

Registration-Authority-Service

Evidence Import API

Classification	C1 –Public
Scope of Application	Registration-Authority-Service
Version	1.1
Publication date	08.Feb.2023
Status	release

Table of Contents

1 Introduction	2
1.1 Objective and Goal of this Document	2
1.2 Overview of RA-Service	2
1.3 Common usage sequence of Evidence Import API.....	2
1.4 Service Endpoints.....	3
1.5 Terms.....	3
2 Service Authentication.....	5
2.1.1 Request	5
2.1.2 Response.....	5
2.1.3 Notes.....	6
3 Evidence Import.....	7
3.1 Evidence data	7
3.2 Create a new evidence.....	7
3.2.1 Request	7
3.2.2 Response.....	11
3.2.3 Examples.....	11
4 Evidence Query	17
4.1 Lookup the registration status of a user.....	17
4.2 (Legacy) Query of evidence for qualified signature.....	17
4.2.1 Request	17
4.2.2 Response.....	17
5 Document Control.....	20



swisscom

1 Introduction

1.1 Objective and Goal of this Document

This document describes the interface used to import the evidence data into Swisscom Registration Authority Service (RA-Service). The focus of the document is the semantics and examples, the formal RESTful API specification ("Swagger Documentation") is available at <https://rasp.scapp.swisscom.com/swagger/index.html>.

The intended Audience is developer and architect.

1.2 Overview of RA-Service

(You can skip this section if you already know the features of RA Service.)

RA Service, a core component of the SRS ([srs]), has implemented the following business functions:

- Encrypted storage of ID document metadata (according to legal regulation on electronic signatures), ID document images, and linked authenticator identifiers (e.g. MSISDN, Mobile ID Serial Number or PWD/OTP Serial Number) of the ID document holder
- Encrypted storage of the evidences of the ID registration process (vetter's data and signature, ID document, user consent to terms and conditions)
- User Consent flow in the ID registration process
- RESTful API for verifying the metadata associated with an identifier (e.g. MSISDN), and the compliance level of ID registration process for digital signature purpose, the linked authenticator identifier
- RESTful API for authentication of privileged users with Mobile ID or PWD/OTP
- Admin Web UI for managing RA Agents (people who identify end users) and privileged RA Service users (Standard RA Agent, Master RA Agent, Global RA Agent, RA Operator), for managing tenants, and for managing status of registered users
- Mobile Application for iOS and Android (RA-App) for supporting the face-to-face ID proofing process and for submitting ID document images
- Standalone UI Application for exporting the evidences (with embedded ID document images).
- RESTful API for importing ID document metadata, ID document images, user identifier (e.g. MSISDN, e-banking user identifier), evidence documents of ID proofing process, authenticator identifier, optionally term and conditions which the user has given consent to.
- e-Learning Workflow for education / certification of RA Agents.
- Management of Terms & Conditions

1.3 Common usage sequence of Evidence Import API

The Evidence Import API is usually invoked in the following sequence. Details of each call are described in later chapters.

1. If the API client is not yet authenticated, or the previous "session" token (JWT token) has expired, the API client must call the service authentication API. After successful authentication, RA service returns a "session" token (JWT token), which the API client should include in all subsequence service calls.

2. The API client calls POST /evidences/import to import a new evidence or to replace an existing evidence. On successful creation of the evidence record in RA Service, RA Service returns the evidence enriched with other meta data (e.g. evidence id, evidence status, compliant assurance level for digital signature).

1.4 Service Endpoints

The productive and test environment of RA Service is running in the Swisscom internal Application Cloud (*.scapp.swisscom.com). The service endpoints are also accessible from Internet. Note that both environments share the same public IP address.

Additional test / development environments are available for Swisscom internal usage.

Environment	Service endpoint
Production	https://ras.scapp.swisscom.com/api
Pre-production (Test)	https://rasp.scapp.swisscom.com/api

For verification of connectivity to RA Service, the GET /info service call can be used. The call does not require authentication.

Example using curl (for production environment):

```
curl -X GET "https://ras.scapp.swisscom.com/api/info" -H "accept: application/vnd.sc.ras.api-info.v1+json"
```

The service response should have HTTP Response Code 200, and a HTTP body with a small JSON object like:

```
{
  "version" : "2.43.1.31",
  "buildDate" : "2022-06-30T11:22:30.13Z",
  "environment" : "cloud,preprod",
  "android" : {"minimumVersion" : 6, "currentVersion" : 45},
  "iOS" : {"minimumVersion" : 6, "currentVersion" : 36}
}
```

1.5 Terms

term	Description
ID attributes	Personal identifiable information of a natural person used in digital signature context. Examples are surname, given name, citizenship.
Identity proofing	Identity proofing is the process to verify identifying attribute to be entered into an identity management system and to establish that the identifying attributes pertain to the subject to be enrolled. [iso29003:2018, sect.4.1]
Identity proofing evidence	Information that documents the Identity proofing process
RA Service tenant	It frequently corresponds to a company, which imports ID attributes and evidences to RA Service and/or consumes ID attributes stored in RA Service. Each imported evidence has a tenant attribute attached to it.



swisscom

		A RA Service tenant has a set of server-side configuration parameters which governs the import and consumption
evidence		The term refers to ID Proofing evidence if there is no ambiguousness in the context.
Tenant		The term refers to RA Service tenant if there is no ambiguousness in the context.
Contextual evidence	evi-	A contextual evidence is an evidence that fulfill a specific Level of Assurance (LoA) of a legal signature standard (jurisdiction), but it has additional constraint in the usage. For example, ZERTES requires that the evidence verified with a video identification method can only be used in the business context of financial intermediaries. The context is modelled in RA-Service as the tenant.

References

[iso29003]	ISO/IEC 29003:2018, "Information technology — Security techniques — Identity proofing"
[ras.swagger]	https://ras.scapp.swisscom.com/swagger/index.html
[srs]	https://trustservices.swisscom.com/smart-registration-service/

2 Service Authentication

2.1.1 Request

POST /auth/login: with empty http body

Request Parameters in HTTP Header

Name	Type	description
X-Auth-Tenant	String	A name that RA Service has assigned to the API client
X-Auth-Key	String	An opaque string that RA Service has given to the API client. The value is security sensitive and must be protected appropriately.

Example (data sent over the wire):

```
POST https://rasp.scapp.swisscom.com/api/auth/login HTTP/1.1
TE: deflate,gzip;q=0.3
Connection: TE, close
Host: rasp.scapp.swisscom.com
User-Agent: Ras::RasClient/0.01
X-Auth-Key: QIxKmKTJlCN0gVutJGkhWjDbROzEOYKU
X-Auth-Tenant: demo01
```

2.1.2 Response

HTTP status code	Description
200	Authentication is successful. The HTTP body contains the JWT token, also referred to as "session token" in this document <ul style="list-style-type: none"> The JWT Token should be cached on the client side and inserted as a HTTP header in all subsequent service calls in the request header : Authorization: Bearer <JWT Token> The JWT Token has a preconfigured life time (default: 24 hours). RA Client can periodically login to get a fresh JWT Token before the existing JWT expires. However, login should not be attempted too frequently because X-Auth-Key should be used only infrequently for security reason.
404	If the Content-Type of the response is not application/json, the underlying infrastructure fails temporarily. The client MIGHT retry the request The recommended maximum number of retries is 2, the 1 st retry 15 seconds after the initial request, the 2 nd retry 35 seconds after the initial request.
502, or 503	Underlying infrastructure fails temporarily. The client MIGHT retry the request The same retry algorithm as in status code 404 should be used.

Example (data received over the wire for example in Chap. 2.1.1):

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
```



swisscom

```
Content-Length: 457
Content-Type: application/json;charset=ISO-8859-1
Date: Tue, 10 Jul 2018 11:52:17 GMT
Expires: 0
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Vcap-Request-Id: 6b6fa16e-bcc5-48a4-5e0f-34820a3bb1de
X-Xss-Protection: 1; mode=block
Connection: close

{
  "token" : "eyJhbGciOiJIUzUxMiJ9..._Ge5XolCnEJ5IsOcSeGS23Q"
}
```

2.1.3 Notes

If a client of RA Service itself is a multi-tenant system and the imported ID attributes cannot be consumed by different tenants of the RA Service client, the client should use a distinct X-Auth-Tenant, X-Auth-Key tuple for each of its tenant, and should maintain the mapping between X-Auth-Tenant value and received session tokens.



3 Evidence Import

3.1 Evidence data

The evidence object in RA Service combines 6 different information items.

1. user's identifier for RA-Service, either a mobile phone number, or the tuple (idpAlias, userId).
2. the person's ID document data, e.g. names, birthday, nationality, ID document expiry date.
3. the data which proves the compliance of a registration process, e.g. photo(s) proving the face-to-face verification, photo(s) of presented ID documents, and/or audio files recorded in a remote registration session. The data is usually provided in form of a single PDF.
4. the language of the user, used in RA Service UI (e.g. Term & Conditions) and RA Service messages (e.g. SMSs, consent confirmation requests).
5. the user's consent for using Swisscom All-In-Signing Service (AIS).
6. the verified identifier of the authenticator (Mobile ID, PWD+SMSOTP) which will be used to authenticate the user.

The first 4 items are mandatory for import of evidences. The imported data is only usable for signature purpose after all items have been defined.

3.2 Create a new evidence

The operation is used to import evidence into RA. It supports the following use cases, triggered by different combination of request parameters.

Table 1 Different use cases of evidence import

use case	request parameters			
	msisdn	idpAlias	userId	enforceArchive
User consent for using Swisscom AIS is managed by RA Service.	non-empty	empty	empty	absent or false
User consent for using Swisscom AIS is managed by RA client	non-empty	empty	non-empty	absent or false
	empty	non-empty		
Imported evidence is only for archival purpose, not for digital signature	non-empty	empty	non-empty	true
	empty	non-empty		
Not supported	Other combinations			

3.2.1 Request

POST /identifications: with a JSON object in HTTP request body

Request Parameters

Name	type	m	description
User's identifier and correspondence language			



msisdn	string	→desc.	<p>Mobile number of the user being registered.</p> <p>Consists of 7..15 digits, including country code, without leading 0 or '+' prefix</p> <p>Example 41791234567</p> <p>msisdn is mutually exclusive to the tuple (idpAlias, userId).</p> <p>Either msisdn or tuple (idpAlias, userId) must be defined and non-empty.</p>
idpAlias	string	→desc.	<p>Name space of userId (s. below), assigned by RA-X.</p> <p>By convention, idpAlias is a short (2-7 chars) alphanumeric string.</p> <p>Example: PFM</p>
userId	string	→desc.	<p>If idpAlias is defined, the parameter must be non-empty, and is the unique identifier of the user within the name space specified by idpAlias.</p> <p>If idpAlias is absent, the parameter is used (for backward compatibility reason) to indicate who is responsible (RA-Service server or client) to managed the user consent to terms and conditions, see Table 1. The semantics of the value is not enforced by RA-Service.</p> <p>The syntax is defined by the importing client. Leading and tailing whitespaces are removed by RA-Service.</p> <p>Example: 70054321</p>
consentSerial-Number	string	o	<p>Identifier of the authenticator bound to the user during the ID proofing process.</p> <p>The authenticator is used by the user to give consent to electronic signature, or to authenticate for other purposes (if any) specified in terms and conditions.</p> <p>The parameter is mandatory if the user consent to terms and conditions is managed by the RA-Service client.</p> <p>Example: MIDCHE0123456789</p>
language	string	m	<p>The correspondence language of the user.</p> <p>Contains the 2-char ISO language code.</p> <p>Example: DE</p> <ul style="list-style-type: none">The information is used in RA Service for SMS messages, Mobile ID messages, UI language in Web, Term & Condition document. <p>RA Service currently supports 4 languages: DE, FR, IT, EN</p>
ID document data			
surname	string	m	<p>Surname of the user as printed in the ID document.</p> <p>Example: Mustermann</p>



			Names in Machine-Readable-Zone (MRZ) may be abbreviated due to space restriction. In this case, the unabbreviated names on idFrontSide (s. definition below) should be used.
givenName	string	m	<p>Given name of the user as printed in the ID document.</p> <p>Example: Hans</p> <p>Names in Machine-Readable-Zone (MRZ) may be abbreviated due to space restriction. In this case, the unabbreviated names on idFrontSide (s. definition below) should be used.</p>
countryCode	string	m	<p>The country of citizenship of the ID document holder.</p> <p>Contains either ISO 3166-1 alpha-2 or alpha-3 country code.</p> <p>Example: CHE</p>
identityType	string	m	<p>Type of the ID document, takes one of the following values:</p> <p>PAS: national passport</p> <p>IDC: Identity card. In the context of RA Service, the issuing country of an identity card and the citizenship of the document holder is always identical.</p>
serialNumber	string	m	<p>Serial Number of the ID document.</p> <p>Example: C1234567</p> <p>The combination of issuerCountryCode, idDocumentType, and serialNumber uniquely identifies an ID document.</p>
idExpiryDate	string	m	<p>Expiry date of the ID document.</p> <p>Either as ISO8601 timestamp string, or digits with hyphen-minus formatted as YYYY-MM-DD</p>
dateOfBirth	string	o	<p>The date of birth of ID document holder.</p> <p>Digits with hyphen-minus, formatted as YYYY-MM-DD</p> <p>Note that MM and DD in ID-documents may contain the special value 00 for unknown birthday, as defined by regulation. These special values are accepted by RA Service.</p>
placeOfBirth	string	see desc.	<p>The place of birth or the place where the identity is registered (national register), may be Bürgerort for Swiss citizens</p> <ul style="list-style-type: none">• For document type PAS and IDC, this attribute is contained in ID document but not in the Machine Readable Zone of a document. For swiss residence permit document, this attribute is not contained in the ID document.• The attribute must<ul style="list-style-type: none">○ be absent, if the ID document has no placeOfBirth information,○ contain the value of placeOfBirth as present in ID document, if it can be retrieved automatically or entered manually before import,



			<ul style="list-style-type: none">The attribute may contain the special value "SEE_DOC_IMAGES", if the information of placeOfBirth is available in ID document but cannot be extracted from ID document before import.
Compliance proof			
pdf	string	m	<p>A base64-encoded string containing a PDF document which proves the compliance of the user registration process.</p> <p>The PDF must be digitally signed. The public key used in the signature must be pre- configured in the RA Service by the RA Service Provider (i.e. Swisscom).</p> <p>The public key shall be provided to RA Service Provider (e.g. via e-Mail) by the RA Service tenant before the import API can be used.</p> <p>More than one public keys can be configured for a RA Service tenant</p> <p>Supported Cryptographical Parameters:</p> <p>Key type: RSA</p> <p>Key Length: 3072-bit or longer</p>
importRefer- ence	string	o	<p>An optional string used by the RA-Service client to correlate the current im- port request with other client-side processes.</p> <ul style="list-style-type: none">The string is not interpreted by RA-Service and stored as-is in the RA- Service DB.
termsAndCon- ditions	List of Json object	o	<p>User consents given to the (jurisdiction specific) terms and conditions (T&C) of AIS, usually represented as T&C PDFs electronically signed by the user.</p> <ul style="list-style-type: none">The RA-Service tenant must be configured to allow import of terms and conditions.
Other attributes			
initialAssur- anceLevel	int	o	<p>The assurance level of the ID proofing process and user authentication ac- cording to jurisdiction-dependent regulations</p> <ul style="list-style-type: none">The value can be 4 (Qualified Electronic Signature, QES) or 3 (Advanced Electronic Signature, AES). The value 2 and 1 are reserved for Swisscom internal usage.If the import request is intended for more than one jurisdictions, and the assurance levels for these jurisdictions differ, then the parameter specifies the highest level among them.The value specifies only the desired level of client. The effective assur- ance levels can be reduced to the levels configured in RA-Service for the client (i.e. tenant).
additionalAt- tributes	Json object	o	<p>Additional optional attributes. These attributes</p> <ul style="list-style-type: none">are not verified by RA-Service,cannot be used as criterion to search for an evidence,



			semantics of keys and values are agreed between client and RA Service.
claimedIdentity	string	o	The value was the name of tenant used in the service authentication (value of X-Auth-Tenant). The value, if specified, is silently discarded.
idpParams	Json object	o	Optional parameters to further specify idpAlias, e.g. authentication/authorization protocol used by IdP.
enforceArchive	boolean	o	See Table 1

Legend:

Column m: m=mandatory in finalized record, o=optional.

Additional request attributes are optional and are documented in the Swagger API [ras.swagger]

3.2.2 Response

HTTP status code	description
200	The evidence has been successfully imported. The response body contains essentially the request enriched with an internal unique id assigned to the evidence, and server-side status information (e.g. evidenceStatus, tenantEvidenceValidity). A client usually does not need to interpret the attributes in the response body. The semantics of the attributes is not described in details further.
404	If the Content-Type of the response is not application/json, the underlying infrastructure fails temporarily. The client MIGHT retry the request The recommended maximum number of retries is 2, the 1 st retry 15 second after the initial request, the 2 nd retry 35 seconds after the initial request.
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 The same retry algorithm as in status code 404 should be used.

3.2.3 Examples

3.2.3.1 Example 1: import evidence for signature, user consent managed by RA-Service, msisdn as identifier

The client has previously authenticated (as encoded in the header Authorization). The user's consent of using RA Service / AIS is managed by RA Service. The evidence contains the minimal set of attributes. Important HTTP header / fields are in bold.

Request

```
POST https://rasp.scapp.swisscom.com/api/evidences/import HTTP/1.1
Host: rasp.scapp.swisscom.com
Accept: application/json
Authorization: Bearer eyJhbGciOiJIUzUxMiJ9..._Ge5XolCnEJ5IsOcSeGS23Q
Content-Type: application/vnd.sc.ras.evidence.v1+json
```



swisscom

C1– Public

Content-Length: 3142673

```
{
  "msisdn": "41790000201",
  "surname": "Mustermann",
  "givenName": "Hans",
  "dateOfBirth": "1970-01-01",
  "language": "en",
  "identityType": "PAS",
  "countryCode": "CHE",
  "serialNumber": "C1234567",
  "idExpiryDate": "2026-05-10T00:00:00.000Z",
  "pdf": "JVB...(snipped)...g0K"
}
```

Response

HTTP/1.1 200 OK

Cache-Control: no-cache, no-store, max-age=0, must-revalidate

Connection: close

Date: Mon, 12 Dec 2022 22:55:27 GMT

Pragma: no-cache

Vary: Origin

Vary: Access-Control-Request-Method

Vary: Access-Control-Request-Headers

Content-Language: en

Content-Type: application/json

Expires: 0

Set-Cookie: JSESSIONID=C5478636E8C9C7D865F3D416AFF8790D; Path=/; Secure;

HttpOnly

Set-Cookie: __VCAP_ID__=82941bf0-4951-419e-7a41-272b; Path=/; HttpOnly; Secure

Strict-Transport-Security: max-age=15768000; includeSubDomains

```
{
  "id" : "6397b15e9554f54aeeb62718",
  "msisdn" : "41790000201",
  "surname" : "Mustermann",
  "givenName" : "Hans",
  "language" : "en",
  "countryCode" : "CHE",
  "identityType" : "pas",
  "serialNumber" : "C1234567",
  "idExpiryDate" : "2026-05-10",
  "dateOfBirth" : "1970-01-01T00:00:00Z",
  "evidenceStatus" : "waitingForUserConfirmation",
  "createdDate" : "2022-12-12T22:55:26.725478",
  "createdBy" : "qa4",
  "lastModifiedDate" : "2022-12-12T22:55:27.629647",
  "lastModifiedBy" : "qa4",
  "pdfFileId" : "User Evidence pdf - 6397b15e9554f54aeeb62718",
  "tenantName" : "qa4",
  "tenantClaimedIdentities" : [ ],
  "tenantEvidenceValidity" : "global",
  "jurisdictions" : [ {
    "jurisdiction" : "ZERTES",
    "initialAssuranceLevel" : 4,
  } ]
}
```



swisscom

```
    "currentAssuranceLevel" : 4
  }, {
    "jurisdiction" : "EIDAS",
    "initialAssuranceLevel" : 4,
    "currentAssuranceLevel" : 4
  } ]
}
```

3.2.3.2 Example 2: import evidence for signature, user consent managed by RA-Service client, msisdn as identifier

The user consent is managed by the RA-Service client in this example.

- The request imports the evidence PDF document signed by the client, and one terms-and-conditions PDF signed with AIS by the user. The request parameter consentSerialNumber also appears in the signer certificate in the terms-and-conditions PDF.
- The user is identified by msisdn.
- The tenant is contextual, entitled only for ZERTIS signatures.

Request

POST https://rasp.scapp-corp.swisscom.com/api/evidences/import

Accept-Language: en

Authorization: Bearer eyJh...(snipped)... o65A

Content-Type: application/vnd.sc.ras.evidence.v1+json

```
{
  "msisdn": "41790000201",
  "userId": "consent managed by client",
  "consentSerialNumber": "SAS0123456789ab",
  "language": "en",
  "surname": "Mustermann",
  "givenName": "Hans",
  "dateOfBirth": "1970-01-01",
  "identityType": "PAS",
  "countryCode": "CHE",
  "serialNumber": "C1234567",
  "idExpiryDate": "2026-05-10T00:00:00.000Z",
  "pdf": "JVB...(snipped)...",
  "termsAndConditions": [
    { "tcPdf": "JVB...(snipped)...0YK", "jurisdiction": "ZERTES" }
  ]
}
```

Response

HTTP/1.1 200 OK

Cache-Control: no-cache, no-store, max-age=0, must-revalidate

Connection: close

Date: Mon, 12 Dec 2022 23:32:23 GMT

Pragma: no-cache

Vary: Origin



swisscom

C1– Public

```
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Content-Language: en
Content-Type: application/json
Expires: 0
Set-Cookie: JSESSIONID=03...(snipped)...D4; Path=/; Secure; HttpOnly
Set-Cookie: __VCAP_ID__=82...(snipped)... 2b; Path=/; HttpOnly; Secure
Strict-Transport-Security: max-age=15768000; includeSubDomains
```

```
{
  "id" : "6397ba079554f54aeeb62721",
  "msisdn" : "41790000201",
  "surname" : "Mustermann",
  "givenName" : "Hans",
  "language" : "en",
  "countryCode" : "CHE",
  "identityType" : "pas",
  "serialNumber" : "C1234567",
  "idExpiryDate" : "2026-05-10",
  "dateOfBirth" : "1970-01-01T00:00:00Z",
  "consentSerialNumber" : "SAS0123456789ab",
  "userId" : "consent managed by client",
  "evidenceStatus" : "confirmedAndSigned",
  "createdDate" : "2022-12-12T23:32:23.100717",
  "createdBy" : "dis01",
  "lastModifiedDate" : "2022-12-12T23:32:23.277973",
  "lastModifiedBy" : "dis01",
  "pdfFileId" : "User Evidence pdf - 6397ba079554f54aeeb62721",
  "tenantName" : "dis01",
  "tenantClaimedIdentities" : ["dis02", "dis01" ],
  "tenantEvidenceValidity" : "contextual",
  "jurisdictions" : [ {
    "jurisdiction" : "ZERTES",
    "initialAssuranceLevel" : 4,
    "currentAssuranceLevel" : 4
  } ]
}
```

3.2.3.3 Example 3: import evidence for signature, user consent managed by RA-Service client, identifier is a banking id

This example is similar to example 2, except that

- the identifier is not MSISDN. The support of non-MSISDN is introduced in RA-Service v3.0.
- the tenant is global and supports both ZERTES and EIDAS jurisdictions

Request

```
POST https://rasp.scapp-corp.swisscom.com/api/evidences/import
Authorization: Bearer ey...(snipped)... VQ
Content-Type: application/vnd.sc.ras.evidence.v1+json
```

```
{
  "idpAlias": "PFM",
```



swisscom

C1– Public

```
"userId":"70012345",
"consentSerialNumber":"e569dd69-568d-47f6-8172-7710236cb507",
"language":"en",
"surname":"Mustermann",
"givenName":"Hans",
"dateOfBirth":"1970-01-01",
"identityType":"PAS",
"countryCode":"CHE",
"serialNumber":"C1234567",
"idExpiryDate":"2026-05-10T00:00:00.000Z",
"pdf":"JV..(snipped)..0K",
"termsAndConditions":[
  {"tcPdf":"dX..(snipped)..M=","jurisdiction":"ZERTES"},
  {"tcPdf":"dX..(snipped)..w==" ,"jurisdiction":"EIDAS"}
]
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Connection: close
Date: Tue, 13 Dec 2022 00:04:06 GMT
Pragma: no-cache
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Content-Language: en
Content-Type: application/json
Expires: 0
Set-Cookie: JSESSIONID=A9...(snipped)...FF; Path=/; Secure; HttpOnly
Set-Cookie: __VCAP_ID__=77...(snipped)..9a; Path=/; HttpOnly; Secure
Strict-Transport-Security: max-age=15768000; includeSubDomains
```

```
{
  "id" : "6397c175c6717611b88d26e3",
  "surname" : "Mustermann",
  "givenName" : "Hans",
  "language" : "en",
  "countryCode" : "CHE",
  "identityType" : "pas",
  "serialNumber" : "C1234567",
  "idExpiryDate" : "2026-05-10",
  "dateOfBirth" : "1970-01-01T00:00:00Z",
  "consentSerialNumber" : "e569dd69-568d-47f6-8172-7710236cb507",
  "userId" : "70012345",
  "evidenceStatus" : "confirmedAndSigned",
  "createdDate" : "2022-12-13T00:04:05.605559",
  "createdBy" : "qa4",
  "lastModifiedDate" : "2022-12-13T00:04:06.036454",
  "lastModifiedBy" : "qa4",
  "pdfFileId" : "User Evidence pdf - 6397c175c6717611b88d26e3",
  "tenantName" : "qa4",
  "tenantClaimedIdentities" : [ ],
  "tenantEvidenceValidity" : "global",
  "jurisdictions" : [ {
```



swisscom

C1– Public

```
"jurisdiction" : "ZERTES",  
"initialAssuranceLevel" : 4,  
"currentAssuranceLevel" : 4  
, {  
  "jurisdiction" : "EIDAS",  
  "initialAssuranceLevel" : 4,  
  "currentAssuranceLevel" : 4  
} ]  
}
```




4 Evidence Query

4.1 Lookup the registration status of a user

Given a user's identifier, RA Service client can use the lookup API to query the current registration status of the user. The client could use the information to determine whether an ID proofing process and evidence import is necessary.

See the `POST /evidences/lookup` call in [ras.swagger] for details.

4.2 (Legacy) Query of evidence for qualified signature

RA Service client can use the verification API for AIS to indirectly query whether a user has completed the registration process for Qualified Signature in a specific context or in any context.

4.2.1 Request

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

Request Parameters

Name	type	m	description
claimedIdentity	string	o	The queried context of Qualified Signature. If the parameter is absent, the "global" context is queried. A user who has been registered for "global" context can sign in any context.
msisdn	string	m	The registered mobile phone number of the user
givenName	string	m	The registered given name of the user. It must be specified as part of distinguishedName
surname	string	m	The registered surname of the user. It must be specified as part of distinguishedName
countryCode	string	m	The registered nationality of the user. It must be specified as part of distinguishedName
distinguishedName	string	m	Combines the parameters givenName, surname, and countryCode in form of string representation of a X.500 Distinguished Name (RFC 4514). The common-name RDN of the distinguished name cannot be empty.
assuranceLevel	string	m	Must be set to 4 in query for Qualified Signature
jurisdiction	string	o	The eligible jurisdiction of evidence. Default: zertes

4.2.2 Response

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

HTTP status code	description
	RA Service returns the public ID of the evidence object which proves the compliance of referred registration process. The ID is returned as the json attribute <code>evidenceId</code> in the HTTP response body.
404	<p>If content type is <code>application/json</code> and the <code>statusCode</code> attribute in response is 404, the user has not been registered for a context or the registration is not compliant compliant for Qualified Signature.</p> <p>Otherwise the underlying infrastructure fails temporarily. The client MIGHT retry the request</p> <p>The recommended maximum number of retries is 2, the 1st retry 15 second after the initial request, the 2nd retry 35 seconds after the initial request.</p>
500	Client-side (e.g. invalid parameter) or server-side application error.
502, or 503	<p>Underlying infrastructure fails temporarily. The client MIGHT retry the request</p> <p>The same retry algorithm as in status code 404 should be used.</p>

Example 1: contextual query, 200 response

The request queries the registration status of a user in the context docu-c1 for Qualified Signature according to ZERTES. The response is positive.

```

POST https://rasp.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: rasp.scapp.swisscom.com
User-Agent: Ras::RasClient/0.01
Content-Type: application/vnd.sc.ras.evidence.v1+json
Content-Length: 133

{"claimedIdentity":"docu-c1","distinguishedName":"gn=Hans,sn=Muster-
mann,cn=not-empty,c=CH","msisdn":"41790000200","assuranceLevel":4}

HTTP/1.1 200 OK
Connection: close
Date: Thu, 07 May 2020 12:06:21 GMT
Content-Language: en
Content-Length: 88
Content-Type: application/vnd.sc.ras.evidence.v1+json; charset=UTF-8
Set-Cookie: JSESSIONID={snipped}; Path=/; HttpOnly
Set-Cookie: __VCAP_ID__=4ac6ea01-4e18-4ef4-5f13-f8f2; Path=/; HttpOnly
Strict-Transport-Security: max-age=15768000; includeSubDomains
X-Request-Id: 9bd6da8b-2b62-493e-8957-d49197e2451a
X-Session-Id: {snipped}
X-Vcap-Request-Id: 294fdc53-134a-47fd-64f7-95b0b5bc19e5

{
  "evidenceId" : "RAS5eb3df21c1a34e0012cf224b",

```



swisscom

```
"serialNumber" : "SAS011k58obxyhr"
}
```

Example 2: "global" query, jurisdiction EIDAS, 404 response

The queries the registration status of a user for Qualified Signature according to EIDAS without any contextual restriction. The response is negative.

```
POST https://rasp.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: rasp.scapp.swisscom.com
User-Agent: Ras::RasClient/0.01
Content-Type: application/vnd.sc.ras.evidence.v1+json
Content-Length: 128
```

```
{"distinguishedName": "gn=Hans, sn=Mustermann, cn=not-
empty, c=CH", "msisdn": "41790000200", "jurisdiction": "eidas", "assuranceLevel": 4}
```

```
HTTP/1.1 404 Not Found
Connection: close
Date: Thu, 07 May 2020 12:18:57 GMT
Content-Language: en
Content-Length: 148
Content-Type: application/json; charset=UTF-8
Set-Cookie: JSESSIONID={snipped}; Path=/; HttpOnly
Set-Cookie: __VCAP_ID__=361ecd86-997e-40b7-777b-0aaf; Path=/; HttpOnly
Strict-Transport-Security: max-age=15768000; includeSubDomains
X-Request-Id: af518410-7f47-485a-81b0-4563949492e6
X-Session-Id: {snipped}
X-Vcap-Request-Id: 69cd4c9f-f189-4629-4368-75286bd55b31
```

```
{
  "statusCode" : 404,
  "message" : "No confirmed evidences found for mobile number 41790000200",
  "exceptionClass" : "EntityNotFoundException"
}
```



swisscom

5 Document Control

Change Control

Version	Date	Executing OE	Description / Nature of tasks
1.1	13.12.2022	DBU-ST5	Update API description and examples for backend v3.0, which supports non-msisdn identifiers. Add lookup call.
1.0	07.05.2020	B2B-BPN-PFR-IDS	Update API description and examples for the current backend version (v2.40.0.11) Add description to special terms. For public release.
0.2	24.07.2018		Documentation completed for RA-Service up to version 2.20. For internal and restricted use only
0.1	12.07.2018		Initial version