

## Incident Report - Misissuances under the old hierarchy

<b>Affected Hierarchy</b>	ANF Global Root CA (expires 2033)
<b>Root SHA-1 Fingerprint</b>	26CAFF09A7AFBAE96810CFFF821A94326D2845AA

<b>Incident</b>	<b>Misissuance of SSL OV Test Certificate</b>
<b>Notification</b>	Bugzilla Bug 555156 (Closed as WONTFIX) 19-09-2019 17:17 PDT
<b>Issue</b>	Internal test certificate (not issued to any customer) not compliant with CA/B Forum Baseline Requirements (BR). Does not include specific test certificate OID (2.23.140.2.1) and validity period longer than 30 days.
<b>Crt ID</b>	1723124144
<b>Crt.sh</b>	<a href="https://crt.sh/?id=1723124144">https://crt.sh/?id=1723124144</a>
<b>Reason</b>	During a request process testing this certificate was validated by the Issuance Reports Manager by error.
<b>Issuing CA</b>	ANF High Assurance EV CA1
<b>Result</b>	<p>Certificate was revoked. Revocation informed in Bugzilla Bug 555156. ANF AC stopped issuing certificates until this incident was resolved. ANF AC has quickly applied measures to prohibit and technically prevent the issuance of badly constructed test certificates due to human error. The ANF AC certificate request software verifies any indication that the certificate is a test, such as any of the fields containing the word "Test", "Testing", "Prueba", or non-coherent words such as "asdfghjl" or similar. Test certificates have a validity of 30 days and the OID 2.23.140.2.1 is now included in Certificatepolicies extension, which will be marked critical. CA system was made more robust. Permanent fix and already implemented. Evidence can be provided if necessary. ANF AC considers the matter to be fully resolved at this point.</p> <p>Furthermore, ANF AC has planned to have cablint integrated into our issuance system by 11<sup>th</sup> October 2019.</p>
<b>Incident</b>	<b>Misissuance of EV certificate (QWAC PSD2)</b>
<b>Notification</b>	Bugzilla Bug 555156 (Closed as WONTFIX) 20-09-2019 08:56 PDT
<b>Issue</b>	Internal Test EV certificate (QWAC for PSD2, no customer affected) issued in March 26 <sup>th</sup> with OrganizationIdentifier in the SubjectDN prior to IPR review period of Ballot SC17. New 1.7.0 EV Guidelines were adopted the 21 <sup>st</sup> of May.
<b>Crt ID</b>	1319475442
<b>Crt.sh link</b>	<a href="https://crt.sh/?id=1319475442">https://crt.sh/?id=1319475442</a>
<b>Reason</b>	<p><b>ETSI TS 119 495 V1.1.2 (2018-07)</b> in GEN-5.2.1-1 stated:</p> <p><i>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.</i> Which was contradictory to EV Guidelines in force at the time.</p> <p>Test certificate was issued in accordance to ETSI TS 119 495. The OrganizationIdentifier was included in the SDN 2 months prior to the adoption of the 1.7.0 EVG, which implies a non-compliance. This was due to confusion, human error.</p> <p>ETSI TS 119 495 v.1.1.2 (page 10):  <a href="https://www.etsi.org/deliver/etsi_ts/119400_119499/119495/01.01.02_60/ts_119495v010102p.pdf">https://www.etsi.org/deliver/etsi_ts/119400_119499/119495/01.01.02_60/ts_119495v010102p.pdf</a></p>
<b>Issuing CA</b>	ANF High Assurance EV CA1
<b>Response</b>	<p>Test certificate was revoked. Revocation informed in Bugzilla bug 555156. ANF AC stopped issuing certificates until this incident was resolved.</p> <p>In the issuance process, any change in the certificate profile has been associated to an application date. The logic implemented makes it impossible to issue a certificate with a change in structure if the date has not yet been reached. Permanent fix and already implemented. Close follow-up of CA/B forum ballots.</p>