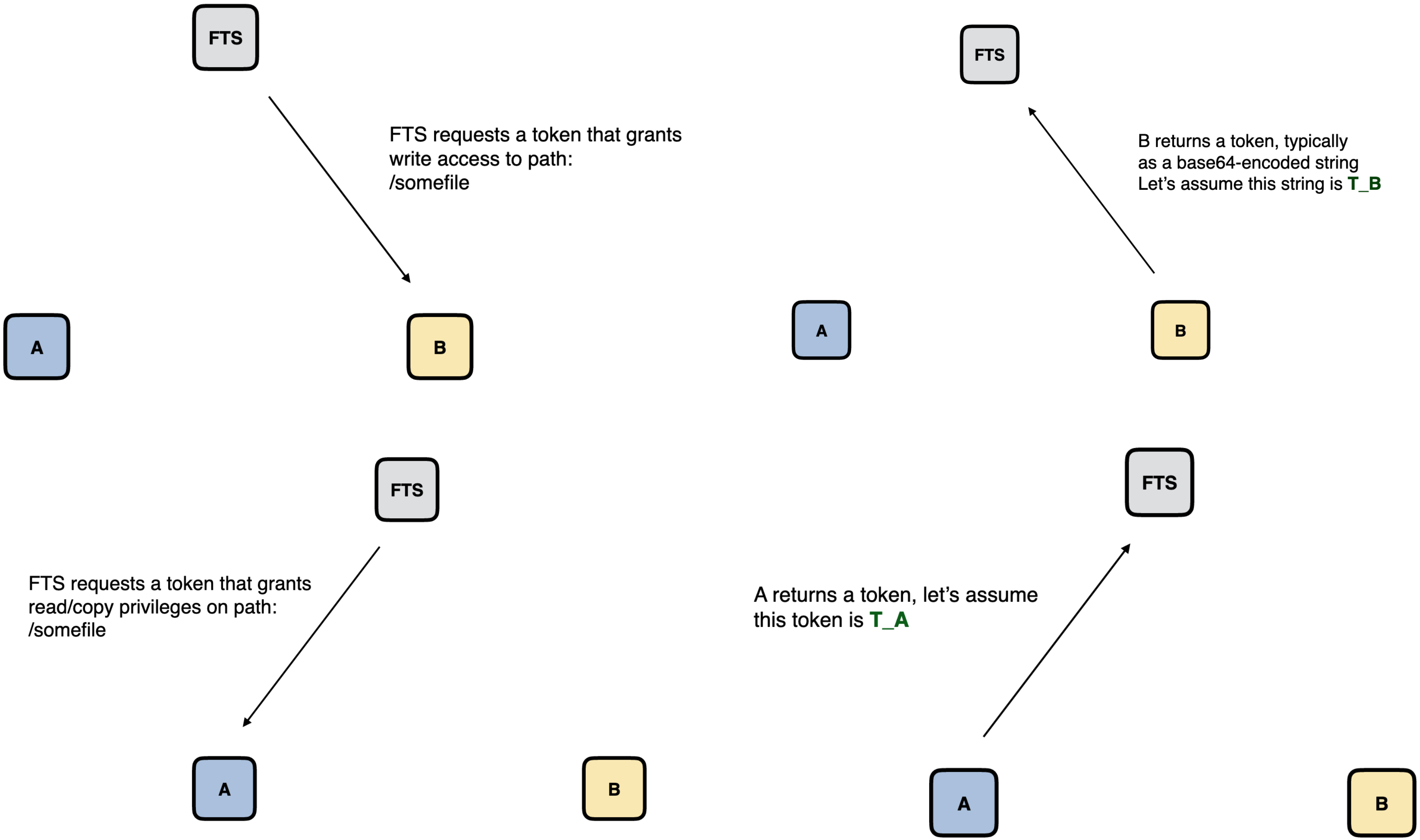


Requirement Source	Requirement	EGI-Check-in	INDIGO-IAM
WLCG WG Requirements Document	Membership requests must be possible with different user owned credential types (e.g. SAML, certificate, OIDC/OAuth2) as defined by the VO	Yes. SAML, OIDC, X.509 certificate authentication through IGTF SAML proxy	Yes. SAML, OIDC and native certificate authentication
	VOs should be able to know the level of assurance of the VO identity (identity & authentication method)	Configurable, requires policy guidelines	Configurable, requires policy guidelines
	Step-up for critical services e.g. 2FA	No. Delegated to CERN SSO for LHC VOs	No. Delegated to CERN SSO for LHC VOs
	Users must be able to link multiple accounts, to cope with e.g. home organisation changes	Yes	Yes
	Periodic membership renewal should be supported, as defined by policy	Yes, configurable	Yes, configurable
	Periodic credential verification should be supported, as defined by policy	Yes	Yes
	Periodic AUP Signing should be supported, as defined by policy, including: - user suspension upon failure to sign - controlled delegation and consent	Yes	Yes

Tokens on grid services

- Storage
  - HTTP protocols on grid storage
  - Development carried out to do TPC with token authorization rather than X509 delegation
    - Involved also a large amount of work for token definition
- Computing Elements
  - HTCondor-CE added 4500 lines of code 2 weeks ago for token support
  - ARC-CE now involved in discussions in the WLCG AuthZ TF for the tokens schema.
- Rucio
  - Working on implementing tokens authorization
- Other experiment services
  - Assumption is that they'll work with proxies.

TPC http tokens authorization



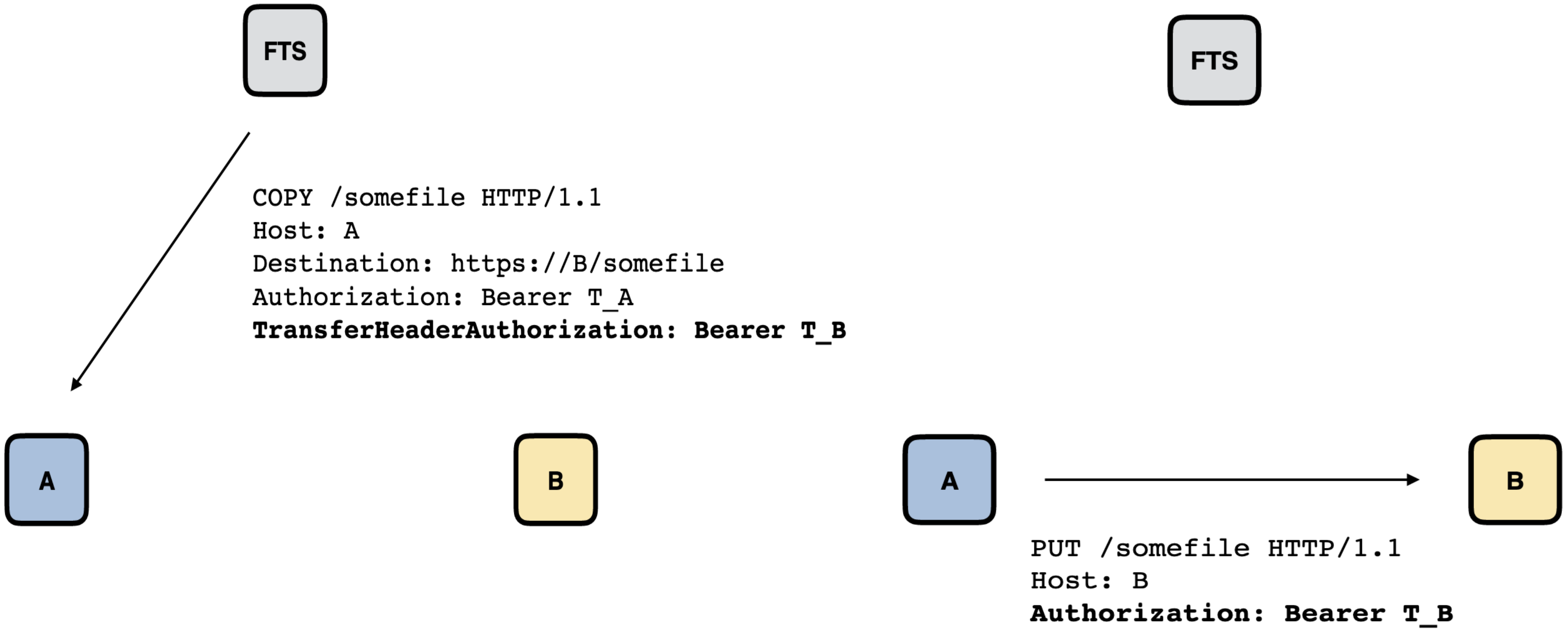
FTS requests a token that grants write access to path: /somefile

B returns a token, typically as a base64-encoded string Let’s assume this string is **T_B**

FTS requests a token that grants read/copy privileges on path: /somefile

A returns a token, let’s assume this token is **T_A**

TPC http tokens authorization



```
COPY /somefile HTTP/1.1
Host: A
Destination: https://B/somefile
Authorization: Bearer T_A
TransferHeaderAuthorization: Bearer T_B
```

```
PUT /somefile HTTP/1.1
Host: B
Authorization: Bearer T_B
```

- + Tokens issued by the storage and understood only by the same storage
- + Tokens format independent (JWT & macaroons)
- + Capability based authorization rather than role based authorization
- – Client still needs a X509 to request the tokens

Conclusions

- WLCG has done a large amount of evaluation and development work to move away from the x509 based AAI
    - 2 sw stack to replace VOMS-Admin have been identified
    - Token schema being developed
- Grid services
    - Expected to work with a translation DOMA TPC work to enable http protocol token authorization
    - CE developers on board with the changes or actively developing token support
- Infrastructure evolving to incorporate other services better suited to an Oauth (2.0) infrastructure
    - May give another push in this direction.