

itsme Generic Signature Validation Service Policy Version 1.0

This document describes which policy requirements are implemented by the default itsme Signature Validation Service.

31-07-2018

| | |
|----------------------|---|
| Name | COMPL_POL_GenericSignatureValidationServicePolicy |
| OID | 1.3.6.1.4.1.49274.1.1.4.1.0 |
| Applicable from | 02-08-2018 |
| Status | Approved |
| Author | Wim Coulier |
| Owner | Wim Coulier |
| Classification level | Public |



Table of content

| | | |
|-------------|---|----------|
| 1. | INTRODUCTION | 4 |
| 1.1. | Overview | 4 |
| 1.2. | Business or Application Domain | 4 |
| 1.3. | Document and policy(ies) names, identification and conformance rules | 4 |
| 1.3.1. | Policy identification | 4 |
| 1.3.2. | Distribution points | 4 |
| 1.4. | Signature validation service policy document administration | 4 |
| 1.4.1. | Signature validation service policy authority | 4 |
| 1.4.2. | Contact person | 5 |
| 1.4.3. | Approval procedures | 5 |
| 1.5. | Definitions and Acronyms | 5 |
| 1.5.1. | Abbreviations | 5 |
| 1.5.2. | Definitions | 5 |
| 2. | SIGNATURE APPLICATION PRACTICES STATEMENTS | 6 |
| 3. | BUSINESS SCOPING PARAMETERS | 7 |
| 3.1. | BSPs mainly related to the concerned application/business process | 7 |
| 3.2. | BSPs mainly influenced by the legal/regulatory provisions associated to the concerned application/business process | 7 |
| 3.2.1. | Legal type of the signatures | 7 |
| 3.2.2. | Commitment assumed by the signer | 7 |
| 3.2.3. | Level of assurance on timing evidences | 7 |
| 3.2.4. | Longevity and resilience to change | 7 |
| 3.3. | BSPs mainly related to the actors involved in creating/augmenting/validating signatures | 8 |
| 3.3.1. | Identity (and roles/attributes) of the signers | 8 |
| 3.3.2. | Level of assurance required for the authentication of the signer | 8 |
| 3.3.3. | Signature creation devices | 8 |



| | | |
|-------------|---|-----------|
| 3.4. | Other BSPs | 8 |
| 3.4.1. | Other information to be associated with the signature | 8 |
| 3.4.2. | Cryptographic suites | 8 |
| 3.4.3. | Technological environment | 8 |
| 4. | REQUIREMENTS / STATEMENTS ON TECHNICAL MECHANISMS AND STANDARDS IMPLEMENTATION | 8 |
| 5. | OTHER BUSINESS AND LEGAL MATTERS | 10 |
| 6. | COMPLIANCE AUDIT AND OTHER ASSESSMENTS | 10 |



1. INTRODUCTION

1.1. Overview

This document describes the requirements that are being followed for the default BMID Signature Validation Service. This service receives signed data and signature from the Driving Application (DA) from a Service Provider via an API and performs signature validation on the received signatures.

1.2. Business or Application Domain

This signature validation service does not pose any limitations on the scope and boundaries of the business (application) domain in which the signature validation service policy(ies) is(are) suitable for use.

This signature validation service policy does not pose any limitation on the transactional context in which the signature is created. See also clause 3.1.

1.3. Document and policy(ies) names, identification and conformance rules

1.3.1. Policy identification

Signature validation service policy name: COMPL_POL_GenericSignatureValidationServicePolicy

OID: 1.3.6.1.4.1.49274.1.1.4.1.0

1.3.6.1.4.1.49274 (BMID organization).1 (Compliance Domain).1 (Policies).4
(COMPL_POL_GenericSignatureValidationServicePolicy).1 (major version).0 (minor version)

1.3.2. Distribution points

The latest version of this policy will always be present at <https://www.itsme.be/legal/document-repository>

Older version of this policy will be present at the same location.

At this moment no machine processable formats are available for the signature policy related to this signature validation service policy.

1.4. Signature validation service policy document administration

1.4.1. Signature validation service policy authority

The BMID TSP Management Board is the authority that is responsible for the signature validation service policy document and the signature validation policy(ies) it covers. The BMID TSP Management Board is part of Belgian Mobile ID SA/NV (registered under number 0541.659.084).

The BMID TSP Management Board can be contacted via the contact form at the itsme website at <https://www.itsme.be/en/contact> or via postal mail at TSP Management Board; Belgian Mobile ID SA/NV; Sint Goedele plein 5, 1000 Brussels.



It shall also provide information identifying the public key certificate corresponding to the private key used by the BMID TSP Management Board to digitally sign the signature validation service policy document.

1.4.2. Contact person

Questions about this signature validation service policy should be directed to the president of the BMID TSP Management Board via the contact form on the itsme website at <https://www.itsme.be/en/contact> or via postal mail at TSP Management Board; Belgian Mobile ID SA/NV; Sint Goedele plein 5, 1000 Brussels..

1.4.3. Approval procedures

The approval procedures for this signature validation service policy consists of a formal approval by the members of the BMID TSP Management Board during a meeting or via and e-mail procedure.

1.5. Definitions and Acronyms

1.5.1. Abbreviations

| | |
|---------|--|
| AdES | : Advanced Electronic Signature |
| AdES/QC | : Advanced Electronic Signature created with a Qualified Certificate |
| BMID | : Belgian Mobile ID NV /SA |
| CA | : Certification Authority |
| DA | : Driving Application |
| OCSP | : Online Certificate Status Protocol |
| OID | : Object Identifier |
| PKI | : Public Key Infrastructure |
| QES | : Qualified Electronic Singature |
| QTSP | : Qualified Trust Service Provider |
| QSCD | : Qualified Signature Creation Device |
| SCA | : Signature Creation Application |
| SVA | : Signature Validation Application |
| TSP | : Trust Service provider |
| XML | : eXExtensible Markup Language |

1.5.2. Definitions

(signature) commitment type: signer-accepted indication of the exact implication of a digital signature

driving application: application that uses a signature creation system to create a signature or a signature validation application in order to validate digital signatures or a signature augmentation application to augment digital signatures

eIDAS regulation: Regulation (eu) no 910/2014 of the European parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

itsme Qualified Sign Validation Service: the qualified signature validation service offered by BMID

Qualified Validation Service for qualified electronic signatures: as specified in Regulation (EU) No 910/2014 [i.1], Article 33

relying party: natural or legal person that relies upon the signature validation service

signature applicability rules: set of rules, applicable to one or more digital signatures, that defines the requirements for determination of whether a signature is fit for a particular business or legal purpose



signature augmentation: process of incorporating to a digital signature information aiming to maintain the validity of that signature over the long term

signature creation device: configured software or hardware used to implement the signature creation data and to create a digital signature value

signature validation application: an application that validates a signature against a signature validation policy, consisting of a set of validation constraints and that outputs a status indication (i.e. the signature validation status) and a signature validation report

signature validation policy: list of constraints processed by the SVA

signature validation report: comprehensive report of the validation provided by the SVA to the DA and allowing the DA to inspect details of the decisions made during validation and investigate the detailed causes for the status indication provided by the SVA

Signature Validation Service (SVS) Policy: set of rules that indicates the applicability of a signature validation service to a particular community and/or class of application with common security requirements

signature validation status: one of the following indications: TOTAL-PASSED, TOTAL-FAILED or INDETERMINATE.

signature validation: process of verifying and confirming that a digital signature is technically valid

signature verification: process of checking the cryptographic value of a signature using signature verification data

signer: entity being the creator of a digital signature

subscriber: Legal or natural person bound by agreement with BMID to any subscriber obligations. In the BMID ecosystem, subscribers consist as well from customers (Service Providers) that have signed a contract with BMID as end-users who only have accepted the terms and conditions of the services they are using.

trust service practice statement: statement of the practices that a trust service provider employs in providing a trust service

validation of qualified electronic signature: validation as specified in Regulation (EU) No 910/2014 [i.1], Article 32

validation of qualified electronic seals: validation as specified in Regulation (EU) No 910/2014 [i.1], Article 40

validation service: system accessible via a communication network, which validates a digital signature

validation: process of verifying and confirming that a certificate or a digital signature is valid

verifier: entity that wants to validate or verify a digital signature

2. SIGNATURE APPLICATION PRACTICES STATEMENTS

This signature validation service policy shall be implemented by a solution conform to the latest version of the BMID Practice Statement (with name COMPL_POL_BMIDpracticeStatement and OID 1.3.6.1.4.1.49274.1.1.2.1.0).

The Service Provider who operates the Driving Application is responsible for the security of the Driving Application. Between Driving Application and Signature Validation Application, mutual authentication shall be performed.



3. BUSINESS SCOPING PARAMETERS

3.1. BSPs mainly related to the concerned application/business process

This signature validation service policy is not limited to a certain application or business process. The Driving Application is responsible for all business aspects. This validation service policy does not impose the validation of any signature applicability rules. If the application or business process needs the verification of signature applicability rules, it is the responsibility of the Service Provider that operates the Driving Application to perform such verification.

In case there are multiple signatures on the signed data, the Signature Validation Application shall include a validation result about each signature it was able to detect in the signature validation report. However the Signature Validation Application is not necessarily able to detect all types of electronic signatures (e.g. it cannot detect non-advanced electronic signatures). As such it is the responsibility of the Service Provider to verify whether all signatures that are supposed to be present on the signed data are indeed covered by the signature validation report.

This signature validation service policy does not foresee signatures to be augmented during or after the validation process. Signature augmentation, preservation and archival are the responsibility of the Service Provider.

3.2. BSPs mainly influenced by the legal/regulatory provisions associated to the concerned application/business process

3.2.1. Legal type of the signatures

The signature validation report shall specify whether the validated signature concerns a qualified electronic signatures, advanced electronic signature supported by a qualified certificate, advanced electronic signature, qualified electronic seal, advanced electronic seal supported by a qualified certificate or advanced electronic seal.

3.2.2. Commitment assumed by the signer

In case a commitment type is indicated in the signature the signature validation report will mention this commitment.

3.2.3. Level of assurance on timing evidences

The signature validation report will indicate whether timestamps were used to determine the best signature time. It will however not differentiate between qualified and non-qualified timestamps.

3.2.4. Longevity and resilience to change

The signature validation report does not give any indication on the expected longevity and resilience to change of the signature.



3.3. BSPs mainly related to the actors involved in creating/augmenting/validating signatures

3.3.1. Identity (and roles/attributes) of the signers

In case a signer role/attribute is indicated in the signature the signature validation report will mention this role/attribute.

3.3.2. Level of assurance required for the identity of the signer

The signature validation report will not give an indication on the level of assurance for the identity of the signer. But of course due to the indication on the level (qualified or not) of the signers certificate, the relying party has an indication about this via that parameter.

3.3.3. Signature creation devices

The signature validation report only gives indications about the signing creation devices if the signature contains a Qualified Electronic Signature (in that case the private key was protected by a QSCD). In other cases it does not give any indication about the use of a Signature Creation Device for the protection of the private key.

3.4. Other BSPs

3.4.1. Other information to be associated with the signature

If applicable, the following information will be taken up in the validation report: Content Type, Content Identifier, Content Hints, Signature Production Place.

3.4.2. Cryptographic suites

The validation report will indicate the cryptographic algorithms and key lengths that were used for cryptographic operations. The signature validation report will however not indicate whether the algorithm and key lengths were still trustworthy at the time of use.

3.4.3. Technological environment

The signature validation service will only be offered via the BMID Sign API.

4. REQUIREMENTS / STATEMENTS ON TECHNICAL MECHANISMS AND STANDARDS IMPLEMENTATION

4.1. Technical mechanisms

4.1.1. Approach towards signing time

The signing time against which the validity of the signature will be verified will be defined as follows: The signing time will be attempted to be defined based on a Proof of Existence (e.g. timestamp or evidence record) present in the signature. In case this fails (e.g. no proof of existence can be extracted



from the signature). If such Proof of Existence is not available, and the Driving Application has indicated a time that should be used as signing time, this time indication will be used. In absence of a Proof of Existence and indication from the Driving Application, the signing time will be set to the validation time.

Note: The embedded (claimed) signing time is never used.

4.1.2. Defining the qualified status of a signature or seal

In order to define whether a signature or seal is a qualified electronic signature or seal with a private key residing in a QSCD, the following verifications will be performed by the Signature Validation Application.

4.1.2.1 Definition of the list of trusted services for the signing or sealing certificate

The validation service will verify whether the signing or sealing certificate can be chained to a trust anchor that is indicated on a EU Member State trusted list (TL). In order to do so the TLs will be downloaded and the validity of the TLs will be verified (signature on the TL and expiration).

The trusted services defined in these TLs will then be filtered according to the signing / sealing certificate's root anchor and it will be verified that the trust anchor is listed with the correct service type (CA for Qualified Certificates) and service status statements.

4.1.2.2 Defining the qualified status of the signing or sealing certificate

In order to verify if the signing or sealing certificate is a qualified certificate, the use of 'QcCompliance' statement and the corresponding information of the applicable EUMS trusted list will be verified.

The list of trusted services that are the result of the process defined in section 4.1.2.1 are further filtered based on the date that should be checked.

The captured qualifiers of the selected trusted service (for the certificate and date) are checked in case they exist. If no selected trusted service is found, the signing or sealing certificate is considered *not* qualified.

The result of the TL takes precedence over the information in the certificate.

4.1.2.3 Defining whether the private key resides in a QSCD

In order to verify if the private key is protected on a QSCD, the presence of SSCD or QSCD statement in the certificate will be verified.

The list of trusted services that are the result of the process defined in section 4.1.2.1 are further filtered based on the date that should be checked. The Validation Service will check the QSCD status for the signing time.

The captured qualifiers of the selected trusted service (for the certificate and date) are checked for SSCD or QSCD statement in case they exist. If no selected trusted service is found, the private key is considered *not* QSCD.

The result of the TL takes precedence over the information in the certificate.

4.1.2.4 Defining the type of the signature/seal

The type of signature/seal will be determined based on the presence of the combination of QC and SSCD or QSCD statements in the certificate.



The list of trusted services that are the result of the process defined in section 4.1.2.1 are further filtered based on the date that should be checked. The Validation Service will check the type for the signing time.

The captured qualifiers of the selected trusted service (for the certificate and date) are checked in case they exist for Service Info Extension statements that indicate a QC. If no selected trusted service is found, the type as defined in the certificate is returned.

The result of the TL takes precedence over the information in the certificate.

4.1.2.5 Defining type consistency between certificate and TL

In case the trusted service has no Service Info Extension statements that indicate a QC, the presence of 'Additional Service Information' extensions are checked and need to be consistent with the defined type in the certificate.

4.2. Standards implementation

The validation service will perform the validation according to the validation algorithm defined in ETSI 319 102..

The signature validation reports will be formatted in XML and sealed with a XAdES seal with the itsme Sign Validation Service qualified seal certificate issued by QuoVadis to Belgian Mobile ID NV/SA.

5. OTHER BUSINESS AND LEGAL MATTERS

This signature validation service policy does not impose or implement any business matters. All legal matters are governed by the contract or Terms and Conditions that were accepted by the Subscriber before starting to make use of the signature validation service.

6. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

This signature validation service policy is a policy that for the itsme Sign Validation Service, which is a Qualified Signature Validation Service. This service is subject to the rigorous eIDAS accreditation scheme. This service is operated by BMID and is within the scope of the BMID ISO 27001/2 certification.

No other compliance audits or assessments are applicable.