Relying Party Agreement - version 1.3.2

The Relying Party Agreement (RPA) below applies to certificates issued by KPN. However, the certificate that referred you to this page may have been issued by an organization with a specific RPA. If a specific RPA applies, the standard KPN RPA is not applicable. The applicable terms and conditions that apply to your reliance on the certificate can be found at the location stated in the Policy Qualifier field of the end-user certificate. In applications such as your browser or your email application, you can review these terms and conditions by opening the certificate and clicking the "Issuer Statement" button. Please note that by relying on the certificate, you agree to the terms and conditions referred to in the Policy Qualifier field of the certificate.

You must read this Relying Party Agreement ("Agreement") before validating a Symantec Trust Network ("STN") digital certificate ("Certificate"), using KPN's Online Certificate Status Protocol ("OCSP") services, or otherwise accessing or using KPN's database of Certificate revocations and other information ("Repository") or any Certificate Revocation List issued by KPN ("KPN CRL"). If you do not agree to the terms of this Agreement, do not submit a query and do not download, access, or use any KPN CRL because you are not authorized to use KPN's Repository or any KPN CRL.

1. Background. This Agreement becomes effective when you submit a query to search for a Certificate, or to verify a digital signature created with a private key corresponding to a public key contained in a Certificate, by downloading a KPN CRL, or when you otherwise use or rely upon any information or services provided by KPN's Repository, KPN's website, or any KPN CRL, or when you use KPN's OCSP services. Relying Party Agreements in force within KPN's Subdomain of the STN appear at: https://certificaat.kpn.com/RPA

2. Definitions. The capitalized terms used in this Agreement shall have the following meanings unless otherwise specified:

"Certificate" shall mean a digitally signed message that contains a Subscriber's public key and associates it with information authenticated by KPN or a KPN-authorized entity.

"Certificate Chain" shall mean an ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.

"Certification Authority" or "CA" shall mean an entity authorized to issue, manage, revoke, and renew Certificates in the STN.

"Registration Authority" or "RA" shall mean an entity approved by a CA to assist an individual or organization in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.

"Relying Party" shall mean an individual or organization that acts in reliance on a Certificate or a digital signature.

"Repository" shall mean a portion of the KPN website where Relying Parties, Subscribers, and the general public can obtain copies of KPN literature, including but not limited to, the KPN CPS, agreements, whitepapers, and CRLs.

"Subscriber" shall mean a person who is the subject of and has been issued a Certificate.

"Subscriber Agreement" shall mean an agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.

"KPN CPS" shall mean the KPN Certification Practice Statement, as amended from time to time, which may be accessed from https://certificaat.kpn.com/CPS

The KPN CPS states the practices that KPN Certification Authorities ("KPN CAs") employ in providing Certification services that include, but are not limited to, issuing, managing, revoking, and renewing Certificates.

3. Sufficient Information. You acknowledge and agree that you have access to sufficient information to ensure that you can make an informed decision as to the extent to which you will choose to rely on the information in a Certificate. You acknowledge and agree that your use of the Repository, your use of any KPN CRL, and your use of KPN's OCSP services are governed by this Agreement and the KPN CPS. For more educational material, see the tutorial at https://certificaat.kpn.com/repository. You are solely responsible for deciding whether or not to rely on the information in a Certificate. You also acknowledge and agree that you shall bear the legal consequences of your failure to comply with the Relying Party obligations set forth in this Agreement.

4. STN Certificates. The Certificates relied upon in accordance with this Agreement are issued within the STN. The STN is a global public key infrastructure that provides Certificates for both wired and wireless applications. KPN is one of the service providers within the STN, together with Symantec, Inc. and its affiliates and partners throughout the world.

The STN includes three different classes of Certificates, Class 1, 2 and 3 and two different types of Qualified Certificates, one with and one without a Secure Signature Creation Device (SSCD). Each level, type, or class, of Certificate provides specific functionality and security features and corresponds to a specific level of trust. KPN currently only offers Classes 2 and 3 Certificates and Qualified Certificates within its Subdomain of the STN.

Class 2 Certificates offer a medium level of assurances, and are individual Certificates. Class 2 validation procedures are based on a comparison of information submitted by the Certificate applicant against information in business records or databases or the database of a KPN-approved identity proofing service. These validation procedures add on assurances that the Subscriber's distinguished name is unique and unambiguous within the CA's Subdomain and that a certain e-mail address is associated with a public key. They can be used for digital signatures, encryption, and access control, including as proof of identity in medium-value transactions.

Class 3 Certificates provide a high level of assurances within KPN's Subdomain. Class 3 Certificates are issued to individuals, organizations, and Administrators for CAs and RAs. Class 3 individual Certificates may be used for digital signatures, encryption, and access control, including as proof of identity, in high-value transactions. Class 3 individual Certificates provide assurances of the identity of the Subscriber based on the personal (physical) presence of the Subscriber before a person that confirms the identity of the Subscriber using, at a minimum, a well-recognized form of government-issued identification and one other identification credential. Other Class 3 organizational Certificates are issued to devices to provide authentication; message, software, and content integrity; and confidentiality encryption. Class 3 organizational Certificates provide assurances of the identity of the Subscriber based on a confirmation that the Subscriber organization does in fact exist, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Subscriber was authorized to do so. Class 3 organizational Certificates for servers (Secure Server IDs and Global Server IDs) also provide assurances that the Subscriber is entitled to use the domain name listed in the Certificate Application.

Qualified Certificates are specific Certificate types. Qualified Certificates are issued in accordance with the requirements set forth under the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures ("EU Directive"). Qualified Certificates are issued only to individuals and shall only be used for advanced electronic signatures (digital signatures). Qualified Certificates both provide assurances of the identity of the Subscriber based on the direct or indirect personal (physical) presence of the Subscriber before a RA that check's the Subscriber's identity documentation against a well-recognized form of government-issued identification, such as a passport, or national identity card, and one other identification credential.

Qualified Certificates are appropriate for digital signatures for applications in which the level of validity provided by Article 5(1) of the EU Directive is necessary or desired. Qualified Certificates support the use of digital signatures that are equivalent in legal effectiveness to handwritten signatures.

5. Your Obligations. As a Relying Party, you are obligated to:

(i) independently assess the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose;

(ii) utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations you wish to perform, as a condition of relying on a Certificate in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain. You agree that you will not rely on a Certificate unless these verification procedures are successful;

(iii) check the status of a Certificate on which you wish to rely, as well as all the Certificates in its Certificate Chain. If any of the Certificates in the Certificate Chain have been revoked, you agree that that you will not rely on the end-user Subscriber Certificate or other revoked Certificate in the Certificate Chain;

(iv) rely on the Certificate, if all of the checks described in the previous paragraphs are successful, provided that reliance upon the Certificate is reasonable under the circumstances and in light of Section 3 of this Agreement. If the circumstances indicate a need for additional assurances, it is your responsibility to obtain such assurances for such reliance to be deemed reasonable; and

(v) if you are also a Subscriber, you agree to be bound by the relevant Subscriber Agreement.

6. Limitations on Use. Certificates issued under the STN are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. KPN, and its CAs and RAs are not responsible for assessing the appropriateness of the use of a Certificate. You agree as a Relying Party that Certificates will not be used or relied upon by you beyond the limitations set forth in this Agreement.

7. Compromise of STN Security. You agree that you shall not monitor, interfere with, or reverse engineer the technical implementation of the STN, except upon prior written approval from KPN, and shall not otherwise intentionally compromise the security of the STN.

8. Effect of a Certificate. You acknowledge and agree, to the extent permitted by applicable law, that where a transaction is required to be in writing, a message or other record bearing a digital signature verifiable with reference to a Certificate is valid, effective, and enforceable to an extent no less than had the same message or record been written and signed on paper. Subject to applicable law, a digital signature or transaction entered into with reference to a Certificate shall be effective regardless of the geographic location where the Certificate is issued or the digital signature created or used, and regardless of the geographic location of the place of business of the CA or Subscriber.

9. KPN Warranties. KPN warrants to Relying Parties who reasonably rely on a Certificate (i) that all information in or incorporated by reference in the Certificate, is accurate; (ii) that Certificates appearing in the Repository have been issued to the individual or organization named in the Certificate as the Subscriber, and the Subscriber has accepted the Certificate by downloading it from a website or via an email message sent to the Subscriber containing the Certificate; and (iii) the entities that approved the Certificate Application and issued the Certificate have substantially complied with the KPN CPS when issuing the Certificate.

KPN additionally warrants to Relying Parties who reasonably rely on a Qualified Certificate: (i) The Qualified Certificate contains all the details prescribed for a Qualified Certificate under the Directive; and (ii) The Subscriber of such Qualified Certificate held the private key correspond

ing to the public key within such Qualified Certificate at the time the Qualified Certificate was issued; and (iii) The CA and/or RA exercises reasonable care to provide notice of the revocation of Qualified Certificates.

Records associated with a Certificate are retained for at least the time periods set forth below following the date the Certificate expires or is revoked:

- Ten (10) years and six (6) months for Class 2 and Class 3 Certificates
- Seven (7) years after the expiry date or date of revocation for Qualified Certificates

If necessary, KPN may implement longer retention periods in order to comply with applicable laws.

10. Additional Obligation for Qualified Certificates. If the Certificate corresponding to the digital signature you are relying on is a Qualified Certificate, then one of the following object identifiers ("OID") is present in the Certificate. The following table indicates the relation between the OID and the type of Qualified Certificate.

OID	*EU Directive Article*	*ETSI Policy terminology*	*EDSP terminology*
id-edsp-dl2 (2.16.840.1.113733.1.7.44.2)	Article 5.1	**QCP public + SSCD**	DL2

The following terms shall also apply to you if the Certificate you are relying on is a Qualified Certificate: (i) You shall verify the validity, suspension or revocation of the Certificate using current revocation status information prior to relying on a digital signature created with a private key corresponding to a public key contained in a Certificate; (ii) You shall take into account the limitations on the usage of the Certificate placed on the Relying Party in this Agreement; and (ii) You shall take any other precautions prescribed in this Agreement.

11. Disclaimers. You agree that your use of KPN's service(s) is solely at your own risk. You agree that all such services are provided on an "as is" and as available basis, except as otherwise noted in this agreement. KPN expressly disclaims all warranties of any kind, whether express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose and non-infringement. Other than the warranties as set forth in section 9, KPN does not make any warranty that the service will meet your requirements, or that the service will be uninterrupted, timely, secure or error free; nor does KPN make any warranty as to the results that may be obtained from the use of the service or to the accuracy or reliability of any information obtained through the service. You understand and agree that any material and/or data downloaded or otherwise obtained through the use of KPN's services is done at your own discretion and risk. No advice or information, whether oral or written, obtained by you from KPN or through KPN's services shall create any warranty not expressly made herein. To the extent jurisdictions do not allow the exclusion of certain warranties, some of the above exclusions may not apply to you. KPN is not responsible for and shall have no liability with respect to any products and/or services purchased by you from a third party.

12. Indemnification. You agree to release, indemnify, defend and hold harmless KPN and any non-KPN CAs or RAs, and any of their respective contractors, agents, employees, officers, directors, shareholders, affiliates and assigns from all liabilities, claims, damages, costs and expenses, including reasonable attorney's fees and expenses, of third parties relating to or arising out of (i) your failure to perform the obligations of a Relying Party, (ii) your reliance on a Certificate that is not reasonable under the circumstances, or (iii) your failure to check the status of a Certificate to determine if the Certificate is expired or revoked. When KPN is threatened with suit or sued by a third party, KPN may seek written assurances from you concerning your promise to indemnify KPN, your failure to provide those assurances may be considered by KPN to be a material breach of this Agreement. KPN shall have the right to participate in any defense by you of a third-party claim related to your use of any KPN services, with counsel of our choice at your own expense. You shall have sole responsibility to defend KPN against any claim, but you must receive KPN's prior written consent regarding any related settlement. The terms of this Section 12 will survive any termination or cancellation of this Agreement.

13. Limitations of Liability. This section 13 applies to liability under contract (including breach of warranty), tort (including negligence and/or strict liability), and any other legal or equitable form of claim. If you initiate any claim, action, suit, arbitration, or other proceeding relating to services provided under this section 13, and to the extent permitted by applicable law, KPN's total liability for damages sustained by you and any third party for any use or reliance on a specific Certificate shall be limited, in the aggregate, to the amounts set forth below.

or Type	*Liability Caps*
Class 2	Five Thousand Euro (€ 5.000)

or Type	*Liability Caps*
Qualified Certificate	One Hundred Thousand Euro (€ 100.000)
Class 3	One Hundred Thousand Euro (€ 100.000)

The liability limitations provided in this Section 13 shall be the same regardless of the number of digital signatures, transactions, or claims related to such Certificate. KPN SHALL NOT be obligated to pay more than the total liability limitation for each Certificate that is relied upon.

14. Protection of Private Key. You are hereby notified of the possibility of theft or other form of compromise of a private key corresponding to a public key contained in a Certificate, which may or may not be detected, and of the possibility of use of a stolen or compromised key to forge a digital signature to a document. For more educational material on private key protection, see the tutorial at https://certificaat.kpn.com/repository

15. Governing Law. The parties agree that any disputes related to the services provided under this Agreement shall be governed in all respects by and construed in accordance with the laws of The Netherlands, excluding its conflict of laws rules. The parties agree that the United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement.

16. Dispute Resolution. In case of a dispute that arises from or is connected with this Agreement, parties shall first try to seek dispute resolution amongst themselves. All disputes that cannot be resolved amongst parties shall be exclusively referred to the competent court in Amsterdam, The Netherlands.

17. Severability. If any provision of this Agreement, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this Agreement (and the application of the invalid or unenforceable provision to other persons or circumstances) shall not be affected by such finding of invalidity or unenforceability, and shall be interpreted in a manner that shall reasonably carry out the intent of the parties.

18. Force Majeure. Except for payment and indemnity obligations hereunder, neither party shall be deemed in default hereunder, nor shall it hold the other party responsible for, any cessation, interruption or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, act of God, war, armed conflict, terrorist action, labor strike, lockout, boycott, provided that the party relying upon this Section 18 shall (i) have given the other party written notice thereof promptly and, in any event, within five (5) days of discovery thereof and (ii) shall take all reasonable steps reasonably necessary under the circumstances to mitigate the effects of the force majeure event upon which such notice is based; provided further, that in the event a force majeure event described in this Section 18 extends for a period in excess of thirty (30) days in aggregate, the other party may immediately terminate this Agreement.

19. Survival. This Agreement shall be applicable for as long as you rely on a Certificate, use the OCSP service, access or use the KPN database of CRL information and in any matter of respect concerning the subject matter of this Agreement.

20. Non-Assignment. Except as otherwise set forth herein, your rights under this Agreement are not assignable or transferable. Any attempt by your creditors to obtain an interest in your rights under this Agreement, whether by attachment, levy, garnishment or otherwise, renders this Agreement voidable at KPN's option.

21. Independent Contractors. The parties to this Agreement are independent contractors. Neither party is an agent, representative, or partner of the other party. Neither party shall have any right, power or authority to enter into any agreement for or on behalf of, or incur any obligation or liability of, or to otherwise bind, the other party. This Agreement shall not be interpreted or construed to create an association, joint venture or partnership between the parties or to impose any partnership obligation or liability upon either party. Each party shall bear its own costs and expenses in performing

this Agreement.

22. Notices. You will make all notices, demands or requests to KPN with respect to this Agreement in writing to

KPN bv
Attn: PMA
Fauststraat 1
P.O. Box 9105
7300 HN Apeldoorn
The Netherlands

23. Entire Agreement. This Agreement constitutes the entire understanding and agreement between KPN and you with respect to the transactions contemplated, and supersedes any and all prior or contemporaneous oral or written representation, understanding, agreement or communication between KPN and you concerning the subject matter hereof. Neither party is relying upon any warranties, representations, assurances or inducements not expressly set forth herein. Section headings are inserted for convenience of reference only and are not intended to be part of or to affect the meaning this Agreement. Terms and conditions in any purchase orders that are not included in this Agreement or that conflict with this Agreement are null and void.