Belgian Mobile ID

itsme Practice Statement Version 2.3

This document describes what practices are in place for the provisioning of the Trust Services from Belgian Mobile ID.

Name	COMPL_POL_itsmePraticeStatement
OID	1.3.6.1.4.1.49274.1.1.2.2.3
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. SCOPE

This document describes the practices applied by Belgian Mobile ID NV / SA with registered offices at Sint Goedeleplein 5, 1000 Brussel and enterprise number BE0541.659.084 (BMID) for the provisioning of eIDentification Means and Trust Services.

2. STANDARDS CONFORMITY

This practice statement claims conformity with ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

3. DEFINITIONS AND ABBREVIATIONS 7

3.1. Definitions

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
eIDentification Means: electronic identification means as per the eIDAS regulation
itsme Sign SSA: the Server Signing Application offering from BMID
itsme Qualified Sign Validation Service: the qualified signature validation service offered by BMID
relying party: natural or legal person that relies upon the electronic identification or signature validation service
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.

3.2. Abbreviations

AdES	: Advanced Electronic Signature
AdES/QC	: Advanced Electronic Signature created with a Qualified Certificate
BMID	: Belgian Mobile ID NV /SA
CA	: Certificate Authority
DA	: Driving Application
DPO	: Data Protection Officer
FW	: Firewall
ISMS	: Information Security Management System
OCSP	: Online Certificate Status Protocol
OID	: Object Identifier
PKI	: Public Key Infrastructure
QES	: Qualified Electronic Singature
QTSP	: Qualified Trust Service Provider
RQSCD	: Remote Signature Creation Device
SCA	: Signature Creation Application
SCASP	: Signature Application Service Provider
SSA	: Server Signing Application

SVA : Signature Validation Application
TSA : Timestamping Authority
TSP : Trust Service Provider
WAF : Web Application Firewall

4. OVERVIEW

BMID provides eIdentification Means and Signature Validation Services (this does include seal validation, anywhere further in the document where reference is made to signature validation, this should be understood as signature and/or seal validation). The current practice statement describes the practices and procedures that BMID implements in order to guarantee compliance with the requirements of the eIDAS regulation and the Belgian Government (regarding the eIdentification Means) and the eIDAS qualification framework (regarding the Signature Validation Service). These practices and procedures are used company wide and are also applied to services for which BMID is not recognized under the 2 above-mentioned schemes. They are also applicable to the operations of the Remote Qualified Signature Creation Device that is used in the framework of the itsme SSA and is also subject to eIDAS requirements.
At this moment BMID is not offering Signature Augmentation Services. During the validation of signatures, no signature augmentation is performed.

5. RISK ASSESMENT

BMID has implemented an ISO 27.001/2 certified ISMS. As part of this ISMS, BMID implemented a Risk Process, dealing with risk assessment, treatment, communication and monitoring. In this process the information security risk management is handled as a continual process.

6. POLICIES AND PRACTICES

6.1. Trust Service Practice statement

The current BMID Practice Statement is approved by the BMID TSP Management Board. The TSP Management Board is composed of members of the BMID management team and has been set up to manage the TSP and eIdentification compliance matters. The BMID Practice Statement is made publicly available via the document repository on the itsme website.
Any changes to the BMID Practice Statement leads to a publication of the revised BMID Practice Statement to the document repository. Old version of the BMID Practice Statement will still be available in the document store.
Changes that have no impact on the Subscribers or Relying Parties will not be notified up front. Changes that impact Subscribers or Relying Parties and that do not impact the secure and compliant operation of the services will be notified via the itsme website at least 2 weeks in advance of the implementation of the change or via direct contact. In case of changes that impact Subscribers or Relying Parties that are urgent because they are required to maintain the security or compliance of the solution, a best effort will be performed to notify via the itsme website or direct contact as soon as possible.

The present Practice Statement supports the provisioning of trust services that can reach the eIDAS qualified level. This is the case of the BMID signature validation service. To achieve this level of service,

this practice statement claims conformity with ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

In order to offer proof of origin and integrity, this practice statement sealed with a qualified sealing certificate with itsme as subject.

6.2. Terms and Conditions

BMID makes its terms and conditions available in as well the itsme app as on the itsme website.

6.2.1. End-user obligations

End-users are obliged to maintain security of their device on which their itsme app is installed and the confidentiality of their itsme PIN code and promptly block their itsme account via the itsme website in case of any circumstance raising suspicion or risk of their itsme account being compromised (including loss or theft of their itsme device). See the Terms and Conditions documents for detailed obligations.

6.2.2. Obligations of all external organizations

Obligations for external parties exist for external organizations such as suppliers as well as the different Members of the Mobile ID Scheme.

6.2.2.1 Suppliers offering trust services

Suppliers offering trust services, such as Certification Authority delivering signing or sealing certificates and Time Stamp Authorities delivering timestamps with regards to services in scope, have to comply with the eIDAS regulation.

6.2.2.2 Mobile ID Scheme Obligations

The Mobile ID Services are made available by Belgian Mobile ID, through the itsme App or Website, with the intervention of several Identity Registrars, which act as Scheme Members. These third party entities can verify the identity of subscribers.
Belgian Mobile ID acts as data 'controller' under the applicable Belgian privacy laws, and as such Belgian Mobile ID is responsible for the collection and use of the personal data of Data Subjects.

For all the Members of the Mobile ID Scheme, functioning as external parties to BMID, the Mobile ID Scheme is detailed in the ID Scheme Rulebook: The Rulebook has been drawn up by Belgian Mobile ID and set out the Rules and regulations governing the Mobile-ID Scheme, including the relationship between Belgian Mobile ID and its Members, and the relationship between the Members. These rules are contained in the Rulebook and in any Agreement as well as in any other manual or document issued by Belgian Mobile ID from time to time and that specifies that it contains Rules, such as any product-, process-, security-, technology-, regional- or other specific manual, as amended from time to time. Via the Rulebook BMID imposes to every member to take the correct responsibility in terms of a.o. security, compliance and privacy protection. Further to its Agreement, each Member has acknowledged and has agreed that its relationship with Belgian Mobile ID is governed by the Rulebook.

6.2.2.3 *Information Security Obligations for Suppliers*

For Suppliers, the supplier management policy specifies how obligations are applied to external suppliers.
The agreement between BMID and suppliers clearly defines each party's responsibilities toward the other by defining, a.o. the functions or services being provided (i.e. SLA – Service Level Agreement), the return of the assets, the liabilities, the escrow and the limitations on use of sub-contractors. All suppliers must agree in writing to comply with all applicable information security policies, confidentiality agreements, third party connectivity agreements, standards, controls, and regulations. Additionally, the contract enforces the supplier to implement controls, in relation to the type of assets the supplier is accessing and/or the service rendered.

The supplier has to monitor and report its compliance toward the agreement, even for ISO 27001 certified suppliers and report any incident having a potential impact on the services. The agreement includes the right for BMID to audit the supplier.
With regard to privacy, risks involving external party access to personal identifiable information is identified upfront and proper controls are implemented prior granting access to those data. Specifically, the transfer of personal data outside of the European Economic Area (EEA) is strictly prohibited, except of prior BMID agreement.

6.3. Information security policy

BMID has implemented an ISO 27.001/2 ISMS, which has been approved by the BMID Executive Committee. The scope of this ISMS applies to the provision of its core services to subscribers, i.e. the enrolment, share ID, sign up, login, confirm and signature services.
The scope includes staff, assets, data centers and suppliers that support these services independently of the collaborator physical location. It covers the management of information and business activities that support these services.
Different checks are performed on the configuration of the TSPs systems for continued compliance with the BMIDs security policies. Some of these are automated and others are performed manually. The frequency of execution depends on the type of check but are minimally performed once a year.

7. TSP MANAGEMENT AND OPERATION

7.1. Internal organization

7.1.1. Organization reliability

Internally within BMID the governance model is specified for attribution of responsibilities, as well as the specification of processes to guarantee availability, continuity, security and privacy across its services. More specifically, these are detailed by the:

- Organisation Chart
- RACI table, specifying the roles and responsibilities for business critical roles (a.o. trusted roles)
- Operational Model, defined by ITIL v.3 processes with regard to customer support, incident response and escalation management, change and release, capacity and availability management
- ISMS for Information Security Management, certified to ISO 27001/2

- Mobile ID Scheme Management process and the underlying contractual framework (Rulebooks)

7.1.2. Segregation of duties

The BMID definition of Roles and Responsibilities as defined by the Organisation Chart and corresponding RACI, which is part of the BMID ISO 27001/2 certified ISMS, specifies the requirements for segregation of duties across these roles.
The BMID Access Control Policy which is part of the BMID ISO 27001/2 certified ISMS ensures that segregation of duties is verified and maintained when granting new access.

7.1.3. Dispute Resolution

BMID has created an open scheme that describes the rights and obligations of the different parties that take part in the ecosystem around the services offered by BMID. Any party that complies with the requirements and obligations as defined in this scheme can participate to the scheme and become a scheme member.

Any disagreement, dispute or claim arising of or in connection with the Rulebook or any Agreement that has not been settled between the usual contacts of BMID and a scheme member will be referred to a joint committee comprised of representatives of BMID and the scheme member concerned (the Resolution Committee).
The Resolution Committee will be set up by the scheme member and BMID within five (5) Business Days as from the notification by one of the Parties, to the other, of the disagreement, dispute or claim.
The Resolution Committee will attempt to resolve the matter through good faith negotiations within ten (10) Business Days as from the setting up of the Resolution Committee.
If the unresolved disagreement, dispute or claim is having a material effect on the rights or obligations of the scheme member or of BMID under the Agreement(s) or the Rulebook or on the security of the integrity of the Mobile ID scheme, the Parties will use their respective reasonable efforts to reduce the elapsed time in reaching a resolution of the dispute.

Any party that is not a scheme member can contact BMID via the itsme website or phone to record an incident. This will then be treated via the BMID incident management procedures. Specifically, for privacy related topics, a separate e-mail address can be used.

The BMID ISMS defines the governance of subcontracting and outsourcing.

7.2. Human resources

The HR and Supplier policies part of the BMID ISO 27.001/2 certified ISMS ensure that employees and contractors support the trustworthiness of the BMID operations.

7.3. Asset management

7.3.1. General requirements

BMID maintains updated inventories of its assets, including information assets. Security and asset classification is assigned in consistency with the risk assessment. This is ensured via the BMID ISO 27.001/2 certified ISMS asset management policy.

7.3.2. Media handling

Media containing sensitive data is securely handled and disposed when no longer required. This includes a thorough erasure process or a secure disposal for physical media containing sensitive data. This is ensured via the BMID ISO 27.001/2 certified ISMS asset management policy.

7.4. Access control

The BMID Access Control Policy which is part of the BMID ISO 27.001/2 certified ISMS ensures that system access is limited to authorized individuals.

7.5. Cryptographic controls

The Cryptographic Controls Policy that is part of the BMID ISO 27.001/2 certified ISMS ensures the proper management of cryptographic keys and cryptographic devices throughout their lifecycle.
This is the case for all cryptographic keys that are being used in relation to the services (a.o. end-user symmetric keys, end-user asymmetric keys, keys to protect data during transmission) and includes key generation, key distribution, key storage, key backup and key destruction.
The TSP Management Board monitors that the algorithms and key sizes that are prescribed by the Cryptographic Controls Policy is deemed secure as per the latest version of ETSI TS 119 312 “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”.

7.6. Physical and environmental security

7.6.1. Secure areas

This section is mainly covered from within the use of the ISO 27001/2 certified DataCenters. The relevant Datacenter Supplier ISMS SOA has been validated by BMID to cover the relevant safeguards and security controls.

7.6.2. Equipment

Partially covered from within the use of the fore mentioned ISO 27001/2 certified DataCenters. Specific requirements and attention points that remain for BMID are covered in the BMID Acceptable Use Policy which is part of the BMID ISO 27.001/2 certified ISMS.

7.7. Operation security

7.7.1. Operational procedures and responsibilities

The operational procedures and responsibilities are defined by the BMID Operating Model which defines the ITIL Version 3 based elaboration of the following: support (first line, Tier 2, Tier 3), request fulfilment, incident management, problem management, change management, release and deployment management, and service asset and configuration management.

Instantiated for specific provisions, the Security and Architecture guidelines provide the policy principles for: separation of the different environments, overall protection from malware and information backup procedures.

7.7.2. Logging and monitoring

This includes event logging, protection of log information, administrator and operator logs, clock synchronization, as well as control of operational software, via the installation of software on operational systems.

The datacenter provides 24/7 monitoring on the infrastructure, network and security components as part of their service offering. BMID provides continuous monitoring for systems (infrastructure as well as application level).

During the whole transactional process each step is logged. BMID collects all technical logging (FW, WAF, Syslog), which provides log collection, log normalization, log correlation and querying capabilities. BMID also collects functional logging. Logs are protected as per the BMID Information Security Management System (ISO 27001 certified). The BMID / itsme® Information Security Management System (ISO 27001 certified) integrates regular Risk Assessments, regular (daily) vulnerability scans as well as a Bug Bounty & Responsible Disclosure via our partner Intigriti. This includes specifically the assessment of log data protection. Backups are taken on a regular (up to hourly) basis to minimize the loss of critical data.

Based on specific queries and correlations, alerts are triggered to investigate for possible suspicious connections. BMID collects, and protects, all functional logs centrally as the main source for fraud investigations. Together, this allows BMID to configure triggers for activity and alerts.
On a daily basis, reports on such logs and alerts resulting from them are reviewed and trigger additional actions where required. Such actions can include reporting incidents for (attempts for) unauthorized access, data breaches or any other Information Security incident.

Operational Logs are kept online at least for 1 year (excluding further archiving, extending this retention period). Transaction logs have a retention period of 10 years based on legal obligations for archiving and for providing proof in case of disputes. The signature validation report obtained by the subscriber contains all data that was used during the validation (signature itself, revocation data, timestamps, certificates, etc.) so that in case of later doubts, these elements can be used as evidence.

7.7.3. Technical vulnerability management

BMID provides a dedicated vulnerability management process, covering:

- the checks for (new) vulnerabilities
- identifying them on our infrastructure and systems, verifying for the actual exploitability, mitigating them either by configuration changes, patching or other work-arounds if required.

The datacenter also foresees vulnerability management for the hosting hardware and firmware on regular basis.

7.7.4. Information systems audit considerations

Information systems audit controls and pentesting are applied. A running audit plan summarizes the planned audit work packages and refers to results of past audits. This audit plan is an in integral part of the ISMS documentation.

7.8. Network security

The BMID network design includes network controls, security of network services and segregation of networks.

BMID enforces the following security principles on the network architecture:

- Dual-layer Firewall design with separated Network segments / zones internally
- Front-End termination infrastructure
- Protection against (D)DOS
- Secured connections with our partners
- All flows, internal/external are encrypted on transport level to protect from eavesdropping or session hi-jacking

7.9. Incident management

The management of security incidents and improvements is integrated within the overall operations model and the standard incident management procedures there. Incidents are logged into the Service Desk tooling and assigned based on their classification. Security and privacy incidents are also/automatically forwarded to the CISO or DPO respectively, to keep him/her informed, and take immediate appropriate action.

On a monthly basis, incidents and events are reviewed on the Operational Management Committee, in order to further determine appropriate actions for further mitigation if required.

7.10. Collection of evidences

BMID maintains records concerning the operation of the services in scope for the purposes of providing evidence of the correct operation of these services. These records will only be disclosed to law enforcement authorities under court order and to persons with right to access to them upon legitimate request.
These records are protected and backed up to avoid information loss or compromise. Log backups are retained for a minimum period of 10 years.

7.11. Business continuity management

BMID has an ITIL process in place that ensures business continuity management. The services are designed with business continuity in mind. The whole operational environment has a passive redundancy in a backup datacenter.
In case of a P1 level incident a crisis committee is set up to coordinate the activities and communication towards impacted parties. The procedures, frequency and means of communication are described in the P1 crisis management procedure (BMID internal document).

7.11.1. Information security continuity

As part of the overall Business Continuity Management, the following aspects are integrated from within the ISMS: planning information security continuity, implementing information security continuity and verify, review and evaluate information security continuity.

An important aspect here is the continuous monitoring of events on the BMID infrastructure and applications, from which suspicious behavior can be identified. This is ensured by the centralized logging, as well as the continuous monitoring of all infrastructure by the datacenter as well as BMID on a 24/7 basis to guarantee their correct functioning.

Based on alerts generated here, either interventions to recover / restart services are initiated, or events are escalated to other (security) experts to further analyze possible impact and risk.

7.11.2. Redundancies

Availability of information processing facilities is guaranteed through application of required redundancy on critical "single-points-of-failure".

Throughout the setup of the infrastructure and applications of BMID, the continuity is guaranteed using:

- Redundant Data Processing facilities on 2 locations that are sufficiently remote from each other to avoid impact on both sites at the same time.
- Transactions are committed across these locations to remain in synch on both locations
- Redundancy in infrastructure elements per location to avoid Single Point of Failure (SPOF) on any of the infrastructure elements that are critical for the BMID services
- Secure backups of data that are available to restore services within an acceptable timeframe

7.12. TSP termination and termination plans

BMID has created a termination plan that deals with termination notification, subcontractors management, information maintenance, private key destruction, termination phasing and updating of the termination plan procedure. BMID has taken measures to ensure that funds will be available for the execution of the termination plan, also in case of bankruptcy.

7.13. Compliance

The TSP Management Board monitors evolution of legislation to make sure that the services are created and maintained in line with any applicable legal requirements. BMID employs personnel with the required legal skills and has that fulfill the required roles (e.g. DPO) in order to guard the correct implementation of legal requirements.

BMID is ISO 27.001/2 certified.

BMID has successfully undergone each of the external audits as required by the Royal Decree of October 22, 2017 on the means for electronic identification for government applications and has been recognized by the Belgian Government. In this framework, BMID is undergoing regular surveillance audits.

BMID has obtained the Qualified status for its Sign Validation Service and is in this regard under supervision of the Belgian national supervisory body.

BMID provides identity proofing, subject device provisioning and revocation components services towards Digicert / Quo Vadis for the issuance of qualified signing certificates. BMID is eIDAS certified

for these component services and via Digicert / Quo Vadis these component services are under supervision of the Belgian national supervisory body.

7.13.1. Compliance with legal and contractual requirements

As part of the continuous audit plan, as well as part of the Risk management process, the different aspects for compliance have been assessed, are continuously monitored for compliance and updated if changes in the business context occur.
More specifically, the following important aspects are addressed: eIDAS, Data Privacy, Competition Law, Financial services, Telecom Regulations, Others (IPR, Crypto-regulations, labor law, …).
In order to ensure that the ecosystem around itsme respects all compliance requirements impacting the compliance of the BMID services, BMID has elaborated the BMID Scheme Management based on its (set of) Rulebooks. These specify the back-to-back rights and obligations of the Scheme Members towards each other, which in turn allows BMID to fulfill the compliance requirements for the frameworks as specified above.
Within BMID, compliance with eIDAS related requirements is guarded by the TSP Management Board.

7.13.2. Information security reviews

On top of the Information Security Audit-plan, and based on the continuous risk monitoring performed, BMID regularly verifies the effectivity of its ISMS. When and where relevant, results from such security reviews are shared with, or presented to, stakeholders and senior management to allow the evaluation of effectiveness of the overall security management process, and implementation of the information security safeguards.

8. SIGNATURE VALIDATION SPECIFIC PRACTICES

8.1. Signature Validation Service Policies

There is only one Signature Validation Service Policy that is currently supported by the itsme Sign Validation Service: itsme Generic Signature Validation Service Policy with OID 1.3.6.1.4.1.49274.1.1.4.

This validation services policy only performs a technical validation of the signature (signature validation policy), without any verification, of signature applicability rules (e.g. business or legal requirements). The signature applicability rules are to be determined by the subscriber (e.g. according to the reported cause(s) of an indetermination or specific information on the signature mentioned in the report).

8.2. Service level

The itsme sign validation service is of Qualified level.

8.3. Signature validation process

The itsme Sign Validation Service allows a subscriber to deliver signed data and signature to be validated via an API (no human interface is foreseen at this moment). The validation service performs the validation according to the validation algorithm defined in ETSI 319 102. The validation on AdES, AdES/QC and QES requirements is performed according to ETSI 119 172-4. Via the same API, an XML formatted validation report is returned that is sealed with an itsme Sign Validation Service certificate.

This certificate is a Qualified Seal Certificate, of which the private key is protected by a Qualified Seal Creation Device.

The subscriber should:

- integrate with the itsme Sign Validation Service via the offered API and respect the requirements of this API.
- verify the seal on the validation report.

Relying parties should:

- validate the seal on the validation report.

It is not possible for the subscriber to give a conflicting indication on the signature validation policy. At this time, it is not allowed that the subscriber specifies other validation policies than the ones that are predefined by the itsme Sign Validation Service (currently there is only one, but possibly other Signature Validation Service Policies will be added in the future that will be differentiated based on OID reference in the API). The API prescribes an identification of the validation policy via OID. If an unknown OID is specified, an error will be returned and no validation will be performed.

The itsme Sign Validation Service validates a.o. QES and reports proactively on requirements being met (use of qualified signing certificate and QSCD). Only the ETSI specified AdES signature formats are supported.

8.4. Service validation report

The validation report contains three parts: summary validation results, detailed validation results and diagnostic data.
Each report is sealed with a Qualified Seal Certificate on HSM. The subject name of the certificate is “itsme Qualified Sign Validation Service”.

9. REMOTE SIGNATURE CREATION PRACTICES

9.1. Server Signing Application Service Policies

There is only one Server Signing Application Service Policy that is currently supported by the itsme Sign SSA: itsme Generic Signature Creation Service Policy with OID 1.3.6.1.4.1.49274.1.1.6.

9.2. Service level

The itsme Sign SSA cannot be of Qualified level, since the eIDAS regulation did not include the possibility for an SSA to become a qualified trust service. However, during the audit of BMID for qualified trust service provider the RQSCD that is part of the itsme Sign SSA was included in the audit scope. The other components of the itsme Sign SSA are subject to the same policies, procedures and controls as the ones that are applicable to the components that are part of the itsme Qualified Signature Validation Service and the recognized eIdentification Means.

9.3. RQSCD

During a setup process that is performed before the signer signs for the first time, the key pair for the signer is generated in the RQSCD (Remote Qualified Signature Creation Device) that is managed by

BMID, and the private key is cryptographically linked to the itsme app of the signer. The RQSCD then requests a qualified certificate from the qualified CA for the signer.
Revoking a certificate for itsme Sign should normally never be required. As long as the itsme account remains secure, no one is able to abuse the signing certificate. However, if an itsme account is blocked via the itsme website, any active signing certificate linked to the account is revoked automatically. (NOTE: the signing certificate is not revoked when an itsme account is blocked by entering a wrong PIN code three times in the app.) The next time the user tries to use itsme Sign, he will need to accept the creation of a new certificate again and a new key pair will be generated and certified, similar as at first signature.
The RQSCD used by BMID is the Intesi PkBox, Version 3.3 which has been certified as Secure Signature Creation Device (and through eIDAS legislation automatically recognized as RQSCD) by Zentrum für sichere Informationstechnologie - Austria (A-SIT) under Reference number A-SIT-VIG-18-051. The RQSCD has been implemented with the Gemalto Ezio identification as OTP provider. This is the same set-up that is used for the eIDentification Means service (see below).

9.4. Signature creation process

itsme Sign only offers the Signing Server Application functionality (meaning that it allows the user to create the raw signature with a private signing key that is managed on his behalf by itsme). It does not offer SCA functionality (presentment of the data to be signed and formatting of the signature format in an Advanced Electronic Signature format). That role is taken up by BMID partners (the Signature Creation Application Service Providers SCASPs).
The SCA interacts with the signer and other parties to receive the data to be signed. It then presents that data in a WYSIWYS fashion (What You See Is What You Sign) to the signer. When the signer is satisfied with the data presented and indicates that he wants to go ahead with the signature the SCA communicates with itsme via an API to retrieve the user's certificate in order to calculate the hash to be signed. It communicates the latter to itsme via the API after which itsme requests the signer to approve the transaction via the itsme app which acts as Sole Control Mechanism. By entering the itsme code, the itsme device generates a cryptographic token that is transferred to the RQSCD. The RQSCD validates that token directly with the OTP verifier. Only if that validation is successful, the RQSCD uses the private key of the user for the signing operation. The itsme Sign SSA creates the raw signature and transfer it back via the API to the SCA which formats the signature in an Advanced Electronic Signature format.

The SCASP should:

- integrate with the itsme Sign SSA via the offered API and respect the requirements of this API.
- respect the requirement that BMID sets forth in its document COMPL_POL_RequirementsOnSCASPForHashSigning (that mainly references ETSI requirements for SCASPs and adds a few supplementary requirements).

The signer should:

- ensure himself that the document shown to him by the SCA is indeed the document he wishes to sign
- Ensure himself that the signing transaction shown to him in the itsme app corresponds with the signing transaction started in the SCA
- never divulge his itsme code to any other party

9.5. External components

The itsme Sign SSA uses an external CA for the issuance of the end-user certificates. Some itsme components are used with relation to the issuance of these certificates: ID Proofing (the certificates are issued based on the ID data that was collected during the itsme enrolment), subject device provisioning (itsme provides the secure management of the private key on behalf of the user with his itsme device as sole control mechanism) and revocation services (when the user blocks his account via the itsme website, any active certificate for the user is automatically revoked).
Certificates for the end-users are created on the fly when the user wants to sign with itsme Sign and does not have an active certificate at that moment with itsme.

10. EIDENTIFICATION

10.1. Service level

We perform identification and authentication services based on an ID proofing process (not recognized by the Belgian government at this moment but certified at AL High) based on the readout of an NFC capable identity document combined with biometric verification as identified in the itsme Scheme document "21200 ID template eligible ID doc NFC and Biometric - AL High - 1.1 - 29.01.2021".
Itsme has been recognized by the Belgian government as Authentication Means of Assurance Level High for users for which the ID proofing was done based on an ID process as identified in the itsme Scheme document "21100 -ID template Belgian e-ID Card and Belgian e-Resident Card - AL High - compliant e-ID means" (only accessible to Scheme members).

10.2. Login process

The itsme login service is based on the Gemalto Ezio technologies. The Gemalto SDK is present on the mobile device of the end-user as part of the itsme app. The Gemalto Ezio server is installed in the BMID Datacenter. During the setup of the itsme app, the OTP environment is set-up, so that the Gemalto Ezio Server can verify whether an OTP was generated by the app of the user concerned or not.
A Service Provider that wishes to authenticate an end-user, uses the BMID API to send an identifier of the claimed identity to BMID or redirects the user to an itsme identification page where the user can identify via his mobile number. BMID creates a login action for the itsme app of the user concerned. The user can answer to that action and enter his itsme code in the itsme app in order to authenticate himself. When he does, the Gemalto SDK in his app creates an OTP that is sent to the BMID back-end. The BMID Back-End then requests the Gemalto Ezio server to verify the OTP for that user. If the result is positive, the authentication was successful, and this result is returned to the Service Provider via the BMID API.