OCF "Cleveland" – OCSP RFC Compliance – Security WG CR 2631

Legal Disclaimer

****** Section OID Annex (add new line on top of CR 2549)******

1.1 OCSP Profile

OCSP is used to check the revocation status of certificates and signed by the CA or by the OCSP Responder that issued the Certificates whose revocation status is being checked.

1.5.2 Contact Person

Inquiries regarding this CP MUST be directed to the PKI-PA at pki_team@members.openconnectivity.org.

3.2.2 Authentication of Organization Identity

The CA's certificate issuance process MUST authenticate the identity of the organization named in the Ecosystem Member Agreement by confirming that the organization

:

- Is a member of the Open Connectivity Foundation.
- Exists in a business database (e.g., Dun and Bradstreet), or alternatively, has organizational documentation issued by or filed with the applicable government (e.g., government issued business credentials) that confirms the existence of the organization, such as articles of incorporation, Certificate of Formation, Charter Documents, or a business license that allow it to conduct business
- Conducts business at the address listed in the agreement
- Is not listed on any of the following U.S. Government denied lists: US Department of Commerce' Bureau of Industry and Security Embargoed Countries List, and the US Department of Commerce' Bureau of Industry and Security Denied Entities List

Second, the CA's certificate issuance process validates the information in the Certificate Application including the Icon and Friendly Name to be inserted into the certificate.

- Authentication of the contacts listed in the customer profile
- The information listed in the certificate application is verified for accuracy and validity for the given organization

~~3.2.3 Conduct a trademark search of the logo in the U.S. Patent and Trademark Office or equivalent international trademark office. Authentication of Individual Identity~~ CA Issuance Process

The CA's certificate issuance process MUST authenticate that the:

- Representative submitting the Ecosystem Member Agreement and Certificate Application, is a duly authorized representative of the organization as an employee, partner, member, agent, etc., and is authorized to act on behalf of the organization
- Corporate Contact listed in the Ecosystem Member Agreement is an officer in the organization and can act on behalf of the organization

- Administrator listed in the Ecosystem Member Agreement and Certificate Application, is a duly authorized representative of the organization as an employee, partner, member, agent, etc. and is authorized to act on behalf of the organization.

5.1.1 Site Location and Construction

All CA operations MUST be conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems. The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CAs, MUST be consistent with facilities used to house high-value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, MUST provide robust protection against unauthorized access to the CA equipment and records.

Such requirements are based in part on the establishment of physical security tiers. A tier is a barrier such as a locked door or closed gate that provides mandatory access control for individuals and requires a positive response (e.g., door unlocks or gate opens) for each individual to proceed to the next area. Each successive tier provides more restricted access and greater physical security against intrusion or unauthorized access.

CAs SHALL construct the facilities housing their CA functions with at least three physical security tiers, Tiers 1 through 3. CAs SHALL perform all validation operations within Tier 2 or higher. CAs SHALL place Information Services systems necessary to support CA functions in Tier 3 or higher. Online and offline cryptographic modules MUST be placed in Tier 3 or higher. CAs SHALL further protect offline cryptographic modules by placing them within Tier 3 or higher.

Each successive Tier is wholly enclosed within the previous Tier (e.g. no shared wall).

CAs SHALL describe their Site Location and Construction in more detail in their CPS.

****** Section 9.3.2.1 Certificate Profile and Fields ******

The following X.509 v3 extensions are required for End-Entity Certificates:

Extension	Required/ Optional	Criticality	Value / Notes
...			
certificatePolicies	OPTIONAL	Non-critical	End-entity certificates chaining to an OCF Root CA SHOULD contain at least one PolicyIdentifierId set to the OCF Certificate Policy OID – (1.3.6.1.4.1.51414.0.1.2) corresponding to the version of the

			OCF Certificate Policy under which it was issued. Additional manufacturer-specific CP OIDs may also be populated.
...			

Table 1 - X.509 v3 extensions for End-Entity Certificates

****** End of Change ******

****** Section 10.3 Device Authentication with Certificates******

End-Entity certificates which chain to an OCF Root CA SHOULD contain at least one PolicyIdentifierId set to the OCF Certificate Policy OID – (1.3.6.1.4.1.51414.0.1.2) corresponding to the version of the OCF Certificate Policy under which it was issued. Additional manufacturer-specific CP OIDs may also be populated.

****** End of Change ******

****** Section OID Annex (add new line on top of CR 2549)******

Annex X
(informative)

(OID definitions)

This annex captures the OIDs defined throughout the document. The OIDs listed are intended to be used within the context of an X.509 v3 certificate. MAX is an upper bound for SEQUENCES of UTF8Strings and OBJECT IDENTIFIERs and should not exceed 255.

```
id-OCF OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) dod(6) internet(1)
     private(4) enterprise(1) OCF(51414) }

-- OCF Security specific OIDs

id-ocfSecurity OBJECT IDENTIFIER ::= { id-OCF 0 }
id-ocfX509Extensions OBJECT IDENTIFIER ::= { id-OCF 1 }


-- OCF Security Categories

id-ocfSecurityProfile ::= { id-ocfSecurity 0 }
id-ocfCertificatePolicy ::= { id-ocfSecurity 1 }

-- OCF Security Profiles

sp-unspecified ::= OBJECT IDENTIFIER { id-ocfSecurityProfile 0 }
sp-baseline ::= OBJECT IDENTIFIER { id-ocfSecurityProfile 1 }
sp-black ::= OBJECT IDENTIFIER { id-ocfSecurityProfile 2 }
sp-blue ::= OBJECT IDENTIFIER { id-ocfSecurityProfile 3 }
sp-purple ::= OBJECT IDENTIFIER { id-ocfSecurityProfile 4 }


sp-unspecified-v0 ::= ocfSecurityProfileOID (id-sp-unspecified 0}
sp-baseline-v0 ::= ocfSecurityProfileOID {id-sp-baseline 0}
sp-black-v0 ::= ocfSecurityProfileOID {id-sp-black 0}
sp-blue-v0 ::= ocfSecurityProfileOID {id-sp-blue 0}
sp-purple-v0 ::= ocfSecurityProfileOID {id-sp-purple 0}


ocfSecurityProfileOID ::= UTF8String

-- OCF Security Certificate Policies

ocfCertificatePolicy-v1 ::= { id-ocfCertificatePolicy 1}
ocfCertificatePolicy-v2 ::= { id-ocfCertificatePolicy 2}

-- OCF X.509v3 Extensions
…
```

****** End of Change ******

c