Answering the [Bug 1102143] Add Renewed Autoridad de Certificacion Firmaprofesional root certificate

Version: 190301

Classification: Public

Index

Index 1

https://crt.sh/?caid=430&opt=cablint,zlint,x509lint&minNotBefore=2014-01-01 2

X.509 lint 2

ERROR: Issuer without organizationName 2

ERROR: No OCSP over HTTP 2

ERROR: No Subject alternative name extension 2

ERROR: Subject with organizationName, givenName or surname but without stateOrProvince or localityName 3

WARNING: Policy information has qualifier other than CPS URI 3

WARNING: Unknown extended key usage 3

WARNING: explicitText is not using a UTF8String 3

WARNING: explicitText is not using an UTF8String 3

ZLint 4

ERROR: Explicit text has a maximum size of 200 characters 4

ERROR: Root and Subordinate CA certificates MUST have a organizationName present in subject information 4

WARNING: Compliant certificates should use the utf8string encoding for explicitText 5

WARNING: Root CA certificate basicConstraint extension pathLenConstraint field SHOULD NOT be present 5

WARNING: Subscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present. 5

WARNING: Root CA Certificate: certificatePolicies SHOULD NOT be present. 5

https://crt.sh/?caid=430&opt=cablint,zlint,x509lint&minNotBefore=2014-01-01

X.509 lint

ERROR: Issuer without organizationName

Firmaprofesional has SHA1 root issued in 2009. To keep cryptographic suite up to date AND also to keep already issued certificates validation path still valid for both the SHA1 and the new SHA256 root, we kept issuer and subject data the same in the new CA and so did the key pair.

Firmaprofesional is a QTSP pursuant eIDAS regulation and our only business is being a QTSP, that is, this business is not a part of the company linked to a specific Organization Unit, but the whole company is intended to issue certificates. The Organization is also clearly identified in the ES Trust Services List (https://sede.minetur.gob.es/Prestadores/TSL/TSL.xml).

On the other hand, the root CA does not issue end-entity certificates but Intermediate CA certificates, where the O field is in place and the Organization is clearly identified.

The whole hierarchy is eIDAS compliant even for QWAC certificates.

Nevertheless, we will add the O field when a new hierarchy is released.

ERROR: No OCSP over HTTP

As far as we know, over OCSP service is working on HTTP, and the certificates have the noCheck extension enabled.

ERROR: No Subject alternative name extension

According to the X.509 lint report, the affected certificate is the one with crt.sh ID 201187042, which an OCPS certificate, not a SSL certificate.

We do not understand the error.

ERROR: Subject with organizationName, givenName or surname but without stateOrProvince or localityName

According to the X.509 lint report, the affected certificate is the one with crt.sh ID 201187042, which an OCPS certificate, not a SSL certificate.

We do not understand the error.

WARNING: Policy information has qualifier other than CPS URI

The affected certificates are either revoked or not issuing SSL certificates.

Additionally, according to RFC3280, "User notice is intended for display to a relying party when a certificate is used. The application software SHOULD display all user notices in all certificates of the certification path used, except that if a notice is duplicated only one copy need be displayed. To prevent such duplication, this qualifier __SHOULD__ only be present in end entity certificates and __CA certificates issued to other organizations.__" the use of useNotice field in CA certificates is not prohibited.

Additionally, all the affected certificates are CA certificates except the OCSP one. For this one we renew it in a yearly basis and will fix any issue (not related with the issuing CA). For the rest of them, some belong to other organizations (crt.sh ID 240192053 and 408789249) and we can fix when a new hierarchy is released

Finally, we understand that this issue do not undermine security nor interoperability.

WARNING: Unknown extended key usage

See answer above

WARNING: explicitText is not using a UTF8String

See answer above

WARNING: explicitText is not using an UTF8String

See answer above

ZLint

For Issued Certificates with notBefore >= 2014-01-01:

ERROR: Explicit text has a maximum size of 200 characters

The report states that there are seven affected certificates, but looking into it we only find four of them: crt.sh ID 240192053, crt.sh ID 495029017 (already revoked), crt.sh ID 495029018 (already revoked), crt.sh ID 12716475

For crt.sh ID 240192053 and crt.sh ID 12716475, they are not issuing SSL certificates and the first one is technically constrained. The part exceeding the 200 characters is an URL that can be found also in the CPS field.

ERROR: Root and Subordinate CA certificates MUST have a organizationName present in subject information

Firmaprofesional has SHA1 root issued in 2009. To keep cryptographic suite up to date AND also **to keep already issued certificates validation path still valid** for both the SHA1 and the new SHA256 root, we kept issuer and subject data the same in the new CA and so we did with the key pair. So we issued the certificate like this to keep backwards compatibility.

Firmaprofesional is a QTSP pursuant eIDAS regulation and our only business is being a QTSP, that is, this business is not a part of the company linked to a specific Organization Unit, but the whole company is intended to issue certificates. The Organization is also clearly identified in the ES Trust Services List (https://sede.minetur.gob.es/Prestadores/TSL/TSL.xml).

On the other hand, the root CA does not issue end-entity certificates but Intermediate CA certificates, where the O field is in place and the Organization is clearly identified.

The whole hierarchy is eIDAS compliant even for QWAC certificates.

Nevertheless, we will add the O field when a new hierarchy is released.

WARNING: Compliant certificates should use the utf8string encoding for explicitText

WARNING: Root CA certificate basicConstraint extension pathLenConstraint field SHOULD NOT be present

Despite the Baseline requirements state that "The pathLenConstraint field **SHOULD NOT** be present", we find it quite useful in terms of security, to explicitly state the size of the hierarchy, and directly untrust trust paths longer than the pathLength.

Our idea is to keep it if it is not forbidden.

WARNING: Subscriber Certificate: extKeyUsage either the value id-kp-serverAuth or id-kp-clientAuth or both values MUST be present.

According to the ZLint report, the affected certificate is the one with crt.sh ID 10601239. This certificate is not a Subscriber certificate but an Intermediate CA certificate (CA: True), additionally with booth `TLS Web Server Authentication` and `TLS Web Client Authentication` EKUs.

WARNING: Root CA Certificate: certificatePolicies SHOULD NOT be present.

From our point of view it is an useful extension in a Root certificate, to let relying parties know the basic rules ruling this root even if there are chained Intermediate CA from other organizations.

Our idea is to keep it if it is not forbidden.