Initial Incident Report

Affected Hierarchy	ANF Global Root CA (SHA 256 - expires 2033)
Root CA SHA-1 Fingerprint	26CAFF09A7AFBAE96810CFFF821A94326D2845AA

3 Incidents detected:

Incident #1

Incident	Misissuance of wrong constructed test certificate in contravention to Baseline Requirements (BR).
Explanation	Identified 1 wrong constructed internal test certificates issued as production certificate, not containing CABF OID (2.23.140.2.1) in a critical extension and with a maximum validity period higher than 30 days as established by the Baseline Requirements. Incident: issued from a public hierarchy. Fields were wrongly filled with random values. • countryName "España" instead of ISO Contry code "ES". BR section 7.1.4.2.2. *countryName MUST contain the two-letter ISO 3166-1 country code.* Also containing a invalid "ñ" Printable String value. • localityName = sdcsdc Invalid locality. • stateOrProvinceName = asad Invalid State. • serialNumber = asdasd Invalid. As for BR serial number must be *non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.* • DNS:cdcdcd Unqualified domain. BR section 7.1.4.2.1. …*MUST be either a dNSName containing the Fully-Qualified Domain Name*
How and when ANF AC first became aware of the problem, time and date.	A problem notification was submited by Ryan Sleevi to Bugzilla Bug 555156 (Closed as WONTFIX) Comment 122, on 2019-09-19 17:17 PDT
Summary of the problematic certificates.	1 wrong constructed test certificate was issued Jul 30 17:45:57 2019. https://crt.sh/?id=1723124144
Resulting action:	Revoked 2019-09-20 09:38:19 UTC
Timeline of the actions ANF AC took in response.	• **2019-09-19 17:17 PDT:** Ryan Sleevi reports misissuance of certificate crt ID1723124144 on Bug 555156 • **2019-09-20 00:29 PDT:** ANF AC ceases issuance from the affected part and proceeds to problem source diagnosis. ANF AC scanns for other misissued certificates. • **2019-09-20 02:38:19 PDT:** ANF AC revokes the misissued certificate with ID 1723124144 reported by Ryan Sleevi. • **2019-09-20 02:38:33 PDT - 2019-09-20 02:56:17 PDT:** ANF AC revokes other misissued certificates identified (analised in Incident #3). • **2019-09-20 08:39 PDT:** Pablo Díaz notifies in Bug 555156 the revocation of the certificate. No need to notify subscriber as this certificate was not issued to any subscriber. • **2019-09-20:** Measures explained below are applied to prevent the incident from happening again. • **2019-09-23 04:29 PDT** Issuace service is resumed as problem has been diagnosed and ANF AC is sure this problem will not repeat.

	Certificate revoked within 24h of notification, in compliance with Baseline Requirements section 4.9.1.1: *"CA must revoke a certificate within 5 days if: 7. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement"*
Whether ANF AC has stopped, or has not yet stopped, issuing certificates with the problem.	No other certificates wrong constructed test certificates have been issued since this case.
How and why the mistakes were made or bugs introduced, and how they avoided detection until now.	The system for requesting test certificates is different from that used for user production certificates. The test circuit suffered from organizational and technical deficiencies. In the request of certificates for end user, the use of an application called AR Manager is required. This application incorporates all the logic necessary for regulatory compliance and with different security controls. Among the different existing controls, it is worth highlighting: • In all cases of processing of end-user certificate requests, the intervention of a Registration Authority Operator is required, which assumes responsibility for the personal identification process and assumes its responsibility by electronically signing the identification document that has been completed, which is issued by AR Manager, and, together with the supporting documents, is transferred to the Issuance Reports Manager (IRM) Department (defined in 1.3.5 of ANF AC's CPS, personel of ANF AC's Legal department, responsible for double checking the documentation provided by the RA's). • In all cases, the intervention of said IRM Operator is required, whose function is to verify the identification document, documents provided by RA and carry out the necessary checks in external sources. In its control activity they must use the IRM application, which incorporates OCR processes, which automate data control through the corresponding computer logic, in addition to human eye review. • The conformity issued by the IRM Operator is reflected in an electronically signed act authorizing the issuance of the certificate, which is transferred to the issuer. • These control and consistency measures were not applied when the certificate was in test mode. It was mistakenly considered that its internal nature would not cause risks. In the case of requests for the issuance of test certificates, the IRM operator simply validated the electronic signature of the application certificate issued by personnel of the Engineering Department. The Engineering Department receives requests for configuration of certificates and processes, and has the need to perform laboratory tests to achieve the objectives set. This first test phase is carried out by qualified engineers, but at the junior level without high expertise in PKI. Senior engineers focus their attention on the management of applications that are in operation. As it has been credited for the incidents suffered, the risk of issuing a test certificate was not being considered. The junior engineers had the autonomy to issue requests for the issuance of test certificates to the IRM, but such a TEST nomenclature actually only had internal effects, since it is only a test if the certificate incorporates the

	requirements established to be able to have such consideration, and ANF AC did not have a control to ensure that what is internally qualified as a test is comparable under general rules in this area. This certificate should have not been issued as it is, and out of this hierarchy. The audits performed did not detect these incidents because the risk involved was not considered. This risk was not outlined in the risk matrix, and internal rules that have been found to be deficient in not considering the test processes had been followed. A problem notification was submited by Andrew Ayer to Bugzilla Bug 555156 (Closed as WONTFIX) Comment 121, on 2019-05-29 17:17 PDT. However, Primary point of contact in CCADB changed to pablo@anf.es in 2019-05-21 19:00 UTC as ANF AC dismissed the responsible Enric named in Bugzilla. Once we received notification of the next comment 122 by Ryan Sleevi Pablo responded immediately.
Measures already taken to solve the situation. How ANF AC systems of have been reinforced so that it does not return to happen.	ANF AC has taken organizational and technical measures so that these types of incidents do not occur again. Specifically: 1. 2019/09/20: The role of Regulatory Compliance Officer has been created. This role currently has two operators of ANF AC, one assigned to the legal department and the second responsible for monitoring the Mozilla Forum and CA/B forum ballots. 2. 2019/09/20: The IRM application currently has been reinforced with the following security controls. The application checks: a) If the request process comes from a operator of the engineering department it is flagged as test certificate. b) That the issuance request act is not only signed by the engineering department operator, but is signed by a regulatory compliance officer; c) the inclusion of mandatory fields and its syntax in the construction of the certificate; d) in case of detecting an incident, the request is rejected, the application sends email to the person in charge of regulatory compliance; e) verifies any indication that the certificate is a test, such as any of the fields containing the word "Test", "Testing", "Prueba". **f) derives the issuance to a non publicly trusted hierachy created for TEST purposes, not subject to the Baseline Requirements (BR).** 3. Certificate requests flagged as Test are issued with a validity period of 30 days and include the OID (2.23.140.2.1) in certificatepolicies extension, marked as critical. 4. 2019/10/09: Inclusion of a certlint automatic verification for any SSL certificate issued. 5. 2019/10/03: The risk of issuance of test certificates has been included in the risk matrix, incorporating the safeguard measures and making an assessment that the residual risk is acceptable after its application. 6. 2019/10/03: The rules governing all aspects related to the processing of test certificates have been incorporated into the internal regulations of the Engineering Operators and IRM Operators. 7. 2019/10/03: In the role of the Responsible for Regulatory Compliance, a requirement for periodic follow-up of the Forum and attention to incident reports has been incorporated, and it has been established that a new gap in time cannot be produced as occurred by the departure of the previous responsible. It has been established that in the absence of this responsible, their functions will be temporarily assumed by a person assigned to the legal department, as long as a new person is appointed.

	8. 2019/10/03: The HR Department has updated the Disciplinary Measures and Sanctions document, in order to have this resources available in case of infringement.
List of future steps ANF AC is taking to reinforce its systems. Timeline of when are expected to be accomplished.	The creation of a new reinforcement 8-hour regulatory compliance course aimed at junior Engineering personnel has been ordered on the eLearning Campus of ANF AC. This course must be developed within 90 days, and the staff must have completed it within a maximum period of six months. The course incorporate knowledge acquisition control that must be overcomed. ANF AC is open to any observation or improvement the community can provide.
Current validation protocols would have discovered the error (Yes/No)	Yes

Incident #2

Incident	OrganizationName containing an invalid character "·" not supported by Printable String.
Explanation	OrganizationName contained the organization's exact legal name: "*Col·legi de Graduats Socials de Barcelona*" as verified under Section 3.2.2.2 of the BR. However it contained an invalid character "·" not supported by Printable String: RFC 5280, Appendix B. ASN.1 Notes: *The character string type PrintableString supports a very basic Latin character set: the lowercase letters 'a' through 'z', uppercase letters 'A' through 'Z', the digits '0' through '9', eleven special haracters ' = ( ) + , - . / : ? and space.*
How and when ANF AC first became aware of the problem, time and date.	Problem detected by ANF AC on 2019-10-09 on an already revoked certificate when scanning its corpus of certificates to look for potential related problems to remediate.
Summary of the problematic certificates.	1 certificate issued with this problem on Jul 30 11:28:40 2019 https://crt.sh/?id=1722106741
Resulting action:	Certificate was already revoked: 2019-10-03 19:47:11 UTC
Timeline of the actions ANF AC took in response.	• **2019-10-03 09:48 UTC** Subscriber requested in writing that ANF AC revokes the certificate. Informs it had not been used. • **2019-10-03 19:47:11 UTC** Certificate is Revoked. • **2019-10-09 around 18:30 UTC** Problem with PrintableString is detected by ANF AC.
Whether ANF AC has stopped, or has not yet stopped, issuing certificates with the problem.	No other certificates have been issued with this problem, not before and not after. ANF AC has removed further incidents of this type through a system update in October 2019.
How and why the mistakes were made or bugs introduced, and how they avoided detection until now.	OrganizationName field was always encoded in *PrintableString* as permitted by RFC 5280. ANF AC did not have a control established to prevent characters not supported by PrintableString to be introduced in this field.
Measures already taken to solve the situation. How ANF AC systems of have been reinforced so that it does not return to happen.	2019-10-09**:** "*OrganizationName*" Field, has been established to be encoded in *PrintableString* by default, except in cases where the content includes characters beyond: lowercase letters 'a' through 'z', uppercase letters 'A' through 'Z', the digits '0' through '9', eleven special characters ' = ( ) + , - . / : ? and space. In that case it is encoded with *UTF8String* as permitted by RFC 5280 (page 113). That was already applied to "*streetAddress*", "*localityName*", "*stateOrProvinceName*" and "*OrganizationalUnitName*" fields.

	2019-10-10**:** Certificate requests containing special characters other than accents, "ñ", "·", "º", "ª" (which are common special characters in our geographical market) are flagged in the verification system for further verification.
List of future steps ANF AC is taking to reinforce its systems. Timeline of when are expected to be accomplished.	ANF AC considers that appropiate measures have been established so that this incident does not happen again. We establish a supervision period for the next issued certificates that contain special characters and are open to any observation the community can provide.
Current validation protocols would have discovered the error (Yes/No)	Yes

Incident #3

Incident	id-etsi-qcs-QcLimitValue not containing currency code.
Explanation	The certificates identified in this Incident #3 are missing the alphabetic or numeric currency code (ISO 4217) in the QC Statement of the type id-etsi-qcs-QcLimitValue as for ETSI EN 319 412-5, section 4.3.2. Are also internal test certificates, and, however, do not contain CABF specific OID (2.23.140.2.1) in a critical extension and have a maximum validity period higher than 30 days.
How and when ANF AC first became aware of the problem, time and date.	As stated in Incident #1, **2019-09-20 00:29 PDT**, after notification of a misissuance made by Ryan Sleevi, ANF AC starts the scan of its corpus of certificates to look for others with the same issue and other certificates potential related problems which can also be remediated at the same time.
Timeline of the actions ANF AC took in response.	**2019-09-20 02:38:21 PDT to 2019-09-20 02:56:17 PDT**, ANF AC identifies and revokes 19 "test" certificates with the incident described. While the issuance system was ceased by Incident #1. **2019-09-20 08:39 PDT:** Pablo Díaz notifies in Bug 555156 the revocation of the certificates. No need to notify subscriber as this certificate was not issued to any subscriber.
Whether ANF AC has stopped, or has not yet stopped, issuing certificates with the problem.	Since the last issued certificate with this problem and the applied measures, no other certificates have been issued with this problem.
Summary of the problematic certificates.	19 certificates of test purposes with this issue, first issued Mar 5 18:33:22 2019 GMT and last issued Jul 29 10:00:13 2019.
Complete certificate data for the problematic certificates (fingerprints or crt.sh IDs)	https://crt.sh/?id=1717719528 https://crt.sh/?id=1703565338 https://crt.sh/?id=1703445480 https://crt.sh/?id=1645893334 https://crt.sh/?id=1630700055 https://crt.sh/?id=1630676987 https://crt.sh/?id=1635981809 https://crt.sh/?id=1375668487 https://crt.sh/?id=1341644902 https://crt.sh/?id=1341538528 https://crt.sh/?id=1341095450 https://crt.sh/?id=1340880513 https://crt.sh/?id=1337488605 https://crt.sh/?id=1328391014 https://crt.sh/?id=1328391000 https://crt.sh/?id=1328391034 https://crt.sh/?id=1319475442 https://crt.sh/?id=1257315805 https://crt.sh/?id=1276499222

How and why the mistakes were made or bugs introduced, and how they avoided detection until now.	Tests with inclusion of this QCStatement were being made and ANF AC due to a misconfiguration, the currency was not being included.
Measures already taken to solve the situation. How ANF AC systems of have been reinforced so that it does not return to happen.	Certificates were not issued to subscribers as were for internal test purposes and have been revoked immediately. Refer to Measures taken in Incident #1: Inclusion of a certlint automatic verification for any SSL certificate issued which would have detected this error. The system derives the issuance of TEST certificates to a non publicly trusted hierachy created for TEST purposes, not subject to the Baseline Requirements (BR).
List of future steps ANF AC is taking to reinforce its systems. Timeline of when are expected to be accomplished.	ANF AC considers that appropiate measures have been established so that this incident does not happen again. We establish a supervision period for the next issued certificates that contain special characters and are open to any observation the community can provide.
Current validation protocols would have discovered the error (Yes/No)	Yes

Details for each misissued certificate (Incident #3)

Certificate info:	https://crt.sh/?id=1717719528	**Resulting action:**	Revoked 2019-09-20 09:38:21 UTC
Certificate info:	https://crt.sh/?id=1703565338	**Resulting action:**	Revoked 2019-09-20 09:38:21 UTC
Certificate info:	https://crt.sh/?id=1703445480	**Resulting action:**	Revoked 2019-09-20 09:38:22 UTC
Certificate info:	https://crt.sh/?id=1630676987	**Resulting action:**	Revoked 2019-09-20 09:38:24 UTC
Certificate info:	https://crt.sh/?id=1635981809	**Resulting action:**	Revoked 2019-09-20 09:38:24 UTC
Certificate info:	https://crt.sh/?id=1375668487	**Resulting action:**	Revoked 2019-09-20 09:38:25 UTC
Certificate info:	https://crt.sh/?id=1341095450	**Resulting action:**	Revoked 2019-09-20 09:38:25 UTC
Certificate info:	https://crt.sh/?id=1341644902	**Resulting action:**	Revoked 2019-09-20 09:38:26 UTC
Certificate info:	https://crt.sh/?id=1341538528	**Resulting action:**	Revoked 2019-09-20 09:38:28 UTC
Certificate info:	https://crt.sh/?id=1340880513	**Resulting action:**	Revoked 2019-09-20 09:38:29 UTC
Certificate info:	https://crt.sh/?id=1337488605	**Resulting action:**	Revoked 2019-09-20 09:38:29 UTC
Certificate info:	https://crt.sh/?id=1328391014	**Resulting action:**	Revoked 2019-09-20 09:38:30 UTC
Certificate info:	https://crt.sh/?id=1319475442	**Resulting action:**	Revoked 2019-09-20 09:38:33 UTC
	Internal Test EV certificate (QWAC for PSD2, no customer affected) issued in March 26th with OrganizationIdentifier in the SubjectDN prior to IPR review period of Ballot SC17. New 1.7.0 EV Guidelines were adopted the 21st of May. ETSI TS 119 495 V1.1.2 (2018-07) in GEN-5.2.1-1 stated: The PSD2 Authorization Number, or other identifier recognized by the NCA, shall be placed in organizationIdentifier attribute of the Subject Distinguished Name field in the certificate. Which was contradictory to EV Guidelines in force at the time. The OrganizationIdentifier was included in the SDN 2 months prior to the adoption of the 1.7.0 EVG, which implies a non-compliance. Certificate is revoked 2019-09-20 09:38:33 UTC.		
Certificate info:	https://crt.sh/?id=1257315805	**Resulting action:**	Revoked 2019-09-20 09:38:33 UTC
Certificate info:	https://crt.sh/?id=1276499222	**Resulting action:**	Revoked 2019-09-20 09:38:33 UTC
Certificate info:	https://crt.sh/?id=1328391034	**Resulting action:**	Revoked 2019-09-20 09:56:16 UTC
Certificate info:	https://crt.sh/?id=1328391000	**Resulting action:**	Revoked 2019-09-20 09:56:17 UTC