Message Signing Sensor API V3

V3 Signature Creation and validation for incoming Api-requests and outgoing Api-responses

For all V3-incoming-api calls signature creation and -validation is done using the following procedure:

The following http-headers must be added to the message:

- SensorID - contains the hub-assigned sensorid (format is GUID), *lowercase* and *without dashes*

if a sensor is configured to use a certificate, the following http-headers must be added to the message:

- CertificateThumbprint - contains *uppercase*-string value of thumbprint of certificate used for signing the message
- Client-Signature - contains the signature **converted to Base64**

payload for the signature will be concatenation of {httpMethod}|{UPPER(requestUrl)}|{SensorID}|UPPER({thumbprintValue})|{messagepayload} where the messagepayload is the JSON-body of the message to be sent and the sensorid is represented as a lowercase string without dashes.

example of payload:

'POST|HTTPS://SERVER.SERVER.COM/SENSOR/V3
/TRIGGER|88666a8a218746aca3193c7e7135ad96|5A4B1162987B139DD540EB751A92FB2EA11C61CC|{"Transaction": {"PropertyBag": null,"
ReferencedTransaction": null,"Timestamp": "20191003150441398+0200","Counter": 133713371337,"SensorId": "88666a8a-2187-46ac-a319-
3c7e7135ad96","ExternalTransactionId": "App-133713371337"},"Tokens": [{"TokenValue": "88a36968-1337-1337-1337-13f35bea54ef","
TokenType": "ACCOUNTID","PropertyBag": []}],"Sensor": {"Identifiers": [{"IdentifierValue": "1337","IdentifierType": "WP"}],"SensorLocation":
{"Latitude": 52.3782272,"Longitude": 4.89759,"Altitude": 0.0,"CellId": 0,"LocationAreaCode": 0,"MobileCountryCode": 0,"MobileNetworkCode":
0}},"Service": {"ServiceId": 21},"ServiceRequestData": {"RequestInternalIpAddress": null,"RequestExternalIpAddress": null,"
RequestSensorLocalTimestamp": "20191003150441398+0200","Amount": 0,"CurrencyCode": "EUR","RequestMode": "1","PropertyBag": [{"Key":
"starttime","Value": "20190926145313+0200"}, {"Key": "energylabel","Value": "D"}]}}'

The signature is created by hashing the payload mentioned above with a **SHA256 hash** using the private key of the used certificate.

For all V3-outgoing responses signature creation and -validation is done using the following procedure:

Verify message:

- CertificateThumbprint: <Platform certificate thumbprint>
- Server-Signature: <*Signature*> Base64EncodedByte string

payload for the signature will be concatenation of {statusCode}|{certificate.Thumbprint}|{messagepayload} where the messagepayload is the JSON-body of the message received.