DESCRIPTION OF CHANGES IN THE STRUCTURE OF FINA DIGITAL CERTIFICATES

Version 1.1

Information on the document

Name of document:	Description of changes in the structure of Fina digital certificates
Distribution code	Public
Document owner	FINA
Contact	info.pki@fina.hr

Amendment history

Version	Date	Reason for amendment
1.0	1 Sep 2014	
1.1	17.02.2015.	Changes in the names of production CAs and supplementary services of the future production environment.

CONTENTS

1. Introduction

Fina is preparing changes to its systems for the issuance of digital certificates and time-stamps. These changes pertain to the implementation of the root CA certificate, changes in the structure of the CA certificates, and changes in the structure of end-user certificates and time-stamps. These changes will affect the existing users IT solutions that use Fina certificates and time-stamps, and therefore, **all user solutions using Fina certificates will need to be previously verified to ensure their readiness to use the amended certificates, and if necessary adjustments will have to be made to the user solutions.**

All user IT solutions will, prior to the start of application of these changes in production, will have to be adapted for work with the amended certificates that will be issued in the manner described in this document. Meanwhile, they will also need to continue to support operations with the existing certificates until their expiry. The expiry period for existing user certificates on smart cards and USB tokens (mid-level security certificates) is two years from their date of issuance. The expiry period for the majority of soft certificates (standard level security certificates) is five years from the date of their issuance. Two years from the start of application of these changes, the last issued mid-level security certificates will expire, and five years after the start of application of these changes, the last standard level security certificates issued in the existing production system will expire.

Furthermore, until the start of application of these changes, all solutions using the existing time-stamping service must be adapted for work with the new time-stamping service, as described in this document.

Certificates and time-stamps will be issued pursuant to the changes outlined in this document and will be aligned with the valid international standards in the field of issuing digital certificates, EU standards in the field of electronic signatures, and best practices.

This document provides a detailed description of planned changes in order to provide Fina certificate users complete information on these changes.

The current version of this document can be downloaded from the link:
http://rdc.fina.hr/dokumentacija/description_of_changes_2014.pdf.

1.1. Reasons for introducing changes

Cryptographic algorithms lose their strength over time and gradually provide a decreasing level of security. This occurs as the consequence of the increase of processor strength of new computers, and as the result of progress in cryptographic analysis. In order to maintain or increase the level of security and trust in the issued certificates and time-stamps, and to ensure their continued unhindered usage, it is necessary to implement timely changes to the length of cryptographic keys, i.e. to switch to the use of adequately secure cryptographic algorithms. Fina, as an certification-service-provider (CSP), is obliged to implement changes to its certificates and time-stamps, pursuant to the legislation from the field of electronic signatures and the relevant binding international normative documents.

The objective of these changes is to increase security and trust in the issued certificates and time-stamps issued by Fina, and in doing so, to increase security and trust in the advanced electronic signature, authentication and other applications of certificates and time-stamps.

2. Existing production certificates and Demo certificates

Fina issues its users **production certificates and time-stamps** on its production systems. These certificates and time-stamps are issued and used pursuant to the Electronic Signatures Act.

For the purposes of testing, demonstration and alignment of IT solutions of the users that use Fina certificates and time-stamps, Fina issues **Demo certificates** on its Demo system.

This chapter describes the **existing production certificates and existing Demo certificates** and **existing production time-stamps** issued by Fina. The descriptions given in this section correspond to the existing state, prior to the introduction of the changes.

The description of **future production certificates and future time-stamps** that will be issued by Fina, and the description of the **future two-tiered architecture of production CAs** is found in Section 3.

The description of the **new Demo certificates and new time-stamps** issued by Fina, and the description of the **new two-tiered architecture of CAs in the new Demo environment** is found in Section 4.

2.1. Issuance of production certificates and time-stamps

In the **existing** Fina production environment, production certificates are issued by two certification authorities (CAs): **FINA RDC CA** and **FINA RDC-TDU CA**, and the production time-stamps are issued by the time-stamping service **FINA Servis vremenske ovjere**.

Fina performs the provision of services to issue production certificates and time-stamps pursuant to the Electronic Signatures Act. This Act also regulates the use and reliability of such issued certificates and time-stamps.

2.1.1. Certification authority FINA RDC CA

FINA RDC CA issues qualified, normalised and lightweight certificates for:

- Natural persons – citizens (personal certificates);
- Natural persons associated with legal persons (business certificates); and
- IT equipment associated with legal persons (business certificates for IT equipment).

FINA RDC CA has its own *root* certificate that is intended for the verification of certificates issued by FINA RDC CA.

The basic information on the FINA RDC CA *root* certificate is provided in Table 1. In this table, and those that follow, information is provided in particular regarding the cryptographic algorithms used in the described certificates: signing algorithms used for signing certificates (*signatureAlgorithm*), algorithm associated with the public key in the certificate and in the length of the public key (*SubjectPublicKeyInfo*).

Basic field	Value for the FINA RDC CA *root* certificate
Version	X.509 V3, value=“2“
serialNumber	3f 1b ce 21
signatureAlgorithm	**sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)**
Issuer	ou=RDC, o=FINA, c=HR
Validity	NotBefore: 21 July 2003 11:57:43 NotAfter: 21 July 2023 12:27:43
Subject	ou=RDC, o=FINA, c=HR
SubjectPublicKeyInfo	**rsaEncryption** (**OID: 1.2.840.113549.1.1.1), 2048 bit public key** With the accompanying private key, FINA RDC CA signs every issued certificate and CRL.

Table 1. Basic information on the FINA RDC CA root certificate

The FINA RDC CA *root* certificate may be downloaded from the address http://rdc.fina.hr/CA/RDCca.cer, and the value of its SHA-1 *Thumbprint* (or *Fingerprint*) is:

4c:4b:ed:f2:a8:d7:64:c1:fe:dc:81:af:d6:37:0f:50:30:7a:0a:12.

The basic information on the user certificates issued by FINA RDC CA is shown in Table 2.

Basic field	Value for the certificate issued by FINA RDC CA
Version	X.509 V3, value=“2“
serialNumber	32-bit non-repeatable integer
signatureAlgorithm	**sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)**
Issuer	ou=RDC, o=FINA, c=HR
Validity	NotBefore: Time of issuance of certificate NotAfter: Depending on type of certificate: 1, 2, or 5 years.
Subject	Depending on type of certificate
subjectPublic KeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), 1024 or 2048 bit public key, depending on type of certificate**

Table 2. Basic information on the user certificates issued by FINA RDC CA

A detailed description for each type of certificate issued by FINA RDC CA is found in clause 7.1.1.1 of the document Certificate Policy (currently only available in Croatian).

2.1.2. Certification authority FINA RDC-TDU CA

FINA RDC-TDU CA issues qualified and normalised certificates to state officials and employees in state administration bodies (TDUs).

FINA RDC-TDU CA has its own *root* certificate that is intended for verification of certificates issued by FINA RDC-TDU CA.

The basic information on the FINA RDC-TDU CA *root* certificate is shown in Table 3.

Basic field	Values for the FINA RDC-TDU CA *root* certificate
Version	X.509 V3, value="2"
serialNumber	41 db f1 61
signatureAlgorithm	**sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)**
Issuer	ou=RDC-TDU, o=FINA, c=HR
Validity	NotBefore: 5 January 2005 14:23:47 NotAfter: 5 January 2025 14:53:47
Subject	ou=RDC-TDU, o=FINA, c=HR
SubjectPublicKeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), 2048 bit public key** The accompanying private key FINA RDC-TDU CA signs every issued certificate and CRL.

Table 3. Basic information on the FINA RDC-TDU CA root certificate

The FINA RDC-TDU CA *root* certificate may be accessed at the address http://rdc-tdu.fina.hr/CA/RDC-TDUCA.cer, and the value of its SHA-1 *Thumbprint* (or *Fingerprint*) is:

6e:46:67:b5:5e:5e:e3:4e:ad:8c:c2:1c:fa:a1:0b:b8:bf:c9:a5:30.

Basic information on the user certificates issued by FINA RDC-TDU CA is shown in Table 4.

Basic field	Values for the certificates issued by FINA RDC-TDU CA
Version	X.509 V3, value="2"
serialNumber	32-bit unrepeatable integer
signatureAlgorithm	**sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)**
Issuer	ou=RDC-TDU, o=FINA, c=HR
Validity	NotBefore: Time of issuance of certificate NotAfter: Time of issuance of certificate + 2 years.
Subject	cn=name and surname of signatory, serialNumber=serial number, l=place of TDU seat, ou=organisational unit of 2nd level TDU, oU=organisational unit of 1st level TDU, o=name and identifier of TDU, c=HR
subjectPublic KeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), 1024 bit public key**

Table 4. Basic data on user certificates issued by FINA RDC-TDU CA

A detailed description for each type of certificate issued by FINA RDC-TDU CA is found in clause 7.1.1.2 of the document Certificate Policy (currently only available in Croatian).

2.1.3. Verification of the status of existing production certificates

Prior to its expiry, a certificate may be revoked, suspended or reactivated. Once revoked, a certificate is deemed permanently invalid. A suspension is a temporary revocation of a certificate, and a suspended certificate may be revalidated following the reactivation procedure. The certificate may be deemed reliable by the relying party if the certificate has not expired, and has not been revoked or suspended. The relying party intending to trust a certificate must first perform a verification of the certificate status so as to check any possible revocation or suspension of the certificate.

The verification of the certificate status is performed by verifying the *Certificate Revocation List* (CRL) that is published by the CA. FINA RDC CA and FINA RDC-TDU CA publish the relevant lists of revoked certificates. Each of these two CAs publishes its CRL via the HTTP and LDAP protocols. HTTP and LDP URI to access the CRL where it is possible to verify the certificate status is listed in the extension of the *CRL Distribution Points* in each production certificate. More information on the publication of CRLs for the existing FINA RDC CA and FINA RDC-TDU CA is available in clause 4.10.1 of the document Certificate Policy (currently only available in Croatian).

2.1.4. The time-stamping service FINA Servis vremenske ovjere

The time-stamping service FINA Servis vremenske ovjere is part of the existing production environment, and may be used for any application that requires the reliable determination of the existence of a specific electronic record prior to a moment in time. The time-stamp issued by FINA Servis vremenske ovjere is used to preserve the longevity of electronic signatures.

Users of the time-stamping service may be:

- natural persons – citizens;
- legal persons and state administration bodies;
- natural persons within legal persons or within the state administration bodies.

Basic information on the certificate by which the time-stamping service FINA Servis vremenske ovjere signs time-stamps are provided in Table 5.

Field	Values for the certificate of FINA Servis vremenske ovjere
Version	X.509 V3, value="2"
serialNumber	32-bit unrepeatable integer: 3f 1c 8a 93
signatureAlgorithm	**sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)**
Issuer	ou=RDC-TDU, o=FINA, c=HR
Validity	NotBefore: 8 June 2006 11:33:09 NotAfter: 8 June 2016 12:03:09
Subject	cn=SERVIS VREMENSKE OVJERE TSA1, o=FINA 00332852, c=HR
SubjectPublicKeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), 2048 bit public key** With the accompanying private key, FINA Servis vremenske ovjere signs every issued time-stamp.

Table 5. Basic information on certificate used by FINA Servis vremenske ovjere

The basic information on the profile of the time-stamp issued by FINA Servis vremenske ovjere is provided in Table 6. Information on the used cryptographic algorithm for the calculation of the summary data for which the issuance of the time-stamp is requested (*messageImprint*) and on the signature algorithm used to sign the time-stamp (*signatureAlgorithm*) is also provided.

Field	Values for the time-stamp issued by FINA Servis vremenske ovjere
Version	V1, value="1"
Policy OID	1.3.124.1104.2.1.1.1.2
messageImprint	**hashAlgorithm: sha-1 (OID: 1.3.14.3.2.26)**
serialNumber	integer
genTime	UTC time, 1 second intervals
Nonce	integer
signatureAlgorithm	**sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)**

Table 6. Basic information on the time-stamp issued by the FINA Servis vremenske ovjere

2.1.5. Existing production environment

More detailed information on the existing FINA production environment for the issuance of certificates and time-stamps are available in the documents Certificate Policy , Certification Practice Statement for Qualified Certificates, Certification Practice Statement for Non-Qualified Certificates, Time-Stamping Policy (all documents are currently only available in Croatian), and on the website www.fina.hr/finadigicert.

2.2. Issuance of Demo certificates

Fina Demo digital certificates are digital certificates that are issued for the purposes of testing, demonstration and alignment of users IT solutions, such that these solutions may be properly used by the existing FINA production digital certificates. In the technological and functional manner, Demo certificates are fully identical to the existing FINA production certificates.

Demo certificates are issued on the **existing FINA Demo environment** by **FINA Demo CA** which was established in 2003. Demo certificates are signed by the FINA Demo CA private signing key.

Considering that the existing and new IT solutions should continue to support work with certificates issued by the existing production CAs (FINA RDC CA and FINA RDC-TDU CA), persons and bussines entities that test and develop IT solutions based on FINA certificates may request the issuance of a Demo certificate on the existing FINA Demo environment that corresponds to a certain type of existing FINA production certificate.

The existing and new solutions should also support the work with altered certificates that will be issued by the future production certification authorities Fina RDC 2015 and Fina RDC-TDU 2015. The changes to be introduced in the issuance of production certificates and time-stamps are described in Section **3**, and the time period for the commencement of application of those changes and for the adaptation of the user IT solutions is given in clause 3.6.

2.2.1. Certification authority FINA Demo CA

The FINA Demo CA issues all types of certificates that are, in the technological and functional manner, fully equivalent to the types of certificates issued by the production certification authorities FINA RDC CA and FINA RDC-TDU CA. Though technologically and functionally equivalent to production certificates, the certificates issued by the **FINA Demo CA** may be used **exclusively for testing purposes and for the verification of the proper operation of IT solutions.** The use of Demo certificates may result in trust in an electronic signature, authentication, encryption or any other form of use of a Demo certificate for exclusive use in a test or presentation environment.

The FINA Demo CA has its own root certificate that is intended for the verification of certificates issued by FINA Demo CA.

The basic information on the FINA Demo CA root certificate is provided in Table 7.

Field	Values for the FINA Demo CA root certificate
Version	X.509 V3, value="2"
serialNumber	3e c9 fd 21
signatureAlgorithm	**sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)**
Issuer	ou=DEMO, o=FINA, c=HR
Validity	NotBefore: 20 May 2003 11:32:11 NotAfter: 20 May 2023 12:02:11
Subject	ou=DEMO, o=FINA, c=HR
SubjectPublicKeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), 2048 bit public key**
Thumbprint	Thumbprint algorithm: SHA-1 64 51 28 b9 d9 42 60 64 1b d5 a5 f6 af 4f a6 8e 35 e2 f1 ae

Table 7. Basic information on the FINA Demo CA root certificate

The FINA Demo CA root certificate may be accessed from the http://demo-pki.fina.hr/crl/democacert.cer, and the value of its SHA-1 *Thumbprint* (or *Fingerprint*) is:

64:51:28:b9:d9:42:60:64:1b:d5:a5:f6:af:4f:a6:8e:35:e2:f1:ae.

2.2.2. Verification of status of existing Demo certificates

The verification of the status of existing Demo certificates is performed by verification of the CRL, i.e. in the same manner as the verification of the status of the existing production certificates. The FINA Demo CA publishes the CRL via the HTTP and LDAP protocols. The HTTP and LDP URI to access the CRL where the status of the certificate may be verified is listed in the *CRL Distribution Points* extension in each issued Demo certificate.

2.2.3. Issuance of Demo time-stamps

Time-stamps are not issued within the Fina Demo environment (existing Demo environment).

The new time-stamping service is established in the **Fina Demo 2014 environment (new Demo environment)**.

The Fina Demo 2014 environment is described in Section 4, while the new time-stamping service **Fina Demo TSA 2014** is described in clause 4.1.5 of this document.

3. Changes in the issuance systems for production certificates and time-stamps

The changes introduced in the issuance of production certificates and time-stamps pertain to:

- establishment of a two-tiered architecture of certification authorities (CAs);
- transition to the use of more secure cryptographic algorithms and longer cryptographic keys;
- establishment of new services for the verification of certificate status;
- transition to the service of a qualified time-stamp.

The remainder of this section gives a detailed description of the changes to the system for issuance of production certificates and time-stamps.

3.1. Future two-tier architecture of production Certification Authorities

As part of these changes, Fina is introducing a two-tiered architecture of production Certification Authorities (CAs). The system for certificate issuance will be composed of the new *Root Certification Authority* (*Root CA*) that issues the certificates for the *Subordinate Certification Authorities* (*Subordinate CAs*). The Subordinate Certification Authority issues certificates to end users.

In the future two-tiered architecture of production Certificate Authorities, Fina will have:

- one Root Certification Authority: **Fina Root CA**
- two Subordinate Certification Authorities:
  - **Fina RDC 2015**
  - **Fina RDC-TDU 2015**

Fina RDC 2015 CA will take on the role of the current FINA RDC CA and will issue qualified, normalised and lightweight certificates for:

- natural persons – citizens (personal certificates);
- natural persons associated with a legal persons (business certificates); and
- IT equipment associated with a legal person (business certificates for IT equipment).

Fina RDC-TDU 2015 CA will take over the role of the current FINA RDC-TDU CA and will issue qualified and normalised certificates to state officials and employees in state administration bodies.

The Fina Root CA will issue certificates for the subordinate **Fina RDC 2015** and **Fina RDC-TDU 2015** CAs**.**

Figure 1 shows the future two-tiered architecture of the Fina production CAs.

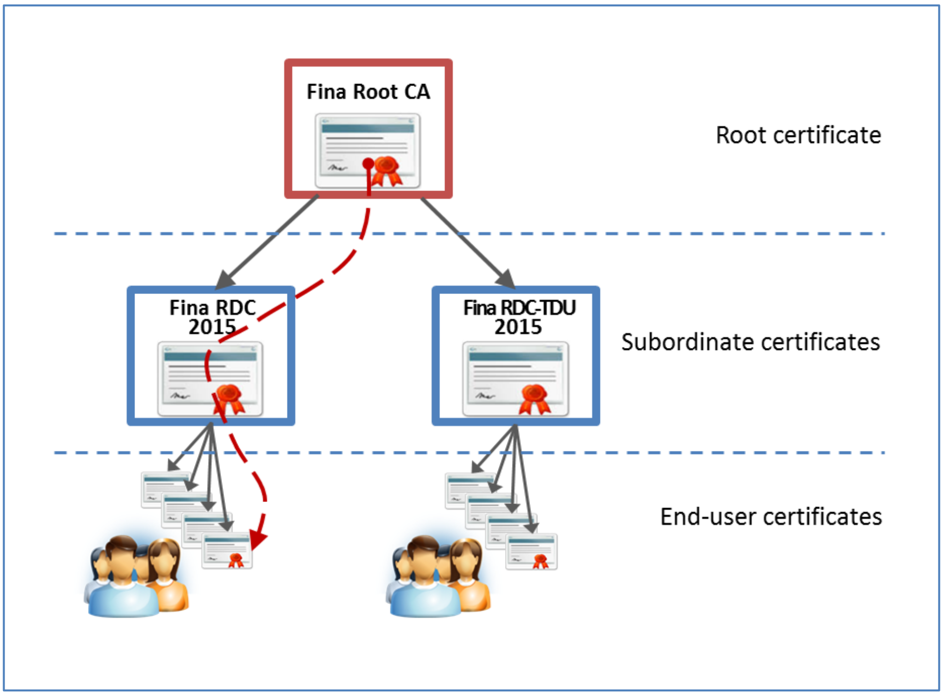

Figure 1. Future two-tier architecture of the Fina production certification authorities

The end-user certificates shown in Figure 1 are issued by, i.e. signed by Fina RDC 2015, or Fina RDC-TDU 2015 CA, respectively, while the Fina RDC 2015 and Fina RDC-TDU 2015 certificates are signed by the Fina Root CA as the *root* CA of the future two-tiered architecture of Fina's production CAs.

The accompanying certification chain, beginning from the Fina Root CA certificate, via one of the subordinate certificates (Fina RDC 2015 or Fina RDC-TDU 2015) to the end-user certificate forms the certificate hain, or chain of trust. Figure 1 shows this in the red dotted line that marks the certificate chain: Fina Root CA - Fina RDC 2015 – End-user certificate.

The Fina Root CA certificate is a self-signing *root* CA certificate that is issued and signed by the Fina Root CA. The Fina RDC 2015 certificate is issued and signed by the Fina Root CA for Fina RDC 2015 CA. The end-user certificate is the certificate which based on the user requirements is issued and signed by Fina RDC 2015 or Fina RDC-TDU 2015 CA.

This type of CA architecture affects the implementation of certificate verification process, which must be carried out by each party wishing to ensure trust in the certificate (relying party). In order for a certain user certificate to be considered valid, one of the steps of certificate verification is construction and verification of the complete Certificate Chain, beginning from the end-user certificate via certificate of the subordinate CA to the root CA certificate. Therefore, it is necessary to verify whether a certain user IT solution using a certificate is able to properly carry out the construction and verification of the complete Certificate Chain. The construction and verification of the Certificate Chain is explained in clause 5.3.

To verify the signatures in the certificate, the public key of the CA issuing the certificate is required. If during the construction of the Certificate Chain a specific CA certificate is not available, it can be accessed using the value of the *Certification Authority Issuer* within the *Authority Information Access* certificate extension. These values contain information on the manner of accessing the CA certificates.

3.2. Transition to more secure cryptographic algorithms and longer keys

Pursuant to the provisions of the legislation in the field of electronic signatures, for issuance of certificates and time-stamps, it is necessary to implement changes to the length of cryptographic keys, and to switch to the use of adequate, more secure cryptographic algorithms. This will increase security and trust in the issued certificates and time-stamps, and ensure their continued unhindered use.

The transition to the use of more secure cryptographic algorithms and longer cryptographic keys will take place as follows:

- Changes to the hash algorithm – instead of the current use of the SHA-1 signature algorithm. For signing certificates, CRL and time-stamps the **SHA-256** algorithm will be used.
- Increasing the length of RSA key pairs:
  - Instead of the current RSA 2048 bit public key, all CA certificates will contain a RSA **4096 bit** public key.
  - Instead of the current 1024 bit public key, all end-user certificates will contain an RSA **2048 bit** public key.

The following provides a detailed description of the changes to the cryptographic algorithms and length of algorithm keys.

3.2.1. Characteristics of the Root CA certificate

Fina Root CA will be the *root* CA for all Fina production certificates, and will issue and sign the Fina Root CA certificate, which will serve as the trust anchor for the future Fina two-tiered architecture, as shown in Figure 1. The Fina Root CA certificate will contain the RSA 4096 bit public key of the Fina Root CA, and each certificate and CRL issued by this CA will be signed by the appropriate private key of the Fina Root CA. The cryptographic algorithms SHA-256 and RSA will be used to sign the certificates and the CRL of the Fina Root CA. The Fina Root CA will issue and sign certificates for the subordinate CAs, Fina RDC 2015 and Fina RDC-TDU 2015.

Information on the future Fina Root CA certificates is provided in Table 8.

Field	Values for the Fina Root CA certificate
Basic field	
Version	X.509 V3, value="2"
serialNumber	Serial number, length 12 or 13 bytes
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**
Issuer	cn=Fina Root CA, o=Financijska agencija, c=HR
Validity	NotBefore: Time of issuance of certificate NotAfter: 31 December 2029
Subject	cn=Fina Root CA, o=Financijska agencija, c=HR
subjectPublicKeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), 4096 bit public key**

Field	Critical	Value
Ekstenzije		
KeyUsage	YES	KeyCertSign, cRLSign
BasicConstraints	YES	cA=true
AuthorityKeyIdentifier	NO	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (determined according to RFC 5280, point 4.2.1.2 method (1))
SubjectKeyIdentifier	NO	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (determined according to RFC 5280, point 4.2.1.2 method (1))

Table 8. Data on the future Fina Root CA certificate

3.2.2. Characteristics of the Fina RDC 2015 and Fina RDC-TDU 2015 CA certificates

The certificates of Fina RDC 2015 and Fina RDC-TDU 2015 will be subordinate certificates to the Fina Root CA certificate, as shown in Figure 1. In relation to the existing certificates for FINA RDC CA and FINA RDC-TDU CA as described in clauses 2.1.1 and 2.1.2, the certificates for Fina RDC 2015 and Fina RDC-TDU 2015 will contain RSA 4096 bit public keys, and will be signed by the Fina Root CA with a RSA 4096 bit private key using the cryptographic algorithms SHA-256 and RSA.

Information on the future certificates for Fina RDC 2015 and Fina RDC-TDU 2015 CAs is provided in Table 9.

Field	Values for Fina RDC 2015 and Fina RDC-TDU 2015 certificates
Basic field	
Version	X.509 V3, value="2"
serialNumber	Serial number, length 12 or 13 bytes
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**
Issuer	cn=Fina Root CA, o=Financijska agencija, c=HR
Validity	NotBefore: Time of issuance of certificate NotAfter: Time of issuance of certificate + 10 years

Subject	For Fina RDC 2015:
	cn=Fina RDC 2015, o=Financijska agencija, c=HR
	For Fina RDC-TDU 2015:
	cn=Fina RDC-TDU 2015, o=Financijska agencija, c=HR

subjectPublic KeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), 4096 bit public keys**

Field	Critical	Value
Extension		
KeyUsage	YES	KeyCertSign, cRLSign

BasicConstraints	YES	cA=true
		pathLen=0

AuthorityKeyIdentifier	NO	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (determined according to RFC 5280, point 4.2.1.2 method (1))
SubjectKeyIdentifier	NO	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (determined according to RFC 5280, point 4.2.1.2 method (1))
certificatePolicies	NO	policyIdentifier: CertPolicyId (OID) for the Fina subordinate certificate, policyQualifiers: policyQualifierId and URI for CP/CPS
Authority Information Access	NO	[1]Authority Info Access accessMethod=Online Certificate Status Protocol (OID: 1.3.6.1.5.5.7.48.1), accessLocation: URL OCSP responder [2]Authority Info Access accessMethod=Certification Authority Issuer (OID: 1.3.6.1.5.5.7.48.2) accessLocation: HTTP URL FINA Root CA certificate
CRLDistributionPoints	NO	• Address of segmented CRL accessible via LDAP protocol • Address of CRL accessible via LDAP protocol • HTTP URL at which CRL list is accessible

Table 9. Data on certificates of Fina RDC 2015 and Fina RDC-TDU 2015

3.2.3. Characteristics of the certificate to be issued by Fina RDC 2015 and Fina RDC-TDU 2015

In relation to the existing end-user certificates issued by FINA RDC CA, or FINA RDC-TDU CA, and whose basic fields are shown in Tables 2 and 4, the end-user certificates to be issued by Fina RDC 2015, or Fina RDC-TDU 2015 will have basic fields as per Table 10.

Basic field	Values for certificates to be issued by Fina RDC 2015 and Fina RDC-TDU 2015 CAs
Version	X.509 V3, value="2"
serialNumber	Positive integer, length 16-17 bytes
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**

Issuer	For Fina RDC 2015:
	cn=Fina RDC 2015, o=Financijska agencija, c=HR
	For Fina RDC-TDU 2015:
	cn=Fina RDC-TDU 2015, o=Financijska agencija, c=HR

Validity	NotBefore: Time of issuance of certificates NotAfter: Depending on type of certificate: 1, 2 or 5 years from issuance of the certificate
Subject	Depending on the type of certificate, equivalent for certificates issued by the existing FINA RDC CA and FINA RDC-TDU CA
subjectPublic KeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), 2048 bit public key**

Table 10. Basic information on the user certificates to be issued by Fina RDC 2015 and Fina RDC-TDU 2015 CAs

3.3. Establishment of new services for verification of certificate status

With the increase in the number of issued certificates, the number of revoked or suspended certificates will also increase, and the length of the CRL will increase, which in turn makes it more demanding for transfer. Furthermore, due to the obligations of the relying party to perform verification of the status of each certificate prior to establishing trust in that certificate, the length of the CRL increases the processing time and certificate status verification time. For that reason, for certificate status verification, the use of a particular online protocol is more recommended: *Online Certificate Status Protocol* (OCSP), and in the near future, we can expect its mandatory application.

The OCSP service is based on the client-responder model in which the OCSP client of the relying party sends the OCSP *Responder* a request regarding the certificate status, and the OCSP Responder sends its response to the client regarding the certificate status.

Within the framework of the future two-tiered architecture, Fina will establish an OCSP service entitled **Fina OCSP 2015,** which will provide information on the status of certificates issued by the Fina Root CA, Fina RDC 2015 and Fina RDC-TDU 2015, as shown in Figure 2 in clause 3.5. Information on the access address of the Fina OCSP 2015 service is contained within the *Authority Information Access* extension of each Fina production certificate. The operation of the Fina OCSP 2015 service will be aligned with the IETF RFC 6960 recommendation.

The Fina OCSP 2015 service will sign responses with the OCSP certificate issued by the Fina production CA that issued the end-user certificate whose status is under verification. If status verification is requested for end-user certificate issued by Fina RDC 2015, then the Fina OCSP 2015 service response will be signed by the certificate issued to the OCSP service by Fina RDC 2015. This is also valid for user certificates issued by Fina RDC-TDU 2015. The response for the status of the Fina RDC 2015 certificate and status of the Fina RDC-TDU 2015 certificate will be signed by the certificate issued to the OCSP service by the Fina Root CA.

The Fina OCSP 2015 service will sign responses with the RSA 2048 bit private key, using the cryptographic algorithms SHA-256 and RSA.

The use of the Fina OCSP 2015 service will reduce the quantity of network traffic, and will accelerate certificate status verification.

In addition to using the Fina OCSP 2015 service, for certificate status verification it will also continue to be possible to use the CRLs. It is recommended that certificate status verification be carried out using the OCSP service, and the status verification using the CRLs may be used as an alternative verification method in the case of inaccessibility of the OCSP service.

Table 11 shows the basic information on the certificates which the Fina OCSP 2015 service uses to sign responses.

Field	Value for certificates of Fina OCSP 2015 service
Version	X.509 V3, value=“2“
serialNumber	Positive integer, length 16-17 bytes
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**
Issuer	Certificate for the OCSP service will be issued by: • cn=Fina Root CA, o=Financijska agencija, c=HR; • cn=Fina RDC 2015, o=Financijska agencija, c=HR; i • cn=Fina RDC-TDU 2015, o=Financijska agencija, c=HR.
Validity	NotBefore: Time of issuance of certificate NotAfter: To be defined
Subject	Depending on the issuer of the certificate for the OCSP service, the Subject DN will be: • cn=Fina Root OCSP, o=Financijska agencija, c=HR; • cn=Fina RDC OCSP 2015, o= Financijska agencija, c=HR; or • cn=Fina RDC-TDU OCSP 2015, o= Financijska agencija, c=HR.
SubjectPublicKeyInfo	**rsaEncryption** (**OID: 1.2.840.113549.1.1.1), 2048 bit public key** The OCSP service will sign responses using the appropriate private key.

Table 11. Basic information on the certificates of the Fina OCSP 2015 service

3.4. Transition to the qualified time-stamping service

Within the framework of these changes, Fina will establish a new time-stamping service that will issue advanced time-stamps pursuant to the legislation in the field of electronic signatures. Since advanced time-stamps can be used together with qualified certificates and are issued on a system that, in terms of the level of security, is equivalent to a qualified certificate issuance system, such advanced time-stamps are also called qualified time-stamps. Qualified time-stamps will be issued by the qualified time-stamping service **Fina QTSA 2015**, which will replace the existing time-stamping production service, i.e. FINA Servis vremenske ovjere. The manner of accessing the Fina QTSA 2015 service will be the same as accessing the existing FINA Servis vremenske ovjere, i.e. only those authorised users signing into the service with a certificate (SSL/TLS with client authentication certificate – two-way SSL) will be able to use the Fina QTSA 2015.

The certificate for Fina QTSA 2015 will be issued by Fina RDC 2015, and the qualified time-stamps will be signed with the RSA 2048 bit private key of the Fina QTSA 2015 service, using the cryptographic algorithms SHA-256 and RSA.

The basic data on the certificate of the service Fina QTSA 2015 with which that service will sign qualified time-stamps is provided in Table 12.

Field	Value for the certificate of the Fina QTSA 2015 service
Version	X.509 V3, value=“2“
serialNumber	Positive integer, length 16-17 bytes
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**
Issuer	cn=Fina RDC 2015, o=Financijska agencija, c=HR

Field	Value for the certificate of the Fina QTSA 2015 service
Validity	NotBefore: Time of issuance of certificate NotAfter: To be defined
Subject	cn=*Naziv TSU*, o=Financijska agencija, c=HR
SubjectPublicKeyInfo	**rsaEncryption** (**OID: 1.2.840.113549.1.1.1), 2048 bit public key** The accompanying private key of the Fina QTSA 2015 service signs every issued qualified time-stamp.

Table 12. Basic information on the certificate of the Fina QTSA 2015 service

The basic information on the profile of the time-stamps to be issued by the Fina QTSA 2015 service is provided in Table 13. Special emphasis is placed on information on cryptographic algorithms used to calculate hash of data for which the issuance of the time stamp (messageImprint) is requested and the signing algorithm used to sign the time stamp (signatureAlgorithm).

Field	Value for the time-stamp of the FINA QTSA 2015 service
Version	V1, value="1"
Policy OID	*Fina's Policy OID for the qualified time-stamping service*
messageImprint	**Supported hash algorithms:** • **hashAlgorithm: sha-1 (OID: 1.3.14.3.2.26) and** • **hashAlgorithm: sha-256 (OID: 2.16.840.1.101.3.4.2.1)**
serialNumber	Integer
genTime	UTC time, 1 second intervals
Nonce	Integer
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**

Table 13. Basic information on the time-stamp to be issued by the Fina QTSA 2015 service

3.5. Overview of the future production environment

Figure 2 shows the certificates and services of the future two-tiered Fina production environment for the issuance of certificates and time-stamps that is described in clauses 3.1 to 3.4.

In order to facilitate the verification and adaptation of existing user IT solutions with the operations with the future production certificates and time-stamps, Fina has established the new Fina Demo 2014 environment, which is described in Section 4.

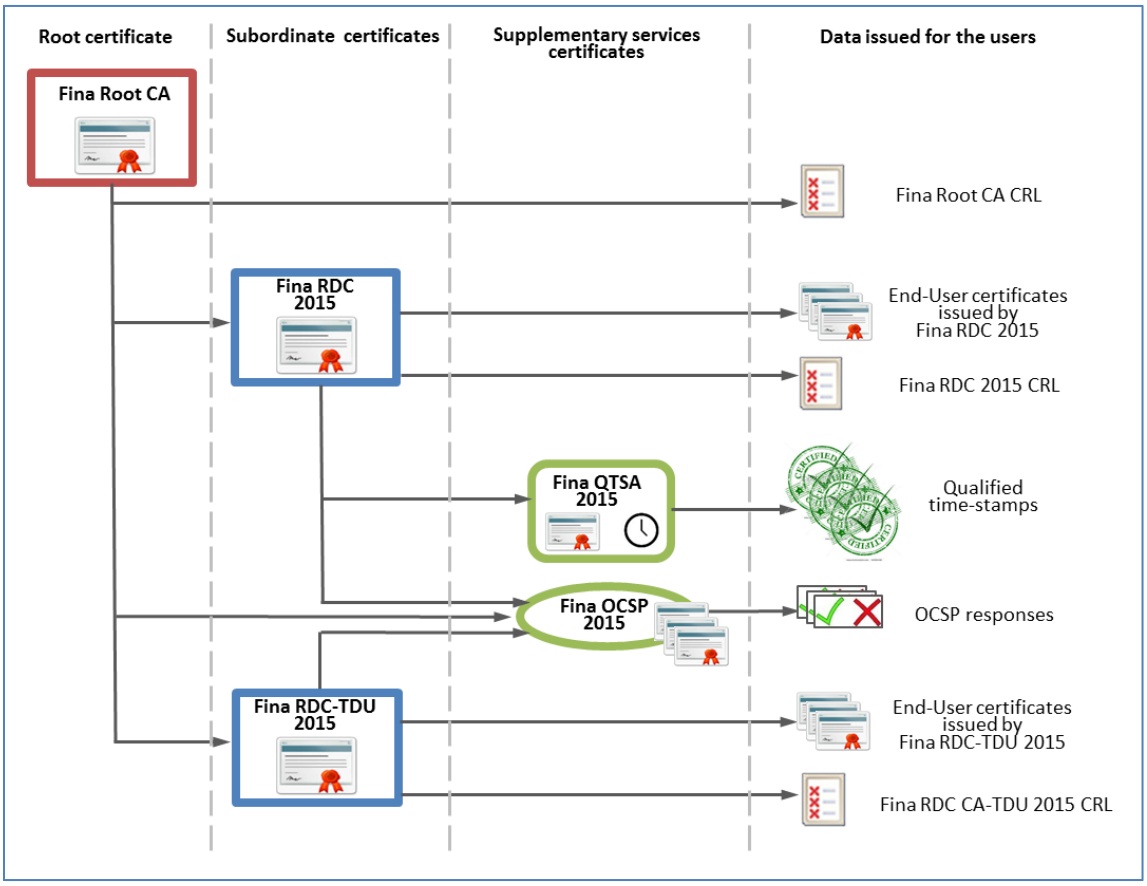

Figure 2. Future production environment for the issuance of certificates and time-stamps

3.6. Start of application and the necessary adaptations for IT solution users

The changes described in this section will affect existing and new user IT solutions that use Fina certificates and time-stamps. Therefore, it will be necessary to conduct previous checks of all user solutions to verify their readiness to use the amended future production certificates and, if necessary, to conduct adjustments to certain solutions.

The scope of adaptations depends on the concrete solution, the way in which the solution is actualised, and the possibilities built into the solution. Due to the large number of users and the diversity of existing solutions on the one hand, and given the necessity and importance of changes on the other, in selecting a deadline for the start of applications, efforts were made to ensure sufficient time for the testing and adaptation of IT solutions, while also ensuring a timely start to the said changes, in which certificate security will not be diminished.

The start of application of these changes in production will be in the **4th quarter of 2015**. At that time, Fina RDC 2015 and Fina RDC-TDU 2015 will begin issuing the first production user certificates, and the status of those certificates will be able to be verified using the Fina OCSP 2015 service. Each issuance and renewal of certificates will be performed on Fina RDC 2015, or on Fina RDC-TDU 2015. Directly before the start of issuance of the first production user certificates by Fina RDC 2015 and Fina RDC-TDU 2015, the existing FINA

RDC CA and FINA RDC-TDU CA will cease the issuance and renewal of user certificates, but will continue to issue the accompanying CRL in the prescribed time periods.

Furthermore, the start of application of these changes also includes the start of operations of the Fina QTSA 2015 service, which will begin to issue qualified time-stamps to all current users of the time-stamping service FINA Servis vremenske ovjere. Immediately prior to the start of application of changes in production, FINA Servis vremenske ovjere will cease its operations.

Until the start of application of the said changes in production, all solutions using the existing time-stamping service FINA Servis vremenske ovjere should be adapted for the use of the qualified time-stamping service Fina QTSA 2015.

The existing user certificates, whose validity deadlines expire after the start of application of these changes in production, will continue to be valid, and will be able to be used without hindrance until the end of their expiry period. As until that time, the status of certificates will be able to be verified using the FINA RDC CRL, or the FINA RDC-TDU CRL. These certificates will, as previously, be able to be renewed prior to their expiry, and renewed certificates will be issued by Fina RDC 2015, or Fina RDC-TDU 2015.

Until the start of application of the said changes in production, all the adjusted user IT solutions and possible new solutions should be adapted to operate with:

- certificates issued by Fina RDC 2015 and Fina RDC-TDU 2015, including performing proper certificate verifications according to the described two-tier CA architecture, and
- certificates issued by the existing FINA RDC CA and FINA RDC-TDU CA.

Every adapted user solution should ensure the stated simultaneous support, as for a period of two or five years (depending on the type of certificates the solution is using), there will be existing users that have been issued certificates by the existing FINA RDC CA and FINA RDC-TDU CA, while an increasing number of users will appear that have certificates issued by the future Fina RDC 2015 and Fina RDC-TDU 2015. Namely, the certificates issued in the 4th quarter of 2015 by the existing CAs (depending on the certificate types) will be valid until the 4th quarter of 2017, or the 4th quarter of 2020. Until that time, there will be final users that still have valid certificates issued by the existing FINA RDC CA and FINA RDC-TDU CA, and meanwhile, users with certificates issued by Fina RDC 2015 and Fina RDC-TDU 2015 CAs will gradually appear and their numbers will increase.

In order to facilitate the testing and adaptation of existing solutions for owners of IT solutions that use the Fina digital certificates, the Fina Demo 2014 environment was created. This environment issue Demo certificates and time-stamps for the purposes of testing and adapting solutions. The issuance of certificates and time-stamps in the Fina Demo 2014 environment is described in the following section.

4. Issuance of new Demo certificates and time stamps

The Fina Demo CA 2014 environment is a newly established Demo environment in the Fina two-tiered CA architecture. In this environment, Demo digital certificates and Demo time-stamps are issued, and used to verify and adapt existing user IT solutions for work with future production certificates and time-stamps. The certificates and time-stamps issued in the Fina Demo 2014 environment may be used **exclusively for the purpose of testing and verification of the operation of IT solutions.** The use of Demo certificates and Demo time-stamps may result in trust in an electronic signature, authentication, encryption or any other form of use of a Demo certificate or Demo time-stamp for the exclusive application in a test or presentation environment.

Demo certificates are issued in the Fina Demo 2014 environment in line with the new (amended) profiles that, in the technological and functional sense, are completely equivalent to the profiles of the future Fina production certificates. In this environment, certificates for end-users are issued by the **Fina Demo 2014 CA**.

Status verification of certificates issued by the **Fina Demo 2014 CA** may be performed using the CRLs or using the **Fina Demo OCSP 2014** service. The operating mode of the Fina Demo OCSP 2014 service is equivalent to the operating mode of the future production Fina OCSP 2014 service.

The Demo time-stamps issued in the Fina Demo 2014 environment are, in the technological and functional manner, fully equivalent to the amended profile of the future Fina qualified time-stamps. In the Fina Demo 2014 environment, time-stamps are issued by the **Fina Demo TSA 2014** time-stamping service.

The *Root* CA for the Fina Demo 2014 environment is the **Fina Demo Root CA,** which issues itself self-signed Fina Demo Root CA certificate.

4.1. Two-tier architecture of certification authorities in the new Demo environment

The CA architecture in the Fina Demo 2014 environment is shown in Figure 3, and consists of the Fina Demo Root CA and subordinate Fina Demo CA 2014.

End-User Demo certificates are issued and signed by the Fina Demo CA 2014, while the certificate of Fina Demo CA 2014 is signed by the Fina Demo Root CA.

The red dotted line in Figure 3 shows the certification chain, which begins with the Fina Demo Root CA certificate, via the Fina Demo CA 2014 to the end-user certificate, thereby forming the Certification Chain.

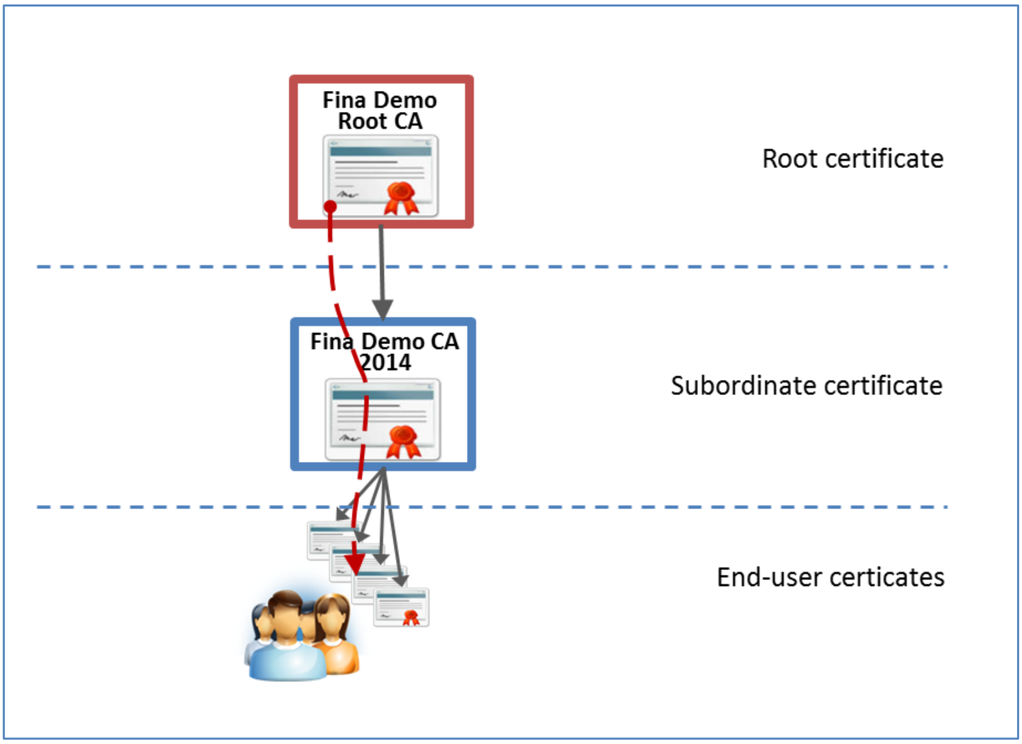

Figure 3. CA architecture in the Fina Demo 2014 environment

4.1.1. Characteristics of the Fina Demo Root CA certificate

The Fina Demo Root CA is the *root* CA for the Fina Demo 2014 environment, and has an issued Fina Demo Root CA certificate which contains the RSA public key of that CA. The public key length is 4096 bits, and each certificate and CRL issued by the Fina Demo Root CA is signed by the accompanying Fina Demo Root CA private key. The cryptographic algorithms SHA-256 and RSA are used to sign the certificates and the CRL of the Fina Demo Root CA.

Information on the Fina Demo Root CA certificate is shown in Table 14.

Field	Value for the Fina Demo Root CA certificate
Basic field	
Version	X.509 V3, value="2"
serialNumber	Serial number, length 12 or 13 bytes
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**
Issuer	cn=Fina Demo Root CA, o=Financijska agencija, c=HR
Validity	NotBefore: 18 March 2014. 11:45:00 NotAfter: 18 March 2034. 12:15:00
Subject	cn=Fina Demo Root CA, o=Financijska agencija, c=HR
subjectPublicKeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), 4096 bit public key**

Field	Critical	Value
Extension		
KeyUsage	YES	KeyCertSign, cRLSign

Field	Critical	Value
Extension		
BasicConstraints	YES	cA=true
AuthorityKeyIdentifier	NO	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (determined according to RFC 5280, point 4.2.1.2 method (1))
SubjectKeyIdentifier	NO	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (determined according to RFC 5280, point 4.2.1.2 method (1))

Table 14. Information on the Fina Demo Root CA certificate

The Fina Demo Root CA certificate may be accessed at the address: http://demo-pki.fina.hr/certifikati/demo2014_root_ca.cer, and the value of its SHA-1 *Thumbprint* (or *Fingerprint*) is:

cf:06:2e:51:85:79:c3:ad:c6:ce:20:a9:4a:88:52:89:88:3b:aa:2a.

4.1.2. Characteristics of the certificate for Fina Demo CA 2014

The certificate for the Fina Demo CA 2014 is the subordinate certificate of the Fina Demo Root CA certificate as shown in Figure 3, and contains an RSA 4096 bit public key. This certificate is signed by the Fina Demo Root CA with its RSA 4096 bit private key, using the cryptographic algorithms SHA-256 and RSA.

Information on the certificate for Fina Demo CA 2014 is provided in Table 15.

Field	Value for the Fina Demo CA 2014 certificate
Basic field	
Version	X.509 V3, value="2"
serialNumber	Serial number, length 12 or 13 bytes
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**
Issuer	cn=Fina Demo Root CA, o=Financijska agencija, c=HR
Validity	NotBefore: 25 March 2014 6:45:47 NotAfter: 25 March 2024 7:15:47
Subject	cn=Fina Demo CA 2014, o=Financijska agencija, c=HR
subjectPublic KeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), 4096 bit public key**

Field	Critical	Value
Ekstenzije		
KeyUsage	YES	KeyCertSign, cRLSign

BasicConstraints	YES	cA=true
		pathLen=0

AuthorityKeyIdentifier	NO	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (determined according to RFC 5280, point 4.2.1.2 method (1))
SubjectKeyIdentifier	NO	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (determined according to RFC 5280, point 4.2.1.2 method (1))

Field	Critical	Value
Ekstenzije		

certificatePolicies	NO	policyIdentifier: CertPolicyId (OID): 1.3.124.1104.5.1.1 policyQualifiers: • policyQualifierId za CP/CP • http://demo-pki.fina.hr/cps/cpdemoroot1-0.pdf
Authority Information Access	NO	[1]Authority Info Access accessMethod=Online Certificate Status Protocol (OID: 1.3.6.1.5.5.7.48.1) accessLocation: URL=http://demo2014-ocsp.fina.hr [2]Authority Info Access accessMethod=Certification Authority Issuer (OID: 1.3.6.1.5.5.7.48.2) accessLocation: http://demo-pki.fina.hr/certifikati/demo2014_root_ca.cer
CRLDistributionPoints	NO	• HTTP URL at which the CRL list is accessible • Address of the segmented CRL accessible via the LDAP protocol

Table 15. Information on the certificate for Fina Demo CA 2014

The Fina Demo CA 2014 certificate may be accessed from the address: http://demo-pki.fina.hr/certifikati/demo2014_sub_ca.cer, and the value of its SHA-1 *Thumbprint* (or *Fingerprint*) is:

be:50:56:0c:61:64:97:ce:7d:75:8d:0c:f3:b9:89:76:6e:ef:8f:81.

4.1.3. Characteristics of end-user certificates issued by Fina Demo CA 2014

The profiles of end-user certificates issued by the Fina Demo CA 2014 are equivalent to the future profiles to be issued by Fina RDC 2015 and Fina RDC-TDU 2015. The basic fields of the end-user certificates issued by the Fina Demo CA 2014 are shown in Table 16.

Basic field	Value for the certificates issued by Fina Demo CA 2014
Version	X.509 V3, value="2"
serialNumber	Positive integer, length 16-17 bytes
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**
Issuer	cn=Fina Demo CA 2014, o=Financijska agencija, c=HR
Validity	NotBefore: Time of issuance of certificate NotAfter: Depending on type of certificate: 1, 2 or 5 years from issuance of certificate
Subject	Depending on type of certificate, equally as for certificates issued by the existing FINA RDC CA and FINA RDC-TDU CA
subjectPublic KeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), 2048 bit public key**

Table 16. Basic information on the end-user certificates issued by Fina Demo 2014 CA

The complete description of all profiles of end-user certificates issued by Fina Demo 2014 CA is provided in the document Profiles of user Fina Demo 2014 certificates.

4.1.4. Fina Demo OCSP 2014 service

Within the Fina Demo 2014 environment, an OCSP service has been established, and is called **Fina Demo OCSP 2014.** This provides information on the status of the certificates issued by the Fina Demo Root CA and Fina Demo CA 2014, as shown in Figure 4 in clause 4.2. The operation of this service is aligned with the IETF RFC 5019 recommendation, while the future production Fina OCSP 2015 service will be fully compatible with the IETF RFC 6960 recommendation.

The access address of this service is http://demo2014-ocsp.fina.hr. Information on the access address of the service is found in the *Authority Information Access* extension of every certificate issued in the Fina Demo 2014 environment.

The Fina Demo OCSP 2014 service will sign the response to the OCSP certificate issued by Fina Demo CA 2014, or the Fina Demo Root CA, depending on the issuer of the certificate whose status is requested. If verification is requested for an end-user certificate issued by Fina Demo CA 2014, then the Fina Demo OCSP 2014 service response will be signed with the certificate issued to the OCSP service by Fina Demo CA 2014. The response for the status of the Fina Demo CA 2014 certificate will be signed with the certificate issued to the OCSP service by the Fina Demo Root CA.

The Fina Demo OCSP 2014 service will sign responses with an RSA 2048 bit public key, with the use of the cryptographic algorithms SHA-256 and RSA.

The status verification of Demo certificates may continue to be performed using the CRL.

Table 17 shows the data of certificates with which the Fina Demo OCSP 2014 service will sign responses.

Field	Value for the certificate Fina Demo OCSP 2014 service
Basic field	
Version	X.509 V3, value="2"
serialNumber	Serial number, length 12 or 13 bytes
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**
Issuer	cn=Fina Demo Root CA, o=Financijska agencija, c=HR
Validity	NotBefore: Time of issuance of certificate NotAfter: Time of issuance of certificate + 12 months

Subject	For signing the status of certificates issued by the Fina Demo Root CA
	cn=Fina Demo Root OCSP, o=Financijska agencija, c=HR
	For signing the status of certificates issued by Fina Demo CA 2014
	cn=Fina Demo OCSP 2014, o=Financijska agencija, c=HR

subjectPublic KeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), 2048 bit public key**

Field	Critical	Value
Extension		
KeyUsage	YES	digitalSignature, nonRepudiation
extKeyUsage	NO	OCSPSigning
ocsp-nocheck	NO	value NULL

Field	Critical	Value
Extension		
AuthorityKeyIdentifier	NO	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (determined according to RFC 5280, point 4.2.1.2 method (1))
SubjectKeyIdentifier	NO	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (determined according to RFC 5280, point 4.2.1.2 method (1))
certificatePolicies	NO	policyIdentifier: CertPolicyId (OID): 1.3.124.1104.5.32.9.3.2 policyQualifiers: • policyQualifierId for CP/CP • http://demo-pki.fina.hr/cps/cpdemoroot1-0.pdf
Authority Information Access	NO	[1]Authority Info Access accessMethod=Online Certificate Status Protocol (OID: 1.3.6.1.5.5.7.48.1) accessLocation: URL=http://demo2014-ocsp.fina.hr [2]Authority Info Access accessMethod=Certification Authority Issuer (OID: 1.3.6.1.5.5.7.48.2) accessLocation: For signing the status of certificates issued by Fina Demo Root CA http://demo-pki.fina.hr/certifikati/demo2014_root_ca.cer For signing the status of certificates issued by Fina Demo CA 2014 http://demo-pki.fina.hr/certifikati/demo2014_sub_ca.cer
CRLDistributionPoints	NO	• HTTP URL at which the CRL list is available • Address of the CRL accessible via the LDAP protocol • Address of the segmented CRL accessible via the LDAP protocol

BasicConstraints	NO	cA=FALSE
		pathLenConstraint=None

Table 17. ***Information on the certificates of the Fina Demo OCSP 2014 service***

4.1.5. Fina Demo TSA 2014 time-stamping service

Within the Fina Demo 2014 environment, the time-stamping service **Fina Demo TSA 2014** has been established. Access to this service and the form of the time-stamp is equivalent to the qualified time-stamp that will be issued by the future qualified time-stamping service Fina QTSA 2014.

Only authorised users have access to the Fina Demo TSA 2014 service. Sign in to this service is performed using a user certificate (establishment of SSL/TLS with the client authentication certificate – *two-way* SSL). The user certificate for sign in to the service is issued by Fina Demo CA 2014.

The certificate for the Fina Demo TSA 2014 is issued by Fina Demo CA 2014, and the issued time-stamps are signed by the RSA 2048 bit private key of the Fina Demo TSA 2014 service, using the cryptographic algorithms SHA-256 and RSA.

Information on the certificates of the Fina Demo TSA 2014 service, with which the time-stamping service signs time-stamps, is shown in Table 18.

Field	Values for the certificate of the Fina Demo TSA 2014 service
Basic field	
Version	X.509 V3, value=“2“
serialNumber	Serial number, length 16 or 17 bytes
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**
Issuer	cn=Fina Demo CA 2014, o=Financijska agencija, c=HR
Validity	NotBefore: Time of issuance of certificate NotAfter: To be defined
Subject	cn=Fina Demo TSA1 2014, o=Financijska agencija, c=HR
subjectPublic KeyInfo	**rsaEncryption (OID: 1.2.840.113549.1.1.1), 2048 bit public key**

Field	Critical	Value
Ekstenzije		
KeyUsage	YES	digitalSignature, nonRepudiation
extKeyUsage	NO	timeStamping
AuthorityKeyIdentifier	NO	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (determined according to RFC 5280, point 4.2.1.2 method (1))
SubjectKeyIdentifier	NO	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (determined according to RFC 5280, point 4.2.1.2 method (1))
certificatePolicies	NO	policyIdentifier: CertPolicyId (OID): 1.3.124.1104.5.32.52.4.3 policyQualifiers: • policyQualifierId for CP/CP • http://demo-pki.fina.hr/cp/cpdemo2014v1-0.pdf
Authority Information Access	NO	[1]Authority Info Access accessMethod=Online Certificate Status Protocol (OID: 1.3.6.1.5.5.7.48.1) accessLocation: URL=http://demo2014-ocsp.fina.hr [2]Authority Info Access accessMethod=Certification Authority Issuer (OID: 1.3.6.1.5.5.7.48.2) accessLocation: http://demo-pki.fina.hr/certifikati/demo2014_sub_ca.cer
CRLDistributionPoints	NO	• HTTP URL at which the CRL list is accessible • Address of the CRL accessible via the LDAP protocol • Address of the segmented CRL accessible via the LDAP protocol

BasicConstraints	NO	cA=FALSE
		pathLenConstraint=None

Table 18. Information on the certificates of the Fina Demo TSA 2014 service

Basic information on the profile of time-stamps issued by the Fina Demo TSA 2014 service are provided in Table 19.

Field	Value for the time-stamps issued by the Fina Demo TSA 2014 service
Version	V1, value=“1“
Policy OID	1.3.124.1104.2.32.1.1.0
messageImprint	**Supported hash algorithms:** • **hashAlgorithm: sha-1 (OID: 1.3.14.3.2.26) and** • **hashAlgorithm: sha-256 (OID: 2.16.840.1.101.3.4.2.1)**
serialNumber	Integer

Field	Value for the time-stamps issued by the Fina Demo TSA 2014 service
genTime	UTC time, 1 second intervals
Nonce	Integer
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**

Table 19. Basic information on the time-stamps issued by the Fina Demo TSA 2014 service

4.2. Overview of the new Demo environment

Figure 4 shows the certificates and services of the new two-tiered Fina Demo 2014 environment for the issuance of certificates and time-stamps, as outlined in clauses 4.1.1 to 4.1.5.

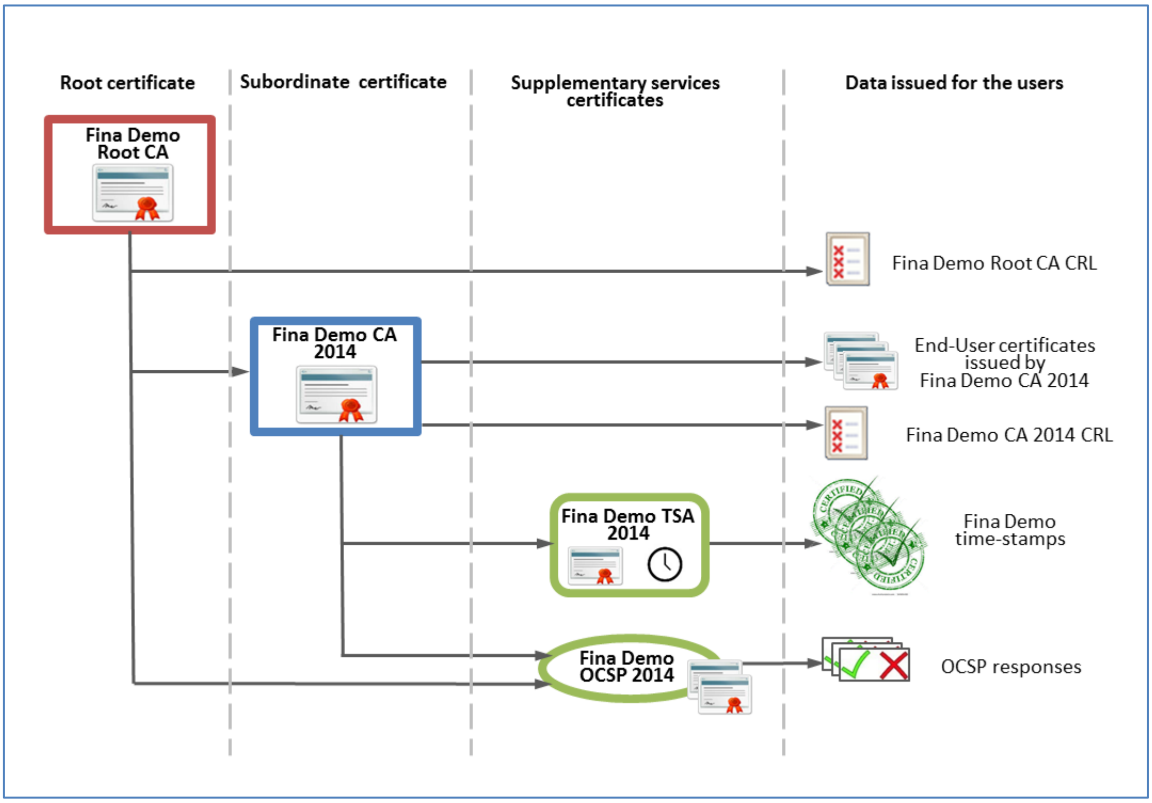

Figure 4. Fina Demo 2014 environment

5. Additional information

5.1. Valid legislation

An overview of the valid legislation in the field of electronic signatures is given below.

The legislation in the field of electronic signatures in the Republic of Croatia is comprised of:

- Electronic Signatures Act (OJ 10/02, 80/08 and 30/14);
- Ordinance on records of certification services providers in the Republic of Croatia (OJ 107/10);
- Ordinance on the creation of electronic signatures, use of electronic signatures creation means, general and special operating conditions for providers of the services of issuing time-stamps and certificates (OJ 107/10 and 89/13);
- List of normative documents in the field of application of the Electronic Signatures Act and the Ordinance on the creation of electronic signatures, use of electronic signatures creation means, general and special operating conditions for providers of the services of issuing time-stamps and certificates in the operations of certification services providers in the Republic of Croatia (OJ 89/13);
- Regulation on the scope, content and leader of certification tasks for electronic signatures for state administration bodies (OJ 146/04).

The said legislation is aligned with Directive 1999/93/EC of the European Parliament and of the Council within the framework of the Electronic Signatures Community.

5.2. List of standards documents and recommendations

In the area of changes described in this document, the following HRN and HRS Croatian normative documents, and the IETF RFC recommendations are competent:

Profile of certificates and CRLs

- IETF RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- IETF RFC 6818 – Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Profile of qualified certificates

In addition to the previous two documents that regulate the profile of certificates and CRLs, two additional documents are relevant for the profile of qualified certificates:

- HRN ETSI/EN 319 412-5 V1.1.1:2013 – Electronic Signatures and Infrastructures (ESI) – Profiles of Trust Service Providers issuing certificates; – Part 5: Extensions for Qualified Certificateprofile (EN 319 412-5 V1.1.1:2013)

- IETF RFC 3739 – Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

OCSP service

- IETF RFC 6960 – X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol - OCSP
- IETF RFC 5019 - The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments

Cryptographic algorithms and parameters

- HRS ETSI/TS 102 176-1 V2.1.1:2012 – Electronic Signatures and Infrastructures (ESI) – Algorithms and Parameters for Secure Electronic Signatures; – Part 1: Hash functions and asymmetric algorithms (ETSI/TS 102 176-1 V2.1.1:2011)

Profile of time-stamps

- HRS ETSI/TS 101 861 V1.4.1:2012 – Electronic Signatures and Infrastructures (ESI) – Time stamping profile (ETSI/TS 101 861 V1.4.1:2011)
- IETF RFC 3161 (2001) Internet X.509: Public Key Infrastructure: Time-Stamp Protocol (TSP)

5.3. Construction and verification of the Certificate Chain

For the construction and verification of the Certificate Chain, in addition to the certificate under verification, all the certificates forming the Certificate Chain to the *root* certificate (*trust anchor*) are required. In order to verify the certificate validity status, it is necessary to verify the certificate validity status of all certificates in that chain. For the validity status of the construction of the Certificate Chain, it is necessary that the implementation be aligned with the IETF RFC 5280 and IETF RFC 6818 recommendations.

The only certificate that must be previously determined is the *root* certificate. It is possible to reach the remaining certificates for construction of the Certificate Chain by using the data in the *Authority Information Access* extension on the issued certificate, using the series of certificates available through the exchange of messages or from the temporary certificate storage.

It is recommended that only the *root* certificate is defined, as fixed for example, as the resource of the software solution or at the level of the operating system, or the software library (depending on the intended use of the software solution), and that the certificates of direct issuers be considered variable.

During implementation, the IETF RFC 5914 recommendations may be consulted.

Furthermore, it is recommended that the entire Certificate Chain is included in the exchange of messages, from the top certificate to the certificate in question (i.e. signing or server certificate).

For example, in the SSL/TLS initial exchange, the server may include the entire Certificate Chain in the *Server Certificate* message. Furthermore, the XAdES standard for the advanced XML electronic signature permits a series of certificates in the *CertificateValues* element.

5.4. Processing and overview of names in certificates

The distinguished names in certificates (e.g. DNs in the attributes *Subject* and *Issuer*) issued by Fina CAs are encoded in the UTF-8 code page (UTF8String according to ISO/IEC 10646, IETF RFC 2279). Therefore, in the display, or the manipulation of these data (i.e. comparison or analysis operations), the possibility that names may contain symbols not on the US-ASCII code page must be taking into consideration.

For name files, the X.501 *Name* (ISO/IEC 9594-2:2005) structure is used, which consists of a series of *Relative Distinguished Names* (RDN), and each relative name consists of one or more pairs of attributes – attribute values whose order may be arbitrary.

It is recommended that the support of the operating system or software library containing all the necessary rules of name encoding and analysis of their individual parts be used in processing names in certificates. The implementation of analysis of individual parts of names implemented over the name from the certificate encoded as a series of symbols could lead to the incorrect interpretation of the name.

The recommendation of this document is that the name from the certificate, encoded as a series of symbols, is used only for the purpose of display, and that the standard representation of names be used in the series of symbols as defined by the IETF RFC 4514 recommendation.