OCF “Fargo” – Specify format of Subject Id in Common Name field of End-Entity certificate – Security WG CR 2927

Legal Disclaimer

START OF CHANGE

10 Device Authentication

10.1 Device Authentication General

When a Client is accessing a restricted Resource on a Server, the Server shall authenticate the Client. Clients shall authenticate Servers while requesting access. Clients may also assert one or more roles that the server can use in access control decisions. Roles may be asserted when the Device authentication is done with certificates.

10.2 Device Authentication with Symmetric Key Credentials

When using symmetric keys to authenticate, the Server Device shall include the ServerKeyExchange message and set psk_identity_hint to the Server's Device ID. The Client shall validate that it has a credential with the Subject UUID set to the Server's Device ID, and a credential type of PSK. If it does not, the Client shall respond with an unknown_psk_identity error or other suitable error.

If the Client finds a suitable PSK credential, it shall reply with a ClientKeyExchange message that includes a psk_identity_hint set to the Client's Device ID. The Server shall verify that it has a credential with the matching Subject UUID and type. If it does not, the Server shall respond with an unknown_psk_identity or other suitable error code. If it does, then it shall continue with the DTLS protocol, and both Client and Server shall compute the resulting premaster secret.

10.3 Device Authentication with Raw Asymmetric Key Credentials

When using raw asymmetric keys to authenticate, the Client and the Server shall include a suitable public key from a credential that is bound to their Device. Each Device shall verify that the provided public key matches the PublicData field of a credential they have, and use the corresponding Subject UUID of the credential to identify the peer Device.

10.4 Device Authentication with Certificates

10.4.1 Device Authentication with Certificates General

When using certificates to authenticate, the Client and Server shall each include their certificate chain, as stored in the appropriate credential, as part of the selected authentication cipher suite. Each Device shall validate the certificate chain presented by the peer Device. Each certificate signature shall be verified until a public key is found within the "/oic/sec/cred" Resource with the "oic.sec.cred.trustca" credusage. Credential Resource found in "/oic/sec/cred" is used to terminate certificate path validation. Also, the validity period and revocation status should be checked for all above certificates, but at this time a failure to obtain a certificate's revocation status (CRL or OCSP response) MAY continue to allow the use of the certificate if all other verification checks succeed.

If available, revocation information should be used to verify the revocation status of the certificate. The URL referencing the revocation information should be retrieved from the certificate (via the authorityInformationAccess or crlDistributionPoints extensions). Other mechanisms may be used to gather relevant revocation information like CRLs or OCSP responses.

A Device retrieves the Subject UUID from the Common Name component of the Subject Name property of the End-Entity certificate which has the following format: "uuid: X",, where X is provisioned by the CMS to match the "deviceuuid" Property of the "/oic/sec/doxm" Resource. The Device treats all requests arriving over a connection authenticated by this End-Entity certificate as having originated from the Device with this Subject UUID. The Device shall use

this Subject UUID to match against the "subjectuuid" Property of the provisioned ACL entries to perform access control checks.

Devices must follow the certificate path validation algorithm in clause 6 of IETF RFC 5280. In particular:

– For all non-End-Entity certificates, Devices shall verify that the basic constraints extension is present, and that the cA boolean in the extension is TRUE. If either is false, the certificate chain MUST be rejected. If the pathLenConstraint field is present, Devices will confirm the number of certificates between this certificate and the End-Entity certificate is less than or equal to pathLenConstraint. In particular, if pathLenConstraint is zero, only an End-Entity certificate can be issued by this certificate. If the pathLenConstraint field is absent, there is no limit to the chain length.

– For all non-End-Entity certificates, Devices shall verify that the key usage extension is present, and that the keyCertSign bit is asserted.

– Devices may use the Authority Key Identifier extension to quickly locate the issuing certificate. Devices MUST NOT reject a certificate for lacking this extension, and must instead attempt validation with the public keys of possible issuer certificates whose subject name equals the issuer name of this certificate.

– The End-Entity certificate of the chain shall be verified to contain an Extended Key Usage (EKU) suitable to the purpose for which it is being presented. An End-Entity certificate which contains no EKU extension is not valid for any purpose and must be rejected. Any certificate which contains the anyExtendedKeyUsage OID (2.5.29.37.0) must be rejected, even if other valid EKUs are also present.

– Devices MUST verify "transitive EKU" for certificate chains. Issuer certificates (any certificate that is not an End-Entity) in the chain MUST all be valid for the purpose for which the certificate chain is being presented. An issuer certificate is valid for a purpose if it contains an EKU extension and the EKU OID for that purpose is listed in the extension, OR it does not have an EKU extension. An issuer certificate SHOULD contain an EKU extension and a complete list of EKUs for the purposes for which it is authorized to issue certificates. An issuer certificate without an EKU extension is valid for all purposes; this differs from End-Entity certificates without an EKU extension.

The list of purposes and their associated OIDs are defined in 9.4.2.3.

If the Device does not recognize an extension, it must examine the `critical` field. If the field is TRUE, the Device MUST reject the certificate. If the field is FALSE, the Device MUST treat the certificate as if the extension were absent and proceed accordingly. This applies to all certificates in a chain.

NOTE Certificate revocation mechanisms are currently out of scope of this version of the document.

END OF CHANGE