Assessment of AAI and LoA for Accessing Personal/Sensitive Data

Petr Holub, Irene Schlünder

January 2, 2018

1 Introduction

This document has been delivered as a part of AARC2 project, assessing the Authentication and Authorization Infrastructure (AAI) architecture from the perspective of providing/obtaining access to the personal data. The document uses

2 Relevant Documents

Architecture Blueprint

REFEDS LoA Proposal

3 Use Cases

3.1 Institutional researcher requesting transfer (download) of personal (sensitive) data set from order institution repository

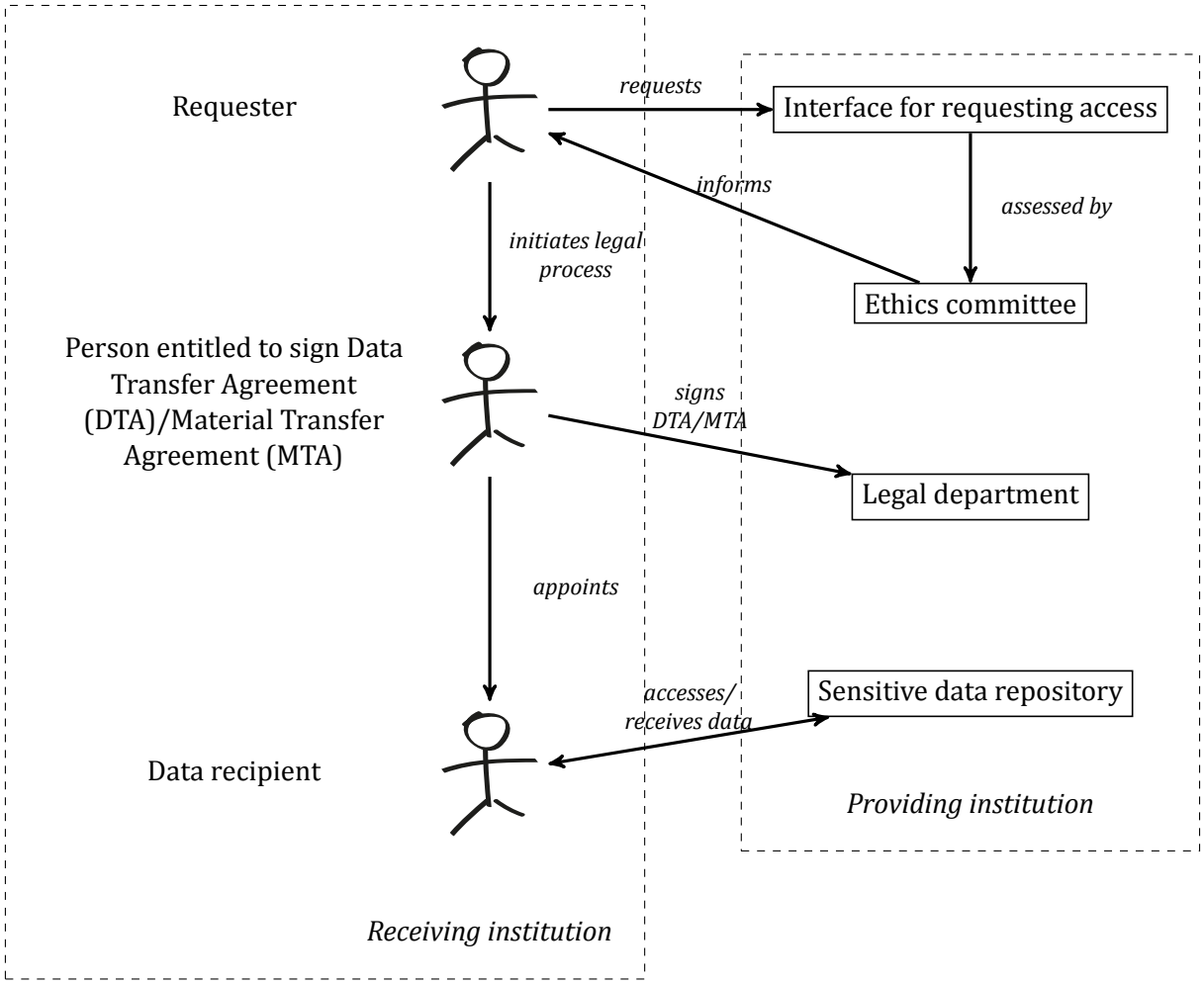

Figure 3.1: A diagram of access procedure for institutional researcher requesting transfer (download) of sensitive data set from order institution repository.

Access procedure in this case looks as follows (see also Figure 3.1):

1. *A request is issued by the requester* (a natural person). This may be the person which will be the intended recipient of the data, but it can be also a person designated to procure the data for the research institution, or a person designated by the intended recipient to act on her/his behalf.

   The request shall typically contain also a research project description and ethics vote on it, or other justification of legal basis for the request of access to the personal data

2. The request is *assessed by an access committee and possibly ethics committee*. The access procedure only proceeds if the request (and project) found adequate.
3. The DTA or MTA, if also biological material is transferred, is signed by persons of both providing and receiving institutions, also clearly and unambiguously designating recipient of the data at the receiving institution. The signing persons must be *entitled to sign MTA/DTA contracts* on behalf of the given institution. If the contracts involve any payment or other financial obligations (such as fines for potential breaches of the contract), the person must be also *entitled to sign financial obligations* on behalf of the institution.
4. The designated recipient of the data authenticates to the secure repository and obtains the data via a secure transfer protocol.

4 Requirements on AAI

- **Data access/transfer request.**
  - *Required identifiers:*
    `https://refeds.org/assurance/ID/unique`
  - *Required identity vetting/proofing assurance:*
    `https://refeds.org/assurance/IAP/assumed`
  - *Required authentication instance assurance:*
    `https://refeds.org/assurance/profile/sfa`
  - *Required attributes:*
    (a) institutional affiliation, *(b)* employee status.
  - *Required attribute assurance:*
    `https://refeds.org/assurance/ATP/ePA-1m`
- **Signing DTA/MTA.**
  - *Required identifiers:*
    `https://refeds.org/assurance/ID/unique`
  - *Required identity vetting/proofing assurance:*
    `https://refeds.org/assurance/IAP/verified`
  - *Required authentication instance assurance:*
    `https://refeds.org/assurance/profile/sfa`
  - *Required attributes:*
    (a) institutional affiliation, *(b)* employee status, *(c)* entitled to sign DTA/MTA, *(d)* entitled to sign financial obligations.
  - *Required attribute assurance:*
    Employment status must be updated within `1` day after contract with the person is terminated. Entitlements to sign DTA/MTA and financial obligations must be removed within `1` day after they are withdrawn from the person.
- **Access to personal (sensitive) data.**
  - *Required identifiers:*
    `https://refeds.org/assurance/ID/unique`
  - *Required identity vetting/proofing assurance:*
    `https://refeds.org/assurance/IAP/verified`
  - *Required authentication instance assurance:*
    `https://refeds.org/assurance/profile/mfa` with actual MFA required via `Authentication-ContextClassRef`

- *Required attributes:*
  (a) institutional affiliation, *(b)* employee status.
- *Required attribute assurance:*
  Employment status must be updated within 1 day after contract with the person is terminated.

Note that ePUID should be used to appoint person in the DTA/MTAin order to unambiguously and traceably identify the persons authorized to access the personal (sensitive) data.

5 Assessment

5.1 Blueprint Architecture

- General architecture provides sufficient flexibility.
- Does not prescribe necessary attributes.
- Does not solve the need for M:N negotiations between Identity Providers (IdPs) and Service Providers (SPs).

5.2 REFEDS LoA Document

- 1 month attribute update is too long for certain cases. 1 day is needed for signing contracts and sensitive data access (employment status and entitlements to sign contracts).
- Does not prescribe necessary attributes.

5.3 Beyond current documents

What remains to be addressed:

- List of needed attributes should be subject to a different policy document from the assurance policy.