Belgian Mobile ID

itsme® Signature Creation Service Component Policy
Version 2.2

This document describes the policy requirements for the itsme Server Signing Application Service

Name	COMPL_POL_GenericQualifiedSignaturePolicy
OID	1.3.6.1.4.1.49274.1.1.6.2.2
Applicable from	15/05/2025
Status	Approved
Author	Wim Coulier
Owner	BMID Compliance Committee
Classification level	Public

Table of content

1. INTRODUCTION

1.1. Overview

This document describes the rules to be followed for the creation of signatures with the itsme Sign Creation Service.

1.2. Business or Application Domain

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

OID: 1.3.6.1.4.1.49274.1.1.6.2.2
      1.3.6.1.4.1.49274 (BMID organization).1 (Compliance Domain).1 (Policies).6 (COMPL_POL_GenericSignatureValidationServicePolicy).2 (major version).2 (minor version)

1.3.2. Distribution points

The latest version of this policy will always be present at https://www.itsme-id.com/en-BE/legal/document-repository
Older versions of this policy will be present in the same location.

At this moment no machine processable formats are available for the present signature policy.

1.3.3. Signature on the policy

In order to offer a proof of origin and integrity, this policy is signed by Wim Coulier as president of the BMID Compliance Committee.

1.4. Signature policy document administration

1.4.1. Signature policy authority

The BMID Compliance Committee is the authority that is responsible for the signature policy document. The BMID Compliance Committee is part of Belgian Mobile ID NV/SA (registered under number BE0541.659.084).
The BMID Compliance Committee can be contacted via the contact form at the itsme website at https://support.itsme-id.com/hc/en-us/requests/new, tsp@itsme-id.com or via postal mail at Compliance Committee; Belgian Mobile ID NV/SA; Markiesstraat 1, 1000 Brussels.

1.4.2. Contact person

Questions about this signature policy should be directed to the president of the BMID Compliance Committee via the contact form on the itsme® website at https://support.itsme-id.com/hc/en-us/requests/new, tsp@itsme-id.com or via postal mail at Compliance Committee; Belgian Mobile ID NV/SA; Markiesstraat 1, 1000 Brussels.

1.4.3. Approval procedures

The approval procedures for this signature policy consists of a formal approval by the members of the BMID Compliance Committee 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 Signature
QTSP	: Qualified Trust Service Provider
QSCD	: Qualified Signature Creation Device
RQSCD	: Remote Qualified Signature Creation Device
SCA	: Signature Creation Application
SSA	: Server Signing 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® Sign Creation Service: The server signing application offered by BMID.
relying party: natural or legal person that relies upon the signature
Remote Qualified Signature Creation Device: Signature creation device where the hardware element that protects the private key is not in the hands of the certificate holder, but in a remote datacenter
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 creation device: configured software or hardware used to implement the signature creation data and to create a digital signature value

signature creation application: application within the signature creation system, complementing the signature creation device, that creates a signature data object

signature level: format specific definition of a set of data incorporated into a digital signature, which allows to implement a signature class as per the ETSI AdES format standards, e.g. XAdES-B-LTA, XAdES-E-C, PAdES-B-T, PAdES-E-LTV are examples of signature levels.

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 in 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

2. SIGNATURE APPLICATION PRACTICES STATEMENTS

This signature policy shall be implemented by a solution conform to the latest version of the BMID Practice Statement (with name COMPL_POL_itsmePraticeStatement and OID 1.3.6.1.4.1.49274.1.1.2). The Service Provider who operates the Driving Application is responsible for the security of the Driving Application. The WYSIWYS Provider who operates the Signature Creation Application (SCA) is responsible for the security of the SCA. Between Driving Application and SCA, mutual authentication should be performed. Between SCA and itsme® SSA, mutual authentication is enforced by BMID.

3. BUSINESS SCOPING PARAMETERS

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

This signature policy is not limited to a certain application or business process. The Driving Application and/or SCA is (are) responsible for all business aspects. This signature creation policy does not impose any workflow (sequencing and timing) of signatures. The Driving Application or SCA may implement such workflow if relevant.

The SCA uses the digital signature value created by the itsme® SSA to create an advanced electronic signature format as defined by the eIDAS regulation.

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

Since the itsme® Sign Creation Service always uses Qualified Certificates on RQSCD, and this signature application service component policy imposes the use of an advanced electronic signature format as defined by the eIDAS regulation, the signatures created under this signature policy comply with the requirements for Qualified Electronic Signatures.

3.2.2. Commitment assumed by the signer

It is up to the SCA to define for the specific business process whether and if so, which commitment type will be included in the signature. The definition of the commitment type to be included may be delegated to the Driving Application.

3.2.3. Level of assurance on timing evidences

The itsme SSA is not involved in the addition of timing evidences. It is the SCA that performs this action.

3.2.4. Formalities of signing

It is up to the SCA to offer a WYSIWYS visualization to the signer. Only when the business process does not allow for a WYSIWYS (e.g. signing an electronic registered mail for receipt, where the recipient is only permitted to view the content of the registered mail after the signature), the WYSIWYS may be omitted. This can only be the case if a commitment type is used that does not include a contractual commitment.
It is up to the SCA to indicate to the user, before the signature acceptance from the user, what the signature policy, commitment type (optional) and signer role (optional) are that will be taken up in the signature.
The itsme® SSA will visualize the description of the data to be signed, the signature policy, commitment type (optional) and signer role (optional) in the itsme® app that acts as sole control mechanism.

3.2.5. Longevity and resilience to change

It is up to the SCA to ensure that the signature level and time assertion quality are sufficient to guarantee the longevity and resilience to change that is required for the specific business process in which the signature is created.

3.2.6. Archival

There are no requirements regarding archival.

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

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

The itsme® SSA identifies the signer via the itsme® app.

The SCA may indicate a role of the signer. This may be a claimed role or a certified role. If the SCA includes a role to the signature, it will indicate this role to the itsme® SSA via the signature request. This role will then be shown to the user in his itsme® app used as sole control mechanism.

The SCA may use attributes to define workflows and / or perform access control, however attributes about the signer will not be included in the signatures. The itsme® SSA does not show such attributes to the signer in his itsme® app.

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

The itsme® Sign SSA complies with the requirements for the identity proofing for the creation of Qualified Certificates as imposed by the CA.

3.3.3. Signature creation devices

The itsme® SSA protects the signer's private key in an RQSCD. This RQSCD is operated by a QTSP and the RQSCD environmental aspects are included in the QTSP accreditation scope.

3.4. Other BSPs

3.4.1. Other information to be associated with the signature

No other information associated with the signature is included in the signature.

3.4.2. Cryptographic suites

The cryptographic suite of the signature itself is defined by the itsme® SSA in agreement with the CA that issues the signer's certificate. Currently the following parameters are applicable:

- Signing algorithm: RSA
- Key length: 2048 bits
- Hashing algorithm: SHA256

or

- Signing algorithm: ECDSA
- Key length: 256 bits
- Hashing algorithm: SHA256

or

- Signing algorithm: ECDSA
- Key length: 384 bits
- Hashing algorithm: SHA384 or SHA512

The SCA is responsible to ensure that the cryptographic suites used in objects that are added to compose the AdES format (e.g. in timestamps) respect the guidelines of the latest version of ETSI TS 119 312 "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

3.4.3. Technological environment

The SCA connects with the itsme® Sign services via the itsme® sign API. The certificates used for the creation of the signatures are qualified certificates that are created via the itsme® account of the user on the itsme® service and for which the private key is protected in the RQSCD operated by BMID. The activation of the private key is only possible via the itsme® app of the subject of the certificate.

4. REQUIREMENTS / STATEMENTS ON TECHNICAL MECHANISMS AND STANDARDS IMPLEMENTATION

The SCA is responsible to format the signature in a format compliant with ETSI EN 319 122, ETSI EN 319 132, ETSI EN 319 142, ETSI EN 319 162 or ETSI TS 119 182-1.

5. OTHER BUSINESS AND LEGAL MATTERS

This signature creation 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 itsme Sign.

6. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

This signature creation service component policy is a policy for the itsme® SSA. Although this service is not a Qualified Service (it is not possible to certify signature creation services as a qualified service), the RQSCD is audited and under supervision of the Belgian Supervisory Body together with the itsme® Sign Validation service (which is a Qualified Signature Validation Service). The RQSCD and the Qualified Certificates are thus subject to the rigorous eIDAS accreditation scheme.
The itsme® SSA is operated by BMID and is within the scope of the BMID ISO 27001/2 certification. No other compliance audits or assessments are applicable.