HTTP-Signature

Mandatory header parameters:

Date

Current date in HTTP Date RFC format(https://tools.ietf.org/html/rfc7231#section-7.1.1.2). We will tolerate a drift of +-1 minutes.

Please note that drift is the allowed difference between the exact time when the call was received at Belfius' side, and the content of DATE header. If the DATE headers time value differs by more than +-1 minute, request will be considered as Invalid.

Example:

```
Date: Tue, 15 Nov 1994 08:12:31 GMT
```

Digest

Digest of the payload following RFC3230 on instance digests.

Allowed values by Belfius are SHA256.

Example:

```
payload_string = {\"data\":{\"type\":\"sample-token\",\"attributes\":{\"appReference\":\"12345\"}}}"

digest = "SHA256=" + BASE64_ENCODING(SHA256(payload_string))
```

Signature

Signature header based on https://tools.ietf.org/html/draft-cavage-http-signatures-10.

Steps to create the Signature header parameter

Step 1: Create the Date header

Note that the maximum drift of +-1 minutes is allowed

Example:

Date: Tue, 15 Nov 1994 08:12:31 GMT

Step 2 : Create the Digest (see above)

Example:

digest = "SHA256=" + BASE64_ENCODE(SHA256(payload_string))

Step 3 : Build the (request target) virtual header

In order to build the signature, you will need a virtual header named (request-target) (the parentheses are important). The (request-target) is the string concatenation of the HTTP method (in lowercase) *with the path (excluding host:port) and query parameters if there are*.

Example:

path = "/some-context/sample-tokens"

method = "post"

request_target = method + " " + path

➔ "post /some-context/sample-tokens"

Example with query parameters :

path = "/some-context/sample-tokens?a=1&b=2"

method = "post"

request-target = method + " " + path

➔ "post /some-context/sample-tokens?a=1&b=2"

Notes

- path: it is the complete URI invoked by TPP, including all query and path parameters, but excluding host (and any port if there are).
- TPP must make sure that request-target includes the method+SPACE+full URI

Step 4 : Build the signed headers list

In order to check which headers have been signed and in what order, TPP has to provide a list of the header names (lowercase and in the same order as used to create the signing string).

This list can vary but *at least* the following headers (request-target), date, digest, request-id parameters need to be sign. If the TPP decide to pass an access-token in the authorization header parameter. This header parameter must be used to validate the signature.

Example:

headers = "(request-target) " + "date " + "digest "+ "request-id"

➔ "(request-target) date digest request-id"

Example with additional header parameter:

headers = "(request-target) " + "date " + "digest "+ "request-id "+ "authorization"

➔ "(request-target) host date digest request-id authorization"

Step 5 : Create signing string

The signing string is the concatenation of the signed headers names (in lowercase) and values separated by a 'new line' : \n. Note that if additional header parameters have been passed in step 4, the signing string should contains them

Example:

signing_string = "(request-target): post /some-context/sample-tokens\n" + "date: Tue, 15 Nov 1994 08:12:31 GMT\n" + "digest: SHA-256=ZVJ9LmCElQs4E6QiWwMUGUqe3c74B6gcXhgj3UIZEUPFkrLoXSGAK2Z2vYN7xKZmOgPEby0xb8RWy5U1eoTGew==\n" + "request-id": 2323enkjdgdgjd"

➔ "(request-target): post /some-context/sample-tokens\ndate: Tue, 15 Nov 1994 08:12:31 GMT\ndigest: SHA-256=ZVJ9LmCElQs4E6QiWwMUGUqe3c74B6gcXhgj3UIZEUPFkrLoXSGAK2Z2vYN7xKZmOgPEby0xb8RWy5U1eoTGew==\nrequest-id: 2323enkjdgdgjd"

Example when additional parameter:

signing_string = "(request-target): post /some-context/sample-tokens\n" + "date: Tue, 15 Nov 1994 08:12:31 GMT\n" + "digest: SHA-256=ZVJ9LmCElQs4E6QiWwMUGUqe3c74B6gcXhgj3UIZEUPFkrLoXSGAK2Z2vYN7xKZmOgPEby0xb8RWy5U1eoTGew==\n" + "request-id": 2323enkjdgdgjd\n" + "authorization: bearer FDDFGDFGDFGDFGDFGFDG\n"

➔ "(request-target): post /some-context/sample-tokens\ndate: Tue, 15 Nov 1994 08:12:31 GMT\ndigest: SHA-256=ZVJ9LmCElQs4E6QiWwMUGUqe3c74B6gcXhgj3UIZEUPFkrLoXSGAK2Z2vYN7xKZmOgPEby0xb8RWy5U1eoTGew==\nrequest-id: 2323enkjdgdgjd\nauthorization : bearer FDDFGDFGDFGDFGDFGFDG"

Step 6 : Build the Signature header

The signature header is a combination of several sub-headers

- **keyId**: This is the TPP-ID
- **algorithm**: the digital signature algorithm used to generate the signature, matching the signature algorithm used for the application certificate (e.g. rsa) and SHA-256 as the hashing function.
- **headers**: The list of HTTP headers created in step 4;
- **signature**: the Base64-encoded digital signature of the signing string created in step 5.

Note that all these sub-headers are comma separated (not space).

Example:

key_id = "62f02718-eeee-46e1-b5eb-e8fd6e799c2e"//TPP-ID for now, could be unique-application-id in future.

algorithm = "rsa-sha256"

headers = "(request-target) date digest request-id [OTHER HEADERS]"

signature = BASE64_ENCODE(RSA_SHA256_SIGN(PRIVATE_KEY, SIGNING_STRING_FROM_STEP5)) **//MIN SHA_256 RSA Assymetric**

Signature = "keyId=\"" + key_id + "\"," + "algorithm=\"" + algorithm + "\"," + "headers=\"" + headers + "\"," + "signature=\"" + signature + "\""

➔ "keyId=\"62f02718-eeee-46e1-b5eb-e8fd6e799c2e\",algorithm=\"rsa-sha256\",headers=\"(request-target) date digest request-id authorization-header\",signature=\"SjWJWbWN7i0wzBvtPl8rbASWz5xQW6mcJmn+ibttBqtifLN7Sazz6m79cNfwwb8DMJ5cou1s7uEGKKCs+FLEEaDV5lp7q25WqS+lavg7T8hc0GppauB6hbgEKTwblDHYGEtbGmtdHgVCk9SuS13F0hZ8FD0k/5OxEPXe5WozsbM=\""