Identiway QeID Service
Certificate Practice Statement

Table of Contents

Revision History

Date	**Revision**	**Comment**	**Contributor**
2019-06-21	01	Re Formatting from document	Philip Hallenborg
2019-06-21	02	Published	Philip Hallenborg
2019-06-27	03	Chapters 4.1, 4.2, 4.4, 4.6, 4.7, 4.8	Tomas Zuoza
2019-06-27	04	Wording, adding 4,5,6 parts	Philip Hallenborg
2019-07-03	05	Wording Chapter 4	Philip Hallenborg/Jenny Dybedahl
2019-07-03	06	Chapters 5.4, 5.5	Tomas Zuoza/Ignas Karpiejus
2019-07-15	07	Input	May-Lis Farnes
2019-07-17	08	Review and chapters 6, 7	Tomas Zuoza
2019-07-17	09	Review naimg, links	Philip Hallenborg
2019-07-23	10	Review, links, 2.2 update	May-Lis/Philip Hallenborg
2019-07-24	11	Name change	Philip Hallenborg
2019-07-25	12	Update CRL information	Ignas Karpiejus

1. INTRODUCTION

Identitrade AB, SE556972-4288, (Identitrade) was founded in 2014. It is a Swedish limited liability company (Aktiebolag) held privately by private individuals, Collector Bank, NFT Ventures and Almi Invest. Identitrade is under the supervision of The Swedish Financial Supervisory Authority and The Swedish Post and Telecom Authority (PTS). The principal activities of Identitrade are offering trust services and related technical solutions to the global finance industry with a focus on the European Union.

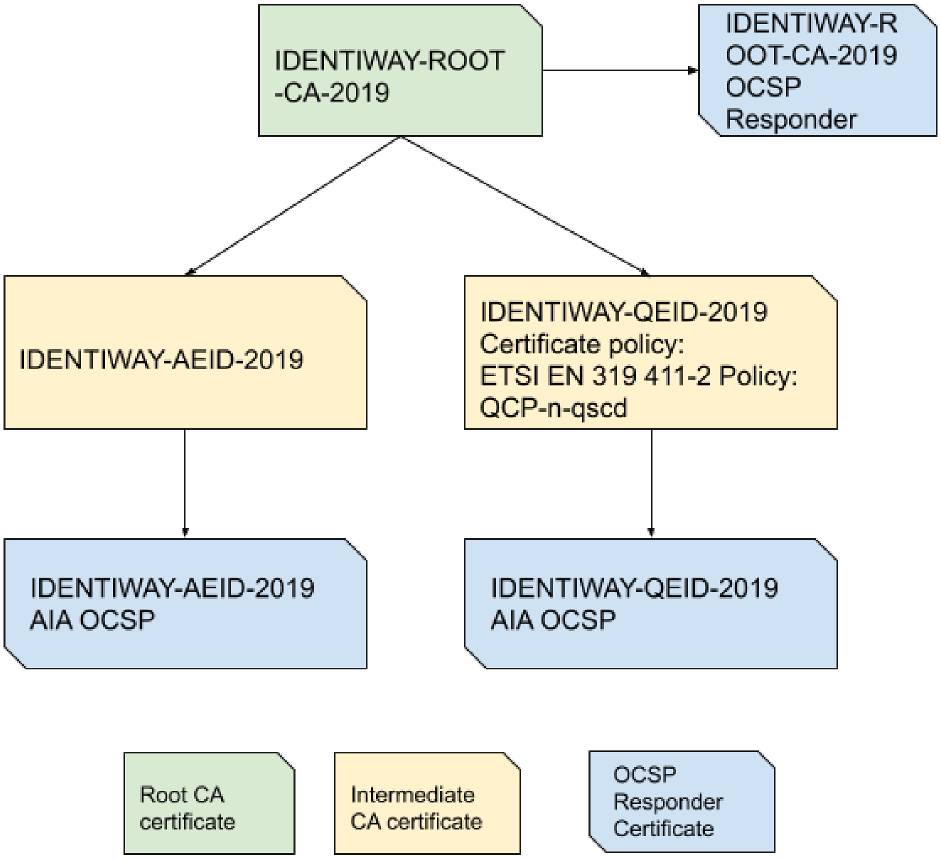
1.1. Overview

This CPS describes the practices for Identitrade's "Identiway QeID Service" based on the Certificate Policy (CP) defined by:

- eIDAS (EU regulation nr 910/2014),
- ETSI 319 401, 319 411-1 and 319 411-2 Policies: NCP+ and QCP-n-qscd
- Relevant ISO standards e.g. 27001
- Relevant elements of national law in Verfügung gemäß § 11 Absatz 1 VDG (Mitteilung Nr. 208 des Amtsblatts-Nr. 11/2018 der Bundesnetzagentur)
- CPS structure is in accordance with IETF RFC 3647

Identitrade currently uses this certificate chains:

- Identiway-Root-CA-2019 valid 2019-2049



IDENTIWAY-ROOT -CA-2019
IDENTIWAY-ROOT-CA-2019 OCSP Responder
IDENTIWAY-AEID-2019
IDENTIWAY-QEID-2019 Certificate policy: ETSI EN 319 411-2 Policy: QCP-n-qscd
IDENTIWAY-AEID-2019 AIA OCSP
IDENTIWAY-QEID-2019 AIA OCSP
Root CA certificate
Intermediate CA certificate
OCSP Responder Certificate

Certificates issued by Identiway QeID Service will be used for

- Providing software based electronic identities (electronic ID) in smartphone applications
- Subscriber non-repudiation electronic signing
- Subscriber authentication

This CPS is based on the structure suggested by Certification Practice Framework IETF RFC 3647. Section order and headings have been kept as close as possible to the suggested framework.

1.2. Document name and identification

This CPS is titled *Identiway QeID Certificate Practice Statement*. The Issuing CPS has the object identifier: OID 1.2.752.251.1.05.51.1.12

1.3. PKI participants

Identiway QeID Service will issue certificates to subscribers in order to providing software based IDs, non-repudiation signing and subscriber strong authentication

1.3.1. Certification authorities

Identitrade is the issuing CA. The name of the CA in the “Issuer” field of the CA certificate is “IDENTIWAY QEID 2019”.

1.3.2. Registration authorities

Registration authorities refer to the entities that establish identity proofing procedures for end-user certificate applicants, perform identification and authentication of certificate applicants, initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a CA. RA’s may also be external to the CA.

Identified RA’s for this CPS are:

- Identitrade’s TRA Service and any external RA’s integrated with Identitrade TRA Service
- External RA’s compliant with eIDAS/ETSI and ISO compliant RA functions.

1.3.3. Subscribers

The subscribers identified in this CPS are natural persons within the scope of their electronic identity.

1.3.4. Relying parties

Relying parties are defined as any Subscriber (as defined in Subscribers above) or any end-entity (also referred to as Customers) relying on the certificate issued by the Identiway QeID Service (CA).

1.3.5. Other participants

No stipulation.

1.4. Certificate usage

1.4.1. Appropriate certificate uses

Certificates under this CPS are issued to Subscribers for non-repudiation signing, strong authentication and issuance of electronic identity that will be issued to end-users.

1.4.2. Prohibited certificate uses

Applications using the certificates issued under this CPS must consider the key usage purpose stated in the “Key Usage” extension field in the certificate.

1.5. Policy administration

1.5.1. Organization administering the document

This CPS is administered by Identitrade:

Identitrade AB
Registry code SE5569724288
Box 3437
111 56 Stockholm
Visiting Address: Jakobsbergsgatan 16

Head Office: +46 (0)10-199 40 00
Email: info@identitrade.com
http://www.idenitway.com

1.5.2. Contact person

Compliance Manager
Email: legal@identiway.com

1.5.3. Person determining CPS suitability for the policy

Compliance Manager.

1.5.4. CPS approval procedures

Spelling corrections, translation activities and contact details updates are documented in the version table of this CPS.

In case of substantial changes, a new CPS version is clearly distinguishable from previous ones. The amended CPS along with the enforcement date, which cannot be earlier than 14 days after publication, is published electronically on Identiway website. All CPS versions are subject to a confirmation and approval by the Identitrade Management Board and amended CPS is enforced by the CEO.

1.6. Definitions and acronyms

1.6.1. Definitions

Term	Definition
Authentication	Unique identification of a person by checking his/her alleged identity.
Certificate	Public Key, together with additional information, laid down in the Certificate Profile rendered non forgeable via encipherment using the Private Key of the Certificate Authority which issued it.
Certificate Authority	A part of the trust service provider’s structure responsible for issuing and verifying electronic Certificates and Certificate Revocation Lists with its electronic signature. Identitrade has created the Identiway QeID Service that issues Certificates under this CPS.
Certificate Pair	A pair of Certificates consisting of one Authentication Certificate and one Qualified Electronic Signature Certificate.
Certificate Policy	A set of rules that indicates applicability of a specific Certificate to a particular community and/or PKI implementation with common security requirements.
Certification Practice Statement	One of the several documents that all together form the governance framework in which Certificates are created, issued, managed, and used.
Certificate Profile	Document that determines the information contained within a Certificate as well as the minimal requirements towards the Certificate.
Certificate Revocation List	A list of invalid (revoked, suspended) Certificates. CRL contains suspended and revoked Certificates during their validity period, i.e. until they expire.

CA Service	Trust service related to issuing Certificates, managing suspension, termination of suspension, revocation, modification and re-key of the Certificates. In this CPS the CA Service is called Identiway QeID Service.
Conformity Assessment Body (CAB)/Certification body	Official registered or accredited certification body that can assess and certify CA Services
Directory Service	Trust service related to publication of Certificate validity information.
Distinguished name	Unique Subject name in the infrastructure of Certificates.
Encrypting	Information treatment method changing the information unreadable for those who do not have the necessary skills or rights.
Identitrade	IdentitradeAB, the legal entity and provider behind the Trust Service and CA Service.
Identiway	The brand name used facing consumers, customers, relying parties and the market in general.
Identiway QeID Service	The specific name of the CA Service issuing qualified electronic signatures.
Identiway TRA Service	Trust service related to the identification and authentication for Identiway QeID Service.
Integrity	A characteristic of an array: information has not been changed after the array was created.
Object Identifier	An identifier used to uniquely name of an object (OID).
PIN code	Activation code for the Authentication Certificate and for the Qualified Electronic Signature Certificate.
Private Key	The key of a key pair that is assumed to be kept secret by the subscriber of the key pair, and that is used to create electronic signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key	The key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by Relying Parties to verify electronic signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Qualified Certificate	A certificate for electronic signatures, that is issued by the qualified trust service provider and meets the requirements laid down in Annex I of eIDAS Regulation [8] .
Qualified Electronic Signature	Advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a Qualified Certificate for electronic signatures.
Qualified Electronic Signature Creation Device	A Secure Signature Creation Device that meets the requirements laid down in eIDAS Regulation [8].
Relying Party	Entity that relies on the information contained within a Certificate. Relying parties are sometimes referred to as Customers.
Registration Authority	Entity that is responsible for identification and Authentication of Subjects of Certificates. Additionally, the Registration Authority may accept Certificate applications, check the applications and/or forward the applications to the Certificate Authority.
Secure Cryptographic Device	Device which holds the Private Key of the user, protects this key against compromise and performs signing or decryption functions on behalf of the user.
Idenittrade TRA Practice Statement	A statement of practices that Identitrade employs in providing RA service (also referred to as the TRA Trust Service Practice Statement - TSPS).
Subscriber	A natural person to whom the CA Service issue certificates and key as a service if he/she has requested it.
Subject	In this document, the Subject is the same as the Subscriber.
Terms and Conditions	Document that describes the obligations and responsibilities of the Subscriber with respect to using Certificates. The Subscriber has to be familiar with the document and accept the Terms and Conditions upon submitting an application for the Certificate based services.

1.6.2. Acronyms

Acronym	**Definition**
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
eIDAS	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
NCP+	Normalised Certificate Policy requiring a Secure Cryptographic Device from ETSI EN 319 411-1
OCSP	Online Certificate Status Protocol
OID	Object Identifier, a unique object identification code
PBGB	Police and Border Guard Board
PKI	Public Key Infrastructure
QSCD	Qualified Electronic Signature Creation Device
QCP-n-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD from ETSI EN 319 411-2 [5]
RA	Registration Authority
TRA Service	Trusted Registration Authority Service provided by Identitrade under the brandname Identiway

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

Identitrade ensures that its repository www.identiway.com/repository is available for the public 24 hours a day, 7 days a week with a minimum of 99% availability.

2.2. Publication of certification information

Identitrade makes the following documents publicly available:

- Trust Service Practice Statement
- Audit Results
- Insurance Policies
- Certificates, including root certificates and CA certificates under which certificates for subscribers are issued
- Profiles
- Terms and Conditions Identiway QeID
- Online Certificate Status Protocol

A published Online Certificate Status Protocol (OCSP) will contain all processed revocation information at the time of publication. Publication of revocation information is according to the provisions found in section 4.9. Publication of information will be within the limitations stipulated in sections 9.3 and 9.4.

2.3. Time or frequency of publication

All documents will be published 30 days before they come into force. All updates will be made with minimum delays.

2.4. Access controls on repositories

Information published in Identitrade's repository is public and not considered confidential information.

Identitrade has implemented all necessary security measures and enforced access control in order to prevent unauthorized access to add, delete, or modify entries into its repository. All CPS versions are subject to a confirmation and approval by the Identitrade Management Board before publication. Publishing into Identitrade's repository is restricted to authorized employees of Identitrade with multi-factor authentication access.

3. IDENTIFICATION AND AUTHENTICATION (I&A)

3.1. Naming

3.1.1. Types of names

3.1.1.1. Subscriber

Type of names assigned to the Subscriber is described in the Certificate Profile.

3.1.1.2. Issuing CA

Attribute	**Value description**
commonName (CN, OID 2.5.4.3)	Identitrade CA
OrganizationalUnitName (OU, OID 2.5.4.11)	www.Identitrade.com
Organization name (O, OID 2.5.4.10)	Identitrade AB
Organizational identifier (OID 2.5.4.97)	SE556972-4288
Country (C, OID 2.5.4.6)	SE

3.1.2. Need for names to be meaningful

All the values in the Subscriber information section of a Certificate are meaningful. Meaning of names in different fields of the Certificates is described in the Certificate Profile.

3.1.3. *Anonymity or pseudonymity of subscribers*

Anonymity or pseudonymity of subscribers is not allowed.

3.1.4. *Rules for interpreting various name forms*

International letters are encoded in UTF-8. The data extracted from an identity document follows ICAO transcription rules where necessary.

3.1.5. *Uniqueness of names*

Subscriber’s distinguished name is compiled according to the certificate profile described in the Certificate Profile. Identitrade does not issue Certificates with an identical Common Name (CN), Serial Number (S) and e-mail addresses in Subject Alternative Name (SAN) fields to different Subscribers.

3.1.6. *Recognition, authentication, and role of trademarks*

Trademarks are not allowed.

3.2. Initial identity validation

3.2.1. *Method to prove possession of private key*

Private Key of the Subscriber is generated using a smartphone app. This can be either the Identiway App or Identiway App SDK. In the Identiway App or App SDK the Subscriber’s Private Key is generated after successful completion of the registration process known as the Identiway TRA Service.

3.2.2. *Authentication of organization identity*

No stipulation.

3.2.3. *Authentication of individual identity*

Identiway TRA Service or an external contracted RA verifies the identity of the Subscriber. This data is submitted to Identiway QeID Service.

3.2.4. *Non-verified subscriber information*

Non-verified Subscriber information is not allowed in the Certificate.

3.2.5. *Validation of authority*

Representation of the Subscriber is not allowed.

3.2.6. Criteria for interoperation

No stipulation.

3.3. Identification and authentication for re-key requests

No stipulation.

3.3.1. Identification and authentication for routine re-key

No stipulation.

3.3.2. Identification and authentication for re-key after revocation

No stipulation.

3.4. Identification and authentication for revocation request

Please refer to 4.9.3. of this CPS.

.

4. CERTIFICATE LIFE-CYC[LE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Who can submit a certificate application

Any natural person can submit a certificate application via Identiway TRA Service or other contracted RA Services of Identitrade.

The Subscriber submits an application for a certificate via Identiway TRA Service or other contracted RA.

Identitrade accepts Certificate requests only from Identiway TRA Service or a contracted external RA. The RAs is responsible for prevention of unwanted applicants (e.g. minors) as part of identification processes.

4.1.2. Enrollment process and responsibilities

The registration and setup of subscriber applicants is done remotely (self-service) by the RA, primarily Idenitway TRA Service. The RA's need to meet requirements of Authentication of Subscribers:

- to a level of assurance based ISO/IEC 29115 level three (LoA3) and eIDAS level “Substantial” including
- demonstrating physical presence according eIDAS article 24, 1d) by being conformant with the same level of assurance and physical presence as defined in EU member state national law e.g. German VideoIdent ordinance of BNetzA

Subscriber applicants need to submit sufficient information to allow Issuing CAs and RAs to successfully perform the required verification. Issuing CAs and RAs shall protect communications and securely store information presented by the Applicant during the application process.

4.1.3. *Annual Control of QSCD*

Identitrade monitors certification status of QSCD-s in use and annually checks that QSCD is recognised by verifying the validity of Common Criteria Certificate issued for the QSCD or that it is continuously valid in the European Commission's list of Secure Signature Creation Devices and Qualified Signature notified by the member states.

If the validity in the European Commission's list of Secure Signature Creation Devices and Qualified Signature notified by the member states is expired due to the modification, then Identitrade will investigate the cause of the modification from the responsible member state or/and designated certification body. If the QSCD certificate is expired or invalidated, then Identitrade will take the following actions:

- notify immediately its supervisory body and conformity assessment body (CAB)
- revoke of any affected certificates;
- Inform all affected subscribers and relying parties.

4.2. Certificate application processing

4.2.1. *Performing identification and authentication functions*

Identiway TRA Service validates the Subscriber's identity as described in the Identiway TSPS. Identiway TRA Service sends the Certificate requests to Identiway QeID Service. Application for a Subscriber will be generated automatically via the TRA Service. All communications shall be securely stored along with all information presented directly by the Subscriber during the application process.

When an external contracted RA is used the data exchange is done via encrypted communication where a unique identifier is used by the RA in order to authenticate it.

Before starting the authentication, the Subscriber shall accept Terms and Conditions.

4.2.2. Approval or rejection of certificate applications

Applications are done by the Subscriber registering in the TRA service using the Identiway smartphone app or app SDK. The acceptance or rejection of a subscriber application is determined by Identiway TRA Service.

Subscriber applications will be approved if they meet the requirements in this CPS and those set forth in the Identiway TSPS there is no other reason for rejection. In case of rejection, a subscriber will be informed as part of the TRA Service as to the reason for the rejection decision, and provided details as to how to proceed for an approval.

Identitrade shall reject applications for Certificates where validation of all items cannot successfully be completed.

<need to also write about our contracted RAs>

4.2.3. Time to process certificate applications

Applications are processed automatically by Identiway QeID Service immediately after the application is submitted from the RA.

4.3. Certificate issuance

4.3.1. *CA actions during certificate issuance*

After verifying that the Subscriber's identification data in the Certificate request matches with the identification data in the data set, Identiway QeID Service automatically issues the corresponding Certificates.

4.3.2. *Notification to subscribers by the CA of issuance of certificate*

The subscriber will be notified of issuance of certificate with a message within the Identiway smartphone app immediately and a separate text message as it an online process.

4.4. Certificate acceptance

4.4.1. *Conduct constituting certificate acceptance*

Identiway QeID Service shall inform the Subscriber that s/he may not use the Certificate until the Subscriber has reviewed and verified the accuracy of the data incorporated into the Certificate. To avoid this being an open-ended stipulation, the issuing service may set a time limit by when the Certificate is deemed to be accepted.

Once the Subscriber verifies accuracy of data and confirms term and conditions, the Certificate is deemed as accepted. The consent and acceptance is logged.

4.4.2. *Publication of the certificate by the CA*

Identiway QeID Service may publish a Certificate by sending the Certificate to the Subscriber and/or publishing in our Certificate Repository. Certificate validity can be checked through OCSP service.

4.4.3. *Notification of certificate issuance by the CA to other entities*

Identiway QeID service will by means of secure data communication inform the contracted RA responsible for the application processing of the certificate issuance.

4.5. Key pair and certificate usage

4.5.1. *Subscriber private key and certificate usage*

The Subscriber is required to use the Certificate and Private Key and lawfully and in accordance with:

- this CPS;
- the Subscriber Terms and Conditions Identiway QeID,
- the Subscriber Terms and Conditions of Identiway TRA Service.
- the TSPS of the Identiway TRA Service

4.5.2. *Relying party public key and certificate usage*

The Relying Party is required to use the Public Key and Certificate lawfully and in accordance with:

- this CPS;
- the Terms and Conditions QeID
- Identiway Master Service Agreement

4.6. Certificate renewal

Renewal of Certificates is not allowed.

4.6.1. *Circumstance for certificate renewal*

No stipulation.

4.6.2. *Who may request renewal*

No stipulation.

4.6.3. *Processing certificate renewal requests*

No stipulation.

4.6.4. *Notification of new certificate issuance to subscriber*

No stipulation.

4.6.5. *Conduct constituting acceptance of a renewal certificate*

No stipulation.

4.6.6. *Publication of the renewal certificate by the CA*

No stipulation.

4.6.7. *Notification of certificate issuance by the CA to other entities*

No stipulation.

4.7. Certificate re-key

Certificate Re-Key initiated by the Subscriber is considered to be a new application and processed accordingly. Certificate re-key is not allowed.

4.7.1. *Circumstance for certificate re-key*

No stipulation.

4.7.2. *Who may request certification of a new public key*

No stipulation.

4.7.3. *Processing certificate re-keying requests*

No stipulation.

4.7.4. *Notification of new certificate issuance to subscriber*

No stipulation.

4.7.5. *Conduct constituting acceptance of a re-keyed certificate*

No stipulation.

4.7.6. *Publication of the rekeyed certificate by the CA*

No stipulation.

4.7.7. Notification of certificate issuance by the CA to other entities

No stipulation.

4.8. Certificate modification

Modification is processed as a new application and not allowed.

4.8.1. Circumstance for certificate modification

No stipulation.

4.8.2. Who may request certificate modification

No stipulation.

4.8.3. Processing certificate modification requests

No stipulation.

4.8.4. Notification of new certificate issuance to subscriber

No stipulation.

4.8.5. Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6. Publication of the modified certificate by the CA

No stipulation.

4.8.7. Notification of certificate issuance by the CA to other entities

No stipulation.

4.9. Certificate revocation and suspension

4.9.1. Circumstances for revocation

If the Subscriber loses control over his/her Private key or PIN codes, the Subscriber shall apply for Certificate revocation immediately.

Identiway QeID Service has the right to revoke Certificates and Private keys if one or more of the following occurs:

- the Subscriber requests revocation using the Identiway App or Site,
- the Subscriber has blocked the PIN code(s)
- Identiway QeID Service obtains evidence that the Subscriber has lost control over Private Keys or PIN codes;
- the Subscriber notifies Identiway QeID Service that the original Certificate request was not authorised and does not retroactively grant authorisation;
- Identiway QeID Service obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a key compromise or no longer complies with the requirements;
- Identiway QeID Service obtains evidence that the Certificate was misused; the service is made aware that the Subscriber has violated one or more of its obligations under the Terms and Conditions;
- Identiway QeID Service is made aware of a material change in the information contained in the Certificate;
- Identiway QeID Service is made aware that the Certificate was not issued in accordance with the CPS and/or CP;
- Identiway QeID Service determines that any of the information appearing in the Certificate is inaccurate or misleading;
- Identiway QeID Service ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- Identiway QeID Service's right to issue Certificates is revoked or terminated, unless Identiway QeID Service has made arrangements to continue maintaining the OCSP repository;
- Identiway QeID Service is made aware of a possible compromise of the Private Key of the CA used for issuing the Certificate;
- revocation is required by the CPS;
- the technical content or format of the Certificate presents an unacceptable risk to Relying Parties;

In case the RA has withdrawn Identity Provider status, the Identiway QeID Service has the right to revoke all the Certificates which were issued for identities provided by this Identity Provider.

4.9.2. Who can request revocation

The Subscriber can request revocation of the Subscriber's Certificates at any time.

RA may request revocation of the Subscriber’s certificates based on Subscriber’s application.

CA may request revocation for any of the reasons listed in this CPS 4.9.1.

4.9.3. Procedure for revocation request

The Subscriber can request revocation in the following way:

- The Subscriber can request revocation of Certificates by deleting the profile in the Identiway smartphone app or SDK app.
- By contacting the Identiway support desk and requesting revocation. The support agent verifies the Subscriber by using the identification data in the Subscriber's application. After the Subscriber's identity and legality is verified, the agent revokes the Certificate.

After Identiway has received an application for revocation, Identiway processes it immediately. The revocation of the Certificate is recorded in the certificate database of Identiway QeID Service, which has it’s time stamping synchronized with UTC at least once per 24 hours. The Subscriber has a possibility to verify from the Identiway System that the Certificate has been revoked.

Revoked Certificate can not be reinstated.

The RA can request revocation in the following ways:

- Using machine interface to flag a Subscriber’s profile for revocation.

4.9.4. Revocation request grace period

The Subscriber is required to request revocation immediately after verifying the loss or theft of the device.

4.9.5. Time within which CA must process the revocation request

Identiway QeID Service immediately processes an application for revocation, after an application for revocation has been submitted.

4.9.6. Revocation checking requirement for relying parties

Please see Terms & Conditions Identiway QeID Service.

4.9.7. CRL issuance frequency (if applicable)

The CRL are not issued. OCSP is used instead.

4.9.8. Maximum latency for CRLs (if applicable)

No stipulation.

4.9.9. On-line revocation/status checking availability

The service is free of charge and publically available 24/7 at http://ocsp.identiway.com

4.9.10. On-line revocation checking requirements

The mechanisms available to the Relying Party for checking the status of the Certificate on which it wishes to rely are established in Terms and Conditions Identiway QeID.

4.9.11. Other forms of revocation advertisements available

Revocation status information of expired Certificates can be requested at support@identiway.com.

4.9.12. Special requirements re key compromise

No stipulation.

4.9.13. Circumstances for suspension

No stipulation.

4.9.14. Who can request suspension

No stipulation.

4.9.15. Procedure for suspension request

No stipulation.

4.9.16. Limits on suspension period

No stipulation.

4.10. Certificate status services

Identiway QeID Service offers OCSP certificate status request services accessible over HTTP.

The URL of the OCSP service is included in the certificate.

4.10.1. Operational characteristics

No stipulation.

4.10.2. Service availability

Identiway QeID Service provides 24 hour availability of Certificate Status Services,, 7 days a week with a minimum of 99% availability overall per year.

4.10.3. Optional features

No stipulation.

4.11. End of subscription

The validity period of the Certificate is described in the Identiway Certificate and OCSP Profile.

4.12. Key escrow and recovery

The Identiway QeID Service does not offer the Subscriber key escrow and recovery services.

4.13. Key escrow and recovery policy and practices

No stipulation.

4.14. Session key encapsulation and recovery policy and practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical controls

Identitrade practices are documented and structured according to recognised standards e.g. ISO/IEC 27001, and other standards required by regulations and law. These form the foundation of Identiway QeID Service physical controls.

Identitrade's IT security management policy documents include the security controls and operating procedures for all facilities, systems and information assets providing the trusted services.

Identitrade performs risk assessment regularly in order to evaluate business risks, IT risks and risks related to the registration authority functions. These risk assessments determine the necessary security requirements and operational procedures. Identitrade management board approves risk assessment, oversees risk mitigation and accepts any residual risks.

Identitrade management establishes the security policy, which forms the basis for its approach to information security and management support.

The Identitrade Management Board approves policies and practices related to information security for the services.

As part of regular training and communication, Identitrade management communicates information security policies and procedures to employees and relevant external parties as appropriate.

In addition, Identitrade supports its practices and information security objectives for Trust Services with several types of reviews, audits and controls.

5.1.1. Site location and construction

Identiway QeID Services are produced within a physically protected environment that deters, prevents, and detects unauthorised use of, access to, or disclosure of Information and systems. The protection provided a high level of protection corresponding to the threat of identified risks. Identitrade ensures that physical access to critical services is controlled and that physical risks to its assets are minimised.

5.1.2. *Physical access*

Identitrade contracted data centre for the Identiway QeID Service are protected by six tiers of physical security, with access to the lower tier required before gaining access to the higher tier.

Access to the highest tier requires the participation of two persons in Trusted Roles.

The employees of Identitrade may gain access to the facilities of the Identiway QeID Services only as authorised resources notified on an approved list.

A log is kept for recording all entries and exits to the data center. The data center (location provider) has no independent access to the Identiway QeID Service hardware or software.

Common areas are outside the Identiway QeID Service rack.

5.1.3. *Power and air conditioning*

The data center has state-of-the-art power systems to ensure uninterrupted access to electric power. The facilities have all necessary heating, ventilation, air conditioning systems to control the temperature and relative humidity.

5.1.4. *Water exposures*

The data center has taken every reasonable precaution to minimise the impact of water exposure to the information systems.

5.1.5. *Fire prevention and protection*

The data centers have taken all reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. This includes high grade early smoke detection apparatus in conditioned modules and monitored automatic smoke detection. Measures comply with the highest fire prevention and protection standards.

5.1.6. *Media storage*

Data media containing confidential information shall be stored in locked physical premises. Highly confidential information may be stored only in a special fireproof safe designed for storing data media.

5.1.7. *Waste disposal*

Media containing Sensitive Information are securely disposed of when no longer required.

Paper documents and materials with sensitive Information are destroyed before disposal or placed in a secure waste handling box. Media used to collect or transmit Sensitive Information are rendered unreadable before disposal.

5.1.8. *Off-site backup*

The Identiway QeID Service performs routine backups to multiple sites of critical system data, audit log data, and other Sensitive Information. There is no off-site backup for the HSM.

5.2. Procedural controls

5.2.1. *Trusted roles*

Identitrade have defined the following critical trusted roles to meet security requirements:

Defined roles	Identitrade roles
Security Officers: Overall responsibility for administering the implementation of the security practices.	**IT Security Manager**
System Administrators: Authorized to install, configure and maintain the TSP's trustworthy systems for service management.	**System Administrator RA** **System Administrator CA**
System Operators: Responsible for	**System Administrator RA** **System Administrator CA**

operating the TSP's trustworthy systems on a day-to-day basis. Authorized to perform system backup.	
System Auditors: Authorized to view archives and audit logs of the TSP's trustworthy systems.	**IT Security Manager**

Identitrade has separated System Administrators with internal regulation into two roles called A- and B-type.

The assignment is made person by person with a decree of the CEO. See clause 5.2.2 for details.

Employees in Trusted Role have job descriptions that define the functions and responsibility related to the Trusted Role.

Identitrade ensures that personnel have achieved trusted status, and departmental approval is given before such personnel are:

- Issued access devices and granted access to the required facilities; or
- Issued electronic credentials to access and perform specific functions on Identitrade or other IT systems.

Security operations are managed by Identitrade personnel in Trusted Roles, but may actually be performed by a non-specialist, operational personnel (under supervision), as defined within the roles and responsibility documents. All requirements and rules for or concerning personnel in Trusted Roles apply equally to personnel with the temporary or permanent employment contract.

5.2.2. *Number of persons required per task*

Identitrade has established, maintains and enforces monitoring and review procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Key Manager	Minimum 2 persons
System Administrator CA System	Minimum 2 persons

The following activities require a minimum of two persons, i.e. two Key Managers:

- Generation of certification keys
- Backup of the certification keys
- Restoration of the certification keys

The following activities require a minimum of two persons, a System Administrator and a Key Manager:

- Management of HSM-s and CA-system
- Backup and restore of the CA-system

5.2.3. *Identification and authentication for each role*

All Trusted Roles are performed by persons qualified and assigned to this role by the Management Board.

Identitrade has implemented an access control system, which identifies authorities and registers all Identitrade information system users. User accounts are created for personnel in specific roles that need access to the system in question.

Any access requires users to log in with their personal account. To access administrative commands explicit permission is necessary and auditing of the execution takes place.

Identitrade employs file system permissions to prevent misuse.

User accounts are locked as soon as possible when the role change dictates. Access logs and rules are audited annually.

5.2.4. *Roles requiring separation of duties*

Trusted Roles are separated and are staffed by different persons. A single person cannot be simultaneously A- and B-type System Administrator.

5.3. Personnel controls

5.3.1. *Qualifications, experience, and clearance requirements*

Identitrade staff are provided relevant and timely training and have the experience and competence required to carry out the duties specified in role descriptions and employment contracts. Identitrade Management System defines a structured hiring process and continuous training process in the operational and security procedures.

Identitrade employees are required to

- Demonstrate that they have not been convicted of intentional crime
- Adhere to confidentiality clauses as part of their employment
- Remain neutral with regards to competing interests such as other business

Employees in Trusted Roles are further required to:

- Not participate in any activity regarding the issuing of certificates in his/her name or legal representative of him/her
- Remain neutral and objective with regards to any interests conflicting with Trust Services operations

Where Identitrade as a Trust Service Provider or as an RA applies for a certificate, personnel in Trusted Roles is obliged to follow all required procedures without exceptions as defined in practice statements.

5.3.2. *Background check procedures*

Identitrade Management System contains routines for personnel seeking to perform Trusted Roles. The routines consist of among other steps:

- Identity verification
- References from previous employers

- Background checks as per legality in respective jurisdictions and code of ethics (criminal record checks are refreshed periodically).

Identitrade background checks are proportionate to the level of information and security risks involved in roles. Background checks are conducted on all candidates for employment and trusted sub contractors performing the Trust Service providing operations with access to production data.

5.3.3. *Training requirements*

In addition to strict requirements on competence and experience at the time of hiring, Identitrade employees undergo regular training. It is key that all personnel have adequate training and necessary experience for the duties specified in the role description and employment contract, and maintain the necessary competency over time. Training includes:

- Internal Management System including Information and IT-security Policies, Routines
- New, updated and/or altered duties and competencies required for specific roles

5.3.4. *Retraining frequency and requirements*

Refresher training is conducted at least once per year, but typically takes place when changes occur.

5.3.5. *Job rotation frequency and sequence*

No stipulation.

5.3.6. *Sanctions for unauthorized actions*

Identitrade enforces human resource policies that stipulate employee sanctions where unauthorised actions are taken. Disciplinary actions are founded in relevant national labour law and include measures up to and including termination and police reports.

5.3.7. *Independent contractor requirements*

Identitrade uses sub-contractors in Trusted Roles. All sub-contractors have documented contracts and follow routines set out in Identitrade's Routines for sub-contractors. Identitrade delegates and defines the relevant requirements to the sub-contractor according to its role and tasks. The sub-contractor is responsible for compliance with defined requirements and its personnel acting in Trusted Roles.

5.3.8. *Documentation supplied to personnel*

Persons in Trusted Roles receive training and Trusted roles are documented and this documentation is provided as needed for the employee to perform job responsibilities.

5.4. Audit logging procedures

5.4.1. *Types of events recorded*

Identitrade ensures that all relevant information concerning the operation of the Trust Services is monitored and recorded for providing evidence for the purpose of legal proceedings. This information includes the archive records that are required for proving the validity of Trust Service Tokens and the audit log of the Trust Service operation.

Identitrade’s information systems leave an audit log of:

Category	Log details
General events	● Software installation, patches and updates ● Backup related information ● Boot and shutdown ● Time synchronization and detection of loss of synchronization ● All requests and reports relating to suspension and termination of suspension ● All requests and reports relating to revocation, as well as the resulting actions.
General Security events	● System subscriber account creation ● Configuration changes to Firewalls, Switches, Intrusion detection systems, and load balancers ● System crashes or other anomalies ● Hardware failures ● PKI System access attempts

	• Activities of system user with super admin rights
Identiway TRA events	• Registration • Backup • Storage • Archival • Destruction • Certificate Applications • Certificate Revocation • Successful or unsuccessful processing of events
Trust Service certificates	• All events relating to the life cycle of keys and certificates managed by Identitrade, including CA keys and certificates and Subscriber key pairs;

Log entries must also include:

- Date and Time
- Identity of the entry generator
- Attribute related to entry type

Identiway TRA Service logs of Certificate Applications include:

- Identifying document presented during application
- Personal data from accounts provided by trusted third parties
- Acceptance of the Subscriber agreement and any specific provisions
- Liveliness check output
- Manual identity verification decision
- Data pertaining to session (e.g. smartphone type) at registration.

5.4.2. *Frequency of processing log*

Processing logs is scheduled at regular intervals depending on the type of log. Instructions related to frequency and work procedure related to a particular logs, is detailed in internal documentation.

Audit logs are reviewed periodically for any evidence of malicious activity and following each important operation.

5.4.3. *Retention period for audit log*

Audit logs are retained no less than 10 years.

In case of Identitrade termination audit logs are retained and accessible until abovementioned term for retention in accordance with clause 5.8 of this Identiway QeID CPS.

5.4.4. *Protection of audit log*

Audit log is stored encrypted in an EC2 instance. The access to the audit log is given to a person who does not have access to Identiway QeID Service hardware or software.

5.4.5. *Audit log backup procedures*

Identitrade performs regular backups of critical system data, audit log data, and other Sensitive Information. Audit log data backup is the part of general back-up system. Identitrade has defined backup strategy and policies in internal documentation.

5.4.6. *Audit collection system (internal vs. external)*

Automated audit data is generated and recorded at the application, network and operating system level. Non-electronically generated audit data is recorded by Trusted Roles.

5.4.7. *Notification to event-causing subject*

No Stipulation

5.4.8. *Vulnerability assessments*

Events in the audit process are logged, in part, to monitor system vulnerabilities. Security vulnerability assessments are performed, reviewed, and revised. These assessments are based on real-time automated logging data and are performed on a daily, monthly, and annual basis.

5.5. Records archival

5.5.1. Types of records archived

Physical or digital archive records about certificate applications, signed Subscriber contracts, registration information (including evidence of Subscriber identity verification) and requests or applications for suspension, termination of suspension and revocation are retained.

5.5.2. Retention period for archive

Physical or digital archive records about certificate applications, signed Subscriber contracts, registration information (including evidence of Subscriber identity verification) and requests or applications for suspension, termination of suspension and revocation are retained for at least 10 years after validity of relevant certificate.

In case of termination Identitrade archive records are retained and accessible until abovementioned term for retention in accordance with clause 5.8 of this Identiway QeID CPS.

5.5.3. Protection of archive

The archive is encrypted and located in Amazon Glacier long term storage service.

The media holding the archive data and the applications required to process the archive data are maintained to ensure that the archive data can be accessed for the time period required.

5.5.4. Archive backup procedures

The archive is not backed up.

5.5.5. Requirements for time-stamping of records

Database entries contain accurate time and date information. The time-stamps are not cryptography based.

5.5.6. *Archive collection system (internal or external)*

Identitrade uses an internal archive collection system.

5.5.7. *Procedures to obtain and verify archive information*

Only authorised personnel in Trusted Roles are allowed access to the archive.

Should the records concerning the operation of services be required for the purposes of providing evidence of the correct operation of the services and for the purpose of legal proceedings, they are made available to legal authorities and/or persons whose right of access to them arises from the law.

The integrity of the information is verified during recovery tests. The archive systems with built-in integrity controls are in use.

5.6. Key changeover

No Stipulation

5.7. Compromise and disaster recovery

Identiway a Routine Business Continuity Plan (BCP) that guarantees a robust set of procedures as well as physical and logical security measures to minimize the impact of disaster. All procedures have been developed to minimize potential impact and restore operations within a reasonable period of time. Business Continuity plans are tested annually to determine whether they meet requirements and business continuity needs.

5.7.1. *Incident and compromise handling procedures*

Within the Information Security Management System an integral part of the Identiway QeID Service, change and incident management procedures have been developed to allow for a controlled, structured and accountable handling of incidents as well as recovery from systems or application disasters.

Detailed instructions can be found in the Identiway Incident Management Routine and in the Information Security Management System. Finally, External Communication routine governs the means of communication that is deemed necessary by Incident Evaluation Team.

The incidents can be submitted using either internal or external submission forms (www.identiway.com "Report an Issue"), or as an email to support@identiway.com

The response time by the Incident Evaluation Team is determined by the severity of the incident, but is no longer than 24 hours on working days.

The objective of Incident Management is the immediate response and recovery of availability and the continuous protection of Identiway QeID service.

In case of private CA key compromise Identitrade will additionally:

- Indicate that Identiway QeID Certificates and validity information issued using this CA may no longer be valid;
- Revoke any CA certificate that has been issued for Identitrade when Identitrade is informed of the compromise of another CA or TSA;
- Inform all affected subscribers and relying parties.

In case of algorithm or associated parameters become insufficient for its remaining intended usage Identitrade will additionally:

- Schedule a revocation of any affected Identiway QeID Certificates;
- Inform all affected subscribers and relying parties.

The critical vulnerability is addressed no later than 48 hours after its discovery; the vulnerability is remediated or a mitigation plan is created and implemented to reduce the impact of vulnerability or a decision has been made and documented that remediation is not required.

In the event of an emergency, Identitrade will inform all the Subscribers and Relying Parties immediately (or at least within 24 hours of the crisis committee's decision) of the emergency situation and proposed solution through public information communication channels.

Identitrade will inform without undue delay but in any event within 24 hours after having become aware of it, the Supervisory Body and, where applicable, other relevant bodies as national CERT of any breach of security or loss of integrity that has a significant impact on the Idenitway QeID Service provided.

If breach is likely to involve personal data and is likely to result in high risk to the rights and freedoms of the natural person, Identitrade will notify Swedish Data Protection Inspectorate without undue delay, but at least in 72 hours after initial discovery of the personal data breach.

5.7.2. *Computing resources, software, and/or data are corrupted*

In such case where computing resources, software, and/or data have been identified as corrupt, appropriate steps are taken for incident investigation, appropriate escalation and incident response. If necessary, Identiway ́s internal documentation in the Management System, Compromise and disaster recovery plan may be applied.

5.7.3. *Entity private key compromise procedures*

Identiway key compromise is handled according to internal Incident Management documentation and considered to be a disaster.

5.7.4. *Business continuity capabilities after a disaster*

In order to ensure the business continuity capabilities after a disaster Identitrade organises periodically crisis management trainings. Identitrade internal documentation defines how crisis management and communication take place in emergency situations.

Identiway has implemented Identiway QeID Service infrastructure in a redundant configuration to minimise the impact of disasters. In addition, important information with respect to restoring the Identiway QeID Service is backed up for disaster recovery purposes.

5.8. CA or RA termination

5.8.1. RA termination

Identiway has a documented Termination Plan for its TRA Service which describes the process of a service termination. Stakeholders affected by any termination will be informed according to the Termination Plan and Routine External Communication.

5.8.2. CA termination

The Identiway QeID Service is terminated:

- with a decision of Identiway Management Board;
- with a decision of the authority exercising supervision over the supply of the service;
- with a judicial decision;
- upon the liquidation or termination of the operations of Identiway.

Identitrade ensures that potential disruptions to Subscribers and Relying Parties are minimised as a result of the cessation of Identiway's services, and in particular, it ensures the continued maintenance of information required to verify the correctness of Identiway QeID Service Tokens.

Before Identitrade terminates a CA Service the following procedures will be executed:

- Identitrade informs all Subscribers and other entities with which Identitrade has contracts or other forms of established relations. In addition, this information will be made available to other Relying Parties;
- Identitrade makes the best effort for doing arrangements with other Trust Service Provider to transfer the provision of services for its existing customers;
- Identitrade destroys the CA private keys, including backup copies or keys withdrawn from use in such a manner that the private keys cannot be retrieved;
- Identitrade resets or destroys any hardware appliances related to this service depending on the security regulations;
- Identitrade terminates authorisation of all subcontractors to act on behalf of Identitrade in carrying out any functions relating to the process of issuing Identiway QeID Service Tokens for this service.

The notice of termination of Identitrade's Identiway QeID Service will be published in the public media.

Identitrade does not assume liability for any loss or damage sustained by the user of the service as a result of such termination provided that Identitrade has given the notice of termination through public information communication channels for at least one month in advance.

Identitrade has an arrangement with an insurer to cover the costs to fulfil these minimum requirements in case the TSP goes bankrupt, or for other reasons, is unable to cover the costs by itself.

The requirements are applicable also in case of RA termination. Identitrade takes over the documentation and information related to the supply of the Trust Service and provides evidence of the operation for a time period defined in relevant service-based Policy and/or Practice Statement.

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

Identitrade uses cryptographic keys for its Trust Services and follows industry best practices for key lifecycle management, key length and algorithms.

6.1.1. Key pair generation

The signing keys of Identiway QeID Service are created in accordance with the internal regulations of Identitrade: Procedure for Creating Identitrade Root Key and Procedure for Creating Keys for Intermediate Certification Authorities. For the key ceremony of Identiway QeID Service key pair generation for all CA's (whether root or intermediate CA-s), OCSP responders or TSA-s, the commission is appointed by CEO with internal regulation. The commission has to include external auditor independent of Identitrade, who confirms the correctness of the procedure and report of key ceremony.

Procedure for Identiway QeID Service key pair generation is carried out according to the detailed instructions created for the specific procedure. The creation of Identiway QeID Service keys is observed by a commission, which after the creation of the keys draws up an appropriate deed containing the public key of the created pair of keys and the hash thereof.

The Identiway QeID key pair generation and the private key storage occur in the HSM, which is used for providing keys that at least meet the requirements established in the security standard ISO/IEC 15408, EL4+. The HSM protects the key from external compromise and operates in a physically secure environment.

Identitrade has documented procedure for conducting Identiway QeID Service key pair generation. Head of the commission creates a report proving that the ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured. Report is signed by the commission members, including external auditor. The more detailed procedures for key ceremony, roles and responsibilities of participants during and after the procedure, requirements for report and collected evidences are defined in internal documentation of Identitrade.

Early enough before expiration of its QeID Service certificate, Identitrade generates a new QeID Service certificate for signing subject key pairs and apply all necessary actions to avoid disruption of any operations that rely on the certificate and to allow all relying parties to become aware of key changeover. Common name of the QeID Service certificate always contains the number of the year which it was created. The new QeID Service certificate is generated and distributed according to this practice statement and service-related practice statements.

6.1.2. Private key delivery to subscriber

The private key is not delivered to the subscriber.

6.1.3. Public key delivery to certificate issuer

6.1.4. CA public key delivery to relying parties

6.1.5. Key sizes

Subscriber keys are 2048 bits when RSA and 256 bits when ECC algorithm is used.

6.1.6. Public key parameters generation and quality checking

6.1.7. Key usage purposes (as per X.509 v3 key usage field)

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards and controls

The HSMs used by Identiway QeID Service are certified with EN 419 221-5 Common Criteria (ISO/IEC 15408).

Identiway QeID Service verifies that HSM is not tampered after its installation. This is documented in a HSM life-cycle protocol.

Identiway QeID Service verifies that HSM is functioning correctly during usage and retains it’s certification status.

6.2.2. Private key (n out of m) multi-person control

The access to Identiway QeID Service keys is divided into three parts that are secured by different persons in Trusted Roles. For activation of the signing key of Identiway the presence of at least two authorized persons is required in accordance with clause 5.2.2 of this CPS.

6.2.3. Private key escrow

No Stipulation.

6.2.4. *Private key backup*

No stipulation.

6.2.5. *Private key archival*

Identiway QeID Service will not archive Trust Service private keys after it has expired. All copies of Identiway QeID Service Trust Service private keys are destroyed after their expiry or revocation so that further use or derivation thereof is impossible.

6.2.6. *Private key transfer into or from a cryptographic module*

All Identiway QeID Service Trust Service keys must be generated by and in the cryptographic module. Identiway QeID Service generates Trust Service key pairs in the HSM in which the keys will be used.

6.2.7. *Private key storage on cryptographic module*

Identiway QeID Service Private Keys held in the HSM are stored in encrypted form.

6.2.8. *Method of activating private key*

Each of the Identiway QeID Service keys is protected with its PIN code.

The Subscriber is prompted to enter the PIN code before any single operation done with the Private Key.

It is not possible to try all possible PIN codes sequentially.

It is possible to create different PIN codes for the keys with different intended purposes - e.g. it is possible to create different PIN codes for the keys of the Authentication and Qualified Electronic Signature Certificates, correspondingly.

The length of the PIN codes is at least:

- for the Authentication Key 4 numbers,
- for the Signature Key 5 numbers.

6.2.9. Method of deactivating private key

6.2.10. Method of destroying private key

Method of destroying Identiway QeID Service Trust Service private keys and internal control mechanisms depend from the options available to specific secure cryptographic module.

6.2.11. Cryptographic Module Rating

See chapter 6.1.2 above.

6.3. Other aspects of key pair management

6.3.1. Public key archival

All certificates issued (including all expired or revoked certificates) are retained and archived as part of Identiway QeID Service routine backup procedures. The retention period is indefinite.

6.3.2. Certificate operational periods and key pair usage periods

The operational period of a certificate ends upon revocation. The operational period for key pairs is the same as the operational period for the certificates, except that they may continue to be used for signature verification.

In addition, Identiway QeID Service stops issuing new certificates at an appropriate date prior to the expiration of the Trust Service certificate such that no Subscriber certificate expires after the expiration of the Trust Service certificate.

If an algorithm or the appropriate key length offers no sufficient security during the validity period of the certificate, the concerned certificate will be revoked and a new certificate application will be initiated. The applicability of cryptographic algorithms and parameters is constantly supervised by Identitrade's management.

6.4. Activation data

6.4.1. Activation data generation and installation

Identiway QeID Service Trust Service private key activation data generation and installation is performed according to the user manual of HSM.

The initial activation data is chosen by Subscriber. PIN codes are not stored by Identiway QeID Service nor by the Identiway Application.

6.4.2. Activation data protection

HSM is kept in secure storage and access to it have only authorized personnel in Trusted Roles. Two Key Managers need to be present physically to conduct any HSM operation.

The Subscriber shall memorise the PIN codes and not share them with anyone else. If the PIN codes are not under the control of the Subscriber, the Subscriber shall apply for a new Identiway QeID Service or apply for Certificate revocation immediately.

6.4.3. Other aspects of activation data

No stipulation.

6.5. Computer security controls

6.5.1. Specific computer security technical requirements

Identitrade ensures that the certification system components are secure and correctly operated, with an acceptable risk of failure.

Identitrade certification services system components are managed in accordance with defined change management procedures. These procedures include system testing in an isolated test environment and the requirement that change must be approved by the IT Security Manager. The approval is documented for further reference.

All critical software components of Identitrade are installed and updated from trusted sources only. There are also internal procedures to protect the integrity of certification service components against viruses, malicious and unauthorised software.

All media containing production environment software and data, audit, archive, or backup information are stored within Identitrade with appropriate physical and logical access controls designed to limit access to authorised personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic). Media management procedures and backup of records and data to different media types protects against obsolescence and deterioration of media within the period of time that records are required to be retained. Media containing Sensitive Information are securely disposed of when no longer required. All removable media are used only for the intended period of the user (either by time or by number of uses).

The performance of Identitrade services and IT systems and their capacity is monitored by System Administrators and changes are done when necessary according to internal change management procedure.

Identiway QeID Service hardware is physically located in a secure location with multiple access and logic controls.

Incident response and vulnerability management procedures are documented in an internal document. Monitoring system detects and alarms of abnormal system activities that indicate potential security violation, including intrusion into the network.

Paper documents and materials with Sensitive Information are securely disposed. Media used to collect or transmit Sensitive Information are rendered unreadable before disposal.

Identitrade security operations include: operational procedures and responsibilities, secure systems planning and acceptance, protection from malicious software, backup, network management, active monitoring of audit logs event analysis and follow-up, media handling and security, data and software exchange. Identitrade has implemented security measures and enforced access control in order to avoid unauthorized access and attempts to add, delete or modify information in applications related to the services, including certificates and revocation status information. User accounts are created for personnel in specific roles that need access to the system in question. Identitrade's personnel are authenticated before using critical applications related to the services. Multi-factor authentication for all accounts capable of directly causing certificate issuance is enforced. All users must log in with their personal account, and administrative commands are only available with explicit permission and auditing of the execution. File system permissions and other features available in the operating system security model are used to prevent any other use. User accounts are removed as soon as possible when the role change dictates. Access rules are audited annually.

6.5.2. *Computer security rating*

Identitrade uses standard computer systems.

6.6. *Life cycle technical controls*

6.6.1. *System development controls*

An analysis of security requirements is carried out at the design and requirements specification stage of any systems development project undertaken by Identiway QeID Service; or an analysis is carried out on behalf of Identiway QeID Service to ensure that security is built into the Information Technology's systems.

The software will be approved by the IT Security Manager and will originate from a trusted source. New versions of software are tested in a testing environment of the appropriate service and their deployment is conducted according to documented change management procedures. Changes to systems are documented.

6.6.2. *Security management controls*

Measures are implemented In the information system of Identiway QeID Service, including all workstations for guaranteeing the integrity of software and configurations, as well as for detecting fraudulent software and restricting its spread.

Only the software directly used for performing the tasks is used in the information system.

6.6.3. Life cycle security controls

Identiway QeID Service policies, assets and practices (including Identiway QeID Service CPS) for information security are reviewed by a person which is responsible for administering and maintaining them at planned intervals or in case of significant changes to ensure their continuing suitability, adequacy and effectiveness.

The configurations of Identiway QeID Service systems are regularly checked for changes that violate Identiway QeID Service security policies. A review of configurations of the issuing systems, security support systems, and front-end/internal support systems occurs at least on a weekly basis. The IT Security Manager approves changes that have an impact on the level of security provided. Identiway QeID Service has procedures for ensuring that security patches are applied to the certification system within a reasonable time period after they become available, but not later than six months following the availability of the security patch. The reasons for not applying any security patches will be documented.

Identitrade manages the registration of information assets and classifies all information assets into security classes according to the results of the regular security analysis consistent with the risk assessment. A responsible person has been appointed for all important information security assets.

6.7. Network security controls

Identiway QeID Service network is divided into zones by security requirements. Communication between the zones is restricted. Only the protocols needed for Identiway QeID Service services are allowed through the firewall.

There are separate and dedicated firewalls in place for enforcing the security policy. Access to the administrative interfaces of IT equipment is not directly accessible from the public Internet. For the most critical tasks a separate workstation is used.

The front-end systems are in a DMZ protected by a firewall and TLS offload servers. Actual securitycritical services and corresponding HSMs run in a secure zone that is separated by dedicated firewall and has no direct Internet access.

The root CA is in a high security zone and is air-gapped from all the other networks. Identiway QeID Service systems are configured with only these accounts, applications, services, protocols, and ports that are used in the Trust Service operations.

Identitrade ensures that only personnel in Trusted Roles have access to a secure zone and a high security zone.

The cabling and active equipment along with their configuration in Identitrade's internal network are protected by physical and organisational measures.

The transfer of Sensitive Information outside Identitrade's internal network is encrypted.

Communication between distinct trustworthy systems is established through trusted channels that are logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

The security of Identitrade's internal network and external connections is constantly monitored to prevent all access to protocols and services not required for the operation of the Trust Services.

Identitrade performs a vulnerability scan once in a year on public and private IP addresses identified by Identitrade.

Identiway QeID Service and Identitrade assets undergo penetration testing on the certification systems annually at the set up and after the infrastructure or application upgrades or modifications determined significant by Identitrade.

Identitrade records evidence that each vulnerability scans and penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

6.8. Time-stamping

All Identiway QeID Service CA components are synchronized daily with a Network Time Protocol (NTP) service. A dedicated authority, such as a timestamping authority, may be used to provide this trusted time. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Issuance of Subscriber end entity Certificates.

Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate profile

Refer to Identiway QeID Service Certificate and OCSP Profile.

7.2. CRL profile

No stipulation.

7.3. OCSP profile

Refer to Identiway QeID Service Certificate and OCSP Profile.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency or circumstances of assessment

The conformity of information systems, policies, practices, facilities, personnel, and assets of Identitrade are assessed by a CAB pursuant to the eIDAS regulation, ETSI Standards and relevant national law. Conformity is assessed at least periodically and when any major change is made to Trust Service operations. Identitrade's internal auditor carries out internal reviews and audits on a rolling yearly schedule.

8.2. Identity/qualifications of assessor

Identitrade's CAB is accredited according to Regulation EC no 765/2008. The CAB is competent to carry out conformity assessments of Qualified Trust Service Providers and its services.

8.3. Assessor's relationship to assessed entity

The auditor of the CAB shall be independent from Identitrade and Identitrade assessed systems. The internal auditor shall not audit his/her own areas of responsibility.

8.4. Topics covered by assessment

The conformity assessment covers the conformity of information system, policies and practices, facilities, personnel, and assets with eIDAS regulation, respective legislation and standards.

The CAB audits all parts of the information system used to provide Trust Services. Activities subject to internal auditing are the following:

- Quality of Service
- Security of Service
- Security of operations and procedures;

The CAB Protection of the data of Subscribers and security policy, performance of work procedures and contractual obligations, as well as compliance with CPS and service-based Policies and Practice statements.

The CAB and the Internal Auditor also audit these parts of the information system, policies and practices, facilities, personnel, and the assets of sub-contractors that are related to providing Identitrade Trust Services (e.g. including RAs).

8.5. Actions taken as a result of deficiency

Where the CAB identifies deviations or non compliance in the assessment, the Supervisory Body requires Identitrade to remedy these to fulfil requirements within a time limit set by the Supervisory Body.

Identitrade makes efforts to stay compliant and fulfil all requirements of the deficiency on time. Identitrade management is responsible to implement a corrective action plan. Identitrade assesses the deviations or non compliance items and prioritizes appropriate actions to be taken. If any deviations relate to the protection of personal data, the Supervisory Body shall inform the data protection authority.

8.6. Communication of results

Certificate(s) for trust service(s) resulting from conformity assessment audits conducted pursuant to the eIDAS regulation, corresponding legislation and standards, are published on Identitrade's website https://www.identiway.com/repository.

Identitrade submits the resulting conformity assessment report to the Supervisory Body within three working days.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Certificate issuance or renewal fees

Subscriber is not required to pay fees for Certificate Issuance.

9.1.2. Certificate access fees

Subscriber is not required to pay fees for Certificate access.

9.1.3. Revocation or status information access fees

Neither Subscribers nor Relying Parties are required to pay fees for accessing revocation or status information.

9.1.4. Fees for other services

Relying parties pay fees according to Master Service Agreements and Service specification signed with Identitrade.

9.1.5. Refund policy

Identitrade handles refund requests from Relying Parties on a case-by-case basis.

9.2. Financial responsibility

9.2.1. Insurance coverage

Identitrade has professional services insurances required by law and published on www.identiway.com/repository.

9.2.2. Other assets

No stipulation.

9.2.3. Insurance or warranty coverage for end-entities

See clause 9.2.1. above

9.3. Confidentiality of business information

9.3.1. Scope of confidential information

Subscriber has the right to access all personal data held by Identitrade. Any other information known to the Subscriber or Relying party whilst using the services, and that is not intended for publication, is confidential.

9.3.2. Information not within the scope of confidential information

Any information not listed as confidential or intended for internal use is public information. Identitrade reserves the right to publish non-personalised statistical data about its services.

9.3.3. Responsibility to protect confidential information

Identitrade safeguards confidential information and information intended for internal use from illicit access and use by third parties.

9.4. Privacy of personal information

9.4.1. Privacy plan

Identitrade strives to minimize the risks for the individual when processing personal data. Identitrade strictly adheres to the principles and regulations required by GDPR. Identitrade services are designed with privacy in mind.

9.4.2. Personal Data Processed

The scope of Personal Data processed by Identitrade is listed under TRA-PS found under www.identiway.com/repsository or by other RA practice statements.

9.4.3. Information not deemed private

No stipulation.

9.4.4. Responsibility to protect personal data

Identitrade ensures protection of personal information by implementing security controls as described in chapter 5 of this CPS.

9.4.5. Notice and consent to use personal data

Identitrade Subscriber terms & conditions describe under which the subscriber grants Identitrade his/her notice and consent to use his/her personal data.

9.4.6. Disclosure pursuant to judicial or administrative process

Where Identitrade is required by law, court of law or law enforcement requests to disclose personal data Identitrade will comply.

9.4.7. Other information disclosure circumstances

9.5. Intellectual property rights

Identitrade is the exclusive holder of all intellectual property rights to this CPS.

9.6. Representations and warranties

9.6.1. CA representations and warranties

Identitrade is a TSP participant in a mutual contract between TSP, Subscribers and Relying Parties. This CPS shall form the basis of such contract.

Identitrade shall:

- provide its services consistent with the requirements and the procedures defined in this CPS and according to the policies under which this CPS is created.
- Be responsible for the effective compliance with the procedures set forth in this CPS
- Provide the service in compliance eIDAS regulation and related legal acts and standards

- Provide publicly published repositories with high electronic availability of all practice statements mentioned in this CPS.
- Honour its part in Subscriber terms and conditions and secure Subscriber availability and access to the services set out in this CPS
- Protect the integrity and confidentiality of personal data and information acquired as part of service provisioning and not subject to publication
- Maintain the integrity of Trust Service Access to Relying parties (e.g. Tokens) and offer effective services to check the validity of certificates
- Inform the Common Criteria Assessment body and National Supervisory Body of any changes to a public key used for the provision Trust Services
- Within 24 hours after having become aware of it, notify the Supervisory Body of any breach of security or loss of integrity that has a significant impact on the Trust Service provided
- Within 72 hours after initial discovery, notify the Swedish Data Protection Authority (Datainspektionen) of any personal data breach
- Where the breach of security or loss of integrity or personal data breach is likely to adversely affect a natural or legal person to whom the Trusted Service has been provided, notify the natural or legal person of the breach without undue delay;
- Preserve all the documentation, records and logs related to Trust Services according to the clauses 5.4 and 5.5;
- Ensure a conformity assessment with a CAB on a recurring basis according to requirements.
- Present the conclusions of the CAB to the Supervisory Body to ensure continual status of Trust Services in the Trusted List;
- Have the financial stability and resources required to operate in conformity with this CPS;
- Publish the terms of the compulsory insurance policy and the conclusion of CAB in the Identitrade online repository
- Secure that Identitrade employees do not have criminal records of intentional crime

Identitrade further warrants that it has documented contracts and contracts with its subcontracting and outsourcing partners.

Identitrade has defined in these contracts liabilities and ensured that partners are bound to implement any requirements and controls required by Identitrade.

Identitrade works with its best to guarantee that all potential service users, especially people with disabilities, can access the services provided by Identitrade on an equal basis. Identitrade accepts that its services imply at least some sort of qualitative capabilities and legal capacity, but nonetheless truly aspires to provide trust services and related technical solutions in a nondiscriminating way.

9.6.2. RA representations and warranties

Where the Identiway TRA Service is acting RA, TRA Service specifically shall:

- Perform its services according to the TRA-PS,
- Meet the level of assurance equivalent to physical presence in remote identification as set forth in German national state-of-the-art legislation conformant to eIDAS

In addition Identiway TRA Service and any other participating RAs shall:

- Provide its services consistent with the requirements and the procedures defined in the contract between Identitrade and RA, in this CPS and all other service-based Policies and Practice statements;
- Meet the level of assurance equivalent to physical presence in remote identification as set forth in any EU state national state-of-the-art legislation conformant to eIDAS
- Provide necessary training for its employees;
- Upon any known security or integrity breach notify Identitrade of any that has an impact on the Trust Service provided or on the personal data maintained therein.
- Enforce policies for background checks to prevent employees convicted of intentional crimes having Trusted Roles.

9.6.3. Subscriber representations and warranties

The Subscriber shall:

- Use all trust services in his/her name with correct and complete information in the application for the services.
- Where data submitted has changed, notify any and all corrections and amendments to the data in accordance terms & conditions and this CPS
- Note that intentionally presented false, incorrect or incomplete information will lead to denial of application and may lead to a police report
- be solely responsible for the maintenance of his/her private key and Trust Service Tokens.

  The Subscriber shall use his/her private key and Trust Service Tokens in accordance with this CPS and service terms and conditions.

9.6.4. Relying party representations and warranties

A Relying Party shall:

- Review and observe the documentation, risks and liabilities related to the acceptance of Trust Service Tokens. The risks and liabilities have been set out in this CPS, and in the service terms and conditions.
- Review and observe all necessary means and methods of integration and data communication as set forth under developer.identiway.com
- Verify the validity of Trust Service Tokens on the basis of validation services offered by Identitrade using the prescribed methods of data communication with and appropriate cryptographic information.

9.6.5. Representations and warranties of other participants

No stipulation.

9.7. Disclaimers of warranties

Identitrade:

- is liable for the delivery of all its obligations specified in clause 9.6.1 to the extent prescribed by Swedish law
- maintains adequate insurance coverage and contracts covering Identitrade Trust Services and providing liability compensation

Identitrade is not liable for:

- Non performance according to this CPS by Force Majeure
- That Subscriber private keys are kept secret or for any abuse of certificates
- Any errors in checking Trust Service Tokens on the part of Relying parties
- Any non-performance where this is due mistakes made by the Supervisory Body, the Data Protection Supervisory Authority or any other public authority or Trusted List,

9.8. Limitations of liability

The limits of liability claims arising from this CPS are established in the insurance policy and can be found at https://identiway.com/repository

9.9. Indemnities

Indemnities between the Subscriber and Identitrade are regulated in service based Terms and Conditions Identiway QeID.

9.10. Term and termination

9.10.1. Term

No stipulation.

9.10.2. Termination

This CPS remains in force until a new version is announced and published or when it is terminated due to Trust Service or Identitrade's termination. In the event of Identitrade's or the Trust Service termination, Identitrade is obliged to ensure the protection of personal and confidential information.

9.10.3. Effect of termination and survival

Identitrade communicates the status of this CPS's on its public repository.

The communication specifies which provisions survive termination. In case of such termination, and to meet its obligations, Identitrade archives and logs personal and confidential information, as well as the public information present on the repository.

Subscriber contracts are in effect until the certificate is revoked or expired, even if this CPS terminates. Termination of this CPS cannot be done before termination actions described in clause 5.8 of this CPS.

9.11. Individual notices and communications with participants

Identitrade uses its website www.identiway.com for all notifications and communications to subscribers and relying parties. In addition, smartphone applications (Identiway app or app SDK) may be used for notifications and communications.

9.12. Amendments

9.12.1. Procedure for amendment

See 1.5.4 of this CPS.

9.12.2. Notification mechanism and period

See 2.2.1 of this CPS.

9.12.3. Circumstances under which OID must be changed

No stipulation.

9.13. Dispute resolution provisions

All disputes between the parties will be settled by negotiations. If parties fail to reach an amicable contract, the dispute will be resolved in the District Court of Stockholm, Sweden.

The Subscriber or other party can submit their claim or complaint on the following email: legal@identiway.com

9.14. Governing law

This CPS is governed by the jurisdiction of the European Union and Sweden.

9.15. Compliance with applicable law

Identitrade ensures compliance with the legal requirements to meet all applicable statutory requirements for protecting records from loss, destruction and falsification, and the requirements of the following:

- eIDAS - 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
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) effective from 2018-05-25
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy

Requirements for Trust Service Providers

- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates Part 2: Policy requirements for certification authorities issuing qualified certificates
- Requirements for Trust Service Providers issuing Time-Stamps

9.16. Miscellaneous provisions

9.16.1. Entire contract

Identitrade mandates each RA by way of contractual obligation to comply with this Identiway QeID CPS. Identitrade also requires each party using its services to sign a contract that outline all terms of the service. If an contract has provisions that differ from this CPS, then the contract with that party prevails, if precedence to this CPS is explicitly defined in the contract.

9.16.2. Assignment

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of Identitrade. Unless specified otherwise in a contract with a party, Identitrade does not provide notice of assignment.

9.16.3. *Severability*

Identitrade may claim indemnification and legal fees from a party for damages, losses, and expenses related to that party's conduct. Identitrade’s failure to enforce a provision of this CPS does not waive Identitrade’s
right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by Identitrade.

9.16.4. *Enforcement*

Identitrade may claim indemnification and legal fees from a party for damages, losses, and expenses related to that party's conduct. Identitrade’s failure to enforce a provision of this CPS does not waive Identitrade’s
right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by Identitrade.

9.16.5. *Force Majeure*

Identitrade and other parties cannot be held responsible for any consequences caused by circumstances beyond his reasonable control, including but without limitation to

- war,
- acts of government or the European Union,
- export or import prohibitions,
- breakdown or general unavailability of public telecommunications networks and logistics infrastructure,
- general shortages of energy, fire, explosions, accidents, strikes or other concerted actions of workmen, lockouts, sabotage, civil commotion and riots.

Communication and performance in the case of Force Majeure are regulated between the parties with the contracts.

Non-fulfilment of the obligations arising from CPS and/or relevant service-related Policies and/or Practice Statements is not considered a violation if such non-fulfilment is occasioned by Force Majeure.

None of the parties shall claim damage or any other compensation from the other parties for delays or non-fulfilment of this CPS and/or relevant service-related Policies and/or Practice Statements caused by Force Majeure.