Belgian Mobile ID

Generic Qualified Signature Policy Version 2.0

This document describes the policy requirements for the creation of qualified signatures without specific limitations.

Name	COMPL_POL_GenericQualifiedSignaturePolicy
OID	1.3.6.1.4.1.49274.1.1.7.2.0
Applicable from	30/08/2022
Status	Approved
Author	Wim Coulier
Owner	BMID TSP Management Board
Classification level	Public

Belgian Mobile ID

Sint-Goedeleplein 5
Place Sainte-Gudule 5
1000 Brussels, Belgium

Table of content

1. INTRODUCTION

1.1. Overview

This document describes the rules to be followed for the creation of signatures according to the itsme® sign Generic Qualified Signature Policy. This is the default signature policy that is applicable when no specific rules are to be applied.

1.2. Business or Application Domain

This signature policy 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 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: 1.3.6.1.4.1.49274.1.1.7.2.0
1.3.6.1.4.1.49274 (BMID organization).1 (Compliance Domain).1 (Policies).7
(COMPL_POL_GenericQualfiedSignatureCreationPolicy).1 (major version).2 (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 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 sealed with a qualified sealing certificate with itsme as subject.

1.4. Signature policy document administration

itsme Digitally signed by itsme Date: 2022.09.08 11:38:44 +02'00'

1.4.1. Signature policy authority

The BMID TSP Management Board is the authority that is responsible for the signature policy document. 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; Sinter Goedelevoorplein 5, 1000 Brussels.

1.4.2. Contact person

Questions about this signature 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; Sinter Goedelevoorplein 5, 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 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 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 signature creation service offered by BMID.
itsme® Server Signing service: The server signing application service offered by BMID.
relying party: natural or legal person that relies upon the signature
Remote Qualified Signature Creation Device: Qualified 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
server signing application: application using a remote signature creation device to create a digital signature value on behalf of a signer

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 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

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_BMIDpraticeStatement and OID 1.3.6.1.4.1.49274.1.x.y).

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.
This signature creation policy does not impose any workflow (sequencing and timing) of signatures. The Driving Application or SCA can implement such workflow if relevant.
There is no limitation on the data to be signed, except that, unless it is sure that the commitment from the signer is not contractual, file formats should be free from possible corruption agents (e.g. macro's) such as PDF/A (not regular PDF) or plain txt.
There is no limitation on the data referencing mechanism, the number of data signed by one signature or the relative position of the signature and its signed data.

The signature formats shall be an advanced electronic signature format as defined by the eIDAS regulation. There is no signature level imposed.
There is no limitation to a certain targeted community and there are no specific community rules applicable.
There is no allocation of responsibility for signature validation and augmentation.

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 policy imposes the use of an advanced electronic signature format as defined by the eIDAS regulation, the signatures created under this signature policy complies with the requirements for Qualified Electronic Signatures.

3.2.2. Commitment assumed by the signer

There is no limitation on the commitment type that can be assumed by the signer.

3.2.3. Level of assurance on timing evidences

Two timestamps from different providers and with different organizational and technical characteristics (e.g. different algorithms) should be used.

3.2.4. Formalities of signing

No formalities of signing are imposed.

3.2.5. Longevity and resilience to change

There is no guarantee to the longevity and resilience to change.

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

There are no limitations regarding the identity and roles of the signers. Attributes about the signer other than the role shall not be included.

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

The level of assurance for the identity of the signer shall comply with the requirements for Qualified Certificates. There are no limitations on rules for roles or attributes.

3.3.3. Signature creation devices

The signer certificate will proof with the Qualified on QSCD statement that the private key is protected in a QSCD.

3.4. Other BSPs

3.4.1. Other information to be associated with the signature

There are no limitations on the use of ContentType, ContentIdentifier, ContentHints or SignatureProductionPlace.

3.4.2. Cryptographic suites

The cryptographic suite of the signature itself will be SHA256/RSA with minimally 2048 bit key length, SHA2 with ECDSA with minimally P-256. There are no limitations on the cryptographic suites for other objects that are added to the AdES.

3.4.3. Technological environment

The Driving Application or SCA will use the itsme® Sign Creation service for the creation of the AdES signature or digital signature value.

4. REQUIREMENTS / STATEMENTS ON TECHNICAL MECHANISMS AND STANDARDS IMPLEMENTATION

The signature format shall be compliant with ETSI EN 319 122, ETSI EN 319 132, ETSI EN 319 142 or ETSI EN 319 162.

5. OTHER BUSINESS AND LEGAL MATTERS

This signature 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 SSA.

6. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The itsme® SSA 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. This 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.