FINA

CERTIFICATE POLICY FOR CERTIFICATES FOR WEBSITE AUTHENTICATION

Version 1.12

Effective date: 25 November 2024

Document OID: 1.3.124.1104.5.0.5.1.1.12

Document details

Document Name:	Certificate Policy for Certificates for Website Authentication
Document OID:	1.3.124.1104.5.0.5.1.1.12
Document Type:	Certificate Policy (CP)
Distribution Designation	Public
Document Owner	Financial Agency, Fina
Contact	pma@fina.hr

Amendment History

Version	Date	Reason for Amendment
1.0	22/05/2017	Initial version
1.1	21/03/2018	Updating referent list of Croatian legal regulations, enhancement to the registration process by adding CAA record check statement, modified validity period of SSL Certificate Level 2 (OVCP) and correction of typographical errors.
1.2	27/07/2018	Adding stipulations of verification of country related to the Subject, validation of domain authorization or control, and authentication for an IP address, updating referent list of Croatian legal regulations, adding a stipulation on the issuance of a certificate for legal persons with registered office location in the Republic of Croatia, adding the conformity declaration of the document with RFC 3647.
1.3	11/09/2018	Adding SHA-256 fingerprint of CA certificates, supplementing provisions concerning termination of provision of trust services, improvement in certification acceptance procedures, reduction of required data collected during revocation of certificates, adding a statement about procedures related to critical vulnerability addressing, adding a declaration of revocation and suspension of the certificate regardless of the status of the payment, and adding a statement of availability of services to persons with disabilities.
1.4	21/05/2019	Removed the certificate Profile "SSL Certificate Level 3 (OVCP)", together with descriptions of the related procedures because of termination of its issuance, in Section 3.1.4 added information about the character set constraints, in Chapters 3 and 4 added clarifications in the registration and data verification procedures and added specification of the level of electronic signatures that Fina accepts on application forms and agreements for certification services, in Section 4.6 and 4.7 added clarifications for the delivery of the public key in the in the process of the certificate renewal, in Section 4.9 an improved description of the reasons for the certificate revocation and the additional specified time periods relating to revocation, in Section 5.2.4 complemented rule for separation of duties, in Section 6.1.7 the description of the purpose of the keys has been expanded, in Section 9.4 added extensions in the description of the protection of personal data, in Section 9.6.1 supplemented a description of the Fina`s responsibility, in Sections 9.7 and 9.9 corrected the Fina disclaimer text and corrected recognized errors in the document.
1.5	30/04/2020	Updated reference list of Croatian legal regulation and corrected recognized minor errors in the document.

Version	Date	Reason for Amendment
1.6	22/09/2020	Provisions have been added to support Certificate Transparency in Sections 2.2, 4.3.1, 4.4.2, and 4.4.3. Also, in Section 6.3.2 the period of validity of new SSL Certificate Level 2 (OVCP) has been shortened to 12 months.
1.7	23/09/2021	Updated the list of "Referente documented information", in the overview of Fina PKI in Section 1.1 added Fina RDC 2020 CA, in Sections 3.2.1, 4.5.1, 4.7, 5.4.1, 6.1.1.2, 6.1.2, 6.1.3, 6.2.3, 6.2.4, 6.4.1 and 9.6.1 appropriate changes have been made regarding termination of Subscriber key pair generation by Fina, in Section 4.6 appropriate changes have been made regarding termination of issuing certificates with previously used Subscriber public keys within Fina RDC 2015 CA, in Section 4.9.1 added a provision on revocation of certificates in case of demonstrated or confirmed method of private key calculation based on knowledge of public key.
1.8	22/09/2022	In Section 1.1.1 added details about the equality of this document written in Croatian and English, in Sections 1.3 and 1.3.2 improved description of Fina Registration Network, in Section 2.2 added repository`s URL for information in English, in Section 2.3 improved description of the publication frequency of this document, in Section 3.1 added information on compliance for name determination, in Section 3.2.5 amended description of identity verification of authorized persons, in Section 3.2.6 added statement related to cross-certification, in Section 4.1.2.1 amended description on verification of certificate applications in electronic form, in Section 4.2.1 added information on the reuse of documents and data and also on the procedure for verifying High Risk Certificate Request, in Section 4.3.1 added statement on the ability to revoke pre-certificate, in Section 4.4.9 added details on signing, certificate and OCSP response, in Section 4.9.12 the procedure for demonstrating the compromise of the private key is described, in Section 5.3.3 added information about education records, in Section 5.7.1 amended text on security-sensitive changes, in Section 6.1.1.2 supplemented information on Subscriber's keys generation, in Section 6.1.2 added provision on archiving Subscriber private keys, in 6.1.5 added information about the characteristics of Subscriber`s RSA keys, in 6.5.1 amended provision for two-factor authentication, in 7.1 added description of the serial number of the certificate, in Section 7.1.4 added provision for standalone metadata, in Section 7.1.5 added information about Name Constraints, Section 8.1.1 amended description of the audit time period, in Section 8.6 amended description of delivery of the audit report and minor errors identified in the document were corrected.
1.9	15/06/2023	In Sections 1.4 and 9.8 amounts converted into euros, Section 9.14 is amended by specifying statements on the applicable legal framework and interpretation of the applied provisions, Section 9.15 is amended by stating the regulations that apply to the provision of trust services from the scope of this document and in Section 9.17 the provisions have been amended and regulations that are applied in order to enable the availability of trust services to persons with disabilities have been stated.
1.10	22/03/2024	In Sections 3.1.1, 3.1.4, 3.2.2.3 and 4.9.1 provisions related to the issuance and revocation of Wildcard certificates have been added, in the reference documented information the versions of the norms have been updated, in Sections 1.4 and 9.8 values expressed in kuna have been removed.
1.11	22/04/2024	In Sections 2.2.1, 4.9.7 and 4.10.1 information on issuing and publishing a partitioned CRL on the web server has been added, in Section 7.2.2 information about the content of the partitioned CRL has been added.

Version	Date	Reason for Amendment
1.12	07/11/2024	The name of the Fina CA that starts issuing subscriber certificates has been changed in all necessary places in the document, the same name of the Fina CA has been added as the CRL issuer. In Section 1.3.1, a description of the Fina CA certificate that starts issuing subscriber certificates has been added and provisions have been added for the Fina CA that stops issuing subscriber certificates, in chapter 8 and in Sections 9.14 and 9.15 the information on the applicable law has been updated, in Sections 5.8, 6.6.2 and chapter 8 the information about the supervisory authority has been changed.

CONTENTS

COPYRIGHT

REFERENT DOCUMENTED INFORMATION

Core legislation

[1] 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

[2] Act on Amendments to the Act on the Organisation and Scope of State Administration Bodies (Croatian Official Gazette (hereinafter referred to as Official Gazette) 57/2024)

Subordinate Regulations

[3] The Ordinance on the provision and use of trust services (Official Gazette 60/2019)

Other legislation

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[5] Act Implementing General Data Protection Regulation (Official Gazette 42/2018)

[6] United Nations Convention on the Rights of Persons with Disabilities and Optional Protocol to the Convention on the Rights of Persons with Disabilities, New York 13 December 2006

[7] Act on Accessibility of the Websites and Software Solutions for Mobile Devices of Public Sector Bodies of the Republic of Croatia (Official Gazette 17/2019)

[8] Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies

Standardization Documents

[9] ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems - Requirements

[10] ETSI EN 319 401 V2.3.1. (2021-05) – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[11] ETSI EN 319 411-1 V1.4.1. (2023-10) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[12] ETSI EN 319 412-1 V1.5.4. (2023-09) – Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 1: Overview and common data structures

[13] ETSI EN 319 412-4 V1.3.1. (2023-09) – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

[14] ETSI EN 319 403-1 V 2.3.1 (2020-06) - Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment – Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers

[15] ETSI TS 119 403-2 V1.3.1 (2023-03) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment – Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates

[16] ETSI TS 119 312 V1.4.3 (2023-08) – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[17] NIST FIPS PUB 140-2 (2001) – Security Requirements for Cryptographic Modules

[18] IETF RFC 3647 – Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework

[19] IETF RFC 5280 – Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile

[20] IETF RFC 6844 – DNS Certification Authority Authorization (CAA) Resource Record (2013)

[21] IETF RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP

[22] IETF RFC 6962 - Certificate Transparency

[23] CA/Browser Forum - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (current version)

Fina's Documents

[24] Certificate Policy and Certification Practice Statement for Fina Root CA, CP/CPS_{ROOT}

[25] Certification Practice Statement for Certificates for Website Authentication, CPS_{WSA}

[26] Certification Practice Statement for Non-qualified Certificates for Electronic Signatures and Seals, CPS_{NQC}

1 INTRODUCTION

Fina PKI was initially designed and established within the Financial Agency (Fina) as a Trusted Third Party with the aim of providing certification services to natural persons - citizens, business entities and public authorities. As a Qualified Trust Services Provider, Fina enables building a relationship of trust necessary for the use and development of electronic business (e-Business) and electronic government (e-Government). By promoting these Trust Services and their use, Fina wishes to encourage and facilitate the development of e-Business and e-Government.

As a state-owned company, with a half-century-long tradition of providing financial services, Fina maintains a partnership with the State and cooperates with the Croatian National Bank, as well as successfully engages in business activities with banks, numerous business systems and other business entities in the Republic of Croatia. Fina's IT system has been put to a test through the most demanding tasks of national priority, while highly professional expert teams have ensured the preparation and implementation of various projects.

Tradition, reliable service provision and orientation towards providing electronic services to natural persons - citizens, business entities and public authorities are the main reasons why Fina is recognized as a Trusted Third Party in e-Business and e-Government.

Fina’s business network covers branches and subsidiaries spread across the country, interconnected by an IT system which guarantees fast and reliable response to requests and which is also used by Fina Registration Authorities (Fina RA Network).

As a Trusted Third Party, Fina has been providing certification services since 2003. The trust services Fina provides shall be in accordance with legal regulations [1] – [5] and thereby also with the applicable international standards within the scope of trust services provision. Fina shall continuously keep track of Subscribers' needs, technology development and modifications to standards within the scope of trust services provision, and improve and adjust its PKI system accordingly.

The certificates for website authentication issued by Fina shall be issued in accordance with this Certificate Policy.

1.1 Overview

Fina PKI is the PKI infrastructure established at Fina by which Fina provides trust services which refer to issuance and management of production certificate life-cycle (hereinafter referred to as: "Certification services") and electronic Time-Stamp issuing.

Hierarchical structure of Fina PKI rests on Fina Root CA and is based on two-tier architecture of production Certification Authorities (hereinafter referred to as: "CA" or "CAs").

Fina's two-tier architecture of production Certificate Authorities includes:

- Root Certification Authority (root CA): Fina Root CA
- subordinate Certificate Authorities:
  - Fina RDC 2020,
  - Fina RDC 2015,
  - Fina RDC-TDU 2015.

Fina Root CA issued a self-signed Fina Root CA certificate as well as certificates to its subordinate Fina RDC 2020, Fina RDC 2015 and Fina RDC-TDU 2015 CAs.

The Certificate Policy which refers to Fina Root CA and Fina PKI hierarchy based on Fina Root CA are described in the document Certificate Policy and Certification Practice Statement for Fina Root CA, CP/CPS_{ROOT} [24].

Fina RDC 2020, Fina RDC 2015 and Fina RDC-TDU 2015 are CAs which issue certificates for end-Subscribers.

1.1.1 Certificate Policy scope and purpose

This Certificate Policy for Certificates for Website Authentication – CP_{WSA} (hereinafter referred to as: "Certificate Policy") contains basic rules and a set of common principles of the certification services provision by which Fina as a Trust Service Provider provides services of issuing (unqualified) Certificates for website authentication, known as TLS/SSL certificates, which include validated data on the identity of the Subscriber organisation (hereinafter referred to as: "OVCP certificate" or "Certificate").

Within the scope of this Certificate Policy shall be the trust services provided by Fina which refer to issuance of production certificates for website authentication and management of their life-cycle. The private key of these certificates shall be protected by software token.

Production Certificates for website authentication from the scope this Certificate Policy shall form an integral part of the Register of Digital Certificates (Fina RDC). The Certification Authority (CA) that starts issuing Subscriber's Certificates, from the scope of this document is Fina RDC 2020 CA, and the Certification Authority (CA) that ceases issuing Subscriber's Certificates from the scope of this document is Fina RDC 2015.

This CP_{WSA} shall be published on the web page https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti in Croatian and https://www.fina.hr/en/legislation-documents-and-conformance-certificates in English

Fina confirms that the English translation of CP_{WSA} is not materially different to the Croatian original document.

The purpose of this document is to define rules referring to the scope of this document, according to which all Fina PKI participants mentioned in Section 1.3 of the Certificate Policy shall act.

The structure of this document is based on the standardization document IETF RFC 3647 [18].

1.1.2 Certificate types

This Certificate Policy shall define certification rules for Certificates for website authentication issued by Fina RDC 2020 CA, which shall be in accordance with the requirements 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 [1] (herein referred to as: Regulation (EU) No 910/2014).

Fina conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

Table 1.1 shows type of Certificates for website authentication within the scope of this Certificate Policy with his titles and pertaining Fina, ETSI and CAB Forum Certificate Policy OIDs (hereinafter referred to as: "CP OID").

Certificates for website authentication			
Certificate group name	**Certificate type name**	**Fina and ETSI CP OID**	**Security level**
Fina RDC 2020 Certificates for website authentication	SSL Certificate Level 2 (OVCP)	Fina CP OID: 1.3.124.1104.5.13.14.2 ETSI CP OID: 0.4.0.2042.1.7 CAB Forum CP OID: 2.23.140.1.2.2	Medium

Table 1.1 Certificate for website authentication

This Certificate Policy defines the following Certificate for website authentication named *SSL Certificate Level 2 (OVCP)* (hereinafter referred to as: "certificate")

- ***SSL Certificate Level 2 (OVCP)*** – a Certificate for website authentication of medium level security, the private key of which shall be stored in a software protected token pursuant to Section 6.2.1 herein. This certificate type shall comply with the "OVCP" certificate policy from the ETSI EN 319 411-1 [11] standard.

SSL Certificate Level 2 (OVCP) is hereinafter referred to as a Subscriber's Certificate.

Fina shall issue website authentication certificate for servers associated to the Legal persons with registered office location in the Republic of Croatia.

1.2 Document name and identification

British Standards Institution (BSI) International Code Designator (ICD) assigned the OID to Fina. Based on that OID, Fina assigned the following OID to Fina PKI: 1.3.124.1104.5.

Listed below are the Document Name and the corresponding identification data.

- Name: Certificate Policy for Certificates for Website Authentication
- Version: 1.12
- Effective date: 25 November 2024
- OID: 1.3.124.1104.5.0.5.1.1.12
- The document is published on the following web-site: https://rdc.fina.hr/RDC2015/CPWSA1-12-en.pdf

1.3 PKI participants

Participants within Fina PKI are:

- Certification Authorities (CAs),
- Fina Registration Network (Fina RA Network) consisting of Central Fina RA and Local Registration Authorities (LRAs),
- Subscribers,
- Relying Parties.

1.3.1 Certification authorities

1.3.1.1 Fina Root CA

Fina Root CA certificate basic data are given in Table 1.2.

Field	Attribute	Value
Issuer	commonName	Fina Root CA
	organizationName	Financijska agencija
	countryName	HR
Validity	notBefore	Time of issuance of the certificate
	notAfter	Time of issuance of the certificate + 20 years
Subject	commonName	Fina Root CA
	organizationName	Financijska agencija
	countryName	HR
SHA-1 *fingerprint*: 62:02:bf:16:9a:f2:7f:a6:7e:d0:ce:c6:6b:78:2b:83:22:61:26:e9		
SHA-256 *fingerprint*:5a:b4:fc:db:18:0b:5b:6a:f0:d2:62:a2:37:5a:2c:77:d2:56:02:01:5d:96:64:87:56:61:1e:2e:78:c5:3a:d3		

Table 1.2 Fina Root CA certificate basic data

Fina Root CA shall not issue Subscriber's Certificates.

Fina Root CA certificate shall be available at the web address listed in Section 6.1.4 herein.

1.3.1.2 Fina RDC 2020 CA

The Certification Authority that issues certificates within Fina PKI under this Certificate Policy shall be Fina RDC 2020.

As a Trust Service Provider, Fina shall provide certificate issuance services to the public and manage the life-cycle of those certificates through this CA in accordance with the this Certificate Policy.

Pursuant to that same Certificate Policy, Fina RDC 2020 CA shall issue certificates to Fina.

In the issued certificates, Fina RDC 2020 CA shall be identified as the Issuer and shall sign certificates by using Fina RDC 2020 CA's private key.

Basic data on Fina RDC 2020 CA-certificate are provided in Table 1.3.

Field	Attribute	Value
Issuer	commonName	Fina Root CA
	organizationName	Financijska agencija
	countryName	HR
Validity	notBefore	Time of issuance of the certificate
	notAfter	Time of issuance of the certificate + 10 years
Subject	commonName	Fina RDC 2020
	organizationName	Financijska agencija
	countryName	HR
SHA-1 fingerprint: 46:d5:d3:e3:76:59:c9:e2:5b:6a:56:78:c7:82:5e:43:4e:53:66:c3		
SHA-256 fingerprint: 41:40:b7:06:29:fd:a4:b8:a3:6f:d5:3f:b0:aa:53:23:71:57:86:99:31:b8:b2:30:8f:d0:5d:f3:ff:7d:78:ab		

Table 1.3 Basic data on Fina RDC 2020 CA certificate

1.3.1.3 Fina RDC 2015 CA

The Certification Authority within Fina PKI that ceases issuing certificates for website authentication shall be Fina RDC 2015.

Basic data on Fina RDC 2015 CA-certificate are provided in Table 1.4.

Field	Attribute	Value
Issuer	commonName	Fina Root CA
	organizationName	Financial Agency
	countryName	HR
Validity	notBefore	Time of issuance of the certificate
	notAfter	Time of issuance of the certificate + 10 years
Subject	commonName	Fina RDC 2015
	organizationName	Financial Agency
	countryName	HR
SHA-1 fingerprint: d8:86:43:90:c7:6c:9b:71:f0:40:4f:f3:76:fc:38:fd:73:78:7d:08		
SHA-256 fingerprint: 85:7b:fc:e4:3b:1b:b4:60:1f:f4:54:3b:46:d3:fb:2e:21:3b:f9:b4:fe:eb:6f:13:be:9e:f4:5c:04:ff:6f:8b		

Table 1.4 Basic data on Fina RDC 2015 CA-certificate

Fina RDC 2015 CA-certificate shall be available on the web address listed in Section 6.1.4 herein.

1.3.2 Registration authorities

Subscriber registration for issuance of Subscriber`s Certificates under the scope of this document shall be performed by Fina Registration Authorities.

Fina RA Network is comprised of Local Registration Authorities (hereinafter referred to as: "Fina LRA") in Fina's business network and the Central Fina RA. Subscriber registration with Fina RA Network shall be carried out by Fina LRA together with the Central Fina RA.

Registration in Fina RA Network shall be conducted by authorized persons who have been assigned the trusted role of the Registration Officer and by authorized persons who have been assigned the role of the Validation Officer.

Fina shall not allow a delegated Third Party to perform registration or domain validation tasks described in Section 3.2.2.3 herein for issuing of *SSL certificate level 2 (OVCP)* certificates.

Fina LRA offices that perform registration for issuing of *SSL certificate level 2 (OVCP)* certificates shall be located only in Fina's premises. RA Officers shall be only employees of Fina.

Registration tasks in Fina RA Network shall be coordinated by the Central Fina RA.

1.3.3 Subscribers

A Subscriber shall be a legal person with registered office location in the Republic of Croatia who undertook contractual obligations of a Subscriber by concluding an agreement with Fina as the Trust Service Provider.

In order to use a certification service, Subscribers shall complete the process of submitting their applications and registering, as well as accept Subscriber obligations and responsibilities referred to in Section 9.6.3 herein. Subscribers shall conclude the Subscriber Agreement with Fina.

1.3.3.1 Certification Subjects

The subject of certification shall be the web server identified by the Domain Name or IP address under control and operation of the Subscriber.

1.3.4 Relying parties

Relying Parties shall be natural persons or Legal persons who rely on the trust service. The certificate shall enable the Relying Party to check Subject’s identity.

1.3.5 Other participants

No stipulations.

1.4 Certificate usage

Based on certificate type purpose, permitted use and use restrictions, the Relying Party shall decide whether a certain certificate is adequate and reliable for use and acceptance. The Relying Party shall be responsible for accepting and acting in reasonable reliance on the certificate which has a certain security level.

Security levels of certificates are described in Table 1.4. The table shows the pertaining scope of application and recommended financial limit for individual security levels.

Security level	Scope of Application	Recommended financial limit
Medium	This level shall be adequate for transactions of medium value and in environments in which the potential certificate misuse may cause medium damage or where the certificate misuse risk is medium.	up to 10,617.82 €

Table 1.5 Security level of certificate

1.4.1 Appropriate certificate uses

Certificates listed in Table 1.1 herein and the pertaining private keys shall be used only for website authentication.

1.4.2 Prohibited certificate uses

Apart from website authentication, all other uses of certificates listed in Table 1.1 and their private keys shall not be allowed.

1.5 Policy administration

1.5.1 Organization administering the document

Fina shall remain authorized and responsible for creation and update of this Certificate Policy document.

Authorized persons in Fina's organizational units participating in the development, maintenance, implementation and approval of policies and practices that are applied in provision of trust services in Fine PKI hereinafter are called collectively the Fina PMA.

Amendments and updates of this Certificate Policy document are performed and based on internal proposals and requirements for harmonization with the legislation and the relevant standards.

1.5.2 Contact person

Contact details for administration and content of this Certificate Policy are given below.

Mailing address:

Fina
Digital Solutions Division
e-Business Policies Management Office
Koturaška cesta 43
10000 Zagreb
Croatia

Telephone: +385-1-6128-171
Telefax: +385-1-6304-081
E-mail: pma@fina.hr

1.5.3 Person determining CPS suitability for the policy

Suitability of CPS_{WSA} [25] for this Certificate Policy shall be determined by Fina PMA.

1.5.4 CPS approval procedures

The CPS_{WSA} [25] document approval procedure by which the document's suitability for the Certificate Policy is confirmed shall be described in the CPS_{WSA} [25] document.

1.6 Definitions and acronyms

1.6.1 Definitions

TERM	MEANING
Activation Data	Confidential data necessary to access or activate the cryptographic module. Activation data may be a PIN, password or electronic key which the person knows or possesses.
Advanced Electronic Signature	Electronic signature that meets the following requirements: (a) it is uniquely linked to the Signatory, (b) it is capable of identifying the Signatory, (c) it is created using electronic signature creation data that the Signatory can, with a high level of confidence, use under its exclusive control, and (d) it is linked to the signed data in such a way that any subsequent change in the data is detectable.
Application Software Supplier	A supplier of Internet browser software or other relying-party application software that displays or uses certificates and incorporates root certificates.
Authentication	An electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.
Business Entity	1. Legal persons, such as ▪ companies, ▪ credit and financial institutions, ▪ public and private institutions, ▪ associations with legal personality, ▪ non-profit and non-government organizations with legal personality, ▪ funds with legal personality, ▪ local and regional self-government units (municipalities, towns and counties) etc. 2. Public authorities, such as ▪ state authorities, ▪ state administration bodies, ▪ state agencies etc. 3. Natural persons - citizens with a registered business, such as ▪ trades people, ▪ attorneys, ▪ notaries public etc.

TERM	MEANING
Central Fina RA	Central registration office that is primarily in charge of coordinating the entire Fina RA Network, but may also directly perform Subscriber registration.
Certificate	See the term "Public Key Certificate".
Certificate for electronic signature	Electronic attestation that connects the electronic signature validation data with the natural person and confirms at least the name or pseudonym of that person.
Certificate for website authentication	An attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued.
Certificate Policy (CP)	A named set of rules which indicates the certificate applicability on a certain group and/or class of applications with common security requirements.
Certificate Revocation	Permanent termination of the certificate's validity before the expiry date indicated in the certificate.
Certificate Revocation List (CRL)	Signed list indicating a set of certificates that are no longer considered valid by the certificate issuer.
Certificate Transparency	An open framework for monitoring and auditing certificates for website authentication.
Certificate Validation	Process of verifying and confirming that a certificate is valid.
Certification Authority (CA)	Authority trusted by one or more users to create and assign public-key certificates. A Certification Authority may be: 1. A trust service provider creating and assigning public-key certificates, or 2. A technical certificate-issuing service used by the certification service provider creating and assigning public-key certificates.
Certification Practice Statement (CPS)	Statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates.
Certification Services	Services of issuance and lifecycle management of certificates.
Certification System	System of IT products and components organised for providing certification services.

TERM	MEANING
Conformity Assessment Body	A body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides.
Coordinated Universal Time (UTC)	Second-based time scale as defined by ITU-R Recommendation TF.460-5. For most practical applications, UTC is equivalent to mean solar time of the Prime Meridian (0°). More precisely, UTC is a compromise between the very stable atomic time (fr. *Temps Atomique International* - TAI) and solar time derived from irregular Earth's rotation (in relation to the agreed Greenwich mean sidereal time (GMST).
Cryptographic Module	Software or device of a certain security level which: ▪ generates a key pair, and/or ▪ protects cryptographic information, and/or ▪ performs cryptographic functions.
CT log	Public network service that provides an append-only, cryptographically-verifiable record of all the valid TLS certificates being submitted.
Custodian	A natural person employed at the Legal person or associated in another way with the Legal person, and who has been authorised by the same Legal person to submit applications for the issuance of business certificates for systems and devices, for the renewal, revocation, suspension and reactivation of certificates, and to accept certificates and corresponding activation data. The Custodian shall be authorised to submit requests for lifecycle management of certificates The Custodian shall be the contact person for managing the life cycle of the Subject certificate.
Distinguished Name (DN)	A unique name of the Subject entered in the certificate. The distinguished name uniquely identifies the Subject to whom the certificate is issued and it is unique within one CA.
Electronic Signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.
Electronic Signature Creation Data	Unique data which is used by the signatory to create an electronic signature.
Electronic Time Stamp	Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.
Fina LRA	Local Registration Authority in Fina business network.

TERM	MEANING
Fina PKI	Public Key Infrastructure (PKI) established in Fina which is intended for providing certification services to natural persons (citizens), business entities and state administration authorities, and which operates as the Trusted Third Party.
Fina RA Network	Fina Registration Authority Network consists of the Central Fina RA and Fina LRA.
High Risk Certificate Request	A Request that the Fina flags for additional scrutiny by reference to internal criteria and databases maintained by the Fina, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, using its own risk-mitigation criteria.
Internal Name	A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.
Internationalized domain name	Internet domain name that contains at least one label that is displayed in software applications, in whole or in part, in a language-specific script or alphabet,
Key Pair	Two uniquely linked cryptographic keys, one of which is a private key and another is a public key.
Legal Representative	A person legally authorised to represent the Subscriber which is a Legal person.
OVCP certificates	A certificate which includes verified information on the identity of the organisation related to the subject.
Policy Management Authority (PMA)	Body with final authority and responsibility for specifying and approving the Certificate Policy.
Precertificate	Data object constructed from the certificate to be issued by adding a special critical poison extension to the Subscriber's TBSCertificate. Precertificate, as described in IETF RFC 6962 [22], is not considered to be a "certificate" subject to the requirements of IETF RFC 5280 [19].
Private Key	In a public key cryptographic system, that key of an entity's key pair which is known only by that entity.
Public Directory	IT system which is used for online publication of information concerning certificates, including information on certificate revocation.
Public Key	In a public key cryptographic system, that key of an entity's key pair which is publicly known.

TERM	MEANING
Public Key Certificate	Public key of an entity, together with some other information, rendered unforgeable by digital signature with the private key of the certification authority which issued it.
Public Key Infrastructure (PKI)	Infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.
Qualified Auditor	Natural or legal person that meets the requirements stated in the document Baseline Requirements [23], published by the CA/Browser Forum.
Qualified CT log	CT log service that operates in accordance with Application Software Supplier's policy.
Qualified Trust Service Provider	A trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body.
Registration Authority (RA)	Authority responsible for identification and authentication of certification subjects, as well as other persons or organisations.
Registration Officer	Person responsible for data confirmation necessary for certificate issuance and authorisation of application for certificate issuance.
Regular Certificate Renewal	Certificate renewal in Fina PKI means issuance of a new certificate the parameters of which are the same as the parameters of the certificate to which the application relates, but with a new public key, new certificate serial number, new operational period and new signature of the same CA, and is carried out in the defined period before the expiry of certificate validity.
Relying Party	Natural or legal person that relies upon an electronic identification or a trust service.
Reserved IP address	IPv4 or IPv6 address which IANA marked as reserved.
Revocation Officer	Person responsible for the change of the certificate's operative status.
Root CA	Certification authority which is at the highest level within trust service providers domain and which is used to sign subordinate CA(s)
Root CA certificate	CA Certificate that the Root CA issued to itself.
Secure Cryptographic Device	Device which holds the Subscriber's private key protects this key against compromise and performs signing or decryption functions on behalf of the user.
Signatory	A natural person who creates an electronic signature.

TERM	MEANING
Signature verification	Process of checking the cryptographic value of a signature using signature verification data.
Signature Verification Data	Data, such as codes and public cryptographic keys used for the purpose of signature verification.
State Administration Body (TDU)	State authority body responsible for performing state administration tasks in the administrative domain of its competence. State administration bodies include ministries, state offices, administrative organizations and county state administration offices or other state administration bodies established by the applicable law in force.
Subject	Entity identified in a certificate as the holder of the private key associated to the public key given in the certificate.
Subscriber	Legal or natural person bound by agreement with a trust service provider to any Subscriber obligations.
Trust Service Provider	A natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider.
Trusted list	List that provides information about the status and the status history of the trust services from trust service providers regarding compliance with the applicable requirements and the relevant provisions of the applicable legislation.
Trusted Roles	Roles which are responsible for safe operation of the trust service provider. Trusted Roles and the corresponding responsibilities shall be clearly described by the Trust Service Provider in the employee's job description.
Validation	Process of verifying and confirming that an electronic signature or a seal is valid.
Validation data	Data used for electronic signature or electronic seal validation.
Validation Specialist	Person responsible for data verification related to certificate issuance according to CA/Browser Forum BRG [23] document.
Wildcard Certificate	A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.
Wildcard Domain Name	A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name (FQDN).

Table 1.6 Definitions

1.6.2 Abbreviations

ABBREVIATION	FULL NAME
CA	*Certification Authority*
CAA	*Certification Authority Authorization*
CAB Forum	*CA/Browser Forum*
CP	*Certificate Policy*
CP_{WSA}	*Certificate Policy for Certificates for Website Authentication*
CPS	*Certification Practice Statement*
CPS_{WSA}	*Certification Practice Statement for certificates for website authentication*
CSPRNG	*Cryptographically Secure Pseudo-Random Number Generator*
CRL	*Certificate Revocation List*
CT	Certificate Transparency
DN	*Distinguished Name*
DNS	*Domain Name System*
FQDN	*Fully Qualified Domain Name*
IDN	*Internationalized Domain Name*
LDAP	*Lightweight Directory Access Protocol*
LRA	*Local Registration Authority*
OCSP	*Online Certificate Status Protocol*
OVCP	*Organizational Validation Certificate Policy*
OID	*Object Identifier*
PKI	*Public Key Infrastructure*
PMA	*Policy Management Authority*
RA	*Registration Authority*
SCT	Signed Certificate Timestamp
TDU	*State Administration Body (Bodies)*
UTC	*Coordinated Universal Time*

Table 1.7 Abbreviations

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Fina PKI repository shall be managed by Fina as a Certification Service Provider. Fina shall be responsible for the work of and publication of documents and information on Fina PKI repository.

Fina shall ensure repository availability 24 hours a day, 7 days a week.

2.2 Publication of certification information

Fina PKI repository shall publish documents and information on certification services provision.

The repository shall consist of a part available on web pages and a part available via public LDAP directory.

The following shall be published on Fina PKI repository web pages:

- Certificate Policy documents,
- Certification Practice Statement,
- Terms and Conditions and PKI disclosure statement,
- Certification services price list,
- Subscriber forms,
- Fina Root CA certificate, Fina RDC 2020 CA and Fina RDC 2015 CA certificates,
- CRL issued by Fina Root CA and subordinate Fina RDC 2020 and Fina RDC 2015 CAs,
- Certificates for checking and testing,
- Notifications to Subscribers and Relying Parties, related to Certification Service Provision,
- External compliance control results,
- Summary of the report of external compliance audits,
- Other information related to Fina RDC 2020 and Fina RDC 2015 CA operation.

The partitioned CRL issued by Fina RDC 2020 and Fina RDC 2015 CAs shall be published on the web server of the repository.

Each issued certificate may be retrieved from Fina PKI repository web pages.

Fina PKI repository web pages are available on the web-site https://www.fina.hr/finadigicert in Croatian and https://www.fina.hr/en/digital-certificates in English.

Subscriber's Certificates, certificates of the subordinate Fina RDC 2020 and Fina RDC 2015 CAs and CRLs issued by Fina RDC 2020 or Fina RDC 2015 CAs shall be available in the

Fina PKI repository section, available through the public LDAP directory. The address of the LDAP directory is ldap://rdc-ldap2.fina.hr.

Information on the revocation status of Subscriber`s Certificates shall be available via Fina OCSP service. The address of Fina OCSP service is http://ocsp.fina.hr.

Confidential data shall not be disclosed in the Fina PKI repository.

Fina publishes precertificate on qualified CT log services if the Legal Representative has given consent.

2.3 Time or frequency of publication

Fina shall maintain, update, approve, publish and apply the Certificate Policy and the Certification Practice Statement [25] at least once a year, or in case of exceptional request for change. Other Fina PKI documents and other relevant information shall be published when required, and are subject to authorisation.

Certificates shall be available on the FINA PKI web pages as soon as they are issued.

The frequency of publishing CRLs for certificates issued by Fina RDC 2020 and Fina RDC 2015 CAs is defined in the Section 4.9.7 herein.

Online information on issued certificates status is available via Fina OCSP service described in Section 4.9.9 herein.

2.4 Access controls on repositories

Documents and information published in the Fina PKI repository shall be free and publicly available for reading.

Fina shall establish access control over the repository with the aim of preventing unauthorised adding, changing or deleting information and protecting its integrity and authenticity.

Fina authorised persons shall have the authorisation to add, change or delete information in the Fina PKI repository.

3 SUBJECT IDENTIFICATION AND AUTHENTICATION

3.1 Naming

Naming, the structure and use of names in certificates shall be in accordance with the RFC 5280 [19], ETSI EN 319 412 [12] and [13] and CA/Browser Forum BRG [23]. CAs names shall be both meaningful and descriptive.

3.1.1 Types of names

Subject information and the Legal person registered office location shall be entered in each certificate. Subject information entered into the certificate shall refer to the Subject's authentic name. The *Subject* field shall be in line with ETF RFC 5280 [19] document.

The *Subjec*t field and the *Subject Alternative Name* certificate extension in OVCP certificates shall contain the Fully Qualified Domain Name (hereinafter referred to as: "FQDN"), Wildcard Domain Name or server IP address.

3.1.2 Need for names to be meaningful

The following rules shall apply to the attributes in the Subject filed of Fina PKI:

- The fully registered name of the Legal person has to be the same as that listed in the official competent national registers,
- the Subscriber's registered office location has to be the same as that listed in the official competent national registers,
- the FQDN or IP address have to comply with the specifications of the certificate application.

Subject Alternative Name certificate extension contains FQDN or server IP address.

3.1.3 Anonymity or pseudonymity of subscribers

Anonymity or pseudonymity of Subscribers shall not be supported.

3.1.4 Rules for interpreting various name forms

The interpretation of the name form in the Subject field of Fina PKI according to X.520 standard shall be carried out in the following way:

- Serial Number

The value of the attribute *Serial Number* in the *Subject* field shall guarantee the uniqueness of individual Subjects. The value of this attribute shall also guarantee the uniqueness of the *Subject* field in certificates within Fina PKI production hierarchy founded on Fina Root CA.

In OVCP certificates the Serial Number field contains the identifier of the Legal person structured in a way that shows the meaning of its content: "VAT", a two-letter ISO country code of the Legal person registered office location, „-„, the Legal person unique identifier (OIB) and by dot separated Fina's internal designation, for example: VATHR-12345678901.1. For business entities in the Republic of Croatia the Legal person unique identifier is OIB.

- Common Name

In OVCP certificates this attribute contains the FQDN, Wildcard Domain Name or server IP address.

In the *Common Name* attribute only one of the values entered in the *Subject Alternative Name* certificate extension (FQDN or Wildcard Domain Name or IP address of the server) which is controlled by the Applicant or which the Applicant has the sole right to use.

The FQDN or IP address also has to be included in the *Subject Alternative Name* certificate extension of OVCP certificates.

- Organization Name

The *organizationName* attribute contains full registered Abbreviated name of the Legal person.

- Locality

The *Locality Name* attribute contains the name of the Legal person registered office location.

- Country

The *Country* attribute contains a two-letter ISO code for Croatia.

- Subject Alternative Name

This certificate extension contains at least one of the following data items and only one of these items is entered in the Common Name attribute:

- FQDN,
- Wildcard Domain Name,
- server IP address.

Fina does not support the use of internationalized domain names (IDNs).

The *Subject Alternative Name* certificate extension does not contain the reserved IP address or internal name.

The *Subject Alternative Name* extension does not contain the underscore ("_") character

3.1.5 Uniqueness of names

The distinguished name of the subject shall be unique within the Fina PKI production hierarchy based on Fina Root CA. The uniqueness of the distinguished name shall be ensured by the *Serial Number* and *Common Name* attribute values in the *Subject* field.

3.1.6 Recognition, authentication, and role of trademarks

In case the Subscriber applies for issuance of a certificate containing a trademark, Fina RA network shall check that the trademark is used legitimately, and in case of a founded complaint, Fina has the right to revoke such a certificate.

In case the Subscriber applies for issuance of a certificate containing a trademark, Fina RA may ask for evidence of registering the trademark with the competent authority.

3.2 Initial identity validation

Through the Fina RA network, Fina shall collect natural persons' personal data and Legal persons' data for the sole purpose of registration for certificate issuance.

Through the Fina RA network, Fina shall carry out the verification of data from the certificate application by comparing it to the data from the delivered or from the relevant and competent source independently collected in accordance with the applicable national laws and regulations.

3.2.1 Method to prove possession of private key

A private key matching the public key delivered to Fina RDC 2020 CA for the issuance of a certificate shall be generated by the Custodian, as described in Section 6.1.1.2 herein.

Fina shall use a technological process and the method of requesting a certificate to check whether the Custodian possesses or controls the private key linked to the public key which is delivered to Fina RDC 2020 CA in a protected manner for the purpose of certificate creation.

3.2.2 Authentication of organization and domain identity

3.2.2.1 Authentication of organization identity

Authentication and verification of organization identity shall be done by checking the following:

- Legal person's registered name,
- Legal person's legal existence,
- Registration with the competent registry,
- Identification number in the competent registry,
- Legal person's OIB,
- Address of the Legal person's registered office.

Legal person is responsible for the accuracy and correctness of submitted data.

3.2.2.2 Verification of Country Related to the Subject

Fina shall carry out the verification of the association between the country that will be entered in *countryName* field in certificate and the Subject that will be entered in certificate. Country listed in the *countryName* attribute of the Subject field shall be Republic of Croatia.

This verification shall be performed in accordance with the methods specified in the CA/Browser Forum BRG [23] document.

3.2.2.3 Validation of Domain Authorization or Control

For every FQDN and Wildcard Domain Name listed in certificate application Fina shall verify the property or right to use the domain name by the Legal person submitting the certificate application.

This verification shall be performed by conducting a documented procedure and in accordance with the methods specified in the CA/Browser Forum BRG [23] document. Domain Contact shall be obtained by implementing appropriate methods to reduce the risk of compromise.

3.2.2.4 Authentication for an IP Address

For each IP Address listed in certificate application Fina shall verify, as of the date the certificate was issued, the right to use and control the IP Address by the Legal person submitting the certificate application.

This verification shall be done in accordance with the methods specified in the CA/Browser Forum BRG [23] document.

3.2.3 Authentication of individual identity

Initial Custodian identification and authentication shall be carried out through direct or indirect identification procedures.

For the purpose of initial natural person's identification and authentication, Fina shall collect and verify the following personal data:

- Name and surname,
- Date, place and country of birth,
- OIB (if it was assigned),
- The data contained in identification document referred to in Section 3.2.3.3 herein,
- Contact data.

For the purpose of issuing a certificate, Fina also collects evidence of the Custodian's affiliation with the Legal person.

3.2.3.1 Direct identification procedure

The direct identification procedure for natural persons shall be performed in their physical presence, based on a valid identification document described in Section 3.2.3.3 herein.

3.2.3.2 Indirect identification procedure

The indirect identification procedure Fina shall perform in the manner assuring an appropriate security level of a natural person's identification.

a) by validation of a qualified or advanced electronic signature based on qualified certificate, or
b) by verifying data from the copies of two different identification documents defined in Section 3.2.3.3 herein

3.2.3.3 Eligible types of identification documents

In the direct identification procedure, natural persons shall prove their identity with a valid ID card, passport or driving licence.

Natural persons who do not possess an ID card or passport issued in the Republic of Croatia shall prove their identity with a valid identification document for entering the Republic of Croatia.

3.2.4 Non-verified subscriber information

All the Legal person's data, domain and IP addresses that are entered in the certificate shall be previously verified by Fina. The Subscriber shall declare that all the information specified in the certification application is correct and complete.

3.2.5 Validation of authority

Before issuing a certificate, Fina shall conduct identity validation of the Legal Representative by verifying the data contained in the documentation provided for the purpose of legal personality determination and identification under Section 3.2.2 and by comparing the data from the copy of a valid identification document of the Legal Representative.

Proxy identification shall be effected on the same way as the Legal Representative identity validation.

Determining the authenticity of the certificate application shall be carried out by determining whether the Legal Representative or his proxy, signed the application by comparing the signature on the application with the signature on the submitted copy of his identification document.

In the case that the application for the issuance of the certificate is submitted in electronic form, the authenticity of the application for the issuance of the certificate shall be determined by validating the electronic signatures on the application in accordance with Section 4.1.2.1 herein.

3.2.6 Criteria for interoperation

Fina shall not allow cross-certification.

3.3 Identification and authentication for re-key requests

Fina shall carry out the procedures of identification and authentication of the Applicant for the following purposes:

- Routine certificate renewal,
- Issuing certificates upon expiration,
- Reissuing certificates upon revocation and
- Certificate recovery.

Upon renewal or reissuing of the certificate, the current terms and conditions for the provision of certification services referred to in 9.17 herein shall be communicated to the Custodian who accepts them prior to certificate issuance.

3.3.1 Identification and authentication for routine re-key

Regular certificate renewal shall be done near the end of the certificate life.

A certificate shall be regularly renewed if the conditions from Section 4.7.1 herein have been met.

Identification and authentication of the Custodian shall be carried out in accordance with Section 3.2.3 herein.

Identification and authentication of the Legal person shall be carried out in through verification of the data from the submitted certificate application with provided and collected data and through enquiries to the national OIB system.

3.3.2 Identification and authentication for re-key after revocation

Identification and authentication of the Applicant for certificate reissuing following its revocation shall be done in accordance with the initial identity validation procedure from Section 3.2 herein.

3.3.3 Identification and authentication for re-key after expiry

Identification and authentication of the Applicant for certificate reissuing following its expiry shall be done in accordance with the initial identity validation procedure from Section 3.2 herein.

3.3.4 Identification and authentication for certificate recovery

Certificate recovery shall be carried out for the reasons and under conditions specified in Section 4.7.1 herein.

Identification and authentication of the Applicant for certificate recovery shall be done in accordance with the initial identity validation procedure from Section 3.2 herein.

3.4 Identification and authentication for revocation request

Fina shall carry out certificate revocation based on submitted requests. Authentication of the Applicant shall be done so as to establish the identity of the natural person acting as the Applicant and whether that person is authorised to submit the request.

Fina shall carry out identification and authentication of the Applicant submitting the certificate revocation request depending on the form of delivery of the request:

- Submitting the revocation request in person to a registration authority of the Fina RA Network

  Identification and authentication shall be carried out by means of direct identification procedure of the Applicant based on the Applicant's identification document or by comparing Applicant's signature and data on request with signature and data collected during the registration.

- Submitting the revocation request by mail or by delivery service

  Identification and authentication shall be carried out at the registration authority of the Fina RA Network by comparing the Applicant's signature and data on the request with signature and data collected during the registration.

- Electronic delivery of the revocation request to the e-mail address

  Applicant's identification and authentication shall be carried out by verifying and validating of request signed at least with electronic signature of advanced level or sealed at least with electronic seal of advanced level.

- Submitting the revocation request by phone

  The Applicant's identification is carried out by applicant presenting himself with his / her name and surname and by specifying the Legal person's name. Authentication of the Applicant is carried out by proving his knowledge of the password for revocation of the certificate.

Fina shall identify and authenticate of the person submitting Certificate Problem Report in the same manner as when submitting a certificate revocation request. If this is not feasible, Fina shall perform identification and authentication in other appropriate ways.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

A certificate application shall be submitted by business entities, unless otherwise provided for in laws and acts adopted thereon.

4.1.2 Enrolment process and responsibilities

For certificate issuance, a certificate application shall be submitted.

Prior to initial issuance of certificate, the Subscriber shall conclude a Subscriber Agreement with Fina.

4.1.2.1 Certificate Application Process

Certificate application shall be submitted by the Custodian.

Certificate application shall be signed by the Custodian and the Legal person's Legal Representative.

By signing the certificate application, the Legal Representative shall confirm the Custodian's authorisation for certificate application.

If the certificate application is submitted in the electronic form, it shall be signed with a qualified electronic signature, or an advanced electronic signature based on qualified certificate issued by Qualified Trust Service Provider or based on certificate issued by Fina CA. Registration Officer in Fina RA Network shall properly validate all electronic signatures on the application and verify the application data.

4.1.2.2 Obligations and Responsibilities in the Certificate Application Process

Subscribers shall conclude a Subscriber Agreement with Fina whereby they shall accept CPS_{WSA} [25] document, this Certificate Policy and terms and conditions of the certification services provision.

Prior to the provision of certification services to a state administration body (TDU) that TDU shall enter into a business relationship with Fina by concluding a specific Certification Service Agreement.

In the certificate application process the Applicants shall submit the certificate application completed accurately and entirely as described in Section 4.1.2.1 herein, and the documentation enclosed or provided shall be accurate and complete, as well as valid at the time the certificate application is submitted.

Subscribers' obligations and responsibilities are given in Section 9.6.3 herein.

The Fina RA Network obligations and responsibilities are given in Section 9.6.2 herein.

The obligations and responsibilities of Fina, as a Trust Service Provider, are given in Section 9.6.1 herein.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The Subscriber's identification and authentication shall be carried out in accordance with Section 3 herein.

Fina RA Network shall not reuse the documents and data provided in Section 3.2 herein to verify certificate information, or reuse previous validations themselves.

Fina shall develop, maintain and implement the documented procedure that identifies and requires additional verification activity for High Risk Certificate Requests prior to the approval of Subscriber's Certificate, as reasonably necessary to ensure that such requests are properly verified.

4.2.2 Approval or rejection of certificate applications

Registration Officer in the Fina RA Network shall check the information in the documents attached by the Applicant and shall confirm the accuracy and integrity of information related to the natural person and Legal person from the certificate application or rejects the application in case of unsuccessful identification or inaccurate submitted information.

The Registration Officer of the Central Fina RA shall carry out the documentation validation procedure which refers to checking Legal person ownership or control over FQDN or IP address specified in the certificate application.

The Central Fina RA shall carry out checks for a CAA record for each *dNSName* in the *subjectAltName* extension of the Certificate to be issued, according to the procedure in RFC 6844 – DNS Certification Authority Authorization (CAA) Resource Record [20], and shall follow the processing instructions for any records found.

The Fina CA's CAA identifying domain shall be "fina.hr".

Should the Fina RA Network reject the certificate application, it shall inform the Applicant therein and provide reasons for rejection.

4.2.3 Time to process certificate applications

In normal circumstances, the certificate application processing time shall be up to five working days from the receipt of the application by the Fina RA Network.

4.3 Certificate issuance

Fina RDC 2020 CA shall issue the certificate after all data verification process has been performed, application approved and the certificate has been accepted by the Custodian. Certificate issuance is carried out in secure manner to ensure the authenticity of the certificate. For this reason, Fina has implemented measures to prevent forgery of certificates.

4.3.1 CA actions during certificate issuance

During certificate issuance process, Fina RDC 2020 CA shall:

- check if the application request is approved by the Registration Officer and Validation Officer,
- generate the Subject's key pair for certificates in line with Section 6.1.1.2 herein,
- in case the Legal Representative has given consent Fina RDC 2020 CA logs the precertificate in qualified CT log services, obtains the SCTs from those log services and append them in Subscriber's Certificate to be issued,
- issue the requested certificate for Subject's public key delivered in line with Section 6.1.3 herein,
- make the certificate available to the Custodian for the purpose of its retrieving,
- make the certificate publicly available in the Fina PKI repository.

Fina shall be able to revoke Precertificate and the corresponding Subscriber's Certificate, even if the Subscriber's Certificate has not been issued. The revocation status information shall be available through CRL and OCSP service.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The Custodian shall retrieve the certificate online and shall be notified of the certificate issuance during this online process of retrieving the certificate.

4.4 Certificate acceptance

Certificate acceptance by the Custodian shall be a prerequisite for issuing and using the certificate.

By accepting the certificate, the Custodian shall accept that all the information that will be held in the certificate is correct at the moment of its acceptance.

4.4.1 Conduct constituting certificate acceptance

The Custodian shall conduct the checking of the contents of the certificate immediately prior to the issuance of the certificate.

The Custodian shall accept the certificate by confirming the certificate acceptance on the CMS interface screen.

After acceptance of the certificate, Fina shell issue the requested certificate to the Custodian.

Fina applies security measures to ensure that the issued certificate contains the same information that the Custodian accepted before issuance of that certificate.

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 shall not issue the certificate relating to this request.

Fina shall enable submitting of a new certificate application to the Custodian in which, if necessary, the corrected data shall be entered in relation to the previous certificate application.

4.4.2 Publication of the certificate by the CA

If the Legal person's Legal Representative, have authorised the public disclosure of the certificate, Fina RDC 2020 CA shall make the precertificate available on qualified CT log services and Subscriber's Certificate in the Fina PKI repository.

The consent for the certificate publication in the Fina PKI repository shall be given when applying for a certificate.

4.4.3 Notification of certificate issuance by the CA to other entities

It is implied that other parties shall be notified of certificate issuance by public disclosure in Fina PKI repository and by public disclosure of corresponding precertificate in qualified CT log services, in accordance with Section 4.4.2 herein.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The Subscriber shall:

- generate key pairs using algorithms stipulated by the ETSI TS 119 312 [16] standardisation document and the length of the keys in accordance with Section 6.1.5 herein,
- use the certificate and the accompanying private key solely for the purposes provided for in this Certificate Policy and in the terms and conditions of certification services provision,
- use the certificate and the accompanying private key in accordance with the laws and other regulations of the Republic of Croatia and in accordance with Sections 1.4.1 and 1.4.2 herein
- use and keep the private key in a manner that shall prevent its unauthorised use,

- use the certificate and the accompanying private key only on servers available through FQDN or IP address specified in the *Subject Alternative Name* certificate extension,
- protect the private key from theft, loss, change, compromise and unauthorised use,
- keep the private key activation data safe, in a protected place separate from the private key,
- notify Fina as the Trust Service Provider and request certificate revocation,
- after the private key has been compromised, immediately cease with its use and the use of the pertaining certificate,
- after becoming aware of the revocation of the certificate or finding out about the compromise of the Fina CA that issued that Subscriber`s Certificate, ensure that the related private key has no longer been used.

4.5.2 Relying party public key and certificate usage

The Relying Party that intends to rely on the certificate issued according to this Certificate Policy is recommended to:

- take care to ensure the appropriate use and limitations of the use of the public key and certificate,
- check the validity period of all the certificates in the certificate chain,
- verify the revocation status of certificate using current revocation status information.

4.6 Certificate renewal

Fina does not perform certificate renewal retaining the public key from the existing certificate.

4.7 Certificate re-key

Fina shall perform a certificate renewal in a way that as part of PKCS#10 request of the Subscriber whose certificate is about to expire, shall obtain the public key and shall issue a new certificate for the received public key.

In PKCS#10 request, the Subscriber shall submit a public key from a newly generated key pair that meets the requirements of Sections 6.1.5 and 6.1.6 herein.

Upon identifying and authenticating the Applicant for:

- routine certificate renewal,
- certificate issuance after expiry,
- certificate re-issuance after revocation, and
- certificate recovery

Fina shall issue a certificate whose parameters are equal to the parameters of the certificate to which the request refers, but with a new certificate serial number, new validity period, new public key and a new signature created by Fina RDC 2020 CA.

4.7.1 Circumstance for certificate re-key

Routine certificate renewal with the generation of a new key pair shall be carried out if the Subscriber's Certificate is expiring soon, and the Subscriber intends to continue using the service. The certificate shall be renewed in this manner if all of the following terms and conditions have been met:

- the validity of the certificate has not expired and the certificate shall expire in less than 45 days,
- the certificate has not been revoked,
- Subject data and other attributes contained in the certificate are accurate and complete at the moment of the routine certificate renewal request.

Certificate recovery shall be carried out in case of deletion or destruction of the Subscriber's private key, or when the Subscriber, due to some other reason, is not able to use the private key connected to the public key in the certificate, and shall be carried out before the onset of deadlines for certificate renewal.

Certificate issuance after expiry shall be carried out if the Subscriber's Certificate has expired, and the Subscriber intends to continue using the service. Certificate issuance after expiry shall not be considered renewal of an existent expired certificate.

A prerequisite for such certificate issuance shall be that the Subscriber data contained in the certificate has not been modified.

4.7.2 Who may request certification of a new public key

Request for the renewal, recovery or issuance of a certificate after its expiry may be submitted by the Custodian or Legal Representative.

4.7.3 Processing certificate re-keying requests

Certificate renewal request shall be submitted in paper or electronic form, in accordance with 4.1.2.1 herein, and the identification and authentication of the identity of natural persons and the legal person referred to in the request shall be conducted pursuant to Section 3.3.1 herein. The Registration Officer shall check the details in the request and shall confirm the accuracy and integrity of information in the request. The approval or rejection of request s is carried out in the central RA Network office.

Upon verifying the authenticity and validity of the request, Fina RDC 2020 CA shall issue a certificate in accordance with Section 4.3.1 herein.

4.7.4 Notification of new certificate issuance to subscriber

Fina shall notify the Custodian of the upcoming certificate expiry and invite for a regular renewal of the certificate.

Notifying the Custodian of the certificate renewal shall be done in accordance with Section 4.3.2 herein.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Conduct constituting acceptance of the certificate with new key pair generation issued in accordance to Section 4.7.1 shall be carried out in accordance with Section 4.4.1 herein.

4.7.6 Publication of the re-keyed certificate by the CA

Publication of a certificate with new key pair generation issued in accordance with Section 4.7.1 shall be carried out in accordance with Section 4.4.2 herein.

4.7.7 Notification of certificate issuance by the CA to other entities

Notifying other parties of a certificate with new key pair generation issued in accordance with Section 4.7.1 shall be carried out in accordance with Section 4.4.3 herein.

4.8 Certificate modification

Legal persons shall notify Fina of the modification of data contained in the certificate and request certificate data modification.

Fina shall carry out certificate data modification only during validity period of the certificate that has not been revoked or suspended.

4.8.1 Circumstance for certificate modification

Reasons for modifications within OVCP certificates can be modifications referring to the Subject:

- change of FQDN or IP address,
- change of Legal person name or registered office.

The reason for modification within the certificate may be modifications to the certificate profiles, as well as modifications to certification systems that affect the content of certificate fields.

4.8.2 Who may request certificate modification

Certificate modifications may be requested by the Custodian or Legal Representative.

4.8.3 Processing certificate modification requests

The certificate modification request shall be submitted to the Fina RA Network office. The Applicant's identification and authentication shall be carried out in accordance with the initial identification procedure referred to in Section 3.2 herein. Request processing and certificate issuance shall be carried out in accordance with Sections 4.2, 4.3 and 4.4 herein.

4.8.4 Notification of new certificate issuance to subscriber

When issuing certificates in the process of certificate modification, notification of Subscribers shall be carried out in accordance with Section 4.3.2 herein.

4.8.5 Conduct constituting acceptance of modified certificate

Conduct constituting modified certificate acceptance shall be carried out in accordance with Section 4.4.1 herein.

4.8.6 Publication of the modified certificate by the CA

Publication of the modified certificate shall be carried out as described in Section 4.4.2 herein.

4.8.7 Notification of certificate issuance by the CA to other entities

Notification of other parties of the modified certificate issuance shall be carried out in the manner described in Section 4.4.3 herein.

4.9 Certificate revocation and suspension

In the following sections the procedures for revoking Subscriber’s Certificates are described.

Procedures for revoking Fina RDC 2020 and Fina RDC 2015 CA certificates are described in 4.9 CP/CPS_{ROOT} [24] document.

4.9.1 Circumstances for revocation

Fina RDC 2020, or Fina RDC 2015 CA shall revoke a *SSL certificate Level 2 (OVCP)* within 24 hours:

- based on submitted request,
- in the event that Custodian or Legal Representative notifies Fina that the original certificate request was not approved by the Subscriber and that Subscriber did not retroactively grant such approval,
- if Fina obtains evidence that the Subscriber's private key corresponding to the public key in the certificate suffered a key compromise or if the private key or activation data are no longer in the sole possession of the Custodian or Legal person,

- in the event Fina is made aware of the demonstrated or confirmed method which can easily be used to calculate the corresponding private key based on the knowledge of the Subscriber's public key,
- in the event that the Custodian or the Legal Representatives report loss or permanent unavailability of the private key corresponding to the certificate,
- if Fina obtains evidence that the validation of domain authorization or control for any FQDN or IP address in the certificate should not be relied upon.

Fina RDC 2020 and Fina RDC 2015 CA shall revoke the Subscriber`s Certificate within planned 24 hours, but no longer than 5 days of receiving the request:

- if the certificate no longer meets the requirements for the type of cryptographic algorithm and the associated key length and does not meet the requirements for generating and verifying the quality of the public key parameters specified herein and in the CA / Browser Forum BRG [23] document,
- in the event that Fina receives evidence that the certificate was misused or receives an official notification on the certificate use for illegal purposes,
- in the event that Fina is made aware that a Subscriber has violated one or more of its obligations under the Subscriber Agreement, Terms of Use, this Certificate Policy or CPS_{WSA} [25] document,
- in the event that Fina is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the certificate is no longer legally permitted,
- if Fina is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN,
- if Fina has knowledge that the certificate has not been issued in accordance with CA/Browser Forum BRG [23] document, this Certificate Policy or CPS_{WSA} [25] document,
- in the event that Fina determines that any of the information appearing in the certificate is inaccurate or misleading,
- in the event that the certificate no longer complies with the Certificate Policy under which it was issued,
- in the event that the revocation is required by this document,
- in the case that Fina is informed about a demonstrated or proven method that compromises the user's private key and is informed about a developed method that can easily calculate a private key from a public key or is informed about the clear evidence that the specific method used to generate the private key was flawed,
- in the event that Fina ceases operations for any reason,
- in the event that for any reason Fina′ doesn’t have the right to issue certificates under CA / Browser Forum BRG [23] document, unless Fina ensures with the competent authorities continuation of the provision of information on the status of revocation of the certificates through CRL or OCSP service,

- in the event that Fina is made aware that technical content or profile of the certificate does not provide an appropriate level of trust to Application Software Suppliers or Relying Parties,
- in the event of termination of the Subscriber Agreement by the Subscriber,
- in cases when this is required by law or other regulations

The reasons for the revoking of the Fina RDC 2020 and Fina RDC 2015 CA certificates are given in Section 4.9.1. of CP/CPS_{ROOT} [24] document.

4.9.2 Who can request revocation

Application for certificate revocation shall be submitted by the Custodian or the Legal person's Legal Representative.

Fina RA Network may file a certificate revocation request.

Fina may revoke a certificate based on an authenticated official notification by a competent body.

Subscribers, Relying Parties, Application Software Suppliers and other third parties may file Certificate Problem Report related to certificate usage to Fina, such as the private key being compromised, certificate misuse, using certificates for illegal purposes, inappropriate use of certificates and other fraudulent actions.

In Section 4.9.1 of the CP/CPS_{ROOT} [24] document it is specified who may request a revocation of the Fina RDC 2020 and Fina RDC 2015 CA certificate.

4.9.3 Procedure for revocation request

Written certificate revocation request shall be submitted in one of the following manners:

- by personal delivery to a registration Fina RA Network office during office hours,
- by mail or courier at the Fina RA Network office address,
- by electronic delivery to the e-mail address.

The certificate revocation request may be submitted also by telephone by calling Fina on the telephone number published in the repository on the web site specified in Section 2.2 herein. This Fina phone number is available from 0 to 24 hours, 7 days a week.

On the basis of an accurately and entirely completed and signed certificate revocation request, or by checking the knowledge of the password for revocation of the certificate that authenticates the applicant in the case of submitting the request by telephone, Fina shall revoke the certificate and notify the Custodian therein, and if applicable, the Legal person with which the Custodian is associated.

In the event that third party filled a certificate revocation request, Fina shall verify the merits of the request.

Certificate Problem Report shall be initially submitted by calling Fina on the phone number that is posted on the repository web pages in Section 2.2.1 herein. This Fina phone number is available from 0 to 24 hours, 7 days a week. If necessary, after making phone call additional necessary information may be submitted by e-mail to address published on repository web pages given in Section 2.2.1 herein.

After reviewing the facts and circumstances, Fina will make a decision regarding the revocation of the certificate.

The procedure for requesting the revocation of the Fina RDC 2020 and Fina RDC 2015 CA certificate is described in Section 4.9.3 of CP/CPS_{ROOT} [24] document.

4.9.4 Revocation request grace period

Applicants requesting certificate revocation referred to in Section 4.9.2 herein shall submit an application for certificate revocation as soon as reasonably practicable from the occurrence of the reason of revocation.

4.9.5 Time within which CA must process the revocation request

Fina performs revocation request immediately after receiving it.

Fina shall within the shortest possible reasonable time, and no later than within the time period which depends on the reason for the revocation, as set out in Section 4.9.1 herein and which is reduced by 60 minutes, make the decision about revocation of the certificate. The time period from the decision to revoke the certificate until the moment that the information about the revocation of the certificate is available to all trusted parties over the new CRL or OCSP response service is maximally 60 minutes.

In the event of processing of Certificate Problem Report, the investigation of the facts and circumstances relating to the report shall be made within a time period of maximally 24 hours, and the time period from the receipt of the report until the moment when the revocation status of the certificate through the new CRL or the OCSP service response is available to all reliable the parties shall not exceed the time limit specified in Section 4.9.1 herein.

4.9.6 Revocation checking requirement for relying parties

Reliance on a revoked certificate can cause personal or business damage to the Relying Party. Therefore, before relying on a certificate, the Relying Party shall check the certificate status with the aim of determining whether it has been revoked in accordance with Sections 4.5.2, 4.9.9 and 4.9.10 herein. If the Relying Party is not able to acquire information on the certificate status at the moment, the Relying Party should not rely on such a certificate.

4.9.7 CRL issuance frequency

CRLs for Subscriber`s Certificates issued by Fina RDC 2020 CA, are issued and signed by Fina RDC 2020 CA.

CRLs for Subscriber's Certificates issued by Fina RDC 2015 CA, are issued and signed by Fina RDC 2015 CA.

CRLs are available via the HTTP web address of the repository server. In accordance with the description from Section 4.10.1 herein, the CRL is also available through the LDAP directory. Information about the HTTP access point for retrieving the CRL is contained in each issued certificate.

CRL shall be published immediately upon the certificate revocation as well as every 6 hours from the previous CRL issuance. Revocation status information shall include information on the status of certificates at least until the certificate expires.

4.9.8 Maximum latency for CRLs

Maximum latency for CRL from the moment of its issuance to the moment of its publication in regular circumstances shall be less than 30 seconds.

4.9.9 On-line revocation/status checking availability

Fina RDC 2020 and Fina RDC 2015 CAs shall support *online* status checking of certificates revocation status via Fina OCSP service compliant with the IETF RFC 6960 [21].

OCSP responses for Subscriber's Certificates issued by Fina RDC 2020 CA shall be signed by the Fina OCSP service with the certificate for OCSP service that is issued by the Fina RDC 2020 CA.

OCSP responses for Subscriber's Certificates issued by Fina RDC 2015 CA shall be signed by the Fina OCSP service with the certificate for OCSP service that is issued by the Fina RDC 2015 CA.

Certificate for OCSP service shall contain an extension of type *id-pkix-ocsp-nocheck*, as defined by RFC6960 [21].

Fina OCSP service address shall be http://ocsp.fina.hr, and it shall be contained in the *Authority Information Access* certificate extension of each Subscriber's certificate.

4.9.10 On-line revocation checking requirements

The Relying Party should have an application solution which can use the OCSP service referred to in Section 4.10.1 herein.

For a certificate serial number that will be "unused" in terms of CA/Browser Forum BRG [23] document, Fina OCSP service shall not respond with a "good" status.

4.9.11 Other forms of revocation advertisements available

No stipulations.

4.9.12 Special requirements to key compromise

Any interested party may submit a key compromise report to Fina to demonstrate compromise of private key of any Subscriber's Certificate. The report must include the proof of private key compromise.

In case of receiving certificate revocation applications or receiving a Certificate Problem Report, Fina shall be able to revoke the subject certificate and the information on the private key compromise and the reason for revocation shall be contained in the notification of the certificate revocation status.

4.9.13 Circumstances for suspension

Fina shall not suspend OVCP certificates.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

Information about the certificate revocation status shall be provided by Fina through the OCSP service and by publishing the CRL. Information on the status of individual certificate shall be available at least during the entire certificate validity period.

Fina OCSP service address shall be http://ocsp.fina.hr, and it shall be provided in the *Authority Information Access* certificate extension of all Subscriber's Certificates.

CRLs shall be published on the web server and in the public directory repository referred to in Section 2.2 herein. Consolidated CRL and partitioned CRL shall be published on the web server and on the public directory.

The *CRLDistributionPoints* certificate extension of each Subscriber's Certificate shall contain the HTTP URL of the corresponding segment of the partitioned CRL.

4.10.2 Service availability

CRL and OCSP service shall be available 24 hours a day, seven days a week. In the event of a system failure, circumstances beyond Fina's control or force majeure, the service shall be available in accordance with the Business Continuity Plan.

The response time to the CRL request or obtaining an OCSP response under normal operating conditions is less than 10 seconds.

4.10.3 Optional features

No stipulations.

4.11 End of subscription

If a Subscriber terminates the Subscriber Agreement before the certificate expiry date, Fina RDC 2015 CA shall revoke all certificates subject to such Agreement.

4.12 Key escrow and recovery

Safe storage of Subscriber private keys for OVCP certificates shall not be allowed.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Fina shall ensure the adequate protection of the property used for certificate provision services and shall, to that aim, keep a comprehensive list of that property with the accompanying classification in accordance with the risk assessment.

Physical protection measures, procedures implemented by Fina in protecting the system for certificate issuance (hereinafter referred to as: "certification system"), as well as system, management and operational procedure controls in Fina PKI shall be internal and the details therein shall not be publicly disclosed.

5.1 Physical controls

As a Certification Service Provider, Fina shall implement certification system physical protection measures aimed at minimising risks related to physical protection and in accordance with Fina's business policy, laws in force.

5.1.1 Site location and construction

Fina's primary certification production system shall be situated inside Fina's building, on separate, protected premises envisaged for this purpose, and subject to implementation of multiple levels of physical and technical protection preventing unauthorized physical access to the system and data and thus hindering compromise of the system and services. The physical protection shall be based on the concept of using security zones with the security level increasing with each passing through to the next zone. The physical protection from intrusion is achieved with security parameters which separate zones established around the certification system wherein certificate generation and revocation take place.

The purpose of Fina's secondary certification system shall be to take over the functions of the primary certification system in case of failure until its recovery and restoration of services. The secondary certification system shall be situated on Fina's isolated remote site and it shall meet equal or higher security requirements compared to the primary system.

Safe premises accommodating Fina's certification system components at the primary and secondary sites shall hereinafter be referred to as: "Fina PKI protected premises".

5.1.2 Physical access

Physical access to the certification system on the Fina PKI protected premises and accompanying sub-premises within these premises shall be achieved with the dual control of passage of Fina PKI authorized personnel and in accordance with their roles and authorizations.

For persons who are not authorized for physical access to the certification system, the access shall be allowed only if accompanied and full-time supervised by authorized persons of Fina PKI with their dual control and in accordance with the Fina internal procedures.

Each access to certification systems shall be recorded.

Equipment, information, media and software from the Fina PKI protected area shall be taken off-site only with at least dual control of authorized persons in the Fina PKI, who have been assigned the appropriate trusted roles and with prior authorization.

Physical access to Subscribers data collected by the RA Network shall be allowed only to authorized Fina PKI and Fina RA Network personnel that shall collect, store, use and delete natural persons personal data in accordance with laws on personal data protection.

5.1.3 Power and air conditioning

Devices and premises where Fina RDC 2020 and Fina RDC 2015 CAs, Fina RA system and repository, as well as technical protection systems are located shall be continuously supplied with electricity and air-conditioning sized to ensure appropriate operational conditions even in case of external supply interruptions.

5.1.4 Water exposures

The location of Fina RDC 2020 and Fina RDC 2015 CAs, Fina RA system and repository shall be protected against flood.

5.1.5 Fire prevention and protection

Fina RDC 2020 and Fina RDC 2015 CAs, Fina RA system and repository shall be protected by a fire alarm system and automatic fire suppression system in accordance with the adopted laws in force.

5.1.6 Media storage

Media containing archived and backup copies of Fina PKI data in the electronic form, repository content copies and software equipment backup copies shall be safely stored to two separate protected locations with established fire protection system, and insured against flood. The media shall be protected against damage, theft and unauthorised access.

5.1.7 Waste disposal

Devices and media containing soft copy of the confidential information which is no longer necessary shall be safely destroyed so that the confidential data are no longer readable nor restorable. Destroying of these devices and media shall take place under the supervision of Fina PKI authorised personnel.

Paper documents and materials which contain confidential data shall be safely destroyed before being disposed of.

5.1.8 Off-site backup

Backup copies of Fina RDC 2020 and Fina RDC 2015 CAs, backup copies of RA system, archive or data backup copies, repository content copies and software backup copies shall be stored on a remote secondary certification system site, away from the primary certification production system. Physical protection level of such backup copies shall be equal or higher than the one applied to their originals.

5.2 Procedural controls

5.2.1 Trusted roles

Information system and communication system management tasks, certificate life cycle management tasks, security procedure administration and implementation as well as Fina PKI operation supervision tasks shall be performed in separate organisational units of Fina.

Employees' tasks, duties and responsibilities shall be assigned according to appropriate trusted roles. Trusted roles shall represent a foundation of trust in Fina PKI and shall be assigned to authorised employees of Fina's competent organisational units. Each trusted role shall be documented and supported by a clearly defined description of tasks and responsibilities.

Trusted roles shall include the roles of Security Officer, System Administrator, System Operator, Registration Officer, Validation Specialist, Revocation Officer and System Auditor.

5.2.2 Number of persons required per task

Fina PKI tasks shall be performed exclusively by authorised persons. Fina shall have a sufficient number of regular employees with knowledge, experience and qualifications required within Fina PKI for the provision of services falling within the scope of this Certificate Policy.

Access and work on Fina PKI protected premises shall be performed solely in the presence of at least two authorised persons having access permissions for such system.

Individual security-sensitive tasks on the Fina PKI protected premises shall be carried out with participation of a prescribed number of persons having specific trusted roles.

5.2.3 Identification and authentication for each role

When logging into critical applications and services within Fina PKI, person accessing the application or service shall be identified and authenticated. The person's identification and authentication shall be carried out by means of an adequate authentication method. Access to and use of applications and services within Fina PKI shall be allowed only to authorised persons in accordance with the trusted role assigned to them. While using critical applications and services, activities of the logged in person shall be duly recorded, saved and kept.

5.2.4 Roles requiring separation of duties

Due to security requirements related to the issuance of certificates, the following separation of duties shall be in place:

- the person assigned the trusted role of Security Officer, Registration Officer, Validation Officer or Revocation Officer shall not be assigned role of System Auditor,
- the person assigned the trusted role of System Administrator shall not be assigned role of Security Officer or System Auditor.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Before starting to work at Fina PKI, the candidates shall have appropriate expertise, experience, qualifications and education in the field of cryptographic technologies, protection of computer systems, information security and personal data protection in the domain of their own scope of work within Fina PKI.

Personnel performing Fina PKI tasks shall not be employed nor have any business relationship with other Trust Service Providers.

5.3.2 Background check procedures

Before starting to perform Fina PKI tasks, Fina shall perform adequate candidate checks in order to assess their expertise, ability and reliability in accordance with the needs of Fina PKI tasks.

5.3.3 Training requirements

Personnel performing tasks within Fina PKI shall receive education and training according to their trusted roles. Fina shall maintain records of these trainings.

5.3.4 Retraining frequency and requirements

Information Security Awareness course shall take place annually for all Fina PKI employees.

Employees with trusted roles in Fina PKI shall have the obligation to acquire and perfect their knowledge.

The knowledge of Fina RA Network employees, especially in terms of tasks they perform, shall be regularly refreshed, at least once every year.

5.3.5 Job rotation frequency and sequence

No stipulations.

5.3.6 Sanctions for unauthorized actions

Not complying with the laid out measures for authorised persons when working in Fina PKI shall be subject to violation of work duties, and potential penalties shall be determined in a disciplinary procedure.

In case of unauthorised actions by contractual partners, provisions defined under the Contract with the contractual partner shall apply.

5.3.7 Independent contractor requirements

Fina shall not have independent contractors performing a part of certification services from the scope of this document.

Requirements for suppliers of goods and services for Fina PKI shall be regulated by internal documents governing work with suppliers. The access to the information property in Fina PKI for independent contractors shall be approved solely under a contract for that particular information which is the subject of the contract and solely for activities referred to in the contract.

5.3.8 Documentation supplied to personnel

Each employee may access the documentation required for the execution of their work tasks according to the trusted role assigned and pertaining authorisations.

5.4 Audit logging procedures

5.4.1 Types of events recorded

In the audit logs all events in Fina PKI shall be recorded related to:

- Life-cycle management of CA keys Fina RDC 2020 and Fina RDC 2015 CAs,
- Registration of a natural person, Legal person and server,
- Life-cycle management of certificates issued by Fina RDC 2020 and Fina RDC 2015 CAs,
- Requests for certificate revocation including accompanying executed actions.

Security events in Fina PKI related to changes of security policy, physical and technical protection of Fina PKI premises, initiation and termination of system work, system errors and hardware faults, firewall and router activities and attempts to access the system shall also be recorded in the audit logs.

5.4.2 Frequency of processing log

The audit logs in Fina PKI shall be regularly reviewed on a daily basis. The audit logs shall be reviewed for the purpose of tracking and determining malicious activities in the system. Fina shall use automatic mechanism for warnings and messages on potential critical security

events. Such notifications shall be delivered to authorised persons in Fina PKI. Actions undertaken based on audit log collection shall be documented.

5.4.3 Retention period for audit log

The audit logs with records referred to in Section 5.4.1 shall be kept for at least 10 years after any certificate based on these logs ceases to be valid.

5.4.4 Protection of audit log

The audit logs in Fina PKI shall be protected during the entire retention period. The protection of the audit logs shall include their protection against unauthorised reading and disclosure, and shall preserve logs integrity.

Audit logs protected in such a manner shall be available only to authorised persons, especially for the purpose of providing evidence on certificates in court proceedings.

5.4.5 Audit log backup procedures

Audit logs of the Fina PKI system shall be archived in two copies on physically separate sites.

Copies of audit logs at the secondary site shall be protected with an equal or higher level of protection compared to audit logs at the primary production site (see Section 5.4.4).

5.4.6 Audit collection system (internal vs. external)

Depending on data type, audit logs shall be collected automatically or by an authorised person.

The audit logs generated in Fina PKI and Fina RA Network shall be collected internally.

5.4.7 Notification to event-causing subject

In case of detecting a significant event log in the Fina PKI operation related to a particular participant, Fina shall reserve the right to decide on informing the participant causing the event.

5.4.8 Vulnerability assessments

Fina shall carry out regular information property risk assessment, vulnerability assessment for identified public and private addresses and penetration testing.

Information risk assessment shall be carried out once every year. System vulnerability assessment for identified public and private addresses Fina PKI shall be carried out once every quarter. Penetration test shall be carried out once every year.

Fina shall address any critical vulnerability not previously addressed, within a period of 48 hours after its discovery and shall act in accordance with established practices.

5.5 Records archival

5.5.1 Types of records archived

Fina PKI shall store in its archives data specified below, which may come in paper or electronic form:

- Fina PKI Certificate Policy and Certification Practice Statements,
- terms and conditions of certification services provision,
- contracts related to certification services provision,
- data and accompanying documentation collected in the registration procedure,
- certificates and data related to life-cycle of individual certificates,
- records of certificate status change,
- audit logs referred to in Section 5.4.1 herein,
- other Fina internal documents.

Each archived record shall contain data indicating time referring to it.

5.5.2 Retention period for archive

Fina shall keep all archived data and documentation for at least 10 years after any certificate based on these data and documentation ceases to be valid.

5.5.3 Protection of archive

Archived data and documentation shall be protected by protection level mechanisms and procedures ensuring archive confidentiality and integrity. The archive shall be protected from unauthorised viewing, modification, and deletion of data.

Archived records protected in such a manner shall be available only at the request to authorised persons, especially for the purpose of providing evidence on issued certificate in court proceedings.

5.5.4 Archive backup procedures

The backup of archived data in the electronic form shall be created on the Fina PKI protected premises and shall be kept safely off-site away from the primary certification production system in accordance with Section 5.1.8 herein.

5.5.5 Requirements for time-stamping of records

No stipulations.

5.5.6 Archive collection system (internal or external)

Records to be archived shall be collected depending on the record type.

Records to be archived which are generated in Fina PKI and Fina RA Network shall be collected and archived internally.

5.5.7 Procedures to obtain and verify archive information

Access to archived records shall be allowed only to persons with authorised access to such data.

Archived data shall be verified by control of their integrity.

5.6 Key changeover

Fina shall ensure that Fina CAs continuously provide trust service with its valid key pairs and pertaining CA certificates. For this reason, Fina CA shall sufficiently in advance generate a new pair of CA keys. Also, Fina CA shall sufficiently in advance generate a new pair of CA keys and in case this change is required by the security level of cryptographic algorithm of the private CA key in use. In both cases, Fina Root CA shall issue a CA certificate for a new public CA key.

Fina CA shall inform the participants in Fina PKI on the change of its public key and on its new CA certificate in a timely manner.

New pertaining public key shall be available to the participants in Fina PKI in the same manner as the previous Fina RDC 2020, or Fina RDC 2015 CA public key, and in accordance with the description referred to in Section 2.2 herein.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The Business Continuity Plan for Fina PKI shall regulate procedures in case of incident or system compromise which shall include procedures for recovery of systems and establishing of security conditions for certification services provision.

The Business Continuity Plan shall be revised at least once a year.

Changes that will be motivated by a security concern such as certificate misissuance or a root or intermediate compromise shall be treated as a security-sensitive

5.7.2 Computing resources, software, and/or data are corrupted

Fina certification system shall be based on trustworthy hardware and software components, and system critical operations are supported with redundant components.

Functionality, proper work and timely damage removal of certification system components shall be ensured under support and maintenance with equipment suppliers.

The Business Continuity Plan for Fina PKI shall regulate procedures for certification system recovery in case of malfunction or damage of equipment and network resources, as well as data recovery.

5.7.3 Entity private key compromise procedures

In case of compromising or suspicion of compromising the private key Fina RDC 2020 or Fina RDC 2015 CA, Fina shall immediately discontinue use of this compromised private key.

After confirming the compromise of the private key, Fina shall make a decision on revocation and the corresponding CA certificate shall be revoked by Fina Root CA.

Fina shall notify the following Fina PKI participants of the CA certificate revocation:

- Fina RA Network,
- Subscribers,
- Relying Parties.

After determining and eliminating the causes responsible for CA key compromise, Fina shall if appropriate, undertake measures to prevent the recurrence of such an event. Fina CA, whose certificate has been revoked, shall generate a new pair of CA keys. Fina Root CA shall issue a new CA certificate for the new public CA key

New CA shall, by using the new private CA key, issue certificates to existing registered subjects and shall sign all further information on certificate revocation by using the new key. New CA certificate shall be available to the participants in Fina PKI in the same manner as the previous CA certificate, and in accordance with the description referred to in Section 2.2 herein.

If the cryptographic algorithms and parameters used cease to provide the required security and protection, Fina will, if possible, notify in due time:

- Fina RA network,
- Subscribers,
- Relying parties.

Fina will consider using other appropriate recommended secure cryptographic algorithms and, if possible, make a decision about using another algorithm. Fina will develop specific plans and procedures that will necessarily include the implementation of the revocation of all certificates that are affected by cryptographic algorithms and parameters whose security is compromised. About those plans and deadlines Fina will inform Subscribers and Relying parties.

5.7.4 Business continuity capabilities after a disaster

The Business Continuity Plan shall define procedures for business continuation after a disaster. Depending on the type of disaster, Fina shall continue providing certification services on its primary certification production system or it shall continue service provision on its secondary certification system referred to in Section 5.1.1 herein, until the recovery of the primary production system.

5.8 CA or RA termination

With regards to the planned termination of certificate services provision, Fina shall:

- inform all Subscribers, relying parties and the state administration body responsible for digital transformation at least three months before the planned termination of certificate services provision,
- make all possible efforts to ensure the continuation of certificate services provision with another Trust Service Provider, and shall deliver all documentation collected in the Subscriber registration process as well as all documentation on issued certificates to that service provider,
- revoke all issued certificates,
- revoke the CA certificates and destroy their related private keys of those Fina CAs that cease its operations.

In case of termination of certificate service provision, Fina shall archive, protect and keep records in accordance with the provisions referred to in Section 5.5 herein to make those records available for evidence in court, administrative or other proceedings in accordance with applicable provisions of legislation, or it shall enter into an agreement with another entity with respect to archiving, protection and keeping of records.

6 TECHNICAL SECURITY CONTROLS

This Chapter shall describe the protection measures undertaken with the aim of achieving the required security level of cryptographic keys, activation data, critical security parameters, key management and other technical security measures regarding Fina RDC 2020 and Fina RDC 2015 CAs and for issuing Subscriber's Certificates.

6.1 Key pair generation and installation

6.1.1 Key pair generation

Fina shall carry out Fina RDC 2020 and Fina RDC 2015 CAs key pair generation using algorithms for key generation that shall be aligned with the standardisation document ETSI TS 119 312 [16].

6.1.1.1 Generation of Fina CA Key Pairs

The Fina RDC 2020 and Fina RDC 2015 CA key pair generation procedure shall be carried out in a formal subordinate Fina CA's key pair generation ceremony.

The Fina RDC 2020 and Fina RDC 2015 CA key pair generation ceremony shall be carried out according to the protocol for key generation in which the steps taken during the ceremony shall be documented. The key generation protocol shall be in compliance with the technical security measures according to standard ETSI EN 319 411-1 [11] and the requirements of the document CA/Browser Forum BRG [23].

Key pairs for Fina RDC 2020 and Fina RDC 2015 CA shall be generated, under at least dual control of authorised persons with trusted roles in Fina PKI, in HSM modules that meet the requirements referred to in Section 6.2.1 herein.

Fina RDC 2020 and Fina RDC 2015 CA shall be located in Fina PKI protected premises referred to in Section 5.1.1 herein during and after the key pair generation ceremony, and access to Fina RDC 2020 and Fina RDC 2015 CAs shall be allowed only to Fina PKI authorised persons with trusted roles exercising at least dual control.

The Fina RDC 2020 and Fina RDC 2015 CA key pair generation ceremony procedure shall be videotaped or the conducted procedure shall be witnessed by a Qualified Auditor.

A transcript of the carried out CA keys generation shall be recorded together with the attached audit logs.

Fina shall be in possession of the Qualified Auditor's report witnessing that the Fina RDC 2020 and Fina RDC 2015 CA key pair generation procedure has been carried out in compliance with the protocol and the requirements for key generation.

6.1.1.2 Key Pair Generation for Subscriber's Certificates

Fina shall not generate key pairs for the Subscriber's Certificates.

The key pair generation for the Subscriber's Certificate shall be carried out in a controlled environment at the location of the Subscriber. Private keys shall be protected in software protected token in the manner described in Section 6.2.1 herein.

Fina shall reject a certificate issuance application in the following cases:

- if the Subscriber public key does not meet the requirements listed in Sections 6.1.5 and 6.1.6 herein,
- if there is clear evidence that the specific method used to create the private key was flawed,
- if Fina is made aware of the demonstrated or confirmed method that compromises the Subscriber's private key,
- if Fina receives Subscriber's Certificate request using a key pair previously generated by one of Fina CA's.

6.1.2 Private key delivery to subscriber

The Custodian shall generate Subscriber key pair at its location and therefore it shall be deemed that the Subscriber is already in possession of a private key.

Parties other than the Subscriber shall not archive the Subscriber's private key without the Subscriber's authorization.

6.1.3 Public key delivery to certificate issuer

The Subscriber public key shall be delivered at Fina RDC 2020 CA in a way that shall ensure verification of the integrity and authenticity of the public key, and in a way that shall securely connect the confirmed identity of the Subject with the corresponding public key being delivered.

The certificate application process shall include authentication of the Custodian and checking whether the Custodian has possession of or control of the private key that corresponds to the public key, which shall be delivered for certificate creation.

6.1.4 CA public key delivery to relying parties

The public key of Fina RDC 2020 and Fina RDC 2015 CA shall be accessible to Relying Parties in Fina RDC 2020, or Fina RDC 2015 CA certificate issued by Fina Root CA.

Web addresses for direct retrieving Fina Root CA, Fina RDC 2020 and Fina RDC 2015 CA certificates are:

- Fina Root CA: https://rdc.fina.hr/Root/FinaRootCA.cer

- Fina RDC 2020 CA: https://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer
- Fina RDC 2015 CA: https://rdc.fina.hr/RDC2015/FinaRDCCA2015.cer

6.1.5 Key sizes

Fina shall use cryptographic algorithms and minimum key sizes accordance with ETSI TS 119 312 [16] and CA/Browser Forum BRG [23] standardisation documents.

The key sizes in Fina PKI shall be as follows:

- Fina Root CA shall use *sha256WithRSA* algorithm with 4096-bit long keys,
- Subordinated Fina RDC 2020 and Fina RDC 2015 CA shall use *sha256WithRSA* algorithm with 4096-bit long keys,
- Fina OCSP service shall use 2048-bit long RSA keys,
- the supported RSA key sizes for Subscriber's Certificates shall be 2048, 3072 and 4096-bits.

Upon reception of the PKCS#10 request for Subscriber's Certificate issuance, Fina shall verify if the key length conforms to the supported length specified in this Section. In case of non-compliance Fina shall reject the PKCS#10 request.

6.1.6 Public key parameters generation and quality checking

Fina RDC 2020, or Fina RDC 2015 CA shall carry out key pair generation using generation parameters in compliance with the standardised document ETSI TS 119 312 [16].

Compliance with the requirements for generation and verification of key quality parameters shall be ensured by using certified HSM modules or cryptographic modules, in accordance with Section 6.2.1 herein, and by strictly abiding by the requirements listed in the documentation of the cryptographic modules.

The Custodian shall carry out the key generation by using generation parameters that comply with the standardization document ETSI TS 119 312 [16] and the document CA/Browser Forum BRG [23]. In case of non-compliance with these requirements Fina shall reject the PKCS#10 request.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The Fina RDC 2020 CA certificate shall have *keyCertSign* and *cRLSign* values set in the *Key Usage* extension.

Fina RDC 2020 CA shall use the corresponding private key only for:

- signing Subscriber's Certificates,
- signing certificates for LRA,
- signing the OCSP service certificates,
- signing the corresponding CRLs.

The Fina RDC 2015 CA certificate shall have *keyCertSign* and *cRLSign* values set in the *Key Usage* extension.

Fina RDC 2015 CA shall use the corresponding private key only for:

- signing the OCSP service certificates,
- signing the corresponding CRLs.

SSL certificate level 2 (OVCP) in the *Key Usage* certificate extension shall have set values *digitalSignature* and *keyEncipherment*. The pertaining private key shall only be used to authenticate the web pages.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The Fina RDC 2020 and Fina RDC 2015 CA private key shall be generated and protected by a HSM module that shall comply with the requirements of FIPS 140-2 [17] Level 3.

Protection of a private key *SSL certificates level 2 (OVCP)* shall be carried out in a software protected token in the controlled environment at the Subscriber location. The Subscriber shall be in charge of the method of protecting private keys of *SSL certificates level 2 (OVCP)*.

6.2.2 Private key (n out of m) multi-person control

Private key multi-person control is a security measure requiring multi-person authorisation for private key control.

A HSM modules protecting private keys of Fina RDC 2020 and Fina RDC 2015 CA shall be located in the premises with the highest level of security within the Fina PKI protected premises. Physical access to such HSM modules shall be subject to dual control of authorised persons with Fina PKI trusted roles.

Fina RDC 2020 and Fina RDC 2015 CA private key management shall be carried out by physical access to the HSM module with at least dual control and authorisation by two authorised persons with Fina PKI trusted roles.

6.2.3 Private key escrow

Fina RDC 2015 CA private key escrow shall not be applied.

Subscriber private key storage associated with OVCP certificates shall not be applied.

6.2.4 Private key backup

Security copies of Fina RDC 2020 and Fina RDC 2015 CA private keys shall be made in the premises with the highest level of security within Fina PKI protected premises with dual

control by authorised persons with Fina PKI trusted roles. A Fina RDC 2020 and Fina RDC 2015 CA private keys shall be copied and retrieved from a cryptographic module exclusively in encrypted form and shall be kept in secure premises of the highest level of security within Fina PKI protected premises at separate locations.

Only authorised persons with Fina PKI trusted roles and implementation of dual control shall have physical access to security copies of Fina RDC 2020 and Fina RDC 2015 CA private keys.

Fina shall never carry out security backup of Subscriber private keys connected to OVCP certificates.

6.2.5 Private key archival

Fina shall not archive Fina PKI private keys and shall not archive Subscriber private keys.

6.2.6 Private key transfer into or from a cryptographic module

If a Fina RDC 2020 and Fina RDC 2015 CA private keys shall be transferred from or into a HSM module, when outside the HSM module, the private keys shall be protected by encryption in a way that ensures the same security level as when it is inside the HSM module. The transfer of a private keys shall only be carried out by authorised persons with trusted roles in Fina PKI, along with dual control. The transfer of a Fina RDC 2020 and Fina RDC 2015 CA private keys shall only be carried out for the purpose of creating security copies.

During the transfer of private keys from one HSM module into another HSM module, the private key shall only be transferred to a HSM module of equal or higher level of security in relation to the HSM module from which the private key is being transferred.

The transfer of private keys for the *SSL certificate level 2 (OVCP)* into another private key security container shall be carried out by the Custodian, in a manner that the private key shall only be transferred into a private key security container of equal or higher level of security in relation to the cryptographic module from which the private key is being transferred.

Before transfer, the private key shall be encrypted so that it would be adequately protected during the transfer.

6.2.7 Private key storage on cryptographic module

Fina RDC 2020 and Fina RDC 2015 CA private keys shall be protected with a HSM module and may be used only if duly activated.

There shall be no limitations regarding the format in which private keys shall be stored in HSM modules.

6.2.8 Method of activating private key

The activation of a Fina RDC 2020 and Fina RDC 2015 CA private key shall be carried out according to procedures and upon compliance with the requirements set in the certification document of the HSM module used and with which Fina RDC 2020 and Fina RDC 2015 CA private keys are protected, with dual control by authorised persons with Fina PKI trusted roles.

Activation of a certificate private key shall only be carried out by the associated Custodian using corresponding activation data. Private key activation shall be carried out in a secure manner.

6.2.9 Method of deactivating private key

The deactivation of a Fina RDC 2020 and Fina RDC 2015 CA private key shall be carried out according to procedures and upon compliance with requirements set in the certification document of the HSM module used, with dual control by authorised persons with Fina PKI trusted roles.

The Custodian shall be responsible for prescribed certificate private keys deactivation and use.

A deactivated certificate private key may be reused only after the reactivation of the corresponding activation data.

6.2.10 Method of destroying private key

The procedure for destruction of a Fina RDC 2020 and Fina RDC 2015 CA private keys shall be carried out after the expiry of the private key validity period because it has been compromised or because of suspicion that a private key has been compromised, or due to cessation of its use, and shall be carried out by authorised persons with trusted roles in Fina PKI with at least dual control. The procedure for destruction of a Fina RDC 2020 and Fina RDC 2015 CA private keys shall also include the destruction of all security copies of this private key.

The destruction of a Fina RDC 2020 and Fina RDC 2015 CA private keys shall be carried out in the manner outlined in internal Fina documents which shall ensure that after the destruction of a private key it may no longer be recovered or reused.

A transcript shall be kept about the destruction of a Fina RDC 2020 and Fina RDC 2015 CA private keys.

It is recommended that the Subscriber destroy every private key of the SSL certificate level 2 (OVCP) that has been put out of use permanently.

The destruction of private keys of *SSL certificate level 2 (OVCP)* shall be the responsibility of the Subscriber.

6.2.11 Cryptographic Module Rating

The rating of HSM modules and other cryptographic modules shall be carried out according to standards for cryptographic modules listed in Section 6.2.1 herein.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Fina RDC 2020 and Fina RDC 2015 CA public keys shall comprise a constituent part of associated CA certificates that shall be archived in accordance with Sections 5.5.3 and 5.5.4 herein, and they shall be kept in the archive for the period referred to in Section 5.5.2 herein.

Subscriber public keys shall comprise a constituent part of associated certificates and shall be archived in accordance with Sections 5.5.3 and 5.5.4 herein, and they shall be kept in the archive for the period referred to in Section 5.5.2 herein.

6.3.2 Certificate operational periods and key pair usage periods

The certificate validity period according to types is defined in Table 6.1.

Certificate	Term
Fina RDC 2020 CA certificate	10 years
Fina RDC 2015 CA Certificate	10 years
Fina OCSP service responder signing certificates	1 year
SSL Certificate Level 2 (OVCP)	1 year

Table 6.1 Certificate Usage Periods

The validity period of Fina RDC 2015 CA certificates shall not exceed the validity period of Fina Root CA certificates.

The private key period of validity shall be equal to the period of validity of the pertaining certificate. Certificates and pertaining keys shall not be used after the expiry of the validity period of certificates or after certificate revocation.

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data connected to Fina RDC 2020, or Fina RDC 2015 CA private keys shall be generated and installed during the carrying out of a formal private key pair generation ceremony for subordinated Fina CAs.

Custodian generates and writes activation data for private keys of the Subscriber. Subscriber shall be responsible for security and compliance with the stipulated quality of the activation data.

6.4.2 Activation data protection

The activation data connected with the Fina RDC 2020, or Fina RDC 2015 CA private key shall be kept in a secure manner.

Custodians shall be in charge of and responsible for the protection and keeping of activation data of corresponding private keys.

6.4.3 Other aspects of activation data

Activation data for certificate private keys may be periodically modified to minimise the possibility of their disclosure.

This Certificate Policy shall not set any additional requirements on the life cycle of activation data for Subscriber's private keys corresponding to the certificates.

Additional rules about the terms and conditions, and life cycle of an activation data for Subscriber's private key corresponding to the certificate may be specified in the Subscriber Agreement.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Only authorised persons after authentication shall have access to the IT system and applications in Fina PKI.

Two-factor authentication shall be enforced for all accounts capable of causing certificate issuance or performing registration process.

Modifications to and publication of the revocation status of certificates shall be carried out with two-factor authentication and mandatory control of access.

The Fina PKI system shall carry out continuous monitoring and shall have a detection system for the purpose of detecting, recording and timely reaction to attempts at unauthorised access to system resources.

6.5.2 Computer security rating

With the aim of providing secure and quality trust services, Fina shall establish an information security management system in compliance with the standard ISO/IEC 27001 [9].

6.6 Life cycle technical controls

6.6.1 System development controls

When procuring development software from an external subcontractor, Fina shall ensure the system development security principles in an agreement with the supplier.

The analysis of security requirements shall be carried out in the design and specification phase of any development project of Fina PKI systems, to ensure that security has been incorporated in the information technology of Fina PKI systems.

Software used to provide certificate issuance services shall originate from a reliable source. New versions of software shall be tested in a test environment. Implementation of software in production shall be carried out in accordance with documented procedures of change management.

6.6.2 Security management controls

Fina shall verify all parts of the certification system in the Fina PKI production hierarchy, which shall be based on Fina Root CA, with respect to security, reliability and quality of operation, all in accordance with laws in force referred to in Section 9.14 herein.

In the event of a breach in certification system security or loss of its integrity which may have a significant impact on the provision of trust services or on the protection of personal data, Fina shall within 24 hours notify the state administration body competent for digital transformation about this, as the authority competent for supervision of Trust Service Providers, and, if necessary, other competent authorities. In the event that the loss of integrity may have a negative impact on the Subscribers of Fina trust services, Fina shall immediately notify all natural persons and Business entities that may be impacted by the security breach.

6.6.3 Life cycle security controls

Fina shall carry out change management in Fina PKI to ensure that changes occur for justified reasons, and in a controlled and formalised way.

The integrity of the certification and information systems shall be protected by anti-virus protection and the use of authorised software.

Monitoring of available certification system capacities shall be carried out, and the compliance of existing capacities for future needs of the system shall be assessed to plan their expansion in a timely manner.

6.7 Network security controls

The computing network security of Fina PKI system shall be based on the concept of network separation by different level network zones. Network zones shall be separated by

firewalls allowing only necessary network traffic. Equal security measures shall be applied to all systems located within the same network zone.

Access and communication between zones shall be limited to authorised employees with trusted roles necessary for providing services. Unnecessary communication, accounts, ports, protocols and services shall be explicitly prohibited or deactivated.

The Fina PKI internal computer network shall be protected against unauthorised access, including access by Subscribers and third parties.

All systems critical for providing Trust Services shall be located in the Fina PKI protected premises.

CA systems shall be specially security adjusted and hardened.

The network component of Fina PKI systems shall be stored in a physically and logically secure environment and the compliance of its configurations shall be periodically checked.

6.8 Time-stamping

Time-stamping shall not be used within the scope of certification services referred to in this Certificate Policy.

Time in the Fina certification system shall be synchronised with UTC time. Fina PKI audit logs shall contain accurate data regarding the date and time they originated, with a deviation of less than +/- 1 second.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

The profiles of certificates issued by Fina RDC 2020 CA shall be aligned with the standards ETSI EN 319 411-1 [11], ETSI EN 319 412 [12] and [13] and document CA/Browser Forum BRG [23].

Fina RDC 2020 CA shall issue a *SSL certificate Level 2 (OVCP)* according to defined profiles. This Certificate Policy for *SSL certificate Level 2 (OVCP)* shall be assigned an individual unique certificate policy OID (CP OID) given in Table 1.1 Section 1.1.2.

For Subscriber's Certificates Fina shall generate non-sequential certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

7.1.1 Version number(s)

Certificates shall be compliant with version 3 according to the X.509 specification.

7.1.2 Certificate extensions

The document with a description of the certificate profile shall be available on the website of Fina PKI repository referred to in Section 2.2 herein.

7.1.3 Algorithm object identifiers

Algorithms with pertaining OID identifiers for all certificates issued by Fina RDC 2020 CA are shown in Table 7.1.

Algorithm	OID
sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1

Table 7.1 Algorithms with Pertaining OID Identifiers

7.1.4 Name forms

Name forms for Fina Root CA and its subordinated Fina RDC 2020 and Fina RDC 2015 CAs are described in Sections 1.3.1.1 and 1.3.1.2 herein.

Name forms for *SSL certificate Level 2 (OVCP)* are described in Sections 3.1.1 and 3.1.4 herein.

Certification Subject attributes shall not contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.5 Name constraints

Fina RDC 2020 CA shall not issue Subscriber's Certificates with *Name Constraints* certificate extensions.

7.1.6 Certificate policy object identifier

The *Certificate Policies* certificate extension shall contain the corresponding OIDs of certification policy listed in Table 1.1 in Section 1.1.2 herein.

7.1.7 Usage of policy constraints extension

The *Policy Constraints* certificate extension shall not be used.

7.1.8 Policy qualifiers syntax and semantics

Policy qualifiers in the *Certificate Policies* certificate extension shall contain two pointers in the URI format that contain the website address of the CPS_{WSA} document [25] in Croatian and English.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulations.

7.2 CRL profile

The CRL profile issued by subordinated Fina RDC 2020 and Fina RDC 2015 CAs shall be in compliance with the IETF RFC 5280 [19] document.

7.2.1 Version number(s)

CRL shall be compliant with version 2 according to the X.509 specification.

7.2.2 CRL and CRL entry extensions

CRL extensions used in CRLs and extensions used in entry elements of CRLs that are issued by Fina RDC 2020 and Fina RDC 2015 CA shall be as defined in Table 7.2.

Extensions	Critical	Value
crlExtensions		
cRLNumber	NO	Monotonically increasing integer for CRL of up to 20 octets in length.
AuthorityKeyIdentifier	NO	160 bits SHA-1 hash. This value is identical to the *subjectKeyIdentifier* extension value of the certificate of Fina CA that issued CRL.

Extensions	Critical	Value
crlExtensions		
IssuingDistributionPoint*	YES	Contains the *DistributionPoint* value, *onlyContainsUserCerts* is set to TRUE
ExpiredCertsOnCRL	NO	Date and time on which the CRL starts to keep revocation status information for expired certificates.
Extensions	**Critical**	**Value**
crlEntryExtensions		
reasonCode	NO	Reason for the certificate revocation

Table 7.2 Extensions of CRLs and entry elements of CRLs issued by Fina RDC 2020 and Fina RDC 2015 CAs

7.3 OCSP profile

The Fina OCSP service responder OCSP profile shall be in accordance with the IETF RFC 6960 [21] document.

7.3.1 Version number(s)

The Fina OCSP service responder OCSP profile shall be in accordance with version 1 according to IETF RFC 6960 [21] document.

7.3.2 OCSP extensions

Fina OCSP services responders shall include the following extensions:

1. *Nonce,*
2. *Extended Revoked Definition.*

* The *IssuingDistributionPoint* extension is only contained in the partitioned CRL.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Supervision over the work of Fina as a Trust Service Provider shall be regulated by Regulation (EU) No 910/2014 [1] and Act on Amendments to the Act on the Organisation and Scope of State Administration Bodies (Official Gazette No. 57/2024) [2] and shall be carried out by the state administration body competent for digital transformation.

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

Compliance audit shall be carried out with the aim of confirming that Fina as a Trust Service Provider and provider of certificate issuance services, meets the requirements stipulated in Regulation (EU) No 910/2014 [1], Act Implementing Regulation (EU) no. 910/2014 [2] and the standard ETSI EN 319 411-1 [11].

8.1 Frequency or circumstances of assessment

Compliance audits of Fina PKI operations shall be external compliance audits and internal compliance audits.

8.1.1 External Compliance Audit

External compliance audit shall include Fina Root CA and all its subordinated CAs, and shall be carried out at least every 12 months, in accordance with the standard ETSI EN 319 403-1 [14] and ETSI TS 119 403-2 [15] and according to the requirements of standard ETSI EN 319 411-1 [11] which includes normative references to ETSI EN 319 401 [10]. This successive period-of-time audits will be contiguous, with no gaps.

External compliance audit will no longer need to be carried out, if Fina Root CA and all its subordinated CA certificates will have expired or have been revoked before commencement of the audit period.

8.1.2 Internal Compliance Audit

Internal compliance audit shall be carried out prior to the commencement of providing new trust service, periodically at least each 12 months, and after significant changes to Fina PKI operations.

Compliance audit of certificates with this Certificate Policy, CPS_{WSA} [25] document and in accordance with the requirements referred to in CA/Browser Forum document, BRG [23]) shall be carried out quarterly on a random sample of more than one certificate and at least 3% of certificates issued after the previous audit.

8.2 Identity/qualifications of assessor

External compliance audits shall be conducted by a Conformity Assessment Body. The competence of the Conformity Assessment Body and the qualification of the associated assessors shall be ensured by the accreditation of the Conformity Assessment Body according to the standard ETSI EN 319 403-1 [14].

Internal compliance audits shall be conducted by internal compliance assessors who together have knowledge and understanding:

- about the provisions of the standard ETSI EN 319 411-1 [11],
- about PKI areas and information security area,
- about legislation in the area of providing trust services.

8.3 Assessor's relationship to assessed entity

The Conformity Assessment Body and associated assessors shall be independent of Fina and Fina's assessment system.

Internal compliance assessors shall not assess compliance within their own scope of responsibilities.

8.4 Topics covered by assessment

The subjects of compliance assessment shall include the following areas of trust services provision:

- integrity and accuracy of documentation,
- implementation of requirements for trust services,
- organisational processes and procedures,
- technical processes and procedures,
- implementing information security measures,
- trustworthy systems,
- physical security at subject locations.

The description of the topics of compliance assessment shall be defined in the compliance assessment plan.

8.5 Actions taken as a result of deficiency

In the event that non-compliance has been detected during the provision of trust services, Fina shall undertake the necessary steps to eliminate the non-compliance, and, if applicable, within the period set by the supervisory body.

During certificate issuance termination due to the identified significant inconsistency, Fina shall issue only those certificates which are indicated as certificates for internal and testing purposes and it shall ensure that those certificates are not available to any other Subscriber.

8.6 Communication of results

The results of internal compliance audits shall be of a confidential nature and Fina shall not make these public.

Fina shall publicly publish summary of the report and attestation of external compliance audits no later than three months after the end of the audit period. Non-compliances established during compliance assessment shall be considered confidential information and they shall not be disclosed.

Also, Fina shall submit attestation of external compliance audits to various parties, such as Microsoft, Mozilla, etc. no later than three months after the end of the audit period.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Fina shall notify Subscribers and Relying Parties about all charged services. Unless otherwise provided for in a separate agreement, services shall be charged in accordance with Fina price list. The price list of all charged services shall be published on the website of the repository referred to in Section 2.2 herein.

Fina shall reserve the right to price changes. Amendments to the price list shall be published on the website of the repository referred to in Section 2.2 herein.

9.1.1 Certificate issuance or renewal fees

In accordance with the published price list, Fina shall charge fees for the services of issuance and renewal of certificates.

9.1.2 Certificate access fees

Fina shall not charge certificate access fees.

9.1.3 Revocation or status information access fees

In accordance with the published price list, Fina shall charge fees for the renewal of certificates.

Fina always, on each request received, performs revocation and suspension of the certificate within the time limits specified in Section 4.9.1 herein, regardless of the payment status of an individual request.

Fina shall not charge for the service of providing information about the revocation status of certificates, which it shall provide as part of OCSP services or publication of CRL.

9.1.4 Fees for other services

Fina may also decide to determine and charge an appropriate fee for other services, such as the registration of Subscribers, modification of data in certificates, etc.

No fee shall be charged for access to this Certificate Policy and CPS_{WSA} [25] document.

9.1.5 Refund policy

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

9.2 Financial responsibility

Fina, as a Trust Service Provider, shall possess financial stability and shall have at its disposal sufficient financial resources to ensure unhindered provision of certification services in accordance with this Certificate Policy.

9.2.1 Insurance coverage

Fina, as a Trust Service Provider, shall insure itself against damage liability risks occurring while carrying out certification services.

Fina shall additionally insure property by means of an insurance policy covering insurance against the risk of fire, severe weather, floods, explosions, vehicle impact, aircraft fall or impact, demonstrations, insurance of equipment, machinery, electronic and communication devices, installations etc.

9.2.2 Other assets

No stipulations.

9.2.3 Insurance or warranty coverage for end-entities

See Section 9.2.1 herein.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Confidential business information shall include all information in relation to certification service establishment and provision, regardless of their form, exchanged by the participants through any means of communication and labelled as confidential, or as being of a specific type or having a specific level of secrecy, by the participants, or which are confidential by their nature, because an unauthorised disclosure therein might cause damage to the participant.

9.3.2 Information not within the scope of confidential information

Data integrated into the content of the certificate, data about certificate status, and data and documents published in the Fina PKI repository shall not be deemed confidential business information.

9.3.3 Responsibility to protect confidential information

Each participant shall protect confidential business information referred to in Section 9.3.1 herein, that he/she somehow became aware of, in accordance with laws regulating the information protection considering information type and information secrecy type and level. Otherwise, he/she shall be held liable for the damage occurred.

9.4 Privacy of personal information

Fina shall pay attention to the protection of personal data collected, stored and used for the purposes of providing certification services in the scope of this document and shall process personal data in accordance with Regulation (EU) 2016/679 [4] and the Act Implementing General Data Protection Regulation [5].

By submitting certificate application natural persons shall give Fina consent to use and process personal data of Natural persons collected in the registration procedure in accordance with valid legislation, and for keeping this data for duration of at least 10 years after any certificate based on this data ceases to be valid.

9.4.1 Privacy plan

Fina shall have and implement a Personal Data Protection Policy that establishes the principles of processing personal data of natural persons and that expresses the awareness, knowledge and commitment to respect the rights and freedoms of individuals in processing personal data, and which Fina must adhere to in its business. Personal data collected for the purpose of providing certification services Fina shall process to the extent that is appropriate, relevant and limited to the provision of this service.

With professional knowledge, reliability, resources, compliance with prescribed technical, organizational and security measures Fina guarantees the processing of personal data in accordance with Regulation 2016/679 [4] and the Act Implementing General Data Protection Regulation [5].

Measures for personal data confidentiality and integrity protection shall apply during the exchange of personal data of natural persons between the Fina RA Network and certification system, and during the keeping and archiving of Subscriber personal data until their extraction from the archive and destruction.

9.4.2 Information treated as private

During and after the Subscriber registration procedure, with the aim of certificate issuance, Fina shall be authorised to collect personal data necessary for duly authentication of a Custodian and Legal Representative, and other data necessary for duly certification service provision. All this personal data shall be deemed confidential and Fina shall duly protect them.

9.4.3 Information Not Deemed Private

Personal data collected by Fina during and after the Subscriber registration procedure are confidential personal data.

9.4.4 Responsibility to protect private information

Fina shall be responsible for the protection of personal data collected for the purpose of providing certification services.

9.4.5 Notice and consent to user private information

Aside from the needs for the purpose of complying with statutory and contractual obligations under the Subscriber Agreement, Fina shall be authorised to use and publish personal data only upon the written consent by the natural person to whom the data relate.

9.4.6 Disclosure pursuant to judicial or administrative process

Fina shall not make the data referred to in Sections 9.3.1 and 9.4.2 herein available except in cases stipulated by law or when required in writing by the competent court, administrative or other government body.

9.4.7 Other information disclosure circumstances

No stipulations.

9.5 Intellectual property rights

Fina shall have intellectual property rights over this Certificate Policy document, as well as other Fina documentation published on the website of the repository referred to in Section 2.2 herein.

Fina shall not exercise intellectual property rights over the software used in Fina PKI which is owned by third parties.

The owner of a private and public key shall be the Subscriber and shall be authorised to use a private key.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Fina shall be responsible for the compliance of this Certificate Policy with legislation, and for implementing the provisions stipulated in this Certificate Policy, CPS_{WSA} [25] document, certification services terms and conditions and in accordance with obligations in Subscriber Agreement concluded with the Subscriber.

Fina shall publish on the website of the repository referred to in Section 2.2 herein the certification services terms and conditions, this Certificate Policy, CPS_{WSA} [25] document and all notifications and information concerning changes in operation that may affect Fina PKI participants in any way.

Fina, as the Trust Service Provider, shall be responsible for damage incurred while providing services caused by the Legal persons with whom Fina has subcontracted part of the certification services. This responsibility between Fina and the Legal person shall be regulated by means of a separate agreement.

Fina as a Trust Service Provider shall be responsible for:

- the compliance of certification services with the provisions of its information security policy, the provisions of the Certification Practice Statement [25] and the provisions herein, including when the part of its certification service Fina has by contract entrusted to another business entity,
- correct verification of identity, data and authorisation of the Applicant with the aim of collecting data for certificate issuance,
- issuance of certificates in a secure manner in order to preserve their authenticity and accuracy,
- compliance with its obligations.

In accordance with representations and warranties, Fina:

- shall verify whether the Applicant for the certificate issuance has control and exclusive right over the domain name or IP address contained in the certificate (or, in the case of a domain name, this right or control is delegated from the subject that has that right),
- shall, before issuing certificates, verify whether the Subscriber has approved the issuance of certificates and that the Applicant has been authorised by the Subscriber to submit a certificate issuance application,
- shall have established procedures with which it shall verify the accuracy of all data contained in a certificate before their issuance,
- shall have established procedures with which it secures a minimum possibility of miscomprehension of data contained in a certificate,
- shall have established procedures for authentication of Applicants and procedures for certificate issuance,
- shall conclude a Subscriber Agreement in all cases when a CA and Subscriber are not connected or are the same entity,
- in cases when Fina RDC 2020 CA issues a certificate for the needs of Fina, then Fina as the Applicant shall be acquainted with certification terms and conditions,
- shall issue a certificate with a profile in accordance with Section 7.1 herein, and according to the certificate type listed in the certificate issuance application,
- shall ensure verification that the Subscriber is in possession of a private key whose pertaining public key shall be delivered for certification,
- shall ensure that the issued certificate shall be accessible in accordance with Section 4.4.2 herein,

- shall on the basis of an authenticated and authorised application, after carrying out the stipulated procedure, revoke a certificate for the reasons listed in Section 4.9.1 of this Certificate Policy,
- shall ensure that the repository is accessible to the public 24 hours a day, 7 days a week and that it provides information about current revocation status of all certificates whose validity period has not expired,
- in the provision of certification services, shall apply the provisions of valid regulations referred to in Section 9.14 herein,
- shall carry out the required security measures for protection of premises and equipment of the certification system,
- shall apply organisational and technical protection measures for keys and certificates in accordance with this Certificate Policy,
- shall, in accordance with the business continuity plan, ensure the unhindered work and maximum availability of certification services,
- shall monitor the availability of capacities, shall plan maintenance and further development of certification systems in accordance with future needs, standard requirements and development of technology,
- shall, in accordance with Sections 9.3 and 9.4 of this Certificate Policy, protect data deemed confidential and shall use this data solely for the needs of certification services within the scope of this Certificate Policy,
- shall ensure that internal and external verification of compliance of Fina as the Trust Service Provider are conducted in accordance with Section 8.1 herein.

In the event of termination of the certification services provision, Fina shall act in accordance with Section 5.8 herein.

9.6.2 RA representations and warranties

Fina RA Network representations and warranties shall be as follows:

- carrying out registration and identification procedures for natural persons and Legal persons and data checking in the manner stipulated by this Certificate Policy,
- forwarding complete, accurate and verified data about Subjects to Fina RDC 2020 CA for further processing,
- retention, archiving and protection of data for at least 10 years after any certificate based on this data ceases to be valid.,
- insuring the archived Subscriber data against loss or breach of confidentiality, integrity and accessibility, as laid down in this Certificate Policy,
- notifying Applicants for certificate issuance about the published and accessible terms and conditions of providing certification services and this Certificate Policy.

9.6.3 Subscriber representations and warranties

Before the initial certificate issuance, the Subscribers shall conclude a Subscriber Agreement with Fina with which they accept this Certificate Policy and the certification services terms and conditions.

For each certificate issuance, a certificate application shall be submitted.

A Subscriber, as a Legal person shall be responsible for the accuracy, integrity and correctness of data submitted in the registration procedure and submission of the certificate application, and subsequently upon Fina's request, the connected certificate issuance.

The Subscriber shall:

- in the registration process, present itself in the manner stipulated in Chapter 3 and in Section 4.1.2.2 herein,
- carefully use and keep private keys and activation data in accordance with this Certificate Policy,
- undertake appropriate protection measures for private keys and activation data against unauthorised access and use in accordance with Chapter 6 herein,
- review and verify the accuracy of the content of the certificate and accept that certificate before its issuance,
- 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 herein,
- if a certificate has been revoked for the reason that a private key has become compromised, in the shortest possible period shall terminate any use of the private key connected with the public key in the certificate,
- respond to Fina's instructions related to the compromised key or incorrect use of certificates,
- use the certificate and the pertaining private key only on servers accessible through FQDN or IP addresses listed in the *Subject Alternative Name* certificate extension, and in accordance with legal and other provisions of the Republic of Croatia, and in accordance with the provisions of Section 1.4.1 and 1.4.2 herein, Subscriber Agreement and certification service provisions terms and conditions,
- use the certificate and corresponding private key in accordance with the provisions of Section 4.5.1 herein,
- act in accordance with all other provisions of this Certificate Policy that refer to Subscriber obligations.

The obligations and responsibilities of the Subscriber related to the use of private keys and certificates shall be described in Section 4.5.1 herein.

The Subscriber, as a Legal person, by concluding a Subscriber Agreement with Fina shall accept that Fina as a Trust Service Provider has the right to immediately revoke the certificate in the case that the Subscriber violates the terms of the Agreement or the

conditions for providing certification services, or if Fina discovers that the certificate is used as to allow criminal activities to be carried out, such as phishing attacks, fraudulent actions, or malicious code distribution.

In the event of changes to contact data, the Subscriber shall forward the changes to Fina at the contact information listed in Section 9.11 herein.

The Subscriber shall be responsible for irregularities resulting from non-fulfilment of obligations determined in the above provisions referred to in this Section.

A Subscriber who does not act in accordance with the undertaken obligations may have their certificate revoked and shall lose all rights ensuing from the Subscriber Agreement.

9.6.4 Relying party representations and warranties

A Relying Party shall make an autonomous and conscious decision on reasonable certificate reliance.

Reasonable reliance shall be deemed a decision by the Relying Party to rely on a certificate if at the time of reliance the Relying Party has:

- undertaken the necessary precautionary measures and used the certificate for the purposes stipulated in the Policy, that is, under circumstances in which reliance shall be reasonable and in good faith, and under circumstances known or that should have been known to the Relying Party prior to relying on a certificate,
- used the application solution and IT environment on which it can rely,
- checked the certificate validity period,
- checked the certificate revocation, which the Relying Party shall confirm by carrying out verification of the certificate status via the OCSP service or on the basis of the last issued CRL, as stipulated in this Certificate Policy,
- checked if the private key used for authentication corresponds to the public key in the certificate within the certificate validity period.

The use of the public key and certificate by a Relying Party shall be described in Section5.4.2 herein, while the requirements for checking the revocation status of the certificate shall be set out in Section 4.9.6 herein.

The Relying Party who has not abided by the regulations and this Certificate Policy, and has not acted in accordance with the obligations and responsibilities referred to in this Section shall alone bear the risks for reliance on such a certificate.

A Relying Party shall bear all the certificate reliance risks if it shall be aware of or has a reason to believe that facts exist that may cause personal or business damage due to reliance on the certificate.

9.6.5 Representations and warranties of other participants

No stipulations.

9.7 Disclaimer of warranties

Fina shall not be 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 Legal Entity or a natural 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 this document and the operating instructions.

9.8 Limitation of liability

Fina's total financial liability for non-qualified certificates issued according to this Certificate Policy and CPS_{NQC} document [26] for transactions carried out in reliance on certificates issued in such a way shall amount to a maximum of 199,084.21 €.

Unless provided for in a separate agreement or determined otherwise, Fina's maximum financial liability towards a Subscriber and Relying Party, showing reasonable reliance in a certificate, shall be limited in accordance to the recommended financial limits shown in Table 1.4 Fina's maximum financial liability for certificates shall be shown in Table 9.1.

Certificate category	Fina's maximum financial liability		
	By category	By transaction	Total
Certificates of medium level of security - *SSL certificate level 2 (OVCP)*	up to 79,633.69 €	up to 10,617.82 €	199,084.21 €

Table 9.1 Fina's maximum financial liability

9.9 Indemnities

Each participant shall be liable to the damaged party for damages caused by failing to comply with the provisions of this Certificate Policy and relevant regulations in force.

Fina shall accept that the contracted Application Software Supplier through which Fina Root CA is distributed assumes no obligation or potential liability of the Fina set out in this

Certificate Policy or other document due to the issuance or maintenance of certificates or due to trust in the certificate by the Relying or other party.

However, the above mentioned shall not apply to any claim, loss, or damage suffered by the Application Software Supplier in connection with the certificate issued by Fina, and when such claim, loss or damage is directly caused the software of that Application Software Supplier in the event that untrusted certificate was presented as still trusted or has presented as a trusted a certificate:

- which has already expired, or
- which was already revoked (but only if the information on the current revocation status of the certificate at that time from Fina was available online and the application software did not properly verify the status of revocation or neglected the revocation information status).

The Relying Party shall be liable to the damaged party, that is, any other participant if it shall rely on the issued certificate without having checked its validity as described in Section 9.6.4 herein or shall use it contrary to the purposes set out in this Certificate Policy.

9.10 Term and termination

9.10.1 Term

This Certificate Policy document shall be valid until a new Policy document comes into force or until its termination is published. A new document version or published termination of the current version shall be published on the website of the repository referred to in Section 2.2 herein, with an indication of the effective date. The new document shall be assigned a new OID and it shall contain an indication of the modifications made thereto.

9.10.2 Termination

By entering into force of the new version of Certificate Policy document for all certificates issued according to this document, stipulations of this document that cannot be meaningfully replaced by the stipulations of the new version of the Certificate Policy document shall remain in force.

This document termination shall not be bound by nor shall it affect the validity of certificates issued under this document.

Fina may amend some provisions of the Certificate Policy in force, as specified in Section 9.12 herein.

9.10.3 Effect of termination and survival

When a new version of the Policy shall come into force, the provisions of such document shall be applied to all certificates issued from that day on.

Certificates issued under previous Policies shall be valid until their termination, whereby they may be renewed in accordance with the Policy from the new document.

9.11 Individual notices and communication with participants

Individual communication with participants shall be primarily conducted through Fina's Call Centre:

- call free of charge 0800 0080

Individual notifications and other official written communication shall be done using the following contact details:

Contact data for delivery of correspondence to Fina	
Mailing address:	Fina e-Business Centre Ulica grada Vukovara 70 10000 Zagreb Croatia
E-mail:	info.rdc@fina.hr
Fax:	+385-1-6304-081

9.12 Amendments

9.12.1 Procedure for amendments

This Certificate Policy shall be revised as required.

Fina may correct spelling mistakes, change contact data and make other minor corrections not materially affecting the participants without notice to the participants.

All participants may send a letter to the Fina PMA contact address referred to in Section 1.5 herein, containing a proposal for corrections or for the amendments to this document. The letter shall include contact data of the person sending the modification proposal. Upon examination, Fina PMA may accept, adjust or reject proposed modifications.

9.12.2 Notification mechanism and period

All amendments to this Certificate Policy document shall be published in electronic form on the website of the repository referred to in Section 2.2 herein.

New versions of the Policy with amended OID of the Policy shall be published in electronic form on the website of the repository referred to in Section 2.2 herein.

The effective date of amendments or newly-published Policy document shall be indicated on its cover page as well as on the website where it shall be published.

9.12.3 Circumstances under which OID must be changed

Major amendments to the Policy document that may materially affect the participants shall require the change of Policy OID. Fina PMA shall determine the new OID for the new document version.

9.13 Dispute resolution provisions

In the event of a dispute or disagreement between Fina and other participants due to actions and/or procedures regarding certification service provision regulated by this Certificate Policy, 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.

Participants may forward a complaint to Fina if they believe there exist a discrepancy in the content of services in relation to the published terms and conditions of service provision. Fina shall reply to the complaint. Complaints shall be filed on in a paper or electronic form to addresses specified under Section 9.11 herein.

9.14 Governing law

Fina, as a trust service provider, operates at all times in accordance with the laws of the Republic of Croatia in force.

Supervision over the work of Fina in the field of providing trust services is regulated by:

- Regulation (EU) No 910/2014 of the European Parliament and 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 [1],
- Act on Amendments to the Act on the Organisation and Scope of State Administration Bodies (Official Gazette No. 57/2024) [2].

For what is not expressly prescribed in this document, the valid laws of the Republic of Croatia are applicable.

All participants mutually agree with the application of Croatian law for interpretation of the applied provisions.

9.15 Compliance with applicable law

This document and the trust services covered by this document are in compliance with the following provisions:

- Regulation (EU) No 910/2014 of the European Parliament and 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 [1],
- Act on Amendments to the Act on the Organisation and Scope of State Administration Bodies (Official Gazette No. 57/2024) [2],
- The Ordinance on the provision and use of trust services (Official Gazette 60/2019) [3],
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [4],
- Act Implementing General Data Protection Regulation (Official Gazette 42/2018) [5],
- standardization documents ETSI EN 319 401 [10] and ETSI EN 319 411-1 [11] and CA/Browser Forum BRG [23].

9.16 Miscellaneous provisions

No stipulations

9.17 Other provisions

Where feasible, Fina makes accessible trust services provided and end-user products used in the provision of those services to the persons with disabilities, in accordance with following provisions:

- United Nations Convention on the Rights of Persons with Disabilities and Optional Protocol to the Convention on the Rights of Persons with Disabilities, New York 13 December 2006 [6], which the Republic of Croatia signed in New York on March 30, 2007,
- Act on Accessibility of Websites and Software Solutions for Mobile Devices of Public Sector Bodies of the Republic of Croatia (Official Gazette 17/2019) [7] transposing Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies [8].

If the Applicant has some sort of disability, Fina assists the Applicant to apply for the Certificate and to register, which with the Applicant's consent may include conducting his direct identification outside the official Fina premises. Assistance to the Applicant is also provided with requests for revocation of the Certificates.

Fina shall publish this Certificate Policy, CPS_{WSA} [25] document and certification services terms and conditions.

The certification services terms and conditions shall be communicated through a document in paper form or document in electronic form whose authenticity shall be protected.

Before concluding a Subscriber Agreement, Subscribers shall be informed about certification services terms and conditions. Acceptance of the certification services terms and conditions shall be a prerequisite for certificate issuance.

In procedures for certificate re-key, certificate re-key after expiry, revocation or modifications to data in the certificate, Fina shall notify the Custodian about possible amendments to the certification services terms and conditions.