Pursuant to Article 15 of the Financial Agency Act (Official Gazette 117/01, 60/04 and 42/05) and Article 23 of the Constitution of the Financial Agency - consolidated text (Class: 010-00/09-03/2, Ref 01-09-3, from November 25, 2009), as amended, the Management Board of the Financial Agency hereby issues the Decision on these:

TERMS AND CONDITIONS OF PROVIDING CERTIFICATION SERVICES FOR BUSINESS CERTIFICATES

I. Introduction

1. These Fina's Terms and Conditions apply to the provision of Certification Services covering Business certificates, Certificates for e-seal and Business certificates for IT equipment (hereinafter referred to as Certificates) are intended for Subscribers and Relying Parties.

   A ***Business Entity*** is a legal person, public authority or a natural person - citizen with a registered business.

   A ***Signatory*** is a natural person who, acting as Associated Person, creates an electronic signature.

   An ***Associated Person*** is a Natural person employed at the Business Entity or otherwise associated with the Business Entity, and who is authorised by the same Business Entity to receive Certificates. Such Certificate identifies both the person and the Business Entity, and indicates that the person is associated with the Business Entity. The Associated Person may be assigned the role of the Signatory or the Authorized Representative.

   A ***Creator of a Seal*** is a legal person who creates an electronic seal.

   An ***Authorized Representative*** is a natural person authorised legally or by proxy to represent the Creator of a seal in the issuance procedure and/or revocation of the Certificate for Electronic seal.

   A ***Custodian*** is a natural person employed at the Business Entity or associated in another way with the Business Entity, and who has been authorised by the same Business Entity to submit applications for the issuance of Business Certificates for systems and devices, for the renewal, revocation, suspension and reactivation of Certificates, and to retrieve Certificates and corresponding activation data.

   A ***Subscriber*** is a Business Entity that assumes Subscriber's obligations by entering into a Certification Service Agreement with Fina as Qualified Trust Service Provider.

   A ***Relying Party*** is a natural person or a Business Entity relying on a Trust Service. A Certificate allows the Relying Party to identify the Signatory and Subscriber and validate their electronic signature or electronic seal.

2. Fina, as Qualified Trust Service Provider, in providing its services for Business Entities or legal persons applies the following laws and acts:

- Provisions of the 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,
- Provisions of the Implementing Act of 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 Council Directive 1999/93 / EC ,
- Fina's Documents for the provision of the Certification Services that have been published on Fina's website at http://www.fina.hr/finadigicert:
  - Certificate Policy and Certification Practice Statement for Fina Root CA, OID: 1.3.124.1104.5.0.2.2.2.4 (hereinafter referred to as CP/CPS_{ROOT}),
  - Certificate Policy for Qualified Certificates for Electronic Signatures and Seals, OID: 1.3.124.1104.5.0.3.1.1.5 (hereinafter referred to as $CP_{QC\text{-}eIDAS}$),
  - Certification Practice Statement for Qualified Certificates for Electronic Signatures and Seals, OID: 1.3.124.1104.5.0.3.2.1.5 (hereinafter referred to as $CPS_{QC\text{-}eIDAS}$),
  - Certificate Policy for Non-qualified Certificates, OID: 1.3.124.1104.5.0.4.1.1.3 (hereinafter referred to as $CP_{NQC\text{-}eIDAS}$),
  - Certification Practice Statement for Non-Qualified Certificates, OID: 1.3.124.1104.5.0.4.2.1.3 (hereinafter referred to as $CPS_{NQC\text{-}eIDAS}$),
  - this Terms and Conditions of Providing Certification Services for Business Certificates.

3. These Terms and Conditions include all types of Certificates, the relevant Certificate policies, and appropriate usage of Certificates and their limitations as described in Section 2 of the Business Certificates PKI Disclosure Statement (hereinafter referred to as the Statement), which is an integral part of these Terms and Conditions.

II. Certificate Lifecycle Management Services

4. Fina's Certificate lifecycle management services includes:

- initial Certificate issuance,
- Certificate renewal,
- revocation,
- suspension,
- reactivation,
- recovery, and
- Certificate archiving.

5. Depending on the type of the Certificate, Fina also provides delivery of secure cryptographic device or QSCD Device to Subscribers, according to Fina's pricelist.

6. Certificate acceptance by the Subscriber is a prerequisite for issuing and using the Certificate.

   By accepting the Certificate by the Signatory, Authorized Representative or by the Custodian, the Subscriber accepts that all the information that will be held in the

Certificate is correct at the moment of its acceptance.

The Signatory, Authorized Representative or Custodian conducts the checking of the contents of the Certificate immediately prior to the issuance of the Certificate.

The Signatory, Authorized Representative or Custodian accepts the Certificate by signing, or by confirming the Certificate acceptance on the application screen.

After acceptance of the Certificate, Fina issues the requested Certificate to the Signatory, Authorized Representative or Custodian.

Fina applies security measures to ensure that the issued Certificate contains the same information that the Subscriber has accepted prior to the issuance of that Certificate.

If the Signatory, Authorized Representative or Custodian does not accept the Certificate, the reasons for the rejection may be given in oral way or in writing. By not accepting the Certificate, the Signatory, Authorized Representative or Custodian waives the Certificate application, and Fina will not issue the Certificate relating to this application.

Fina will enable submitting of a new Certificate application to the Signatory, Authorized Representative or Custodian in which, if necessary, the corrected data will be entered in relation to the previous Certificate application.

III. Obligations and Responsibilities

Fina's Obligations and Responsibilities

7. Fina conducts all procedures in connection with the provision of Certification Services in a non-discriminatory manner and make its services available to all Subscribers and Relying Parties that accept their obligations and responsibilities defined in these Terms and Conditions.

8. Fina performs its Certification Services with due diligence.

9. Fina is responsible for the proper Subscriber, Signatory, Authorized Representative and Custodian identification and verification of their information for Certificate issuance purposes in accordance with Chapter 3 of $CPS_{QC\text{-}eIDAS}$ and $CPS_{NQC\text{-}eIDAS}$ document.

10. Fina issues the Certificate in a secure manner for the purpose of preserving its authenticity and accuracy, in accordance with the information provided in Subscriber's application.

11. Fina retains all archived Certification System information and Subscriber records for at least 10 years after any Certificate based on these information and records ceases to be valid.

12. Fina revokes the Certificate at Subscriber's request.

Fina revokes the Certificate without receiving a request from the Subscriber:

- if the Subscriber fails to perform his obligations under the Agreement,
- if Fina is in possession of evidence or has reasonable suspicion that the Subscriber's private key has been compromised,
- in the event that Fina is made aware the Certificate was not issued according to the relevant request or the provisions of $CPS_{QC\text{-}eIDAS}$ or $CPS_{NQC\text{-}eIDAS}$,
- based on an revocation request of the EU qualified PSD2 certificate for the e-

Seal (QCP-l) from the National Competent Authority identified in the Certificate

- based on an authenticated third party notification, subject to prior verification of the statements made therein,
- if Fina receives an official notification of Certificate's use for illegal purposes,
- in the event of termination of the Subscriber's Certification Service Agreement, based on which the Certificate was issued,
- if Fina received the official notice of death of the Signatory,
- if Fina has received the official notice of loss of the Signatory's legal capacity.

13. Fina provides information about Certificate's revocation or suspension status free of charge.

14. Revocation status information is available via OCSP service and CRL beyond the validity period of the qualified Certificate. The availability of the revocation status information of the expired Certificate in CRL is realised in a way that the Certificate is not removed from CRL after its expiry, i.e. the Certificate revocation status entry of revoked Certificate is included in each new CRL after the expiration of that Certificate.

15. Fina implements organizational and technical measures to protect the keys, the Certificate and personal information of the Signatory, Authorized Representative and Custodian.

16. Any personal information collected by Fina which is not part of the Certificate is treated as confidential personal information that Fina duly protects.

17. In case of termination of Certification Services provision Fina shall:

- use its best efforts to ensure that the Certification Services continue to be provided by another Qualified Trust Service Provider and therefore shall deliver all documentation collected in the Subscriber registration process, as well as all documentation on issued Certificates to that Qualified Trust Service Provider,
- revoke all Subscriber's Certificates issued by the Fina CA that ceases its operations and issue a final CRL,
- transfer to that service provider its obligation to provide the availability of the final CRL for all revoked Subscriber's Certificates and CA certificate of the Fina CA that ceases its operations,
- transfer to that service provider its obligation to provide the information of certificate revocation status of Subscriber's and Fina CA certificates through OCSP service.

If Fina, after all its best efforts, fails to ensure continuity of the certification service by another Qualified Trust Service Provider, Fina shall:

- keep its obligation to provide the availability of the final CRL for all revoked Subscriber's Certificates and CA certificate of the Fina CA that ceases its operations,
- keep its obligation to provide the information of certificate revocation status of Subscriber's and Fina CA certificates through OCSP service.

Subscriber's Obligations and Responsibilities

18. In the registration and identification process, the Subscriber, Signatory and Authorized Representative is obliged to represent themselves as defined in Chapter 3 and Section 4.1.2.2 of $CPS_{QC\text{-}eIDAS}$ and $CPS_{NQC\text{-}eIDAS}$, depending on the type of the Certificate.

19. The Subscriber, Signatory, Authorized Representative or Custodian reviews and verifies the accuracy of the Certificate`s content and accepts this Certificate prior to its issuance.

20. The Subscriber, Signatory and Authorized Representative undertake to use the Certificate and the associated private key in accordance with appropriate Certificate use, and when using the Certificate will comply with the applicable provisions of $CPS_{QC\text{-}eIDAS}$ and $CPS_{NQC\text{-}eIDAS}$ documents.

21. Subscriber shall not use private key and associated Certificate after the expiry date of the Certificate.

22. If the private key is compromised, the Subscriber, Signatory and Authorized Representative shall immediately and permanently discontinue its use.

23. In case of any changes to any information included in the Certificate, the Subscriber shall notify Fina thereof within seven days.

24. The Legal Representative of the Business Entity, Signatory, Authorized Representative and Custodian are entitled to submit a Certificate revocation request.

    Such revocation request must be submitted:

    - if there is reasonable suspicion that or if the private key has been compromised,
    - in case the private key is lost or becomes permanently unavailable, or
    - if there is reasonable suspicion that the private key or the activation data is no longer in Signatory's or Creator of a seal's sole possession or if the private key or activation data is stolen.

25. The Legal Representative of the Business Entity, Signatory, Authorized Representative and Custodian are entitled to submit a Certificate suspension request.

26. The Subscriber, Signatory and Authorized Representative carefully use and keep the Electronic Signature Creation Device, the private key and the activation data.

27. The Subscriber, Signatory and Authorized Representative undertakes appropriate measures to protect the Electronic Signature/Electronic Seal Creation Device, the private key and the activation data against unauthorized access and use in accordance with the private key protection rules applicable to each type of Certificate.

28. Unless otherwise defined by a specific agreement, the Subscriber pays Fina a fee, the amount and payment method of which are defined in the pricelist published on Fina's website at https://www.fina.hr/finadigicert.

Relying Party's Obligations and Responsibilities

29. The Relying Party uses the Certificate in such circumstances where it relies reasonably and in good faith and in such circumstances as are known or should have been known to the Relying Party before relying on the Certificate. Relying Parties should undertake the required measures as defined in Section 5 of the Statement.

IV. Business Certificates PKI Disclosure Statement

30. Fina provides Subscribers and Relying Parties with general information about the Fina Certification Service in the Statement, which is an integral part of these Terms and Conditions.

V. Entry into the Certification Service Agreement

31. By entering into a Certification Service Agreement with Fina, Business Entity or legal entity and the Associated Person acting as Signatory or Authorized Representative accept these Fina's Terms and Conditions and agree to the obligations and responsibilities set forth in these Terms and Conditions and in $CPS_{QC\text{-}eIDAS}$ or $CPS_{NQC\text{-}eIDAS}$, depending on the type of the Certificate for which the Agreement is entered into.

In case of an Application Certificate, that is listed Section 2 of the Statement, the Certification Service Agreement shall be signed by the Authorized Representative on behalf of Business Entity. For all other Certificate types listed in Section 2 of the Statement, the Certification Service Agreement consists of two parts. The first part of the Certification Service Agreement is signed by the Legal Representative of the Business Entity and the second part of the Agreement is signed by Authorized Representative or Associated Person acting as Signatory.

By executing the Certification Service Agreement, Business Entity or legal person accepts or agrees that:

- it is bound by the Subscriber's obligations and responsibilities defined in this Terms and Conditions and $CPS_{QC\text{-}eIDAS}$ or $CPS_{NQC\text{-}eIDAS}$ documents,
- it is required to keep and use the private key associated with the Certificate only on the QSCD or the secure cryptographic device if this is defined for the relevant Certificate type in Section 2 of the Statement,
- in case it generates a Subscriber key pair, it shall generate the key pair as defined in $CPS_{QC\text{-}eIDAS}$ or $CPS_{NQC\text{-}eIDAS}$, depending on the type of the Certificate,
- Fina may publish the issued Certificate in the Public Directory,
- Fina retains all archived information and records collected during Subscriber registration and later on during Certificate lifecycle management for at least 10 years after any Certificate based on these information and records ceases to be valid,
- in case Fina ceases to provide Certification Services, it may ensure that another Qualified Trust Service Provider continues to provide Qualified Certification Services and that it shall provide to such Service Provider all documentation compiled in the Subscriber registration process and all documents concerning the Certificates issued,
- by the acceptance of the Certificate by the Signatory, Authorized Representative

or Custodian the Subscriber agrees that the information contained in the Certificate is accurate.

By executing the Certification Service Agreement, the Authorized Representative or Associated Person acting as Signatory accepts or agrees that:

- he is bound by the Authorized Representative's or Signatory's obligations and responsibilities defined in $CPS_{QC\text{-}eIDAS}$ or $CPS_{NQC\text{-}eIDAS}$,
- by accepting the Certificate, he agrees that the information contained in the Certificate is accurate,
- he is required to keep and use the private key associated with the Certificate only on the QSCD Device or the secure cryptographic device if this is defined for the relevant Certificate type in Section 2 of the Statement,
- Fina retains all archived information and records collected in the registration process and later in the course of Certificate lifecycle management, as well as information about the Signatory and Authorized Representative for at least 10 years after any Certificate based on these information and records ceases to be valid,
- in case Fina ceases to provide Certification Services, it ensures that another Qualified Trust Service Provider continues to provide Qualified Certification Services and that it shall provide to such Service Provider all documentation compiled in the Signatory's and Authorized Representative's registration process and all documents concerning the Certificates issued.

VI. Final provisions

32. These Terms and Conditions of Providing Certification Services for Business Certificates are filed under Class: 106-01/18-02/99, Ref.: 09-04-19-50 and become effective as of 10 June 2019.

33. In case of any amendments to these Terms and Conditions or the Statement, Fina shall make the new documents available to Subscribers and Relying Parties in the same manner as the presently applicable, publicly disclosed documents.

BUSINESS CERTIFICATES PKI DISCLOSURE STATEMENT

1. CONTACT DETAILS

The contact information of Fina as Qualified Certification Service Provider is as follows:

Mailing address:

Fina
e-Business Centre
Ulica grada Vukovara 70
10000 Zagreb
Croatia

E-mail: info.rdc@fina.hr
Fax: +385-1-6304-081
Web: https://www.fina.hr/finadigicert

The certification revocation requests can be submitted in one of the following manners:

- By personal delivery to the RA Network registration office during office hours.
- By mail or courier at the RA Network office address.
- By electronic delivery to e-mail address info.rdc@fina.hr. The Certificate revocation request must be signed at least with the level of advanced electronic signature or sealed at least with level of advanced electronic seal based on a certificate issued by Fina CA or based on a qualified certificate issued by a Qualified Trusted Service Provider.
- By calling Fina on the telephone number +385 (0)1 612 7040. The telephone number is published on the Fina`s public web site and available from 0 to 24 hours, 7 days a week.

The list of Fina registration offices may be found at http://www.fina.hr/finadigicert.

2. TYPES, VALIDATION AND USE OF CERTIFICATES

Fina RDC 2015 CA issues the following types of Business Certificates to the public:

- **Business EU qualified certificate for e-signature (QCP-n-qscd)** – Business qualified certificate for an e-signature, of medium security level, issued to Associated Persons, whose pertaining private key is stored in the QSCD device, pursuant to Section point 6.2.1 of $CPS_{QC\text{-}eIDAS}$ document. This certificate type complies with "QCP-n-qscd" EU certificate policy for qualified certificates in respect of ETSI EN 319 411-2. The Certificate validity period is 2 years.

- **Business EU qualified certificate for e-signature (QCP-n)** – Business qualified certificate for e-signature, of medium security level, issued to Associated Persons, whose pertaining private key is stored in a secure cryptographic device, pursuant to Section 6.2.1 of $CPS_{QC\text{-}eIDAS}$ document. This certificate type complies with the "QCP-n" EU

certificate policy for qualified certificates in respect of ETSI EN 319 411-2. The Certificate validity period is 2 years.

- **Business EU qualified certificate for remote e-signature (QCP-n)** – Business qualified certificate for e-signature, of medium security level, issued to Associated Persons, whose pertaining private key is stored in the Fina's service of remote electronic signing and sealing service eSignature in the cloud, pursuant to Section 6.2.1 of $CPS_{QC\text{-}eIDAS}$ document. This certificate type complies with the "QCP-n" EU certificate policy for qualified certificates in respect of ETSI EN 319 411-2. The Certificate validity period is 2 years.

- **EU qualified certificate for e-seal (QCP-l-qscd)** – Qualified certificate for e-seal, of medium security level, issued to a legal persons, whose pertaining private key is stored in the QSCD device, pursuant to Section 6.2.1 of $CPS_{QC\text{-}eIDAS}$ document. This certificate type complies with the "QCP-l-qscd" EU certificate policy for qualified certificates in respect of ETSI EN 319 411-2. The Certificate validity period is 2 years.

- **EU Qualified PSD2 certificate for e-seal (QCP-l)** – Qualified Certificate for e-seal, of medium security level, issued to a legal person that is Payment Service Provider according to Directive (EU) 2015/2366 Pertaining private key of this certificate is stored in the software protected token, pursuant to Section 6.2.1 in the $CPS_{QC\text{-}eIDAS}$ document. This type of certificate complies with "QCP-l", EU certificate policy for Qualified Certificates in respect of ETSI EN 319 411-2 extended with requirements for certificates for electronic seals from standardization document ETSI TS 119 495. The Certificate validity period is 2 years.

- **EU qualified soft certificate for e-seal (QCP-l)** – Qualified certificate for e-seal, of standard security level, issued to a legal person, whose pertaining private key is stored in the software protected token, pursuant to Section 6.2.1 of $CPS_{QC\text{-}eIDAS}$ document. This certificate type complies with the "QCP-l" EU certificate policy for qualified certificates in respect of ETSI EN 319 411-2. The Certificate validity period is 5 years.

- **EU qualified certificate for remote e-seal (QCP-l)** – Qualified certificate for e-seal, of medium security level, issued to a legal person, whose pertaining private key is stored in the Fina's service of remote electronic signing and sealing service eSignature in the cloud, pursuant to Section 6.2.1 of $CP_{SQC\text{-}eIDAS}$ document. This certificate type complies with the "QCP-l" EU certificate policy for qualified certificates in respect of ETSI EN 319 411-2. The Certificate validity period is 2 years.

- **Business Authentication Certificate (NCP+)** – Business authentication certificate, of medium security level, issued to Associated Persons, whose pertaining private key is kept in a secure cryptographic device or QSCD device, pursuant to Section 6.2.1 of $CPS_{NQC\text{-}eIDAS}$ document. This certificate type complies with the "NCP+" certificate policy from the ETSI EN 319 411-1 standard. The Certificate validity period is 2 years.

- **Business Soft Certificate (NCP)** – Business authentication certificate, of standard security level, issued to Associated Persons, whose pertaining private key is kept in software protected token pursuant to Section 6.2.1 of $CPS_{NQC\text{-}eIDAS}$ document. This certificate type complies with the "NCP" certificate policy from the ETSI EN 319 411-1 standard. The Certificate validity period is 5 years.

- **Business Soft Certificate (LCP)** – Business authentication certificate, of standard security level, issued to Associated Persons, whose pertaining private key is kept in software protected token pursuant to Section 6.2.1 of $CPS_{NQC\text{-}eIDAS}$ document. This

certificate type complies with the "LCP" certificate policy from the ETSI EN 319 411-1 standard. The Certificate validity period is 5 years.

- **Business Remote Certificate (NCP+)** – Business certificate, of medium security level, issued to Associated Persons, whose pertaining private key is stored in the Fina's service of remote electronic signing and sealing service eSignature in the cloud, pursuant to Section 6.2.1 of $CPS_{NQC\text{-}eIDAS}$ document. This certificate type complies with the "NCP+" certificate policy from the ETSI EN 319 411-1 standard. The Certificate validity period is 2 years.

- **Business Remote Certificate (LCP)** – Business authentication certificate, of standard security level, issued to Associated Persons, whose pertaining private key is stored in the Fina's service of remote electronic signing and sealing service eSignature in the cloud, pursuant to Section 6.2.1 of $CPS_{NQC\text{-}eIDAS}$ document. This certificate type complies with the "LCP" certificate policy from the ETSI EN 319 411-1 standard. The Certificate validity period is 5 years.

- **Application Certificate Level 1 (NCP)** – Certificate of standard security level, whose pertaining private key is stored in a software protected token pursuant to Section 6.2.1 of $CPS_{NQC\text{-}eIDAS}$ document.. This certificate type complies with the "NCP" certificate policy from the ETSI EN 319 411-1 standard. The Certificate validity period is 5 years.

- **Application Certificate Level 2 (NCP)** – Certificate of medium security level, whose pertaining private key is stored in a software protected token pursuant to Section 6.2.1 of $CPS_{NQC\text{-}eIDAS}$ document.. This certificate type complies with the "NCP" certificate policy from the ETSI EN 319 411-1 standard. The Certificate validity period is 2 years.

- **Application Certificate Level 2 (NCP+)** – Certificate of medium security level, whose pertaining private key is kept in a secure cryptographic device or QSCD device, pursuant to Section 6.2.1 of $CPS_{NQC\text{-}eIDAS}$ document. This certificate type complies with the "NCP+" certificate policy from the ETSI EN 319 411-1 standard. The Certificate validity period is 2 years.

- **Application Certificate Level 3 (NCP+)** – Certificate of high security level, whose pertaining private key is stored in an HSM module pursuant to Section 6.2.1 of $CPS_{NQC\text{-}eIDAS}$ document. This certificate type complies with the "NCP+" certificate policy from the ETSI EN 319 411-1 standard. The Certificate validity period is 1 year.

The certificate policy OIDs for Certificates are as follows:

Business EU qualified certificate for e-signature (QCP-n-qscd)	Fina CP OID: 1.3.124.1104.5.12.12.8.2 ETSI CP OID: 0.4.0.194112.1.2
Business EU qualified certificate for e-signature (QCP-n)	Fina CP OID: 1.3.124.1104.5.12.12.2.2 ETSI CP OID: 0.4.0.194112.1.0
Business EU qualified certificate for remote e-signature (QCP-n)	Fina CP OID: 1.3.124.1104.5.12.12.6.2 ETSI CP OID: 0.4.0.194112.1.0
EU qualified certificate for e-seal (QCP-l-qscd)	Fina CP OID: 1.3.124.1104.5.12.13.8.2 ETSI CP OID: 0.4.0.194112.1.3
EU Qualified PSD2 certificate for e-seal (QCP-l)	Fina CP OID: 1.3.124.1104.5.12.13.1.4 ETSI CP OID: 0.4.0.194112.1.1
EU qualified soft certificate for e-seal (QCP-l)	Fina CP OID: 1.3.124.1104.5.12.13.1.1

	ETSI CP OID: 0.4.0.194112.1.1
EU qualified certificate for remote e-seal (QCP-l)	Fina CP OID: 1.3.124.1104.5.12.13.6.2 ETSI CP OID: 0.4.0.194112.1.1
Business Authentication Certificate (NCP+)	Fina CP OID: 1.3.124.1104.5.12.12.4.2 ETSI CP OID: 0.4.0.2042.1.2
Business Soft Certificate (NCP)	Fina CP OID: 1.3.124.1104.5.12.12.3.1 ETSI CP OID: 0.4.0.2042.1.1
Business Soft Certificate (LCP)	Fina CP OID: 1.3.124.1104.5.12.12.5.1 ETSI CP OID: 0.4.0.2042.1.3
Business remote certificate (NCP+)	Fina CP OID: 1.3.124.1104.5.12.12.10.2 ETSI CP OID: 0.4.0.2042.1.2
Business remote certificate (LCP)	Fina CP OID: 1.3.124.1104.5.12.12.9.1 ETSI CP OID: 0.4.0.2042.1.3
Application Certificate Level 1 (NCP)	Fina CP OID: 1.3.124.1104.5.12.15.3.1 ETSI CP OID: 0.4.0.2042.1.1
Application Certificate Level 2 (NCP)	Fina CP OID: 1.3.124.1104.5.12.15.3.2 ETSI CP OID: 0.4.0.2042.1.1
Application Certificate Level 2 (NCP+)	Fina CP OID: 1.3.124.1104.5.12.15.4.2 ETSI CP OID: 0.4.0.2042.1.2
Application Certificate Level 3 (NCP+)	Fina CP OID: 1.3.124.1104.5.12.15.4.3 ETSI CP OID: 0.4.0.2042.1.2

The document with a description of the Certificate profile is available on Fina's website at https://www.fina.hr/finadigicert.

$CPS_{QC\text{-}eIDAS}$ document describes certification practices for the following types of Certificates:

- Business EU qualified certificate for e-signature (QCP-n-qscd),
- Business EU qualified certificate for e-signature (QCP-n),
- Business EU qualified certificate for remote e-signature (QCP-n),
- EU qualified certificate for e-seal (QCP-l-qscd),
- EU Qualified PSD2 certificate for e-seal (QCP-l),
- EU qualified soft certificate for e-seal (QCP-l),
- EU qualified certificate for remote e-seal (QCP-l).

Except for the use specified in Section 1.4.1 of the $CPS_{QC\text{-}eIDAS}$ document, all other uses of these types of Certificates are forbidden.

$CPS_{NQC\text{-}eIDAS}$ document describes certification practices for the following types of Certificates:

- Business Authentication Certificate (NCP+),
- Business Soft Certificate (NCP),
- Business Soft Certificate (LCP),
- Business remote certificate (NCP+),
- Business remote certificate (LCP),
- Application Certificate Level 1 (NCP),

- Application Certificate Level 2 (NCP),
- Application Certificate Level 2 (NCP+),
- Application Certificate Level 3 (NCP+).

Except for the use specified in Section 1.4.1 of the $CPS_{NQC\text{-}eIDAS}$ document, all other uses of these types of Certificates are forbidden.

The Relying Parties are recommended to check and use the CP OIDs of the Certificates referred to the table above in this Section and according to Section 1.4.1 of the $CPS_{QC\text{-}eIDAS}$ and $CPS_{NQC\text{-}eIDAS}$ documents to make a right decisions on acceptance or rejection of the use of particular Certificate.

3. SCOPE OF RELIANCE

Each Certificate issued has a CP OID assigned to it in accordance with Section 2 of this Statement, which defines the Certificate's type, intended purpose, scope of use and the security level which determines the scope of reliance on the Certificate in accordance with Section 1.1.2 of $CPS_{QC\text{-}eIDAS}$ and $CPS_{NQC\text{-}eIDAS}$. The intended purposes, permitted uses and usage limitations of each Certificate type are described in Section 1.4.1 of $CPS_{QC\text{-}eIDAS}$ and $CP_{NQC\text{-}eIDAS}$.

All archived information and documentation of the Fina RDC-TDU 2015 System is retained for at least 10 years after any Certificate based on these data and documentation ceases to be valid, especially for the purpose of providing evidence of Certificate's issuance in legal proceedings.

Such archived information is described in Section 5.5 of $CPS_{QC\text{-}eIDAS}$ and $CPS_{NQC\text{-}eIDAS}$.

4. SUBSCRIBER'S OBLIGATIONS

The Subscriber's obligations are set forth in Chapter III of the Terms and Conditions of Providing Certification Services for Business Certificates (hereinafter referred to as the Terms and Conditions) and in Section 9.6.3 of $CPS_{QC\text{-}eIDAS}$ and $CPS_{NQC\text{-}eIDAS}$.

5. CERTIFICATE STATUS VERIFICATION AND RELYING PARTIES' OBLIGATIONS

The Relying Party independently and knowingly makes its decision to reasonably rely on the Certificate.

Such reasonable reliance implies that the Relying Party has made a decision to rely on the Certificate if at the time of reliance:

- it has undertaken the necessary precautions and uses the Certificate for the purposes described in $CPS_{QC\text{-}eIDAS}$ or $CPS_{NQC\text{-}eIDAS}$, in such circumstances where it relies reasonably and in good faith and in such circumstances that are known to the Relying Party or should have been known to it before relying,
- it uses a reliable application solution and IT environment,
- it has verified the Certificate's validity period,
- it has verified the Certificate's revocation or suspension status, which the Relying Party does by using the OCSP Service or based on the most recently issued CRL, as defined in $CPS_{QC\text{-}eIDAS}$ and $CPS_{NQC\text{-}eIDAS}$,

- it has checked that the electronic signature or electronic seal was created using a private key corresponding to the public key in the Certificate during the Certificate's validity period,
- it has checked that the private key used for authentication corresponds to the public key in the Certificate during the Certificate's validity period.

Relying Party's use of the private key and Certificate is described in Section 4.5.2 and the requirements for Certificate status verification are specified in Section 4.9.6 of $CPS_{QC\text{-}eIDAS}$ and $CPS_{NQC\text{-}eIDAS}$.

Relying Party shall not rely on expired, revoked or suspended Certificate.

If the Relying Party fails to comply with the above provisions and fails to act in accordance with the obligations and responsibilities defined in $CPS_{QC\text{-}eIDAS}$ or $CPS_{NQC\text{-}eIDAS}$, it bears all risks of relying upon such Certificate.

The Relying Party bears all risks of relying upon the Certificate if it is aware of or has reason to believe that there are facts that may cause personal or business loss as a result of using the Certificate.

Certificate status verification may be carried out by using Fina's OCSP Service for online Certificate status verification, the internet address of which is specified in *Authority Information Access* extension of the Certificate and in Section 4.9.9 of $CPS_{QC\text{-}eIDAS}$ and $CPS_{NQC\text{-}eIDAS}$.

The revocation status of the Certificate may also be verified using the CRL published in the LDAP directory server and on the web server. The internet addresses where the CRL relevant to revocation status verification is published are specified in the *CRL Distribution Points* extension of Certificates and in Section 4.10.1.1 of $CPS_{QC\text{-}eIDAS}$ and $CPS_{NQC\text{-}eIDAS}$.

6. LIMITATIONS OF LIABILITY

Fina is not liable for damage, including indirect damage as well as for any loss of profit, loss of data or other indirect damage in the following cases:

- when the damage is caused due to unauthorized use of the user keys and Certificates,
- when the damage is caused by the use of Certificate that is not permitted by this document,
- when the damage is caused by fraudulent or negligent use of the Certificate, CRL or OCSP service,
- when the damage was caused as a result of malfunctions and errors in the software and hardware of the Subscriber and the Relying Party,
- when the damage was caused as a result of the fraudulent disclosure and fraudulent presentation of the Business Entity or a physical person during the identification and authentication process if the identification and verification of the data RA Network has carried out in accordance with the requirements of $CP_{QC\text{-}eIDAS}$ and $CP_{NQC\text{-}eIDAS}$ documents and the operating instructions.

Fina's total financial liability for issued Certificates and transactions carried out in reliance to these Certificates is listed in Section 9.8 of $CP_{QC\text{-}eIDAS}$ and $CP_{NQC\text{-}eIDAS}$ documents.

7. FINA'S DOCUMENTS

Fina's publicly disclosed documents applicable to the provision of the Certification Service are $CP_{QC\text{-}eIDAS}$, $CPS_{QC\text{-}eIDAS}$, $CP_{NQC\text{-}eIDAS}$, $CPS_{NQC\text{-}eIDAS}$, the Terms and Conditions and this Statement, the corresponding Certification Service Agreement's form, the associated Certificate request forms, and Subscriber Instructions. These Fina's documents and the legislation relevant to the provision of Certification Services are published on Fina's website at https://www.fina.hr/finadigicert.

8. PERSONAL DATA PROTECTION

Fina as Qualified Trust Service Provider applies the provisions of the Act Implementing General Data Protection Regulation and other acts which regulates protection of personal data. Protection of Subscriber's personal data is described in Sections 15 and 16 of Terms and Conditions and in Section 9.4 of $CPS_{QC\text{-}eIDAS}$ and $CPS_{NQC\text{-}eIDAS}$.

9. FEE REFUND

Fina refunds fees to Subscribers in the event of incorrect payment or overpayment.

10. RESOLUTION OF DISPUTES AND APPLICABLE LAW

Participants may file a complaint and appeal to Fina if they believe there exists a discrepancy in the content of services that are subject of the Certification Service Agreement. Fina shall reply to the complaint and appeal. Complaint or appeal have to be filed in paper or electronic form and submitted to a contact address listed in Section 1 of this Disclosure Statement.

In the event of a dispute or disagreement between Fina and other participants due to actions and/or procedures regarding certification service provisions, the participants shall try to reach an amicable solution. Otherwise, the matter shall be resolved by the competent court in Zagreb by applying Croatian law.

11. SUPERVISION AND COMPLIANCE AUDIT

Fina is a Qualified Trust Service Provider whose qualified status is indicated on a Trusted List of qualified trust service providers in accordance with Regulation (EU) No 910/2014.

Supervision over the work of Fina as a Qualified Trust Service Provider is regulated by Regulation (EU) No 910/2014, Act Implementing Regulation (EU) no. 910/2014, and is carried out by the central state administration authority competent for economic affairs.

Supervision over the Fina, acting as Qualified Trust Service Provider, in the field of monitoring the implementation of personal data protection is carried out by Croatian Personal Data Protection Agency.

Verification of Fina`s conformity as a qualified trust service provider is carried out by a conformity assessment body in the manner prescribed by Regulation (EU) No 910/2014.

Class: 106-01/18-02/99
Ref.: 09-04-19-49
Date: 27 May 2019