InfoCert Certificate Service Provider

Certificate policy for test certificates

OID: 1.3.76.36.1.1.21

Table of Contents

1. Introduction

The present document states the rules and the operational procedures to be followed for the issuing of X.509 certificates with test purposes.

Requiring a certificate under this policy entails the complete acceptance of the rules stated hereafter.
References to this policy are inside the certificates, in compliance with the applicable standard (see the "Normative reference" section).
The relying parties using this certificates for a signature verification are so informed about the purposes of the certificates and the limitations of liability.

InfoCert can change this document at any time. Any new version supersedes the previous one.
For a certificate, the applicable policy is the one in force at the time of its issuing, till the certificate expiration.

Version and issuing date are on the footer of each page. This policy has the OID:1.3.76.36.1.1.21

InfoCert	1.3.76.36
Certification-Service-Provider	1.3.76.36.1
Certificate-policy	1.3.76.36.1.1
Test certificates	1.3.76.36.1.1.21

This policy is published on the web site:http://www.firma.infocert.it

1.1. Changes

Versione/Release n° :	1.0	**Data Versione/Release** :	02/04/2009
Descrizione modifiche:	None		
Motivazioni :	First issue		

1.2. Scope of the certificates

The key pairs and the certificates generated and issued under this policy are for test purposes only and do not have any legal value.
InfoCert assumes NO LIABILITY for the usage of key pairs and certificates issued under this policy.
Any information included in the certificate is for test purposes only.

1.3. Terms and definitions

Refers to the Normative Reference section

1.4. Responsability

InfoCert is responsible of this document.

1.5. Contacts

InfoCert S.p.A.
Responsabile Certificazione Digitale e Sistemi
Corso Stati Uniti 14
35127 Padova
Phone: +39 049828 8111
Fax: +39 049 828 8406
Web: http://www.firma.infocert.it
e-mail: firma.digitale@InfoCert.it

1.6. Normative references

[1] ETSI TS 102 042 "*Policy requirements for certification authorities issuing public key certificates*" – Aprile 2002
[2] RFC 5280 (2008): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile"
[3] RFC 3161 (2001): " Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)"
[4] RFC 2527 (1999): "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"
[5] Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8
[6] PKCS 12 v1.0: Personal Information Exchange Syntax

2. Service features

2.1. Certificate Service provider

Name	**InfoCert - Società per azioni**
Main site	**Via G.B. Morgagni 30H 00161 Roma**
Legal representative	Dott. Daniele Vaccarino
Phone	**+39 06442851**
fax	**390644285255**
VAT number and Business register number	**7945211006**
Web site	http://www.firma.infocert.it/

2.2. Subjects

The certificate subject can be a physical person, a legal entity (i.e. a company/corporation), a device, a website, other.

2.3. Timing

The timing for the key pairs generation and for the issuing of the certificate will be agreed separately.

3. Procedures

Since the scope of the certificate is for test only, there are no strict rules for the issuing of the certificates.
Who requires the certificate SHALL sign an agreement with InfoCert, explicitly accepting the rules stated in this policy. If the agreement foresees a payment, the certificate will be issued only after Infocert will have received the confirmation.
Then, who requires the certificate SHALL send the data to fill in the certificate (fields in bold are mandatory):

- **Country**
- **Common Name**
- Given Name
- Surname
- Title
- Organization
- locality
- **email**
- **validity period (or end of validity time). The validity period CAN NOT be longer than 1 (one) year.**

The data SHALL be sent at the InfoCert contact (§1.4), quoting the agreement and the payment data, if applicable. The agreement may also define alternative methods of payment and data provisioning.
In any case, it is mandatory to supply the email address and phone number of a contact point person, to be contacted for any clarification.

3.1. Key pair generation and certificate issuing

After receiving the foreseen data, InfoCert will check them and, in case of problem, will get in touch with the contact person indicated in the request.
If everything is right, the contact person SHALL choose a passphrase for the protection of key pairs and certificates.

InfoCert will generate the key pairs in its own premises. Then it will issue the corresponding certificate and will fill in the Subject Distinguished Name fields with the user supplied data.
Key pair and certificate are then stored in a PKCS#12 file, encoded PEM, protected by the passphrase chosen by the contact point.

The certificates are based on the RSA algorithm, with a 1024 bit key length.

The certificate is compliant with the standard ITU X.509 v3

The applicant MAY indicate the required value for tha ***KeyUsage*** and the ***ExtendedKeyUsage*** extensions.

The certificates ***KeyUsage*** attribute MAY have one or more of the following values:
digitalSignature (0),
nonRepudiation (1), -- recent editions of X.509 have renamed this bit to contentCommitment
keyEncipherment (2),
dataEncipherment (3),
keyAgreement (4)

Given the scope of the certificate, all the combinations are admitted.
If not specified the ***KeyUsage*** will take the values:
digitalSignature + keyEncipherment + keyAgreement

The related attribute ***ExtendedKeyUsage*** will have the fixed value:
ClientAuthentication + Emailprotection.

3.2. Delivery of the P12 file

The PKCS#12 file with extension p12 will be sent to the contact person, with a commonly agreed procedure.

3.3. Validity

The certificates has a time limited validity, stated by the field (*validity*), with the attributes (*not before*) and *(not after).*

NOTE
The date are expressed in the UTC format (see RFC 5280)

year-month-day-hour-minutes-seconds-timezone
{YYYYMMDDHHMMSSZ}

Outside of this time range, the certificate is not valid.

3.4. Revocation of a certificate

The validity status of a certificate can be reduced by inserting it in the CRL Certificate Revocation List.
A verification application compliant with the normative reference SHALL check the presence of the certificate in the CRL.
A signature based on a certificate expired or revoked SHOULD be considered not valid.

Revocation

The revocation can be required by InfoCert or by the contact person
The revocation SHOULD[1] be required in case of:

[1] Usually the verb used here is SHALL, but given the test purposes, the option is recommended, not mandatory

- suspect or sure compromise of private key;
- certificate not usable;
- end of contractual agreement
- usage of the certificate outside the scope of this policy
- order by a judiciary authority.

The contact person can require the revocation by sending an email to the Infocert contact mail (§1.4), specifying the serial number of the certificate and the revocation reason.

CRL issuing

The CRL is published on the Internet.
The CRL Distribution Point extension of the certificate contains the URL where the CRL can be accessed.

The CRL is published at least every day.