Identity and Record Matching - OOTS

Contents

Introduction

As a general rule, only users authorised to access data should be able access that data. Where a user requests access to data, the data controller typically identifies a user and compares that identity to the identities that are authorised to access that particular data. In case of a positive match, access can be granted, if not, access is not granted.

Where users wish to use OOTS for providing evidences, the above applies. Therefore, identity matching is needed in every evidence request situation.

When using eID-s notified under eIDAS for user identification, the attributes that can be used are the attributes of the natural or legal person provided by the eIDAS data set. It may also be that sometimes users are requested to input additional attributes in combination of the eIDAS data set to improve unique user identification. Therefore, if it is allowed by national law, the Data Service may use the mechanism of user-provided attributes to disambiguate in the process of identity matching. These attributes would be added to the list of identification attributes for the evidence type in the Data Service Directory. The Data Service Directory shall set the level of assurance to "N/A" (as they will be user-provided and therefore unverified) and specify the required format.

As a point of attention: identity matching is typically done by looking up and matching identifiers. For this purpose, the eIDAS Unique Identifier (eIDAS UID) can only be used if it is already known to the evidence provider. This may be true in cases where the evidence provider has already linked the eIDAS UID to a known identifier or has access to such result. To be also noted that some Member States have different outbound identifiers, therefore, for the same user and eID means, a Data Service Provider may receive different eIDAS UID, depending on the characteristics of the requesting Online Procedure Portal (e.g. the Member State in which is it operating).

Record matching done at Data Service side

A short summary of identity and record matching done by a Data Service using the eIDAS provided attributes, and when needed, user-provided attributes, is the following:

0. Succesful eIDAS authentication requested by Online Procedure Portal side. User provides additional attributes as specified in the Data Service Directory for the specific Data Service.

--**Member State with different outbound identifier--**

1. IF request is concerning a user that has used an eID scheme from a Member State with different outbound identifier:

    1.1. IF eID scheme used has been issued in the MS of the Data Service

        1.1.1. IF VERIFIABLE [*****] eIDAS UID

            Use minimum data set (MDS) to find match(es);

```
            For those matches calculate eIDAS UID;
            Identity match: map eIDAS UID  back to national UID ;
            Goto EndProcedure: //identity match, end procedure
        END IF(1.1.1).
     END IF (1.1).

   1.2. IF eID scheme used has not been issued in the Member State of the Data Service AND matching based on
stored eIDAS UID  OOTS-provided is allowed by national law
        1.2.1. IF one match eIDAS UID (eIDAS UID known)
            Identity match; (returning user)
            Goto EndProcedure: //identity match, end procedure
        END IF(1.2.1.).
        1.2.2. IF more than one match eIDAS UID (eIDAS UID known)
            Error;
            Goto EndProcedure: //error
        END IF(1.2.2)
        1.2.3. IF no match eIDAS UID (eIDAS UID unknown)
             Search for match based on MDS and/or additional user-provided attributes;
                  If there is one match, link eIDAS UID to the national record;
                  If there is no match, enroll user, link eIDAS UID to the national record;;
                  If there are more 2+ matches, signal error.
                  Goto EndProcedure: // match or error
         END IF(1.2.3)
    END IF(1.2).

   1.3. IF eID scheme used has not been issued in the Member State of the Data Service AND matching based on
stored eIDAS UID  OOTS-provided is not allowed by national law
         Online Procedure Portal does not send the eIDAS UID OR eIDAS UID is discarded and not stored;
         Search for match using MDS and additional user-provided attributes:
            If there is one match - match found;
            If there is no match - enroll user;
            If there are more 2+ matches - signal error.
            Goto EndProcedure: //identity match, or error
   END IF(1.3).
END IF(1).
```

--Member State with the same outbound identifier--

```
2. IF (eID scheme coming from Member State with the same outbound identifier)
   2.1. IF eID scheme used has been issued in the Member State of the Data Service
        If identifiers are derived, pseudonym:
             Use minimum data set (MDS) to find match(es);
             For those matches calculate eIDAS UID;
             Identity match: map eIDAS UID  back to national UID ;
             Goto EndProcedure: //identity match, end procedure
        Else use the identifier directly for the identity match.
   END IF (2.1)

   2.2. IF one eIDAS UID match
        Identity match; (returning user)
        Goto EndProcedure: //identity match, end procedure
   END IF (2.2)

   2.3. IF more than one eIDAS UID match
        Error;
        Goto EndProcedure: //error
   END IF (2.3)

   2.4. IF no eIDAS UID match
        Search for match using MDS and additional user-provided attributes:
            If there is one match - match found, link eIDAS UID to national record;
            If there is no match - enroll user, and link eIDAS UID to national record;
            If there are more 2+ matches - signal error.
            Goto EndProcedure: //identity match, or error
   END IF (2.4)

END IF (2)

EndProcedure:
END.
```

ⓘ The identify matching can be performed by the Data Service or by another Matching Service available nationally. For this document, for clarity purposes, this was not reflected in the flow.

EXAMPLES

Example 1:

Bianca is using a notified eID issued by MS A (where she was born), to access a MS B procedure portal for which there is a need to retrieve diploma from her home country (MS A). The eIDAS UID provided by MS A when using eIDAS authentication is not MS specific/does not use pseudonym/it is not derived and therefore can be used by the Data Service in MS A to identify the user.

Example 2:

Bianca is using a notified eID issued by MS A, to access a MS B procedure portal for which there is a need to retrieve diploma from MS C (where she studied). The eIDAS UID provided is not MS specific/pseudonym/derived and therefore can be used by the Data Service in MS C to perform identity matching.

Example 3:

Bianca is using a notified eID issued by MS A (where she was born), to access a MS B procedure portal for which there is a need to retrieve diploma from her home country (MS A). The eIDAS UID provided by MS A when using eIDAS authentication is derived/ pseudonym/ therefore the MS A would have to verify and find a match using the one-way function[**] used for derivation.

Example 4:

Bianca is using a notified eID issued by MS A, to access a MS B procedure portal for which there is a need to retrieve diploma from MS C (where she studied). The eIDAS UID provided is MS specific/pseudonym/derived and therefore. MS C allows the linking of eIDAS UID that have been delivered via OOTS and is able to find a match for Bianca, as she had already made another request from Belgium with the same notified eID.

Example 5:

Bianca is using a notified eID issued by MS A, to access a MS B procedure portal for which there is a need to retrieve diploma from MS C (where she studied). The eIDAS UID provided is MS specific/pseudonym/derived and therefore. As in MS C is not possible to link eIDAS UID that have been provided via OOTS, the identity and record matching is done using the MDS and additional user-provided attributes. The provided eIDAS UID is discarded.

[*] VERIFIABLE eIDAS UID - For the MS that use derived identifiers, the derivation is usually done using a one-way function, in order to protect the source identifier. See section 2.5. of eIDAS SAML Attribute Profile, version 1.2, “MUST be constructed using pseudo-random values that have no discernible correspondence with the subject's actual identifier (for example, username).” Therefore just the identifier would not be enough for a Member State even if they have issued the identifier. The Member state would have find the match by using the Member State specific MDS required for the derivation of the identifier.

[**] function used to create the derived identifier from the source identifier, which prevents the disclosure of the input (source identifier) when having just the output (the derived identifier)