Raytonne Trust Services

Certificate Policy

Document Issue: 1.0

Date of Issue: February 22, 2022

Copyright Notice

Contents

1. INTRODUCTION

Raytonne Trust Services Certificate Policy describes general rules and regulations applied by Raytonne for public key certification process, Time-Stamping Authority (TSA) and remaining non-repudiation services. Document defines parties of this process, their responsibilities and obligations, types of certificates and applicability range. Detailed description of the above rules and the subscriber identity verification procedures is disclosed in *Raytonne Trust Services Certification Practice Statement*. The knowledge of the nature, goal and role of the Certificate Policy, as well as Certification Practice Statement is particularly important from the point of view of the subscriber and relying party.

2. CERTIFICATES

Certificate is a string of data (a message), containing at least a name and an identifier of the authority issuing the certificate, subscriber's identifier, his/her/its public key, validity period and the serial number and is signed by the intermediate certification authority subordinated to one of the root certification authorities.

Raytonne Trust Services' root certificates upon indirectly issuing a certificate to the subscriber confirm his/her/its identity or the credibility of other data, such as email address. Authorities also confirm the public key possessed by such subscriber, is the property of this very subscriber. Due to above a relying party upon reception of signed message is able to verify the owner of the certificate, which signed the message and, optionally, account him/her of the actions he/she performed or obligations he/she made.

Raytonne Trust Services provides services in accordance with the WebTrust requirements for the certification authorities. Certification authority keys are protected with the hardware security module. The authority implemented physical and procedural controls of the system. Raytonne Trust Services issues certificates in a various level of credibility. Credibility of the certificate depends of enforced subscriber's identity verification procedure and the effort used by Raytonne to verify the data submitted by the requester in his/her/its registration application. The more information should be verified, and so the procedure is more complex, the more reliable the certificate.

The subscriber has to state by himself/herself/itself the credibility level of the certificate most appropriate for his/her/its needs. Types of the certificates and their credibility level are described in detail in the Certification Practice Statement. The document is available at https://www.raytonne.com/PKI/.

2.1. DV Certificates (Domain Validation)

DV certificates are issued for two separate groups. As a free test certificates for shorter period of validity and the standard certificates with a full usage. Test certificates are intended mainly for the application or device test performance prior to purchasing final certificate. DV certificates are issued by 卧龙 ClientServer 2025.

DV certificates are issued for the protecting data transmission based on SSL/TSL protocols. Raytonne Trust Services verifies all data provided by subscriber in the certification process. Detailed information on verification requirements are described in Certification Practice Statement.

It is not recommended to unambiguously verify the identity of the subject of the certificate on the basis of DV certificates.

End users DV certificates contain following policy identifiers:

Authority Name	Policy Identifier
卧龙 ClientServer 2025	1.3.6.1.4.1.54983.1.1.1

Raytonne Trust Services does not bear any financial liability and no warranties apply to the test certificates (and their content) issued within above policies. However, standard certificates have limited guarantees and liabilities.

2.2. OV Certificates (Organization Validation)

OV certificates are issued by 卧龙 ClientServer 2025.

OV certificates are issued for securing electronic correspondence and protecting data transmission based on SSL/TSL protocols. These certificates are intended also for the certification authorities, non-repudiation authorities and global network-based electronic transaction systems. Raytonne Trust Services operates a procedure for verifying the identity of the subscriber that meets the *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates*. Raytonne Trust Services verifies all data provided by the requesters during the certification process. Detailed information on verification requirements are described in Certification Practice Statement.

It is possible to unambiguously verify the identity of subject, the authenticity of organization or the credibility of external certification authority on the basis of OV certificates.

End users OV certificates contain following policy identifiers:

Authority Name	Policy Identifier
卧龙 ClientServer 2025	1.3.6.1.4.1.54983.1.1.2

Financial responsibility of Raytonne Trust Services for the data in the certificates issued within above policies is presented in Certification Practice Statement. Certificates issued within these policies have full guarantees and liabilities.

2.3. EV Certificates (Extended Validation)

Certificates issued by 卧龙 ClientServer 2025 and 卧龙 CodeSigning 2025 provide a highest level of confidence the identity of the subscriber. The validation process requires to follow by the current version of the *Guidelines for the issuance and Management of Extended Validation Certificates* and the *Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates*.

EV SSL certificates are issued only to legal entities and intended for protecting data transmission based on SSL/TSL protocols.

EV Code Signing certificates are issued only to legal entities and intended for protecting an application or software code. Additionally, subscribers' private keys must be generated and protected on external devices.

Raytonne Trust Services verifies all data provided by the requesters during the certification process. Detailed information on identity verification requirements are described in Certification Practice Statement.

It is possible to unambiguously verify the identity of subject and the authenticity of organization on the basis of EV certificates.

End users EV certificates contain following policy identifiers:

Authority Name	Policy Identifier
卧龙 ClientServer 2025	1.3.6.1.4.1.54983.1.1.4
卧龙 CodeSigning 2025	1.3.6.1.4.1.54983.1.2.2

Financial responsibility of Raytonne Trust Services for the data in the certificates issued within above policies is presented in Certification Practice Statement. Certificates issued within these policies have full guarantees and liabilities.

2.4. Code Signing Certificates

Code Signing Certificates are issued by 卧龙 CodeSigning 2025.

The usage of the code signing certificates is limited to code signing only. Additionally, subscribers' private keys must be generated and protected on external devices.

Raytonne Trust Services operates a procedure for verifying the identity of the subscriber that meets the *Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates*. Raytonne Trust Services verifies all data provided by the requesters during the certification process. Detailed information on identity verification requirements are described in Certification Practice Statement.

It is possible to unambiguously verify the identity of subject, the authenticity of organization or the credibility of external certification authority on the basis of Code Signing certificates:

End users Code Signing certificates contain following policy identifiers:

Authority Name	Policy Identifier
卧龙 CodeSigning 2025	1.3.6.1.4.1.54983.1.2.1

Financial responsibility of Raytonne Trust Services for the data in the certificates issued within above policies is presented in Certification Practice Statement. Certificates issued within these policies have full guarantees and liabilities.

2.5. S/MIME Certificates

S/MIME certificates are issued by certificates are issued for two separate groups. As a free test certificates for shorter period of validity and the standard certificates with a full usage. S/MIME certificates are issued by 卧龙 ClientAuth 2025.

S/MIME certificates are issued to securing electronic correspondence. Raytonne Trust Services verifies all data provided by the requesters during the certification process. Detailed information on identity verification requirements are described in Certification Practice Statement.

End users S/MIME certificates contain following policy identifiers:

Authority Name	Policy Identifier
卧龙 ClientAuth 2025	1.3.6.1.4.1.54983.1.3.1 1.3.6.1.4.1.54983.1.3.2

Raytonne Trust Services does not bear any financial liability and no warranties apply to the test certificates (and their content) issued within above policies. However, standard certificates have limited guarantees and liabilities.

2.6. External Authorities Certificates

Certificates for external CAs are issued by both root certification authorities and intermediate certification authorities. Entities, whom such certificates are issued to, are subjected to thorough verification. Certificates issued by Raytonne Trust Services are valid for 10 years and require hardware protection of private keys.

Policy identifier and financial responsibility of Raytonne Trust Services is specified in dedicated agreements.

3. NON-REPUDIATION SERVICES

Non-repudiation token is a string of data (message) provided by the client to one of the non-repudiation authority, containing at least the following information: cryptographic hash, serial number of certificate, number of request, etc. and is signed electronically by that authority. Non-repudiation authorities, providing services for their clients are affiliated by the Raytonne Trust Services root certification authorities.

Non-repudiation authority, upon token issuance, confirms the occurrence of an event in the past or in that very moment. It might be submission of the electronic document, participation in data exchange, date of signature creation, etc. On the basis of received data relying party accepts the certificate and verifies the correctness of the signature relying on the credibility of Raytonne Trust Services root certification authorities.

3.1. Time-Stamps

Timestamps are issued by the intermediate authority 卧龙 TSA 2025. Timestamps, as the confirmation of non-repudiation, are issued to private and commercial customers. Timestamps may be incorporated in the process of electronic signature creation, acceptance of electronic transactions, archive of the data, notary of electronic documents, etc.

Timestamp token contain identifier of the policy governing the issuance of the token. This identifier has the following form:

Authority Name	Policy Identifier
卧龙 TSA 2025	1.3.6.1.4.1.54983.1.0.2

卧龙 TSA 2025 gives full guarantees for issued timestamps.

3.2. OCSP Confirmation Response

OCSP (Online Certificate Status Protocol) tokens are issued by intermediate authority OCSP validation service. Each Raytonne Trust Services intermediate certification authority has its own dedicated certificate status validation authority. Tokens, as confirmations of certificate status, are issued to private and commercial customers. OCSP may be incorporated mainly in the process of verification of certificate status. These services are available to public and are the alternative for the Certificate Revocation List (CRL). Information on OCSP authority operation and additional information concerning provided services are presented in Certification Practice Statement.

Raytonne Trust Services OCSP validation service has the following policy identifier:

Authority Name	Policy Identifier
OCSP	1.3.6.1.4.1.54983.1.0.1

4. RAYTONNE TRUST SERVICES GUARANTEES

Depending on type of issued certificate, Raytonne Trust Services guarantees, that it uses reasonable efforts to verify information included in the certificates. This verification is particularly important from the point of view of the relying party, who is the addressee of subscriber's messages, confirmed with the certificates issued by Raytonne Trust Services. Due to above, Raytonne Trust Services is financially responsible for every damage resulting from Raytonne Trust Services fault or negligence. Range of the liability and liability cap depends of the level of subscriber's certificate and might include not only the subscriber but the relying party as well.

Raytonne Trust Services guarantees might be limited with many restrictions. Knowledge of this limitations is confirmed by the subscriber in appropriate statement. Raytonne Trust Services guarantees uniqueness of electronic signatures of its subscriber's.

5. CERTIFICATE ACCEPTANCE

Raytonne Trust Services liabilities and guarantees are applicable since the moment of acceptance of the issued certificate by the subscriber. General provision and method of certificate acceptance are described in Certification Practice Statement.

6. CERTIFICATION SERVICES

Raytonne Trust Services, within its infrastructure, provides four basic certification services:

- registration and issuance of a certificate,
- renewal of the certificate,
- revocation of the certificate and,
- verification of certificate status.

Remaining non-repudiation services may be provided irrespectively of Raytonne Trust Services:

- Time-Stamping Authority (TSA),
- Online Certificate Status Protocol (OCSP).

Registration is intended for confirming identity of a subscriber and precedes issuance of a certificate.

Renewal of a certificate is used when registered subscriber wishes to obtain certificate of a new public key or modify any of the data contained within the certificate.

Revocation of a certificates is used when a private key associated with a public key contained within the certificate or a media used for the private key storage is or is suspected to be revealed.

Verification of certificate status applies Raytonne Trust Services confirmation of validity of certificate issued by Raytonne Trust Services and check against placement on CRL and certificate's validity period. Verification of certificate status may be also carried out by OCSP.

Raytonne Trust Services requires every pair of keys (private and public) to be generated by the subscriber. Raytonne Trust Services may recommend devices which allow key pair generation. In rare cases Raytonne Trust Services might generate unique pair of keys on its own and deliver it to the subscriber.

7. RELYING PARTY

Relying party is obligated to appropriately verify every electronic signature created on the document (including the certificate), he/she/it receives. During verification process, relying party should incorporate procedures and resources available to public in Raytonne Trust Services. It applies, among others, to the requirement of verification of CRL published by Raytonne Trust Services and verification of certification paths.

Every document containing deficiency in an electronic signature or resulting from this deficiency doubts should be rejected or, optionally, subjected to other means or procedures of validity verification; e.g., notary verification.

8. SUBSCRIBER

The subscriber is obligated to securely store his/her/its private key, preventing it from being revealed to any third party. In case of the private key revelation or suspicion of such revelation, the subscriber must immediately notify the authority which issued his/her/its certificate. Information about the revelation must be delivered in the manner not arising doubts to the identity of the subscriber.

9. CERTIFICATION POLICY UPDATE

Raytonne Trust Services Certificate Policy may be subjected to periodical modifications. These modifications will be available to all of the subscribers. Subscribers who don't accept implemented modifications must submit appropriate statement to Raytonne Trust Services and resign from services provided by Raytonne Trust Services.

10. FEES

Certification services provided by Raytonne Trust Services are commercial. Height of charged fees depend on the level of issued or owned certificate and of type of requested service.

Appendix A: Change Log

Version	Change Description	Date
1.0	Initial publication	February 22, 2022