Pursuant to Article 15 of the Financial Agency Act (Official Gazette No. 117/01, 60/04, 42/05) and Article 23 of the Constitution of the Financial Agency (Class: 010-00/09-03/2, Ref 01-09-3, dated 25 November 2009 - consolidated text), the Management Board of the Financial Agency hereby issues the Decision on these:

TERMS AND CONDITIONS OF PROVIDING CERTIFICATION SERVICES FOR QUALIFIED WEBSITE AUTHENTICATION CERTIFICATES

I. Introduction

1. These Fina's Terms and Conditions apply to the provision of Certification Services covering Qualified Website Authentication Certificates (hereinafter referred to as Certificates) which are intended for Subscribers and Relying Parties.

   A ***Custodian*** is a natural person employed at the Applicant or associated in another way with the Applicant, and who has been authorised by the same Applicant to submit applications for the issuance of Qualified Certificate for Website Authentication and to and to accept Certificates and corresponding activation data. The Custodian is authorised to submit requests for lifecycle management of Certificates.

   An ***Applicant*** is a Legal Person with registered office in the Republic of Croatia or the Government Entity applying for a Certificate and having a web server under its supervision and operation. After signing the certification contract, the Applicant becomes the Subscriber.

   A ***Certificate Approver*** is a natural person authorized to approve a certificate request on behalf of the Applicant.

   A ***Government entity*** is public authorities carrying out public authority on the basis of the Constitution and the laws of the Republic of Croatia.

   A ***Contract Signer*** is a natural person who has authority on behalf of the Applicant to sign Subscriber Agreements.

   A ***Subscriber*** is a Legal Person with registered office in Republic of Croatia or Government Entity bound by agreement with a qualified trust service provider to any Subscriber obligations.

   A ***Payment Service Provider*** is the body referred to in article 1 of paragraph 1 or a natural or Legal Person who is allowed to exempt under article 32 of the or 33 of Directive (EU) 2015/2366 [3].

   A ***Relying Party*** is a natural person or a Legal person relying on a Trust Service. The Relying Party performs authentication of website based on a valid Certificate and acts

on the basis of reasonable confidence in that Certificate.

2. Fina, as Qualified Trust Service Provider, in providing its services for 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 https://www.fina.hr/finadigicert:
     - Certificate Policy and Certification Practice Statement for Fina Root CA, OID: 1.3.124.1104.5.0.2.2.2.7 (hereinafter referred to as CP/CPS_{ROOT}),
     - Certificate Policy for Qualified Certificates for Website Authentication, OID: 1.3.124.1104.5.0.6.1.1.4 (hereinafter referred to as CP_{QWAC}),
     - Certification Practice Statement for Qualified Certificates for Website Authentication, OID: 1.3.124.1104.5.0.6.2.1.4 (hereinafter referred to as CPS_{QWAC}),
     - this Terms and Conditions of Providing Certification Services for Qualified Website Authentication Certificates.

3. These Terms and Conditions include types of Certificates, the relevant Certificate policies, and appropriate usage of Certificates and their limitations as described in Section 2 of the Qualified Certificates for Website Authentication 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,
   - Certificate revocation,
   - Certificate recovery.

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

   By accepting the Certificate 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 Custodian conducts the checking of the contents of the Certificate immediately prior to the issuance of the Certificate.

The 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 Custodian.

If the 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 Custodian waives the certificate application, and Fina will not issue the Certificate relating to this request.

Fina will enable submitting of a new certificate application to the 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

6. 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.

7. Fina performs its Certification Services with due diligence.

8. Fina is responsible for the proper identification and verification of the Applicant, as well as for proper verification whether the Subscriber has control and exclusive right over the domain name contained in the Certificate, in accordance to Chapter 3 of CPS_{QWAC} document.

9. 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 request.

10. Fina applies security measures to ensure that the Certificate issued contains the same information accepted by the Custodian prior to the issuance of that Certificate.

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 also revokes the EU PSD2 QWAC certificate (QCP-w-psd2) at request submitted by the National Competent Authority responsible for implementing Directive (EU) 2015/2366 in the country where the Payment Service Provider is registered. This National Competent Authority is identified in every EU PSD2 QWAC certificate (QCP-w-psd2).

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

- in the event that Fina is made aware that a Subscriber has violated its obligations and responsibilities specified in the Agreement, this Terms of Use, CP_{QWAC} and CPS_{QWAC} documents,
- if Fina obtains evidence that the Subscriber's private key corresponding to the public key in the Certificate suffered a key compromise, or the private key or activation data are no longer in the sole possession of the Custodian or Subscriber,
- if Fina is made aware of a demonstrated or proven method that can easily compute the Subscriber's private key based on the public key in the Certificate,
- in the event that Subscriber notifies Fina that the original certificate request was not authorized and does not retroactively grant authorization,
- if Fina obtains evidence that the validation of domain authorization or control for any FQDN in the Certificate should not be relied upon,
- if Fina is made aware that the Certificate was not issued according to the provisions of CP_{QWAC} and CPS_{QWAC} documents,
- If Fina is made aware of any circumstance indicating that use of a FQDN contained in the Certificate is no longer legally permitted to Subscriber,
- based on an authenticated third party notification, subject to prior verification of the statements made therein,
- in the event that Fina receives evidence that the Certificate was misused or in the event that Fina receives an official notification from competent authority on the Certificate use for illegal purposes,
- in the event of termination of the Subscriber's Certification Service Agreement, based on which the Certificate was issued,
- in other cases stated in the Section 4.9.1 of CPS_{QWAC} document.

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

14. Fina implements organizational and technical protection measures for keys and Certificates, and personal information of the natural persons that are collected, stored and used for the purpose of providing the Certification Services.

15. Any personal information collected by Fina is treated as confidential personal information that Fina duly protects.

16. 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,
- transfer to that service provider its obligation to enable Relying parties, within reasonable time, to have the availability of Fina's CA certificates with the public keys of Fina CAs as well as the availability of other Certificates with public keys of Fina's Trust services,
- revoke all Certificates issued by the Fina CA that ceases its operations,
- transfer to that service provider its obligation to provide the availability of the final CRL for all revoked Certificates and CA certificates of the Fina CAs that ceases its operations,
- transfer to that service provider its obligation to provide the information of certificate revocation status of Certificates and Fina CA certificates through OCSP service,
- revoke the CA certificates and destroy their related private keys of those Fina CAs that cease its operations.

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 Certificates and CA certificate of the Fina CA that ceases its operations,
- keep its obligation to provide the information of certificate revocation status of Certificates and Fina CA certificates through OCSP service.

Subscriber's Obligations and Responsibilities

17. In the registration and identification process, the Subscriber, Custodian and Certificate Approver are obliged to represent themselves as defined in Chapter 3 and Section 4.1.2.2 of CPS_{QWAC} document.

18. The Subscriber or Custodian reviews and verifies the accuracy the Certificate`s content and accept this Certificate prior to its issuance.

19. The Subscriber is obliged to use the private key associated with Certificate and corresponding activation data in an appropriate manner, and in compliance with the applicable provisions of CPS_{QWAC}.

20. The Subscriber is obliged to undertake appropriate protection measures for private key associated with Certificate and corresponding activation data against unauthorised access and use, in accordance with Chapter 6 of CPS_{QWAC} document.

21. The Subscriber is obliged to use the Certificate and the pertaining private key only on servers accessible through FQDN listed in the *Subject Alternative Name* extension of the Certificate, and in accordance with legal and other provisions of the Republic of

Croatia and regarding the appropriate use of Certificate in accordance with Section 1.4.1 and 1.4.2 and use of its corresponding private key in accordance with Section 4.5.1 of CPS_{QWAC} document.

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

23. If the Certificate is revoked for reason of private key compromise, the Subscriber is obliged to immediately and permanently discontinue the use the compromised private key.

24. The Subscriber is obliged to respond to Fina's instructions related to the compromised key or incorrect use of the Certificate.

25. The Subscriber shall in the shortest possible period, request revocation of a Certificate and terminate use of the corresponding private key in the event of suspicion or actual incorrect use or compromise of a private key, and if any of the information contained in the Certificate shall become incorrect in accordance with Section 4.9 of CPS_{QWAC} document.

26. The Custodian and Certificate Approver are entitled to submit a Certificate revocation request.

27. Subscriber is obliged to submit Certificate revocation request:
    - 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,
    - if there is reasonable suspicion that the private key or the activation data is no longer in Subscriber's sole possession or if the private key or activation data is stolen, or
    - if the information contained in the Certificate is incorrect or leads to incorrect conclusions.

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.

29. The Subscriber agrees to act in accordance with all other provisions stated in CPS_{QWAC} document that refer to Subscriber obligations.

Relying Party's Obligations and Responsibilities

30. 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. Website Authentication Certificates PKI Disclosure Statement

31. Fina provides Subscribers and Relying Parties with general information about the Fina Certification Service in the Qualified Certificates for Website Authentication PKI Disclosure Statement, which is an integral part of these Terms and Conditions.

V. Entry into the Certification Service Agreement

32. By entering into a Certification Service Agreement with Fina, the Legal person or Government Entity, acting as Subscriber, accepts these Fina's Terms and Conditions of Providing Certification Services for Qualified Website Authentication Certificates and agrees to the obligations and responsibilities set forth in these Terms and Conditions, CP_{QWAC} and in CPS_{QWAC}.

The Certification Service Agreement shall be signed by the Contract Signer.

By executing the Certification Service Agreement, the Legal person or Government Entity accepts or agrees that:

- it is bound by the Subscriber's obligations and responsibilities defined in these Terms and Conditions and CPS_{QWAC} document,
- it shall generate a Subscriber key pair as defined in CPS_{QWAC} document,
- Fina may publish the issued Certificate in the Public Directory,
- in case of issuing EU QWAC certificate (QCP-w) Fina:
    - logs the precertificate in three qualified CT log services,
    - obtains the SCTs from those log services and append them in the EU QWAC certificate (QCP-w) to be issued,
- Fina retains all archived information, records and documentation 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 Certification Services and that it shall provide to such Service Provider all data, records and documentation compiled in the Subscriber registration process and all documents concerning the Certificates issued,
- by the acceptance of the Certificate by the Custodian, the Subscriber agrees that the information contained in the Certificate is accurate.

VI. Final provisions

33. These Terms and Conditions of Providing Certification Services for Qualified Website Authentication Certificates are filed under Class: 106-01/22-04/12, Ref: 09-04-22-14 and become effective as of 25 September 2022.

34. 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.

QUALIFIED WEBSITE AUTHENTICATION CERTIFICATES
PKI DISCLOSURE STATEMENT

1. CONTACT DETAILS

The contact information of Fina as Qualified Trust 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 Fina's registration office during office hours.
- By mail or courier at the Fina's registration 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 certificate issued by Fina's 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 available from 0 to 24 hours, 7 days a week.

The list of Fina registration offices with associated postal addresses may be found at https://www.fina.hr/finadigicert.

2. TYPES, VALIDATION AND USE OF CERTIFICATES

Fina RDC 2015 CA issues the following types of Qualified Website Authentication Certificates to the public:

- **EU QWAC Certificate (QCP-w)** – Qualified certificate for website authentication issued to Legal Person with registered office in Republic of Croatia and to Government Entity. The corresponding private key of this type of certificate is stored in software protected token pursuant to Section 6.2.1 of the CPS_{QWAC} document. This certificate type complies with the "QCP-w" EU certificate policy for qualified

certificates from the ETSI EN 319 411-2 standard. The Certificate validity period is 1 year.

- **EU PSD2 QWAC Certificate (QCP-w-psd2)** – Qualified certificate for website authentication issued to Legal Person with registered office in Republic of Croatia that is Payment Service Provider according to Directive (EU) 2015/2366. The corresponding private key of this type of the certificate is stored in software protected token, pursuant to Section 6.2.1 of the CPS_{QWAC} document. This certificate type complies with the "QCP-w" EU certificate policy for qualified certificates from the ETSI EN 319 411-2 standard which has been expanded with the requirements for PSD2 qualified certificates for website authentication from the standardization document ETSI TS 119 495. The Certificate validity period is 1 year.

The certificate policy OIDs for Certificates are as follows:

EU QWAC certifikate (QCP-w)	Fina CP OID: 1.3.124.1104.5.12.14.1.2 ETSI CP OID: 0.4.0.194112.1.4 CAB Forum CP OID: 2.23.140.1.1
EU PSD2 QWAC certificate (QCP-w-psd2)	Fina CP OID: 1.3.124.1104.5.12.14.1.4 ETSI CP OID: 0.4.0.19495.3.1 CAB Forum CP OID: 2.23.140.1.1

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

Certification practices are described in the CPS_{QWAC} document.

Certificates and associated private keys may only be used only to authenticate web sites that are accessed via TLS or SSL protocol. All other uses of these types of Certificates and their corresponding private keys are forbidden.

The Relying Parties are recommended to check and use the CP OIDs of the Certificates and previous provision on the permitted and prohibited use of the Certificate to make a right decision 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 and scope of use. Permitted uses and usage limitations of each Certificate type are described in Section 2 herein.

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

Such archived information, records and documentation is described in Section 5.5 of CPS_{QWAC}.

4. SUBSCRIBER'S OBLIGATIONS

The Subscriber's obligations are set forth in Chapter III of the Terms and Conditions of Providing Certification Services for Qualified Website Authentication Certificates (hereinafter referred to as the Terms and Conditions) and in Section 9.6.3 of CPS_{QWAC}.

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_{QWAC}, 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 validated the Certificate as an EU Qualified Certificate as described in Section 4.5.2 of CPS_{QWAC},
- it has verified the Certificate's validity period,
- it has verified the Certificate's revocation status, which the Relying Party does by using the OCSP Service or based on the most recently issued CRL, as defined in CPS_{QWAC},
- 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_{QWAC}.

Relying Party shall not rely on expired or revoked 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_{QWAC}, 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_{QWAC}.

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_{QWAC}.

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 Subscriber, Custodian, Certificate approver or Contract signer 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 CPS_{QWAC} document 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 CPS_{QWAC} document.

7. FINA'S DOCUMENTS

Fina's publicly disclosed documents applicable to the provision of the Certification Service are $CP_{QWAC,}$ CPS_{QWAC}, 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 13 and 14 of Terms and Conditions and in Section 9.4 of CPS_{QWAC}.

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 [1], Act Implementing Regulation (EU) no. 910/2014 [2], 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 shall be carried out by a conformity assessment body in the manner prescribed by Regulation (EU) No 910/2014.

Class: 106-01/22-04/12

Ref.: 09-04-22-13

Date: 25 September 2022