**Bugzilla ID:** 478418

additional requested information

https://http.icam.pgs-lab.com/

I imported the new root certificate into my Firefox browser, and then tried to browse to the test website. I

got following error:

An error occurred during a connection to http.icam.pgs-

The site was set to require user certificate for 2-way authentication, it has been changed to just be a secure URL – please try again.

CRL URL:

<http://http.fpki.gov/fcpca/fcpca.crl>

OCSP URL:

This is the URL for the OCSP responder for my end-entity certificate.

URL=http://ocsp.managed.entrust.com/OCSP/EMSSSPCAResponder

The FPKIMA does not run an OCSP responder for the Common Policy CA itself.

CP section 4.9.7: CAs operating as part of the Shared Service Providers program that only issue certificates

to CAs…

What restrictions are placed on sub-CAs? E.g. Are sub-CAs constrained to issue certificates only within

certain domains? What sort of sub-CAs can they sign?

All SSPs operating under the Common Policy can only issue certificates to subordinate CAs that also adhere to the Common Policy CP. See bottom of page 1:

“CAs that issue certificates under this policy may operate simultaneously under other policies. Such CAs must not assert the OIDs in this policy in certificates unless they are issued in accordance with all the requirements of this policy.”

Audit Type: eValidated Methodology (Equivalent to WebTrust CA?)

We require that the audit criteria be one or more of the following three, or equivalent. Please indicate

which of these audit criteria are encompassed in the eValidated Methodology.

ETSI TS 101 456

ETSI TS 102 042

WebTrust Principles and Criteria for Certification Authorities

Brian Dilley states he is an approved Mozilla Auditor for that browser forum. The eValidated methodology, a USPTO registered service and trade mark, is equivalent to the following PKI auditing standards;

X9.79

ISO 21188

IETF RFC 2527

IETF RFC 3647, and

WebTrust and Extended Validation for CAs.

This methodology has been accepted by both commercial, State and Federal governments. The TS (T-scheme) is a British or EU program and that program is similar to the Kantara Initiative Framework where Mr. Dilley is the only approved Assessor for that program.

I see how the identity and authority are verified, but I don’t see how the RA confirms that the certificate

subscriber owns or controls the domain name to be included in the certificate.

<https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership>

Every device issued a certificate under the Common Policy CP must have a sponsor. The sponsor is authenticated including their authorization for the device. And again all information included in certificates must be verified. The CPS for the issuing CA will specifcy how that verification takes place.

Are you also requesting to enable the Email trust bit? If yes, how does the RA confirm that the certificate

subscriber owns/controls the email address to be included in the certificate? Where is this documented?

According to the information that you provided below, I see that the identity of the certificate subscriber

is verified. But I don’t see how the ownership/control of the email address is verified.

Yes – we want the Email trust bit set.

All information included in a certificate issued under the Common Policy CP must be verified. Each SSP’s CPS will state exactly how they verify the information.

**1.3.2. Registration Authorities**

The registration authorities (RAs) collect and verify each subscriber’s identity and information that is to be entered into the subscriber’s public key certificate. The RA performs its function in accordance with a CPS approved by the FPKIPA.