Client certificate

Sensaru Cloud supports client certificates for authentication. Client certificates are used internally to connect backend modules. They can also be used to access the REST or RPC backend.

Common name

The common name of all client certificates contains a base64-encoded JSON. No other fields should be set in the certificate. To get the common name, the JSON must first be stripped of whitespaces. For example:

```
{"type":"user","sp":"48109350-1db6-11e9-8e66-2f71a0be4cc5","id":"157d9350-1db8-11e9-8e66-2f71a0be4cc5","in
1,"date":1584008905000,"version":1}
```

This JSON then must be base64-encoded and becomes:

```
eyJ0eXBlIjoidXNlciIsInNwIjoiNDgxMDkzNTAtMWRiNi0xMWU5LThlNjYtMmY3MWEwYmU0Y2M1IiwiaWQiOiIxNT
```

On linux you can use the command `base64` to do that:

```
echo
'{"type":"user","sp":"48109350-1db6-11e9-8e66-2f71a0be4cc5","id":"157d9350-1db8-11e9-8e66-2f71a0be4cc5","in
1,"date":1584008905000,"version":1}' | base64 -w 0
```

Generate and sign a certificate

All certificates must then be signed by the "ib company Root CA 5" using `mellonbot`. See the CA section for more details.

User client certificte

A user client certificate must have a common name with the following JSON:

For a system provider user:

```
{
  "type": "user",
  "sp": "<system provider ID>",
  "id": "<user ID>",
  "index": 1,
  "date": 1584008905000,
```

```
  "version": 1
}
```

For a system distributor user:

```
{
  "type": "user",
  "sd": "<system provider ID>",
  "id": "<user ID>",
  "index": 1,
  "date": 1584008905000,
  "version": 1
}
```

For a business partner user:

```
{
  "type": "user",
  "bp": "<system provider ID>",
  "id": "<user ID>",
  "index": 1,
  "date": 1584008905000,
  "version": 1
}
```

The properties have the following meaning:

Property name	Description
`type`	Always `user` for user client certificates.
`id`	The ID of user.
`index`	Specify `1` for a new certificate. Every new certificate should increment the index. The index can be used to invalidate old certificates.
`date`	The creation date of the certificate.
`version`	The version of the JSON for future extensions.

Impersonate user

With user client certificates it is possible to impersonate other users the client certificate's principal has access to. To do that pass the header `C1-IMPERSONATE` with the system distributor ID or the business partner ID and the user ID to impersonate.

To impersonate a business partner user:

`C1-IMPERSONATE: bp=1aa890e1-6f6b-11ea-8461-c79e27cbb96c,id=1aa890e1-6f6b-11ea-8461-c79e27cbb96c`

To impersonate a system distributor user:

`C1-IMPERSONATE: sd=1aa890e1-6f6b-11ea-8461-c79e27cbb96c,id=1aa890e1-6f6b-11ea-8461-c79e27cbb96c`

System provider users cannot be impersonated.

Module client certificate

Module client certificates are used by modules to authenticate with C1 Core. A module client certificate only differs from the user client certificate in the JSON structure. A module client certificate might look like this:

```
{
  "type": "module",
  "id": "<module ID>",
  "bp|sd|sp": "<business partner ID, system distributor ID or system provider ID>",
  "index": 1,
  "date": 1578005399878,
  "version": 1,
  "environment": "<dev, staging or prod>"
}
```

One line example:

```
{"type":"module","id":"c1-my-module","index":1,"date":1578005399000,"version":1,"environment":"dev"}
```

Property name	Description
`type`	Always `module` for module client certificates.
`id`	The ID of the module. E. g. `c1-device-management`.
`bp`	If this module should be associated to a business partner, specify the business partner ID in this property. Cannot be used together with `sd` or `sp`. When the module is associated to a business partner, it cannot access data of other business partners or higher level principals.
`sd`	If this module should be associated to a system distributor, specify the system distributor ID in this property. Cannot be used together with `bp or sp`. When the

Property name	Description
	module is associated to a system distributor, it cannot access data of other system distributors or higher level principals.
`sp`	If this module should be associated to a system provider, specify the system provider ID in this property. Cannot be used together with `bp` or `sd`. When the module is associated to a system provider, it cannot access data of other system providers or super users.
`index`	Specify `1` for a new certificate. Every new certificate should increment the index. The index can be used to invalidate old certificates.
`date`	The creation date of the certificate.
`version`	The version of the JSON for future extensions.
`environment`	Specifies the environment this certificate can be used in. Can be `dev`, `staging` or `prod`.

Note

When neither `bp`, `sd` and `sp` are specified, the module is available to all principals.

C1 Auth client certificate

For C1 Core to be able to manage users in C1 Auth, a special certificate with the following JSON is needed:

```
{
  "type": "authorizationServiceClient",
  "name": "c1-core",
  "id": "49e9ec70-eed6-11e9-980e-7374595fcc61",
  "index": 1,
  "date": 1584008905000,
  "version": 1
}
```

The ID can be randomly selected. It is used to identify a user and can be used in C1 Auth to block a specific user.

Edge client certificate

Home clients require the following JSON:

```
{
  "type": "apartment",
  "id": "<economic unit ID>[.<property ID>[.<administration unit ID>]]",
  "bp": "<business partner ID>",
  "subId": <sub ID>,
  "index": 1,
  "date": 1578005399878,
  "version": 1
}
```

Property name	Description
`type`	Always `apartment` for edge client certificates (also when it is a certificate for a building).
`id`	The ID of the edge client. It consists of the economic unit ID, the optional property ID and the optional administration unit ID seperated by dots (`.`). These must match the IDs in the ERP system for automatic association.
`bp`	Edge clients are always associated to a business partner. Fill this field with the business partner ID. It is not possible to associate an edge client with a system distributor or system provider.
`subId`	Normally fill this with "1". When there are multiple clients with the same `id`, `subId` can be used to be able to connect them all to Sensaru Cloud. Currently the values `1`, `2` and `3` are supported.
`index`	Specify `1` for a new certificate. Every new certificate should increment the index. The index can be used to invalidate old certificates.
`date`	The creation date of the certificate.
`version`	The version of the JSON for future extensions.

One line example:

```
{"type":"apartment","id":"1000.1.1","subId":1,"bp":"d1faa8d0-2db4-11ea-af75-674069e60b74","index":1,"date":1578005399878,"version":1}
```