Trust and Identity Incubator

Sprint Demo #7 – Oct 10, 2019

Uros Stevanovic

On behalf of the Community Tagging group

Community Tagging - “Pixie Dust” - Usecase

- Research communities have a need to express and potentially share certain trust marks on IdPs and SPs. These trust marks may differ from existing trust marks issued by identity federations, or may be put in to compliment existing ones, in case the federation operator does not support these, like e.g. in the case of SIRTFI.
- This activity tries to implement a technical solution that matches the requirements as described by the SIRTFI community and investigates usability of the solution for research communities and the impact of the solution of Identity federations. It also explores potential other scenarios where a similar methodology could be used, like e.g. REFEDs MFA and in the context of the IdP self assessment tool that was developed in GN42
- It does not consider itself with the questions on where and how such a tool would be used in the context of existing trust frameworks.

Identified requirements

- Web portal
- Metadata handling, i.e. import, export, generation (managing entity categories)
- Self assertion of the tag, by “invitation” only
- Admin flows vs user flows (certain actions are not available to “regular” users)
  - User “asserts” a tag, admin approves/rejects it
- Comprehensive logs

Nice to have:

- Signing metadata

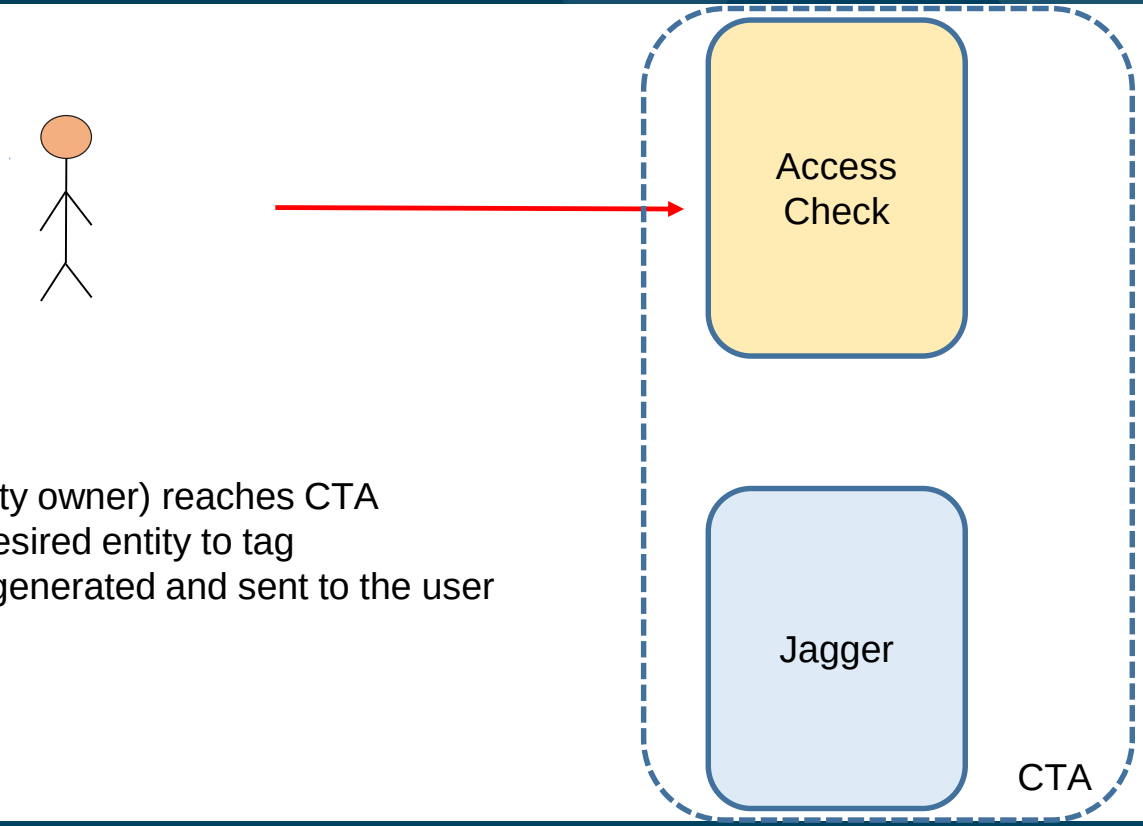
Overview of the work

- Defining requirements
- Evaluation of the current tools
- Tool selection
- Defining usage and admin flows
- Creating first version of the tool
- Documentation

Actual tool

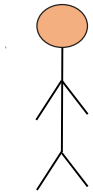
- Two tools (Access Check and Jagger), working together
- Jagger
  - Metadata handling
  - Actions based on user rights discrimination (admin vs user)
  - Managing entity categories
  - Exporting/importing/changing metadata (signing)
- Access Check
  - Invitation flow (selection of the desired entity)
  - Generating credentials for Jagger

Flow (user)

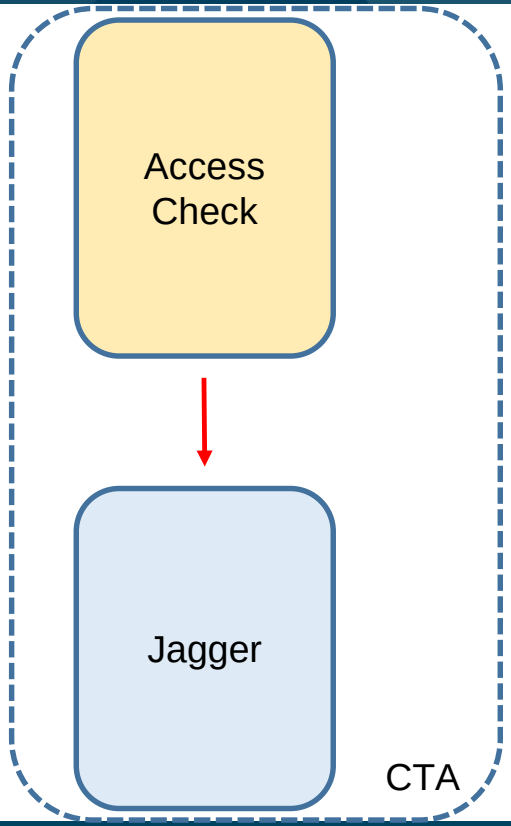


- User (entity owner) reaches CTA
- Selects desired entity to tag
- Token is generated and sent to the user

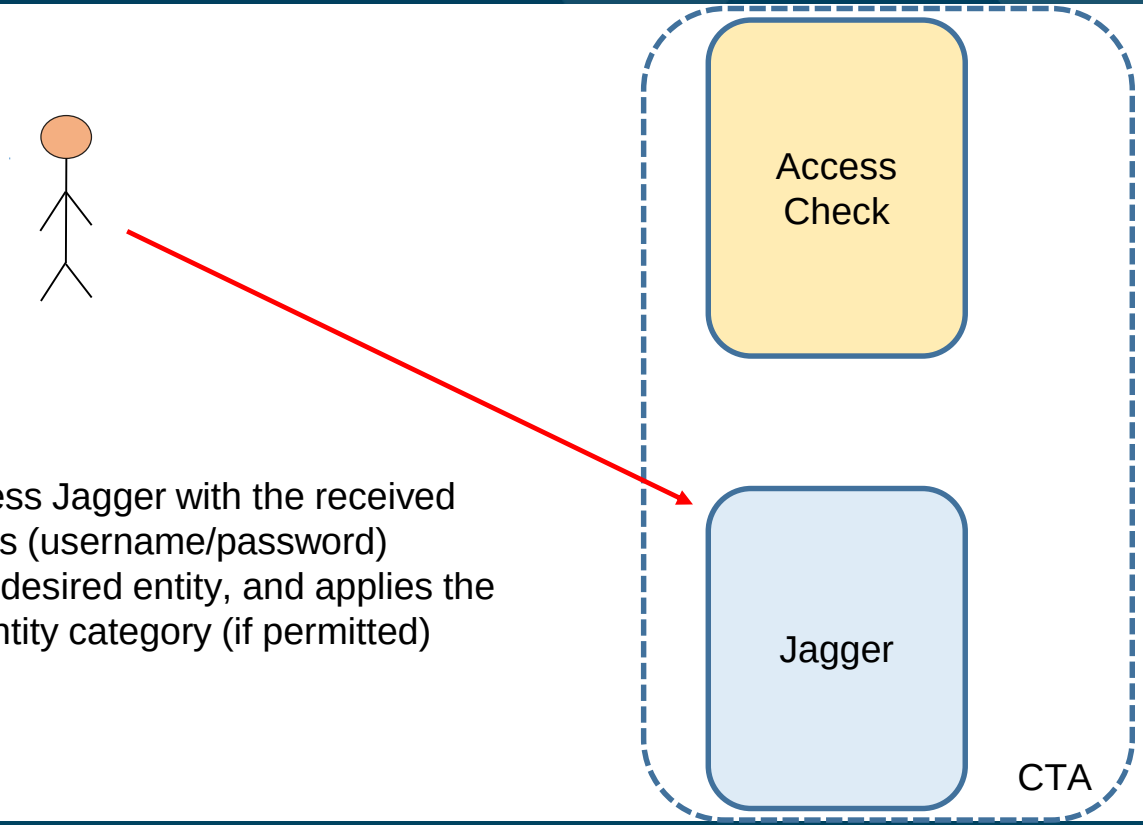
Flow (user)



- One-time password (token) is generated
- Sent to user's email (from metadata tech support)
- Once the token is entered, user account is created in Jagger (associated with the entity)

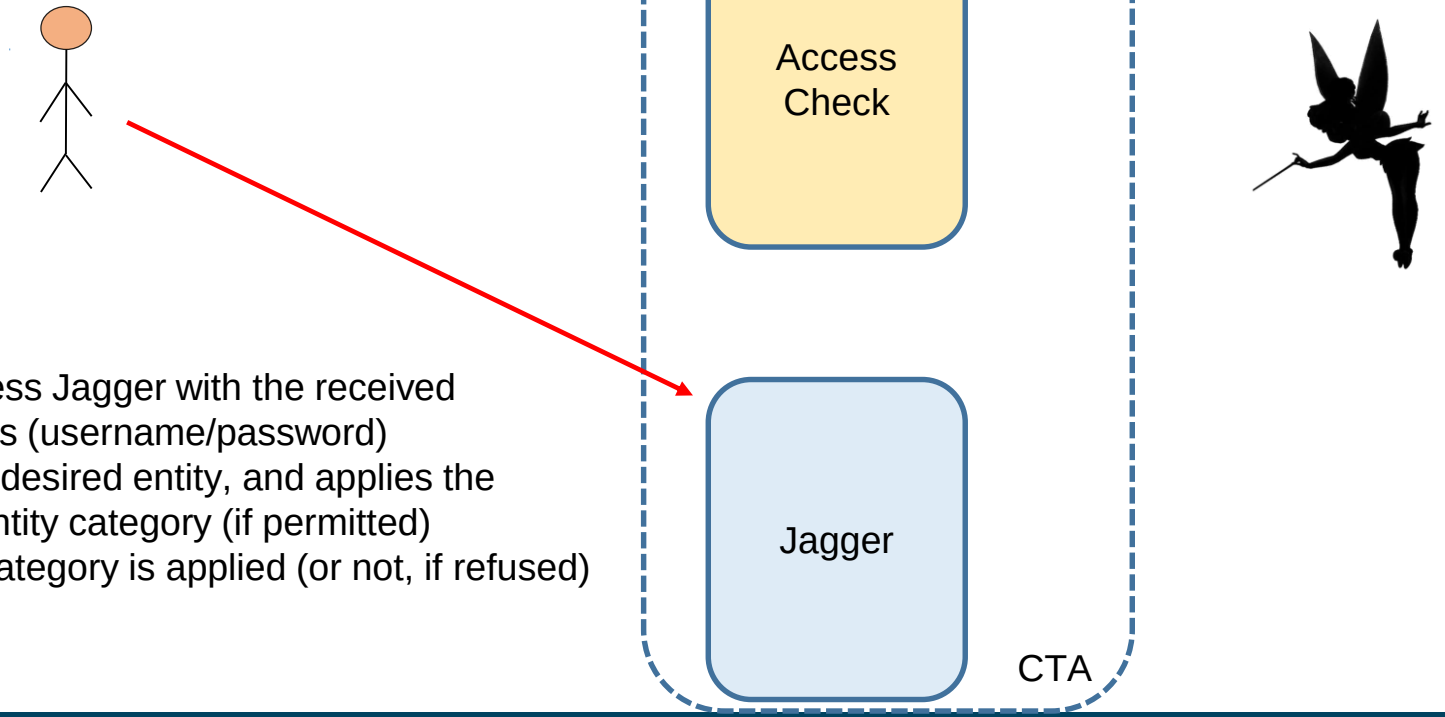


Flow (user)



- User access Jagger with the received credentials (username/password)
- Selects a desired entity, and applies the desired entity category (if permitted)

Flow (user)



- User access Jagger with the received credentials (username/password)
- Selects a desired entity, and applies the desired entity category (if permitted)
- Desired category is applied (or not, if refused)

Demo

- Video 1
  - Importing a desired federation metadata (admin)
  - Create a desired entity category (admin)
- Video 2
  - Invitation flow (access check, user)
  - Creating credentials, accessing Jagger (user)
  - Selecting (i.e. “tagging”) an entity category for the chosen entity (user)
- Video 3
  - Approving the choice of the entity category (admin)

Demo

https://hadem.vm.grnet.gr/rr3/metadata/federation/Pixie_test/metadata.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Metadata was generated on: 2019-11-12 11:14 UTC
TERMS OF USE
One for all, and all for one!!
-->
<md:EntitiesDescriptor ID="prefix-20191119111423" Name="urn:mace:pixiedemo" validUntil="2019-11-19T11:14:23Z" xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui" xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi" xmlns:idpdisc="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol" xmlns:init="urn:oasis:names:tc:SAML:profiles:SSO:request-init" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xi="http://www.w3.org/2001/XInclude">
```

```
10192 https://abuseio.cert.grnet.gr/shibboleth
10193 -->
10194  <md:EntityDescriptor entityID="https://abuseio.cert.grnet.gr/shibboleth">
10195   <md:Extensions xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport">
10196    <mdattr:EntityAttributes>
10197     <saml:Attribute Name="urn:oasis:names:tc:SAML:attribute:assurance-certification" NameFormat="urn:
      oasis:names:tc:SAML:2.0:attrname-format:uri">
10198      <saml:AttributeValue>https://community.org/sirtfiplus</saml:AttributeValue>
10199     </saml:Attribute>
10200    </mdattr:EntityAttributes>
```

Future steps (potentially)

- Demoing the tool at TechEx (Dec 2019)
- Signing of the metadata
- Usage considerations (further entity category, decision process, deployment model)