Belgian Mobile ID

itsme Generic Signature Validation Service Policy
Version 1.3

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

Name	COMPL_POL_GenericSignatureValidationServicePolicy
OID	1.3.6.1.4.1.49274.1.1.4.1.3
Applicable from	19/12/2022
Status	Approved
Author	Wim Coulier
Owner	BMID TSP Management Board
Classification level	Public

Belgian Mobile ID

Markiesstraat 1
1000 Brussels, Belgium

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 8
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 identity 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 9

4. REQUIREMENTS / STATEMENTS ON TECHNICAL MECHANISMS AND STANDARDS IMPLEMENTATION 9

4.1. Technical mechanisms 9

4.1.1. Approach towards signing time 10
4.1.2. Defining the qualified status of a signature or seal 10

4.2. Standards implementation 11

5. OTHER BUSINESS AND LEGAL MATTERS 11
6. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 11

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: 1.3.6.1.4.1.49274.1.1.4.1.3
1.3.6.1.4.1.49274 (BMID organization).1 (Compliance Domain).1 (Policies).4 (COMPL_POL_GenericSignatureValidationServicePolicy).1 (major version).3 (minor version)

1.3.2. Distribution points

The latest version of this policy will always be present at https://www.itsme-id.com/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-id.com/en/contact, tsp@itsme-id.com or via postal mail at TSP Management Board; Belgian Mobile ID SA/NV; Markiesstraat 1, 1000 Brussels.
In order to offer a proof of origin and integrity, this policy is sealed with a qualified sealing certificate with itsme as subject.

itsme Digitally signed by itsme Date: 2022.12.22 14:50:43 +01'00'

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-id.com/en/contact, tsp@itsme-id.com or via postal mail at TSP Management Board; Belgian Mobile ID SA/NV; Markiesstraat 1, 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 an 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
SD	: Signer's Document
SDO	: Signed Data Object
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 of customers (Service Providers) that have signed a contract with BMID as of 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 is implemented by a solution conform to the latest version of the BMID Practice Statement (with name COMPL_POL_BMIDpraticeStatement and OID 1.3.6.1.4.1.49274.1.1.2.x.y).
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 is enforced by BMID.

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. Since there is only one implicit signature validation policy supported, it is not required nor possible for the user to select the signature validation policy. 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. Except for the signing time, it is not supported that the user delivers further inputs for the validation process (i.e. elements to parameterize the validation policy such as the signature class, a trust anchor, etc.). Input to the SVS can be given only via the API. This includes the Signed Data Object (SDO) to verify and the Signer's Document (SD) to verify if it is not included in the SDO, However, it is not possible to indicate the certificate(s) to be used for the validation, e.g. for the case where attributes of the SDO do not contain the certificate(s) needed. The SD always needs to be provided. It is not allowed that the user performs the hash calculation to be used for the signature validation. In case there are multiple signatures on the signed data, the Signature Validation Application includes in the signature validation report a validation result about each signature it was able to detect. 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.
The SVS does not take any responsibility on the activities of the actors listed in clause 4.3.1 of ETSI TS 119 441.

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 specifies whether the validated signature concerns a qualified electronic signature, 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 mentions this commitment.

3.2.3. Level of assurance on timing evidences

The signature validation report indicates whether timestamps were used to determine the best signature time. It does 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 about 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 mentions this role/attribute.

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

The signature validation report does not give an indication about 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 signer's 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 signature creation device 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: ContentType, ContentIdentifier, ContentHints, SignatureProductionPlace, SignaturePolicy, Pseudonym.

3.4.2. Cryptographic suites

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

The following signing algorithms are supported (with the minimal public key length):

- RSA (128-bit)
- DSA (1024-bit)
- ECDSA (192-bit)

The following hashing algorithms are supported:

- SHA1
- SHA224
- SHA256
- SHA384
- SHA512
- SHA3-224

- SHA3-256
- SHA3-384
- SHA3-512
- RIPEMD160

3.4.3. Technological environment

The signature validation service is only available via the itsme Sign API.

4. REQUIREMENTS / STATEMENTS ON TECHNICAL MECHANISMS AND STANDARDS IMPLEMENTATION

4.1. Technical mechanisms

There is only one signature validation policy supported, which is not explicitly written out in a document but which is implicit by implementation and configuration of the signature validation application.

This signature validation policy validates electronic signatures and indicates whether they are Advanced Electronic Signatures (AdES), AdES supported by a Qualified Certificate (AdES/QC) or a Qualified Electronic Signature (QES).

All certificates and their related chains supporting the signatures are validated against the EU Member State Trusted Lists (this includes signer's certificate and certificates used to validate certificate validity status services - CRLs, OCSP, and time-stamps).

To determine the certificate qualification, the SVA follows the standard Electronic Signatures and Infrastructures (ESI); Signature policies; Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists (ETSI TS 119 172-4). It analyses the certificate properties and applies possible overrules from the related trusted list.

The SVS always computes the status of the certificate for two different times: certificate issuance and signing / validation time.

The SVA performs the validation according to the validation algorithm defined in ESI - Procedures for Creation and Validation of AdES Digital Signatures (ETSI EN 319 102-1 V1.1.1). This includes the handling of the validation of signatures with expired or obsolete elements (e.g. expired certificates or timestamps, revoked certificates, usage period of cryptographic algorithms exceeded).

The following signature formats are supported:

Signature Format	Supported ETSI standards	Version
CAdES	ETSI TS 103 173 ETSI EN 319 122-1	v2.1.1 v1.1.1
PAdES	ETSI TS 103 172 ETSI EN 319 142-1	v2.1.1 v1.1.1

XAdES	ETSI TS 103 171 ETSI EN 319 132-1	v2.1.1 v1.1.1
ASiC	ETSI TS 103 174 ETSI EN 319 162-1	v2.1.1 v1.1.1

4.1.1. Approach towards signing time

The signing time against which the validity of the signature is verified is defined as follows: The signing time is attempted to be defined based on a Proof of Existence (e.g. timestamp or evidence record) present in 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 is used. In absence of a Proof of Existence and indication from the Driving Application, the signing time is set to the validation time.

Note: The embedded (claimed) signing time is never used for defining the validity of the signature.

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 are 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 verifies whether the signing or sealing certificate can be chained to a trust anchor that is indicated on an EU Member State trusted list (TL). In order to do so the TLs are downloaded and the validity of the TLs is verified (signature on the TL and expiration).
The trusted services defined in these TLs are then filtered according to the signing / sealing certificate's root anchor and it is verified that the trust anchor is listed with the correct service type (CA for Qualified Certificates) and service status.

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 is 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 is 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 checks 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* protected by a 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 is 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 checks 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 performs the validation according to the validation algorithm defined in ETSI 319 102.
The signature validation reports are formatted in XML and sealed with a XAdES seal with the itsme Sign Validation Service qualified seal certificate issued by Digicert / 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 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.