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

Version: 190423

Classification: Public

Version	Section and changes	Date
190301	First version. Answers to https://crt.sh/?caid=430&opt=cablint,zlint,x509lint&minNotBefore=2014-01-01 findings.	03-March-2019
190423	Added numbering to titles. Added this section. Added page numbering. Answers to https://crt.sh/?caid=994&opt=cablint,zlint,x509lint&minNotBefore=2014-01-01findings.	23-April.2019

1. Index

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

2.1. X.509 lint

2.1.1. 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.

2.1.2. 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.

2.1.3. 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.

2.1.4. 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.

2.1.5. 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.

2.1.6. WARNING: Unknown extended key usage

See answer above

2.1.7. WARNING: explicitText is not using a UTF8String

See answer above

2.1.8. WARNING: explicitText is not using an UTF8String

See answer above

2.2. ZLint

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

2.2.1. 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.

2.2.2. 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.

2.2.3. WARNING: Compliant certificates should use the utf8string encoding for explicitText

2.2.4. 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.

2.2.5. 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 both `TLS Web Server Authentication` and `TLS Web Client Authentication` EKUs.

2.2.6. 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.

3. https://crt.sh/?caid=994&opt=cablint,zlint,x509lint&minNotBefore=2014-01-01

3.1. CA/B Forum lint

3.1.1. FATAL: ASN.1 Error in X520countryName

Already fixed. Only two already expired certificates affected.

3.1.2. ERROR: BR certificates with organizationName must include either localityName or stateOrProvinceName

Fixed in November 2017, when Firmaprofesional was allowed by the Spanish eIDAS Supervisory Body to transition to eIDAS profiles.

Note that there are no affected certificates with *notBefore* date later than 21-Nov-2017.

3.1.3. ERROR: Unallowed key usage for RSA public key (Key Agreement)

Fixed in 30-March- 2016. Due to a misinterpretation of RFC5280.

Note that there are no affected certificates with *notBefore* date later than 30-March-2016.

3.1.4. ERROR: BR certificates must not contain rfc822Name type alternative name

Fixed in November 2017, when Firmaprofesional was allowed by the Spanish eIDAS Supervisory Body to transition to eIDAS profiles.

Note that there are no affected certificates with *notBefore* date later than 21-Nov-2017.

3.1.5. ERROR: commonNames in BR certificates must be from SAN entries

Fixed in December- 2015. Due to a misinterpretation of RFC5280.

Note that there are no affected certificates with *notBefore* date later than 10-December-2015.

3.1.6. ERROR: Unallowed key usage for RSA public key

Fixed in 30-March- 2016. Due to a misinterpretation of RFC5280.

Note that there are no affected certificates with *notBefore* date later than 30-March-2016.

3.1.7. ERROR: Constraint failure in X520OrganizationName: ASN.1 constraint check failed: UTF8String: constraint failed (X520OrganizationName.c:174)

Fixed in November 2017, when Firmaprofesional was allowed by the Spanish eIDAS Supervisory Body to transition to eIDAS profiles.

Note that there are no affected certificates with *notBefore* date later than 21-Nov-2017.

3.1.8. ERROR: BR certificates must not contain directoryName type alternative name

Fixed in November 2017, when Firmaprofesional was allowed by the Spanish eIDAS Supervisory Body to transition to eIDAS profiles.

Note that there are no affected certificates with *notBefore* date later than 21-Nov-2017.

This issue had been already treated, since the previous Spanish profile for Public Administration Electronic Website certificate obliged to use DN in SAN.

3.1.9. ERROR: Constraint failure in X520OrganizationName: ASN.1 constraint check failed: PrintableString: constraint failed (X520OrganizationName.c:115)

Fixed in November 2017, when Firmaprofesional was allowed by the Spanish eIDAS Supervisory Body to transition to eIDAS profiles.

Note that there are no affected certificates with *notBefore* date later than 21-Nov-2017.

3.1.10. ERROR: SHA-1 not allowed for signing certificates

This is a Code Signing certificate issue to ourselves. Nevertheless we do not issue codeSigning certificates anymore.

Nevertheless we will ask to different root programs to turn off the Code Signing EKU for our root given that we are not issuing code signing certificates anymore nor performing its associated audits.

3.1.11. WARNING: Name has unknown attribute 2.5.4.97

We are afraid that this is an eIDAS requirement to identify organizations according to eIDAS and ETSI EN 319 412-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

3.1.12. WARNING: BR certificates should include an HTTP URL of the issuing CA's certificate

Fixed in 29-March- 2017. Updated in 18-April-2019.

Note that there are no affected certificates with *notBefore* date later than 30-March-2017, except https://crt.sh/?id=1370511112&opt=cablint. This certificate includes an "http**s**://". This has been fixed in 18-April-2019.

All affected certificates have already expired, except:

- https://crt.sh/?id=1370511112&opt=cablint

3.1.13. WARNING: Name has deprecated attribute emailAddress

Fixed in 30-March- 2016.

Note that there are no affected certificates with *notBefore* date later than 30-March-2016.

All affected certificates have already expired.

3.1.14. WARNING: BR certificates should include a HTTP URL of the issuing CA's certificate

See 3.1.12. WARNING: BR certificates should include an HTTP URL of the issuing CA's certificate.

3.1.15. WARNING: Cowardly refusing to run CAB check due to previous errors

Fixed in 30-March- 2016.

Note that there are no affected certificates with *notBefore* date later than 30-March-2016.

All affected certificates have already expired.

3.1.16. WARNING: Serial numbers for certificates using weaker hashes should have at least 64 bits of entropy

This is a Code Signing certificate issue to ourselves. Nevertheless we do not issue codeSigning certificates anymore.

Nevertheless we will ask to different root programs to turn off the Code Signing EKU for our root given that we are not issuing code signing certificates anymore nor performing its associated audits.

In spite of the above, the 64 bits of entropy issue has been seen as a major issue due to the fact that CAs using EJBCA by-default S/N generation have, in fact, 63 bits of entropy.

For the case of Firmaprofesional this is being discussed in:

https://bugzilla.mozilla.org/show_bug.cgi?id=1538638

3.2. X.509 lint

3.2.1. ERROR: Subject with organizationName but without stateOrProvince or localityName

Fixed in November 2017, when Firmaprofesional was allowed by the Spanish eIDAS Supervisory Body to transition to eIDAS profiles.

Note that there are no affected certificates with *notBefore* date later than 21-Nov-2017.

24 certificates still valid. We could revoke and reissue them if needed.

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

See above.

25 certificates still valid. We could revoke and reissue them if needed, but the https://crt.sh/?id=282623491. This is a Time Stamping Authority Certificate.

3.2.3. ERROR: Invalid type in SAN entry

Fixed in November 2017, when Firmaprofesional was allowed by the Spanish eIDAS Supervisory Body to transition to eIDAS profiles.

Note that there are no affected certificates with *notBefore* date later than 21-Nov-2017.

This has been already discussed in

3.2.4. ERROR: organizationName too long

Fixed in November 2017. We had to deal with our clients, who are some times Public Institutions or Professional Association with very long names.

In the end we restricted the size of the O name.

4 out of 7 affected certificates still valid.

3.2.5. ERROR: Invalid user notice type

Fixed in 20-April-2016 and the 2 affected certificates are no longer valid.

3.2.6. ERROR: No OCSP over HTTP

Fixed in 29-March-2017 and the 2 affected certificates are no longer valid.

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

3.2.7. ERROR: countryName not 2 characters long

Fixed in January-2016 and the 2 affected certificates are no longer valid.

3.2.8. ERROR: no authorityInformationAccess extension

This is a Code Signing certificate issue to ourselves. Nevertheless we do not issue codeSigning certificates anymore.

Nevertheless we will ask to different root programs to turn off the Code Signing EKU for our root given that we are not issuing code signing certificates anymore nor performing its associated audits.

3.2.9. ERROR: No Subject alternative name extension

Fixed in 29-March-2017 and the 1 affected certificate is no longer valid.

3.2.10. ERROR: Subject with givenName or surname but without the CAB IV policy oid

Fixed in January-2016 and the 1 affected certificate is no longer valid.

3.2.11. WARNING: Policy information has qualifier other than CPS URI

The affected certificates are not valid anymore.

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.

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

3.2.12. WARNING: No HTTP URL for issuing certificate

Fixed in 29-March- 2017. Updated in 18-April-2019.

Note that there are no affected certificates with *notBefore* date later than 30-March-2017, except https://crt.sh/?id=1370511112. This certificate includes an "http**s**://". This has been fixed in 18-April-2019.

All affected certificates have already expired, except:

- https://crt.sh/?id=128907092
- https://crt.sh/?id=1370511112
- https://crt.sh/?id=20413969

3.2.13. WARNING: explicitText is not using a UTF8String

Fixed in 30-March- 2016.

Note that there are no affected certificates with *notBefore* date later than 30-March-2016.

All of the affected certificates are already expired.

3.2.14. WARNING: explicitText is not using an UTF8String

See above

3.2.15. WARNING: Subscriber certificate without Extended Key Usage

Supposedly there are two certificates affected. Both of them have EKU. We do not understand what is the problem.

3.3. ZLint

3.3.1. ERROR: Subscriber Certificate: subject:localityName MUST appear if subject:organizationName, subject:givenName, or subject:surname fields are present but the subject:stateOrProvinceName field is absent.

Fixed in 29-March- 2017.

Note that there are no affected certificates with *notBefore* date later than 30-March-2017.

14 out of 18 still valid. We could revoke and reissue them if necessary.

3.3.2. ERROR: Subscriber Certificate: subject:stateOrProvinceName MUST appear if the subject:organizationName, subject:givenName, or subject:surname fields are present and subject:localityName is absent.

See above.

3.3.3. ERROR: The common name field in subscriber certificates must include only names from the SAN extension

Fixed in 23-12-2015. All affected certificates are no longer valid.

3.3.4. ERROR: The Subject Alternate Name extension MUST contain only 'dnsName' and 'ipaddress' name types.

Fixed in 05-08-2015. All affected certificates are no longer valid.

3.3.5. ERROR: The 'Organization Name' field of the subject MUST be less than 64 characters

Fixed in November 2017. We had to deal with our clients, who are some times Public Institutions or Professional Association with very long names.

In the end we restricted the size of the O name.

1 out of 4 affected certificates is still valid.

3.3.6. WARNING: Compliant certificates should use the utf8string encoding for explicitText

Fixed in 30-March- 2016.

Note that there are no affected certificates with *notBefore* date later than 30-March-2016.

All of the affected certificates are already expired.

3.3.7. WARNING: Subscriber certificates authorityInformationAccess extension should contain the HTTP URL of the issuing CA's certificate

Fixed in 29-March- 2017. Updated in 18-April-2019.

Note that there are no affected certificates with *notBefore* date later than 30-March-2017, except https://crt.sh/?id=1370511112&opt=cablint. This certificate includes an "http**s**://". This has been fixed in 18-April-2019.

All affected certificates have already expired, except:

- https://crt.sh/?id=1370511112&opt=cablint

3.3.8. WARNING: When the id-ad-calssuers accessMethod is used, at least one instance SHOULD specify an accessLocation that is an HTTP or LDAP URI

The only certificate affected is https://crt.sh/?id=1370511112&opt=cablint which includes an "http**s**://". This has been fixed in 18-April-2019.