PKIoverheid PKI Disclosure Statement

Version 2.02, 17 April 2026

Table of Contents

Important Notice about this Document

This document is the DigiCert Europe PKI Disclosure Statement for PKIoverheid hereinafter referred to as the PDS. DigiCert Europe Netherlands B.V. is registered in the Netherlands, hereafter referred to as "DigiCert Europe" within this document.

This document does not substitute or replace the Certification Practice Statement (CPS) under which Digital Certificates are issued by DigiCert Europe.

You must read the relevant Certification Practice Statement for PKIoverheid Certificates at https://www.digicert.com/legal-repository/europe before you apply for or rely on a PKIoverheid Certificate issued by DigiCert Europe .

The purpose of this document is to summarise the key points of the DigiCert Europe CPS for PKIoverheid for the benefit of Subscribers, Subjects, and Relying Parties.

This version of the PDS has been approved for use by the DigiCert Policy Authority (DCPA) and is subject to amendment and change in accordance with the policies and guidelines adopted, from time to time.

The date on which this version of the PDS becomes effective is indicated on this document.

Version Control:

Author	Date	Version	Comment
QuoVadis PMA	27 August 2018	1.0	First version
QuoVadis PMA	11 July 2019	1.1	Updates for dispute resolution and more references to Private CPS and Certificate classes
QuoVadis PMA	10 September 2019	1.2	Updates to reflect consolidated PKIoverheid CPS and where QuoVadis manages Private Keys on behalf of the Subscriber (remote QSCD)
QuoVadis PMA	28 March 2020	1.3	Review and alignment with PKIoverheid CPS
QuoVadis PMA	29 April 2020	1.4	Review and alignment with PKIoverheid CPS
QuoVadis PMA	6 August 2020	1.5	Review and alignment with PKIoverheid CPS
QuoVadis PMA	25 August 2020	1.6	Revisions including addition of PKIo Domain Server 2020 and removal of PKIo EV SSL.
QuoVadis PMA	30 September 2020	1.7	Revisions to Section 1 revocation reporting and Section 4 Relying Party obligations.
QuoVadis PMA	22 March 2021	1.8	Minor editorial updates.

Author	Date	Version	Comment
QuoVadis PMA	28 June 2021	1.9	Alignment with PKIoverheid CPS
QuoVadis PMA	6 December 2021	1.10	Update for ETSI TS 119 461, Remote Identity Verification (RIV), CA/B Forum Ballot SC42.
QuoVadis PMA	20 December 2021	1.11	Clarification of allowed identity verification methods.
QuoVadis PMA	5 July 2022	1.12	Minor editorial corrections including consistent naming and updated revocation contacts.
QuoVadis PMA	23 June 2023	1.13	Consistency updates with CPS, removal of Domain 2020.
DCPA	12 March 2025	2.00	Formatting, organization name change, remove GBA and update URLs.
DCPA	30 May 2025	2.01	Minor editorial changes.
DCPA	17 April 2026	2.02	Removed outdated links, improved readability, and updated contact information.

1. TRUST SERVICE PROVIDER (TSP) CONTACT INFO

Enquiries or other communication about this document should be addressed to the DigiCert Policy Authority (DCPA).

Address:	DigiCert Europe Netherlands B.V. Nevelgaarde 56 Noord 3436 ZZ Nieuwegein, The Netherlands
Telephone:	+31 (0) 30 232-4320
Fax:	+31 30 232 4329
Website:	https://www.digicert.com
Email Contacts:	Support: nl.support@digicert.com Revocation: revoke@digicert.com Complaints: complaints@digicert.com Policy & Compliance: policy@digicert.com

1.1. CERTIFICATE PROBLEM REPORTS AND REVOCATION

Subscribers can revoke their own Certificates 24/7 via the DigiCert Europe Portal https://www.certcentral.digicert.eu/ or the TrustLink Enterprise link https://tl.quovadisglobal.com/. DigiCert Europe provides additional information for entities requiring assistance with revocation or an investigative report also at https://problemreport.digicert.com .

For other types of PKIoverheid problem reports and revocation requests, please email revoke@digicert.com.

During office hours (CET), problem reports and revocation requests can also be made using the DigiCert Europe support line +31 (0) 30 232 4320. Outside of office hours CET the emergency revocation hotline can be used at +1 651 229 3456. For further information, please refer to the practices described in the PKIoverheid CPS in Section 3.4.

Typically, the following information is required:

- Common Name
- Certificate serial number
- E-mail address of the Subject

DigiCert Europe or an RA will authenticate and process problem reports and revocation requests according to Section 4.9 of the PKIoverheid CPS.

2. CERTIFICATE CLASSES FOR PKIOVERHEID

All DigiCert Europe PKIoverheid Certificates have a policy object identifier (OID) which identifies their use. Qualified Certificates meet the requirements outlined in ETSI EN 319 411-2.

PKIo Certificate type	Description Extended Key Usage	Certificate	Policy OID	Requires token?
Organisatie Persoon Authentication	Certificate used for client authentication issued to a natural person linked to an organisation	Client Authentication Document Signing Email protection	2.16.528.1.1003.1.2.5.1	Yes
Organisatie Persoon NonRepudiation	Certificate used for Signing, issued to a natural person linked to an organisation	Document Signing Email protection	2.16.528.1.1003.1.2.5.2	Yes
Organisatie Persoon Encryption	Certificate used for encryption, issued to a natural person linked to an organisation	Encrypting File System Email protection	2.16.528.1.1003.1.2.5.3	Yes
Organisatie Services Authentication	Certificate used for client authentication issued to an organisation	Client Authentication Document Signing Email Protection	2.16.528.1.1003.1.2.5.4	Yes
Organisatie Services Encryption	Certificate used for encryption issued to an organisation	Encrypting File System Email Protection	2.16.528.1.1003.1.2.5.5	Yes
Organisatie Services Seal	Qualified Certificate used for signing issued to an organisation	Document Signing Email Protection	2.16.528.1.1003.1.2.5.7	Yes
Burger Authentication	Certificate used for client authentication issued to a natural person	Client Authentication Document Signing Email Protection	2.16.528.1.1003.1.2.3.1	Yes

PKIo Certificate type	Description Extended Key Usage	Certificate	Policy OID	Requires token?
Burger NonRepudiation	Qualified Certificate used for signing issued to a natural person	Document Signing Email Protection	2.16.528.1.1003.1.2.3.2	Yes
Burger Encryption	Certificate used for encryption issued to a natural person	Encrypting File System Email Protection	2.16.528.1.1003.1.2.3.3	Yes
Private Personen Authentication	Certificate used for client authentication issued to a natural person linked to an organisation from a non-public trusted root	Client Authentication Document Signing Email Protection	2.16.528.1.1003.1.2.8.1	Yes
Private Personen Non-Repudiation	Qualified Certificate used for signing issued to a natural person linked to an organisation from a non-public trusted root	Document Signing Email Protection	2.16.528.1.1003.1.2.8.2	Yes
Private Personen Encryption	Certificate used for encryption issued to an organisation from a non public trusted root	Key Encipherment Data Encipherment	2.16.528.1.1003.1.2.8.3	Yes
Private Services Authentication	Certificate used for client authentication issued to an organisation	Client Authentication Document Signing Email Protection	2.16.528.1.1003.1.2.8.4	Yes
Private Services Encryption	Certificate used for encryption issued to an organisation	Key Encipherment Data Encipherment	2.16.528.1.1003.1.2.8.5	Yes

PKIo Certificate type	Description Extended Key Usage	Certificate	Policy OID	Requires token?
Private Services Server	TLS Certificate from a non-public trusted root	Client Authentication Server Authentication	2.16.528.1.1003.1.2.8.6	No

By requesting a Certificate, an Applicant accepts to undertake one of the following identity proofing methods and the related terms and conditions. DigiCert Europe may provide alternative identity verification methods available to the relevant Certificate Class:

- Physical presence;
- Remote Identity Verification means which provide equivalent assurance in terms of reliability to the physical presence; and/or
- Reliance on a Qualified Electronic Signature

DigiCert Europe only allows use of specific identity proofing means following approval of the method by the relevant Conformity Assessment Body and/or Supervisory Body.

For Remote Identity Verification (RIV) of Applicants for PKIoverheid Certificates, DigiCert Europe uses its RIV4 method which includes Base RIV plus NFC Authentication with manual review in all cases. The RIV4 method has an assurance level of 'High' as set out in Article 8 of Regulation (EU) No 910/2014 (as amended by Regulation (EU) 2024/1183 and Directive (EU) 2022/2555).

Base RIV includes OCR reading of identity documents, video capture, biometric comparison, liveness checks, and other document security checks. NFC options include reading eMRTD data, Passive Authentication, and Active Authentication.

DigiCert Europe checks that a legal organisation is not included in the most recent EU list of banned terrorists and organisations.

2.1. PKIO ADVANCED CERTIFICATES

PKIoverheid Advanced Certificates provide reliable vetting of the holder's identity and may be used for a broad range of applications including digital signatures, encryption, and authentication. Their specific use is determined by the Key Usages and the Subject of the Certificate.

The content of these Certificates meet the relevant requirements from the PKIoverheid Program of Requirements and the relevant ETSI Standards.

Registration Process

Validation procedures for DigiCert Europe Advanced Certificates are based on the Extended Normalised Certificate Policy+ (NCP+) described in ETSI EN 319 411-1.

If the Subject is a natural person evidence of the Subject's identity shall be checked either directly by physical presence of the person, or shall have been checked indirectly using means which

provides equivalent assurance to physical presence.

If the Subject is a natural person evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a nationally recognised identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

If the Subscriber is a natural person who is identified in association with a legal person (organisational entity), additional evidence shall be provided of:

- Full name and legal status of the associated legal person;
- Any relevant existing registration information (e.g. company registration) of the associated legal person; and
- Evidence that the Subscriber is affiliated with the legal person.

If the Subscriber is a legal person (organisational entity), evidence shall be provided of:

- Full name of the legal person; and
- Reference to a nationally recognised registration or other attributes which may be used to, as far as possible, distinguish the legal person from others with the same name.

If the Subscriber is a device or system operated by or on behalf of a legal person, evidence shall be provided of:

- Identifier of the device by which it may be referenced (e.g. Internet domain name);
- Full name of the organisational entity; and
- A nationally recognised identity number, or other attributes which may be used to, as far as possible, distinguish the organisational entity from others with the same name.

2.2. PKIO QUALIFIED

2.2.1. PKIo Qualified Certificate issued to a natural person on a QSCD

The purpose of PKIoverheid Qualified Certificates is to identify the Subscriber with a High level of assurance, for the purpose of creating Qualified Electronic Signatures meeting the qualification requirements defined by the eIDAS Regulation.

This type of Certificate uses a Qualified Signature Creation Device (QSCD) meeting the requirements of Annex II of the eIDAS Regulation for the protection of the Private Key . In some cases, DigiCert Europe generates and manages Private Keys on behalf of the Subscriber and operates the QSCD in accordance with eIDAS. This will be signified by the presence of the 0.4.0.19431.1.1.3 OID in Certificate Policies. This OID is the EUSCP: EU SSASC Policy ‘eu-remote-qscd’ OID defined in ETSI TS 119 431-1.

Registration Process

DigiCert Europe recommends that QCP-n-qscd Certificates are used only for Electronic Signatures.

The identity of the natural person and, if applicable, any specific attributes of the person, shall be verified:

- By the physical presence of the natural person; or
- Using methods which provide equivalent assurance in terms of reliability to the physical presence and for which DigiCert Europe can prove the equivalence according to the eIDAS Regulation. This includes use of the DigiCert Europe RIV4 method for Remote Identity Verification.

Evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a nationally recognised identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

If the Subscriber is a physical person who is identified in association with an organisational entity, additional evidence shall be provided of:

- Full name and legal status of the associated organisational entity;
- Relevant existing registration information of the organisational entity; and
- Evidence that the Subscriber is associated with the organisational entity.

2.2.2. PKIo Qualified Certificate issued to a legal person on a QSCD

The purpose of these EU Qualified Certificates are to identify the Subscriber with a High level of assurance, for the purpose of creating Qualified Electronic Seals meeting the requirements defined by the eIDAS Regulation.

These Certificates use a Qualified Signature Creation Device (QSCD) meeting the requirements of Annex II of the eIDAS Regulation for the protection of the Private Key. In some cases, DigiCert Europe generates and manages Private Keys on behalf of the Subscriber and operates the QSCD in accordance with eIDAS. This will be signified by the presence of the 0.4.0.19431.1.1.3 OID in Certificate Policies. This OID is the EUSCP: EU SSASC Policy ‘eu-remote-qscd’ OID defined in ETSI TS 119 431-1.

Registration Process

Identity validation procedures for these Certificates meet the requirements of ETSI EN 319 411-2 for “Policy for EU Qualified Certificate issued to a legal person where the Private Key and the related Certificate reside on a QSCD” (QCP-l-qscd).

The identity of the legal person and, if applicable, any specific attributes of the person, shall be verified:

- By the physical presence of an authorised representative of the legal person; or
- Using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorised representative of the legal person and for which DigiCert Europe can prove the equivalence according to the eIDAS Regulation. This includes use of the DigiCert Europe RIV4 method for Remote Identity Verification.

Evidence shall be provided of:

- Full name of the organisational entity consistent with the national or other applicable identification practices); and
- When applicable, the association between the legal person and the other organisational entity identified in association with this legal person that would appear in the organisation attribute of the Certificate, consistent with the national or other applicable identification practices.

For the authorised representative of the legal person, evidence shall be provided of:

- Full name (including surname and given names consistent with applicable law and national identification practices); and
- Date and place of birth, reference to a nationally recognised identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.

3. RELIANCE LIMITS

Certificates issued may only be used for the purposes for which they were issued, as explained in the DigiCert Europe PKIoverheid CPS, Master Services Agreement, Subscriber Agreement, and Terms of Use as well as identified in the Key Usage field of the Certificate itself. Certificates are prohibited from being used for any other purpose than described, and all Certificate usage must be within the limits of applicable laws.

4. OBLIGATIONS OF SUBSCRIBERS

Subscribers are required to act in accordance with the CPS, Master Services Agreement, Subscriber Agreement, and Terms of Use. Subscriber obligations include:

1. The obligation to provide DigiCert Europe with accurate and complete information in accordance with the requirements of the CPS, particularly with regard to registration;
2. The obligation for the Key Pair to be only used in accordance with any limitations notified to the Subscriber and the Subject if the Subject is a natural or legal person;
3. The prohibition of unauthorized use of the Subject's Private Key;
4. If the Subscriber has generated their own keys, then;
    - The obligation to generate the Subject keys using an algorithm as specified in ETSI TS 119 312 for the uses of the certified key as identified in the Certificate Policy of the PKIo PA;
    - The obligation to use the key length and algorithm as specified in ETSI TS 119 312 for the uses of the certified key as identified in the Certificate Policy of the PKIo PA during the certificate validity period;
5. If the Subscriber or Subject generates the Subject's keys and certificate Key Usage is for Non-repudiation (signing), Digital Signatures or Key Encipherment, then;
    - The obligation for the Subject's Private Key to be maintained under the Subject's sole control;
    - The obligation to only use the Subject's Private Keys for cryptographic functions within the secure cryptographic device;
6. The obligation to notify DigiCert Europe, without delay, if any of the following occur up to the end of the Certificate validity period;
    - If the Subject's Private Key has been lost, stolen, potentially compromised;
    - Where control over the Subject's Private Key has been lost due to compromise of activation data (e.g., PIN code) or other reasons;
    - Where there are inaccuracies or changes to the Certificate content, as notified to the Subscriber or Subject;
7. The obligation, following compromise of the Subject's Private Key, to immediately and permanently discontinue use of this key, except for Key Decipherment; and
8. The obligation, in case of being informed that the Subject's Certificate has been revoked, or that the issuing CA has been compromised, to ensure that the Private Key is no longer used by the Subject.

For remote identity verification, the Subscriber is obliged to use the identity proofing software distributed by DigiCert Europe and to agree with the processing of biometric data for identity verification purposes during Remote Identity Verification.

See DigiCert Europe PKIoverheid CPS Section 9.6.3.

5. CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES

1. Prior to relying on the Certificate or other authentication product or service, Relying Parties are obliged to check all status information provided by DigiCert Europe related to the Certificate or other authentication product or service to confirm that the information was still valid and that the product or service had not expired or been revoked. For Certificates, this includes checking to ensure that each Certificate in the Certificate Chain is valid, unexpired, and non-revoked (by using any CRL or OCSP information available).
    - To be relied upon as an EU Qualified Certificate, the CA/trust anchor for the validation of the Certificate shall be as identified in a service digital identifier of an EU Trusted List entry with service type identifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC for a Qualified Trust Service Provider. ETSI TS 119 615 provides guidance on how to validate a Certificate against the EU Trusted Lists. ETSI TS 119 172-4 describes how to validate a digital signature to determine whether it can be considered as an EU Qualified electronic signature or seal.
2. Prior to relying on an authentication product or service, Relying Parties must gather sufficient information to make an informed decision about the proper use of the authentication product or service and whether intended reliance on the authentication product or service was reasonable in light of the circumstances. This includes evaluating the risks associated with their intended use and the limitations associated with the authentication product or service provided by DigiCert Europe.
3. Relying Parties' reliance on the authentication product or service is reasonable based on the circumstances. Relying Parties reliance will be deemed reasonable if:
    - The attributes of the Certificate relied upon and the level of assurance in the Identification and Authentication provided by the Certificate are appropriate in all respects to the level of risk and the reliance placed upon that Certificate by the Relying Party;
    - The Relying Party has, at the time of that reliance, used the Certificate for purposes appropriate and permitted by the CP/CPS and under the laws and regulations of the jurisdiction in which the Relying Party is located;
    - The Relying Party has, at the time of that reliance, acted in good faith and in a manner appropriate to all the circumstances known, or circumstances that ought reasonably to have been known, to the Relying Party;
    - The Relying Party has, at the time of that reliance, verified the Digital Signature, if any;
    - The Relying Party has, at the time of that reliance, verified that the Digital Signature, if any, was created during the Operational Term of the Certificate being relied upon;
    - The Relying Party ensures that the data signed has not been altered following signature by utilising trusted application software, the signature is trusted and the results of the signature are displayed correctly by utilising trusted application software;
    - The identity of the Subscriber is displayed correctly by utilising trusted application software; and
    - Any alterations arising from security changes are identified by utilising trusted application software.

Note: If the circumstances indicate a need for additional assurances, it is the Relying Parties' responsibility to obtain such assurances.

See the Digicert Europe PKIoverheid CPS Section 9.6.4.

6. LIMITATIONS OF LIABILITY

DigiCert Europe shall not be liable for any special, indirect, incidental, consequential, or punitive damages (including any damages arising from loss of use, loss of data, lost profits, business interruption or costs of procuring substitute software or services) arising out of or relating to this CPS and related services. See PKIoverheid CPS Section 9.8 for more information and liability limits. DigiCert Europe reserves the right, without liability, to reject any application for a Certificate.

7. APPLICABLE AGREEMENTS, CPS

The DigiCert Europe PKIoverheid CPS and Terms and Conditions (including the Master Services Agreement, Certificate Terms of Use, Privacy Policy and relevant DigiCert Europe CP/CPS) are available at https://www.digicert.com/legal-repository/europe

8. PRIVACY POLICY

The DigiCert Europe Privacy Notice is available at https://privacy.digicert.com/policies/en/ which also includes privacy information for Remote Identity Verification. See PKIoverheid CPS Section 9.4.

9. REFUND POLICY

Details of the refund policy may be contained in relevant contractual agreements. See DigiCert Europe PKIoverheid CPS Section 9.1.5.

10. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

10.1. CUSTOMER COMPLAINTS

DigiCert Europe is committed to ensuring that we provide the best services and products possible to our customers. However, we do realise sometimes customers may want to pass on their concerns. In the event you have feedback, please contact us at complaints@digicert.com. We will acknowledge the receipt of your feedback within 24 hours and will provide a more specific response from the relevant department within 5 working days. In the majority of cases, the relevant team leader will be able to respond to your feedback and resolve any outstanding issues without the need for escalation. In some cases, it may be necessary to involve other departments and team members to ensure the correct response is provided to you. This is at the discretion of the team leader or manager handling the process. You will be informed if this is necessary.

10.2. GOVERNING LAW

All agreements entered into by DigiCert Europe under the DigiCert Europe PKIoverheid CPS are governed by Dutch law, unless otherwise specified. See DigiCert Europe PKIoverheid CPS Section 9.14.

This PDS is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptography products. See DigiCert Europe PKIoverheid CPS Section 9.15.

10.3. DISPUTE RESOLUTION

To the extent permitted by law, before a Participant files suit or initiates an arbitration claim with respect to a dispute involving any aspect of this Agreement, Participant shall notify DigiCert Europe, and any other party to the dispute for the purpose of seeking business resolution. Both Participant and DigiCert Europe shall make good faith efforts to resolve such dispute via business discussions. If the dispute is not resolved within sixty (60) days after the initial notice, then a party may proceed as permitted under applicable law and as specified in the DigiCert Europe PKIoverheid CPS and other relevant agreements. See DigiCert Europe PKIoverheid CPS Section 9.13.

11. TSP AND REPOSITORY LICENCES, TRUST MARKS AND AUDIT

See https://www.digicert.com/webtrust-audits for a list of DigiCert Europe audits and accreditations.