

# Use Case. Legal name required

**Use Case Number** SPREQ01  
**Use Case Name** Legal name required

## Work Package

## Stakeholders & Interests

Service Provider: The SP requires the users Legal Name either because of some legal requirement prior to service provision or because the SP must match the Legal Name with data from a source outside the Federation

Identity Provider: The IdP must be willing to reveal the users Legal Name to this SP. Due to the sensitivity of this data, a bilateral agreement may be required.

User: For privacy reasons the User should be aware of the release of this attribute and possibly have a veto capability

*Conditions that must be true before the use case can be initiated*

## Preconditions

1. User requests service from SP
2. SP requires authentication and Legal Name
3. IdP has Attribute Release Policy for Legal Name to this SP

## Success Guarantee

*Things that will be true when the use case has been completed*

**(Post-conditions)**

1. User will be aware that Legal Name has been disclosed
2. User will be aware of the SP requirement for Legal Name
3. IdP will have released Legal Name and identity LoA to SP
4. SP will observe Federation policy regarding user privacy

*Unauthenticated*

1. User is unauthenticated to SP
2. User makes request for service via browser to SP
3. User is redirected to IdP (possibly via WAYF)
4. User authenticates
5. User is redirected to SP with Authentication assertion and requested Attributes
6. SP PDP processes assertions
7. SP provides/denies service

**Main Success Scenario (Basic Flow)**

*Pre-authenticated with attribute request*

**Extensions (Alternate Flow)**

1. User is already authenticated to SP
2. User makes request for service via browser to SP

3. SP requests Legal Name from IdP (via back-channel)
4. IdP sends assertion containing requested attributes
5. SP PDP processes assertions
6. SP provides/denies service

### **Legal Name**

Legal Name is defined as the name listed on the documentary evidence provided by the user during registration at the IdP. Unfortunately no existing schema attributes fully satisfy this definition. *cn*, *firstName/surname*, *displayName* may describe the users "usual name" or "preferred name" which is often different to the name on Passport/Drivers License/Bank Account etc. *cn* can also be multi valued.

### **Data Items**

### **Identity LoA**

The binding of Legal Name to the issued credential is measured by the identity level of assurance (LoA). This attribute is not defined in existing schema. The Identity LoA is most likely to be of interest to SPs which have a requirement for Legal Name. These two attributes should be considered as one and Identity LoA always asserted along with Legal Name

*Any special requirements*

### **Special Requirements**

1. The Legal Name should only be available for users who have completed an in-person proof of ID based on documentary evidence.
2. The Legal Name should only be asserted in conjunction with the identity level of assurance (LoA). A High Assurance SP may require a minimum identity LoA for service provision.

*Frequency TBD.*

The known scenarios are:

### **Frequency of Occurrence**

1. **Legal requirement:** The SP has a compliance requirement to gather the Legal Name as a condition of service provision.
2. **Need to match with data from external source:** The SP must match the user against a data set from outside the Federation. This data set is indexed by Legal Name and does not contain any other user identity attribute which could be obtained from the federation authentication process.

*Any questions/issues that require resolution for development.*

### **Open Issues**

1. **User privacy:** A number of user privacy aspects are evident.  
User awareness of Legal Name attribute release  
User awareness of the reason for Legal Name attribute release  
Policy governing SPs use of User Legal Name attribute  
Policy governing IdP use of audit log binding  
User to anonymous SP access
2. **User veto on attribute release:** Currently AAF Shibboleth does not provide for user veto on attribute releases.
3. **Bilateral agreement:** This is required between IdP and SP for attribute release
4. **Audit Requirement:** If an SP has an audit requirement to store a record of the users Legal

Name for each provision of service, this may be satisfied by a combination of an opaque user identifier, the identity LoA, and an audit log policy requirement on federation IdPs. This policy requirement may be preferable to the release by the IdP of the users Legal Name in these situations.