swisscom

All-In Signing Service

How to build the Subject Distinguished Name (DN)

Table of Contents

Swisscom (Switzerland) Ltd
Digital Certificate Services
P.O. Box
8021 Zurich

swisscom

1 Integrated Process

1.1 Objective and Goal of this Document

Customers using the Swisscom All-in Signing Service (AIS) for signatures for natural persons have two main options to fulfill the requirements for signatory identification:

1. Customer can become a registration authority (RA) and execute the complete signatory identification by themselves
2. Customers can rely on the existing Swisscom processes and tools built on the "RA Service" (RAS)

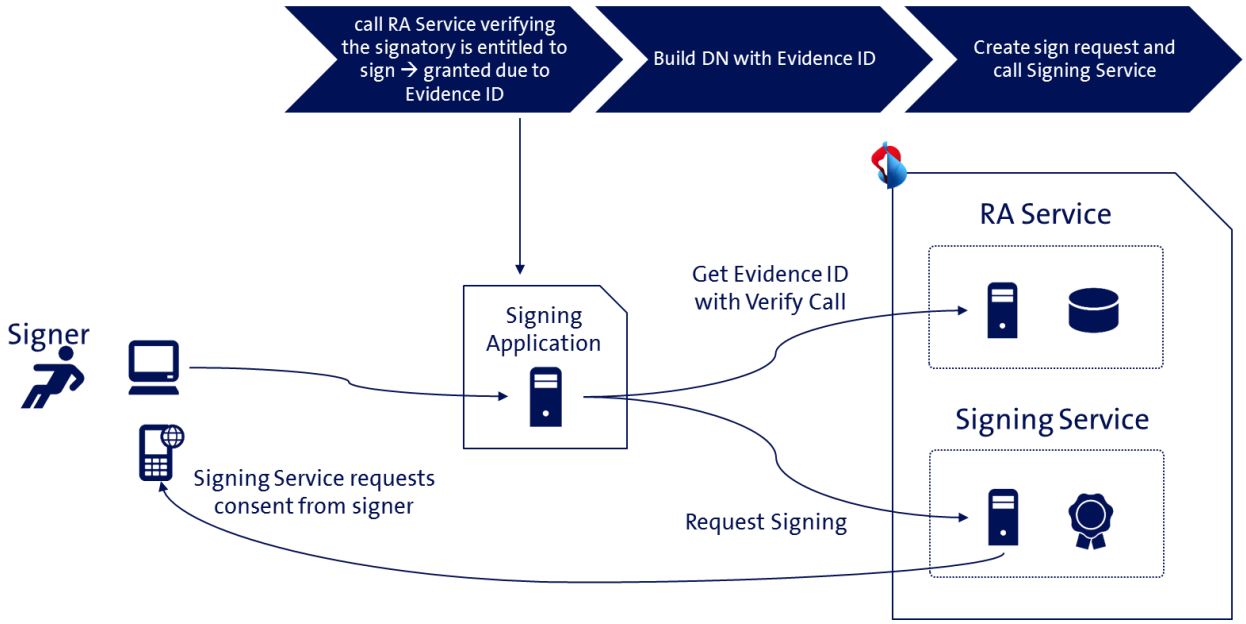
In both cases, the resulting signatory name – called Subject Distinguished Name (DN) – must be unique for the given signatory and can never be assigned to any other signatory. Customers opting for solution 2 (RA Service) must follow Swisscom procedures to ensure, that the resulting Subject DN will be correct and unique.

This document describes the steps required to sign a document including the including the process of creating the distinguished name (DN) by a certain pattern for the signing request and finally calling the signing service (All-In Signing Service, AIS) of Swisscom (Schweiz) AG.

The intended Audience is a developer or an architect.

1.2 Process Flow: Signing a Document with a verified ID

In order to create valid DNs, an application that integrates All-In Signing Service (AIS) for personal Electronic Signatures must also integrate method calls to the RA Service. Recommended flow is depicted in the process chart below.



1. The application (Signing Application) first calls the RA-Service verifying the existence of the signatory's identification evidence (see details in chapter 2). This service call returns the Evidence ID referenced by a mobile number (MSISDN). Depending on the business requirements of signing application, the step 1 may require two distinct calls (see details in chapter 2).
2. After successful call to the RA-Service the Evidence ID should be present and the application must build the distinguished name (DN) for the signing request (see chapter 3). Evidence ID should be part of the DN as value of the serial Number attribute.

3. Finally, the application must create signing request - putting the created distinguished name (DN) into the appropriate service request element and call the signing service. For further details regarding this step please refer to the All-In Signing Service Reference Guide (link).

swisscom

2 Evidence Query by RA-Service

2.1 Query of evidence

RA Service client can use the verification API for AIS to query whether a user has completed the registration process. No Authentication is required.

Response includes the Evidence ID referencing the evidence documents created during the identification process of a natural person.

2.1.1 Request

POST /evidences/verify with a JSON object in HTTP request body

Request Parameters

Name	type	description
claimedIdentity	string	The "claimed identity" provided to the customer when signing the AIS contract with Swisscom.
msisdn	string	The registered mobile phone number of the user
distinguishedName	string	Combines the parameters pseudonym or combination of givenName and surname and countryCode in form of string representation of a X.500 Distinguished Name (RFC 4514), as agreed by the contract. The common-name RDN of the distinguished name cannot be empty.
assuranceLevel	string	Must be set to 3 for advanced signature or must be set to 4 in query for qualified signature
jurisdiction	string	OPTIONAL: jurisdiction if no jurisdiction is passed default is applied ZERTES. Valid values: zertes and eidas.

Example in Production:

```
POST https://ras.scapp.swisscom.com/api/evidences/verify HTTP/1.1
TE: deflate,gzip;q=0.3
Connection: TE, close
Accept: application/vnd.sc.ras.evidence.v1+json
Host: ras.scapp.swisscom.com
User-Agent: Ras::RasClient/0.01
Content-Type: application/vnd.sc.ras.evidence.v1+json
Content-Length: 133

{"claimedIdentity":"dis01","distinguishedName":"gn=heinrich,sn=muster-
mann,cn=heini mustermann,c=CH","msisdn":"41790000200","assuranceLevel":"4"}
```

2.1.2 Response

HTTP status code	Description
200	The user has been registered for the context, and the registration is compliant for Qualified Signature.

swisscom

HTTP status code	Description
	RA Service returns the public ID of the evidence object which confirms the given user may sign a document with AIS. The ID is returned as the json attribute `evidenceId` in the HTTP response body. evidenceID referencing the evidence document that has been created during the identification process of a natural person.
404	If content type is `application/json` and the statusCode attribute in response is 404, the user status is not sufficient for the required signature.
500	Client-side (e.g. invalid parameter) or server-side application error.
502, or 503	Underlying infrastructure fails temporarily. The client MIGHT retry the request

Example 1: 200 Response

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Content-Length: 50
Content-Type: application/vnd.sc.ras.evidence.v1+json
Date: Thu, 12 Jul 2018 12:43:27 GMT
X-Vcap-Request-Id: 173c1ea3-e146-4cae-542a-6778867bd2bf
Connection: close
Strict-Transport-Security: max-age=15768000; includeSubDomains

{
  "evidenceId" : "RAS5b45b027c6d9370008072c48"
}
```

Example 2: 404 Response

```
HTTP/1.1 404 Not Found
Cache-Control: no-cache
Content-Length: 100
Content-Type: application/json
Date: Thu, 12 Jul 2018 12:42:22 GMT
X-Vcap-Request-Id: cf91004e-1b06-4633-6e41-bc971616fc7e
Connection: close
Strict-Transport-Security: max-age=15768000; includeSubDomains

{
  "statusCode" : 404,
  "message" : "The request could not be verified",
  "exceptionClass" : ""
}
```

swisscom

3 Applicable Distinguished Name (DN) Pattern

The following subject DN pattern can be used with the AIS for personal signatures:

3.1 Pattern with pseudonym

cn=<givenname surname**>,**

pseudonym=<mobile number in international format**>,**

c=<domicil due to ID document**>,**

serialNumber=<evidenceID given by evidenceVerify call>

3.2 Pattern with givenname, surname

cn=<surname givenName**>,**

givenname=<firstname due to ID document**>,**

surname=<lastname due to ID document**>,**

c=<domicil due to ID document**>,**

serialNumber=<evidenceID given by evidenceVerify call>

3.3 Pattern for test signatures

All signatures issued by the AIS are valid productive signatures. If you sign documents during development or test phase, make sure to use documents which clearly have non-binding content.

For informational purposes only, you can use the prefix “TEST” in the cn part of the DN.

3.4 Pattern for evidence validation client interaction

What is the level of assurance (LOA) of a user?

- request with "assurancelevel":"4"
- request with "assurancelevel":"3"
- request with "assurancelevel":"2"

if Response is 200, LOA of user is discovered.

Is the ID expired e.g. (evidence older than 5 Years, document expired ...)?

If response is 404 the evidence is not valid / expired on the requested level, so user need to contact RA officer and identify.

For which jurisdiction can the user sign?

- request with "jurisdiction":"zertes"
- request with " jurisdiction":"eidas"

if response is 200, user can sing.

swisscom

4 Organization names

Additionally, the patterns mentioned above can be extended by the organization attribute ("o" or "organization") in the DN. When using an organization name, the country must match the location of head office of the company respectively of the organization.

Note: The use of organization names requires additional contracts with Swisscom and written consent of the company owning the name.

swisscom

Document Control

Change Control

Version	Date	Executing OE	Description / Nature of tasks
1.0	17.07.2018		Initial version
1.1	19.03.2019		Add API use cases