Replay to “Kathleen Wilson 2012-10-09 12:23:37 PDT Comment #13)

In reply to patrick.graber from comment #11)

> Test-Web Site:
> Yes, please provide support; could you please provide the
> "test_ev_roots.txt" file to perform the EV Testing.

Done. Comment #12.

File: Minefield.png

>
> EV Policy:
> EV Policy OID:2.16.756.1.83.2.2

The Policy OID in the SSL cert of the test website that you provided (https://test-quarz-ev-ca-2.pre.swissdigicert.ch) was 2.16.756.1.83.21.0. So that's what I used in the test_ev_roots.txt file. If you use a different OID for EV, then you'll have to change the file, and also provide a new test website with a cert that has the correct EV info.

Yes, policy OID is 2.16.756.1.83.21.0

>
> Baseline Requirements:
> Referring to https://www.cabforum.org/forum.html we have joined CAB-Forum.

As per the CAB Forum Baseline Requirement # 8.3, where is the “Commitment to Comply” statement that should be in your CP or CPS?

File:008_CP_Quartz_EV_SDCS_2.16.756.1.83.4_V2.3_de_en.pdf

- Section 1.1

> There is a WebTrust seal audit cover page:
> Yes, please find enclosed the management assertion by Swisscom
> (Management_Assertion_2012.pdf) and the unqualified Opinion by KPMG
> (Unqualified Opinion (Period of Time).pdf and Unqualified Opinion (Point in
> Time).pdf)

Since this is not posted on cert.webtrust.org, I have to contact KPMG directly to confirm the authenticity of the audit statement. Whom do you recommend that I contact? Please provide their KPMG email address.

KPMG AG
Reto Grubenmann
E-Mail Address: retogrubenmann@kpmg.com

>
> “Swisscom Root CA 2”
> The verification of the ownership and control over an e-Mail address is
> described in internal process documentation. If necessary we can copy this
> section into the CPS.

Yes, please.
https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control

File:002_CPS_Swisscom_Digital_Certificate_Services_2 16 756 83 2 1_V2_2_en.pdf

- Section „3.2.3 Authentication of a natural person“

> Code Signing certificates are handled and issued under Sapphire CA - which
> are smartcard based and based on the strong identification processes of
> class sapphire CA.

Please translate the main parts of the Sapphire CP that describe verification of the subscriber's identity and authorization, as per https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Identity_of_Code_Signing_Certificate_Subscriber

File:007_CP_Smaragd_SDCS_2.16.756.1.83.3_V2.2a_de.pdf

- Section 10.1 „3.2 Identity verification for new application"

>
> Document Handling of IDNs in CP/CPS
> Yes. IDNs are allowed and technically supported.

Which sections of the CP/CPS address this? https://wiki.mozilla.org/CA:Recommended_Practices#Document_Handling_of_IDNs_in_CP.2FCPS

File:008_CP_Quartz_EV_SDCS_2.16.756.1.83.4_V2.3_de_en.pdf

- 10.2 „3.2.8 Checking the domain name of the applicant“

>
> Delegation of Domain / Email validation to third parties:
> As stated in the CPS Enterprise RAs might be able to issue up to any kind of
> certificates. If they want to issue qualified certificates the Enterprise RA
> has to pass the KPMG audit prior to this. For all other kind of certificate
> classes the Enterprise RA has beforehand to pass the Swisscom audit. All
> referred processes are audited by KPMG.

What technical controls do you have in place to ensure that an Enterprise RA only issues certs within their pre-approved domains and uses?

Answer:

We do have the following controls in place:

- We do have contract with the RA
- post issuance validation / monitoring of each issued certificate,
- individual strong authentication of each RA officer
- Swisscom audit of RA's
- Service CISO audit of RA officer activities

- A domain white / black listing is under construction which hooks directly into the CA