PSD2 specific certificate and communication service package for production environments
1. EXECUTIVE SUMMARY ABOUT MICROSEC PSD2 RELATED EXPERTISE, PRODUCTS AND SERVICES

Microsec presents crucial elements for ASPSPs and TPPs to fulfil requirements of PSD2 regulation and corresponding Regulatory Technical Standards. The Public Key Infrastructure expert software vendor and Qualified Trust Service Provider showcases (1) PSD2 specific qualified certificates, (2) certificate validation tool and (3) Strong Customer Authentication tool.

Microsec is a Full Member of the European Telecommunications Standards Institute (ETSI) and has contributed¹ to the development of the ETSI TS 119 495: Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366. This technical specification defines a special type of EU Qualified Certificates, as defined in Regulation (EU) No 910/2014 (eIDAS²), which support the requirements of the Commission Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 (PSD2³) for strong customer authentication, common and secure open standards of communication. ETSI TS 119 495 has been published in May 2018 and available for download⁴.

Microsec is the operator of the e-Szignó Qualified Certificate Authority (CA), a Qualified Trust Service Provider (QTSP), audited by TÜViT (TÜV Nord Group) and supervised by the National Supervisory Authority (called National Media and Infocommunications Authority - NMIA). Besides the trust services, the Hungary-based provider develops multi-platform electronic signature creation solutions, CA software package and it has EU-wide renowned Public Key Infrastructure (PKI) competency.

1.1. Microsec solution glossary
The above mentioned three solutions are the following:

(1) Microsec, as a QTSP, provides eIDAS qualified certificates for website authentication (QWAC) and electronic seals (QSealC). These certificates enable the TPPs and ASPSPs to comply with the access-to-account identification requirements of PSD2 and the related RTS, and also to secure their communication (with respect to confidentiality, integrity, authenticity), as well as to create electronic proofs of transactions capable of having legal effect.

(2) The RTS on SCA and common and secure open standards of communication (CSC) requires PSPs to use eIDAS qualified certificates with PSD2-specific content for identification during the access-to-account communication. The receiving PSP must validate the certificate of the other party in order to prevent fraud and risk of data leak. The Microsec PSD2 certificate validation tool provides a robust and customizable solution for all validation tasks, including certificate path building, revocation status checking, support for EU Trusted Lists and the ETSI standard PSD2 certificate profile.

(3) The Common Criteria EAL2 certified PassBy[ME] service provides powerful eIDAS compliant electronic signatures alongside the PSD2 compliant SCA functionality allowing the end users to transact, sign contracts and do their daily business anywhere, anytime. PassBy[ME] enables an end-to-end digitized, automated and paperless user experience, with legal proofs.

⁵ https://www.etsi.org/standards-search#search=119495
2. PSD2 CHALLENGES ABOUT IDENTIFICATION AND COMMUNICATION

2.1. Communication security
According to PSD2, TPP & ASPSP parties must establish a secure communication during the access-to-account interactions. These interactions in-fact data and information exchange transmissions between entities. According to the standards PKI based approach must be used in the implementation.

The RTS on SCA (Strong Customer Authentication) and common and secure open standards of communication (CSC) requires PSPs to use eIDAS qualified certificates with PSD2-specific content for identification during the access-to-account communication. The receiving PSP must validate the certificate of the other party in order to prevent fraud and risk of data leak.

2.2. Implementation options of PSD2 communication security
Generally, the key communication requirements are listed as: Identification = Confidentiality = Integrity

Whilst there are many technical methods for secure communications, APIs and SCA tooling Microsec selected the most mature PKI technology to develop a board solution. This is “one way to do it” from a technical point of view. This technology also must be extended with defined, carefully developed processes with appropriate mechanisms to achieve compliance.

2.3. Solution package
In the following Microsec present a possible implementation through technology and the required process as well. A working solution requires the following milestones to be reached in order to enable the communication between parties

- Identification & Setup
- Certificate Issuing and Certificate Validation
- Mutual TLS Authentication
- Validation tool

2.3.1. Realization of security concepts through technology
The standard defines the following implementation options – based on Transport Layer Security (TLS). Basic concept is that TLS has three main capabilities that can be used independently or in combination to secure information content transport (establish a network pipe).

These capabilities are:
1. Authenticating a server to a client
2. Encrypting client - server communications
3. Authenticating a client to a server

Most public web sites use TLS only to authenticate the web server to the client. Web server authentication is easily implemented and sufficient for establishing a TLS connection. However, web servers can be configured to request or require that the client authenticate using a certificate. This is known as mutual authentication.

The TPP & ASPSP Setup is an identification process within API Access enablement. Although not mandated in the RTS SCA CSC, it is generally an API industry best practice.

- As the TPP has a QSEALC, they can now digitally identify themselves towards ASPSPs online for PSD2 API Access.
- Successful identification & Setup between the TPP and ASPSP, results in a TPP getting API Access from an ASPSP.

- eIDAS and ETSI TS 119 495 enables a common framework and pan-European interoperability between all TPPs and ASPSPs for this process.
3. PSD2 CERTIFICATES

3.1. Identification & Setup
QSEALC Certificates provide a common and eIDAS secured method for an unknown TPP to become identified to the ASPSP.

- PKI can be used to verify that the TPP is who they claim to be in the QSEALC.
- QSEALC Certificates do not contain all information (e.g. on passporting) and may not be up to date, so ASPSPs may need to check NCA Public Registers (or equivalent).
- Successful application of this Identification process allows TPPs a quick and universal way of secure access to APIs, with ASPSPs.

QWAC and QSEALC are used at different communication layers and provide different effects:

- QWAC for Transport Layer
- QSEALC for Application Layer.

QWAC provides Identification and Confidentiality.
QSEALC provides Identification and Integrity.
When used in combination and with Qualified Certificates, this will fulfil the requirements from RTS SCA CSC and also have legal effect from eIDAS.

3.2. Certificate Issuing & Certificate Validation
Microsec, as a QTSP, identifies the PSP and relies on NCA register to validate PSD2 specific attributes. Microsec takes responsibility that all information in the certificate is correct at the time of issuance. After this Microsec issues qualified certificates according to ETSI TS 119 495, which specifies a standard format and management of PSD2 specific data.

Any PSP can acquire eIDAS certificates, including:

- Qualified certificate for website authentication (QWAC),
- Qualified certificate for electronic seal (QSealC),

This phase assumes that the PSP is already registered and authorized by the NCA.
Certificate request process for Microsec clients are the following (main steps):
1. Generate a key pair e.g. in the PSP secure systems.
2. Visit the Microsec QTSP website, fill out certificate request form, include public key to be certified.
3. Microsec will prepare the papers and contact the PSP.
4. Validation of all data to be included in the certificate.
5. Microsec issues certificate to PSP.
6. Installation of the certificate(s) into PSP secure systems.

Certificate Validation consists of the following (main) steps:

- Is the issuer QTSP trusted? Certificate path building check.
- Formal validation and content checking.
- Is it expired? Dates in the certificate.
- Is it revoked? CRL or OCSP.
  - CRL: Certificate Revocation List
  - OCSP: Online Certificate Status Protocol
This process above is typically done automatically by software. Among the firsts Microsec developed a certificate validator solution for PSD2 certificates – this tool can be integrated into back-end or API systems and provides a reliable validation. More details on this can be found in section “2.3.6 Validation toolbox”.

3.3. Mutual TLS Authentication

Two parties authenticating each other through verifying the provided digital certificate issued by QTSPs. As a result both parties are assured of the other’s identity.

This solution is:

- Very popular in server-to-server communications.
- A client (web browser or client application) authenticating itself to a server (website or server application) and that server also authenticating itself to the client.
- QTSPs listed in EU member states TSLs and the EU list as well (Trusted List of Trust Service Providers). This authentic list and the QTSPs are an important part of the mutual authentication process.

4. VALIDATION TOOLBOX

Qualified certificates in compliance with the RTS contain PSD2-specific regulatory information about the PSP owning the certificate, namely its authorisation number, its roles (types of service), and the name of the National Competent Authority (NCA) which have granted the authorisation. The QTSP issuing the certificate verifies the correctness of these attributes at the time of certificate issuance.

When TPPs communicate with ASPSPs in order to access a payment account on behalf of a PSU, they rely on qualified certificates to provide the above mentioned security assurances, in order to prevent fraud and risk of data leak. During this secure communication the receiving PSP must validate the certificate of the sending PSP, which includes the following controls:

- Parse the certificate according to the standards (ITU-T X.509 and IETF RFC 5280);
- Determine the identity of the PSP being the certificate subject;
- Check that the certificate has not expired;
- Check that the certificate has not been revoked, using information published by the issuer (CRL and/or OCSP);
- Build a certificate chain up to a trust anchor to determine whether the certificate is trusted;
- Check that the certificate is qualified;
- Check that the certificate has been issued by a Qualified TSP, which has the qualified status granted in the EU Member States Trusted Lists as defined in Commission Implementing Decision (EU) 2015/1505 laying down technical specifications and formats relating to trusted lists;
- Check that the certificate is of the appropriate type for the specific usage;
- Check that the certificate conforms to the PSD2 certificate profile as specified in ETSI TS 119 495: Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366;
- Determine and output the PSD2 regulatory information included in the certificate.

The Microsec PSD2 certificate validation toolbox provides a robust and customizable solution for all validation tasks, including the checks detailed above. The toolbox can be used to validate any certificate given as input, or to validate a certificate as part of a complete digital signature validation (e.g. for electronic seal certificates).

The toolbox can be used as a command-line application or can be integrated into almost any software as an SDK. It provides a variety of programming interfaces, including C, COM, Java and .NET, each having a comprehensive developer documentation. Microsec also provides integration support with the SDK.
5. SOLUTION ON STRONG CUSTOMER AUTHENTICATION (SCA)

The PassBy[ME] Mobile ID system is combining BYOD (Bring Your Own Device) features with PKI technology. The system consists of two main group of elements, modules:

1. A complex **back-end system**, with integration abilities using REST API and protocols like LDAP, Active Directory and Radius;
2. A **mobile application** (running on Android, iOS).

The PassBy[ME] system easily fulfils the requirements of PSD2 about SCA tools and offers much more. It provides a persistent protection layer for the customer and also adds comfort and confidence in any workflow where approvals or decisions are needed. Digitally signed evidences are created automatically in the background in order to provide certainty about every transaction. This provides increased security and comfort levels simultaneously.

The PassBy[ME] system seamlessly implements the following standards or technologies:

- PKI (Public Key Infrastructure technology),
- X.509 (RFC 5280),
- OCSP (RFC 6960 Online Certificate Status Protocol),
- TSP (RFC 3161 Time-Stamp Protocol),
- SCEP (Simple Certificate Enrollment Protocol),
- TLS (RFC 5246 Transport Layer Security v1.2).

PassBy[ME] system is a Common Criteria EAL 2 certified product. It was audited and tested by professionals to ensure that it fulfills the requirements of international security standards. The report can be downloaded from the OCSI website (http://www.ocsi.isticom.it/index.php/elenchi-certificazioni/prodotti-certificati#c0418).

Furthermore the PassBy[ME] system was created in a way that it can be integrated into frameworks or programs like EMV® 3-D Secure or Verified by Visa.

Besides PSD2 compliance PassBy[ME] system can send unlimited number of electronically signed messages without any extra costs. The full functionality of PassBy[ME] system provides electronic document signing capabilities for the identified (registered) users – for example during remote (online) contracting process.

These features are enablers of a successful digital transformation for any organization (financial institutions, government agencies, utility providers, etc.).

**Comprehensive features of the PassBy[ME] system:**

- Can be built-up on premise or subscribe for the SaaS version,
- 99.9% availability,
- Geo-redundant service centers, for high availability even during environmental disaster situations.

In the case when customers decide upon SaaS version of PassBy[ME] system Microsec ensures that under the hood the service uses and will use eIDAS ready, TÜViT audited Qualified Trust Services such as Qualified Timestamping or QTSP issued Qualified Certificates.
5.1. **PassBy[ME] system as a PSD2 compliant SCA tool**

PassBy[ME] system complies with PSD2 and the RTS Chapter II. by implementing the following:

- It generates Authentication code,
- Fulfils the Dynamic linking criteria by the unique messages and contents (with the aid of PKI technology),
- Implements the elements categorized as knowledge (password),
- The mobile technology fulfils the requirements of the elements categorized as possession (the mobile device and application instance),
- The PassBy[ME] system provides independent elements.

Microsec PassBy[ME] SCA tool’s architecture relies on PKI technology. PKI is already providing a comprehensive, security embedded approach during the development of the application. Security by design principles made Microsec develop further security features into the PassBy[ME] system:

- The mobile application is registered and possessed by the identified end users,
- Protection by knowledge – the mobile application and administration interfaces are protected by passwords,
- Protection profiles and policies apply during the operation of the application,
- The application protects the encryption key with various techniques – both on server and client side,
- The runtime application uses separation techniques in memory and processing units,
- Standardized implementation of Keychain and Android System Keystore,
- Encryption implementation based on unique data (personal data, passwords, pin codes, etc.),
- Modification detection: Root and Jailbreak detection algorithms used during installation and runtime,
- Keys automatically deleted after 5 unsuccessful guess attempts, brute force attacks.

### 6. DEFINITIONS AND ABBREVIATIONS

**API**: Application Programming Interface  
**CA**: Certificate Authority (see QCA)  
**CRL**: Certificate Revocation List  
**CSC**: common and secure open standards of communication  
**ETSI**: European Telecommunications Standards Institute  
**NCA**: National Competent Authority  
**NSA**: National Supervisory Authority  
**OCSI**: Organismo di Certificazione della Sicurezza Informatica ([http://www.ocsi.isticom.it/](http://www.ocsi.isticom.it/))  
**OCSP**: Online Certificate Status Protocol  
**OCSP**: Online Certificate Status Protocol  
**PKI**: Public Key Infrastructure  
**PSD2**: Payment Services Directive 2 NOTE: See Directive (EU) 2015/2366 [i.2].  
**PSP**: ‘payment service provider’ - means a body referred to in PSD2 Article 1(1) or a natural or legal person benefiting from an exemption pursuant to Article 32 or 33;  
"A payment service provider (PSP) offers shops online services for accepting electronic payments by a variety of payment methods including credit card, bank-based payments such as Direct Debit, bank transfer, and real-time bank transfer based on online banking.”  
**PSP_AI**: Account Information Service Provider (for more information see below)
PSP_ASP: Account Servicing Payment Service Provider (for more information see below)
PSP_IC: Payment Service Provider Issuing Card-based payment instruments
PSP_PI: Payment Initiation Service Provider (for more information see below)
QCA: Qualified Certificate Authority
QSCD: Qualified electronic Signature/Seal Creation Device
QSealC: Qualified electronic Seal Certificate
QTSP: Qualified Trust Service Provider
QWAC: Qualified Website Authentication Certificate

RFC: Request for Comments (RFC) is a type of publication from the technology community, RFCs cover many aspects of computer networking, including protocols, procedures, programs, and concepts.

RTS: Regulatory Technical Standards NOTE: See Regulation 2018/389 [i.3].

SCA: Strong Customer Authentication

SCEP: Simple Certificate Enrollment Protocol

TLS: Transport Layer Security

X.509: is a standard defining the format of public key certificates

AISP: ‘account information service provider’ – means a payment service provider pursuing business activities as referred to in PSD2 point (8) of Annex I; ‘account information service’ means an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider;

ASPSP: ‘account servicing payment service provider’ means a payment service provider providing and maintaining a payment account for a payer;

‘authentication’: means a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user’s personalised security credentials;

‘home Member State’: means either of the following:
(a) the Member State in which the registered office of the payment service provider is situated; or
(b) if the payment service provider has, under its national law, no registered office, the Member State in which its head office is situated;

‘host Member State’: means the Member State other than the home Member State in which a payment service provider has an agent or a branch or provides payment services;

‘payee’: means a natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction;

‘payer’: means a natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order;

PISP: ‘payment initiation service provider’ – means a payment service provider pursuing business activities as in PSD2 point (7) of Annex I; ‘payment initiation service’ means a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider;

‘payment institution’: means a legal person that has been granted authorisation in accordance with PSD2 Article 11 to provide and execute payment services throughout the Union;

‘payment instrument’: means a personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used in order to initiate a payment order;

‘payment service user’: means a natural or legal person making use of a payment service in the capacity of payer, payee, or both;

‘payment transaction’: means an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee;

‘remote payment transaction’: means a payment transaction initiated via internet or through a device that can be used for distance communication;
‘**sensitive payment data**’: means data, including personalised security credentials which can be used to carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data;

‘**strong customer authentication**’: means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;

**TPP**: ‘Third Party Provider’ means an authorised online service provider that has been introduced as part of Open Banking (for example an AISP or a PISP).