OCF 1.0 Security CR - CR35 (1385/1303)

Legal Disclaimer

9.3.5 Certificate Provisioning

The credential management service (e.g., a hub or a smart phone) issues certificates for new devices. The credential management service shall have its own certificate and key pair. The certificate is either a) self-signed if it acts as Root CA or b) signed by the upper CA in its trust hierarchy if it acts as Sub CA. In either case, the certificate shall have the format described in Section 9.3.2.

The CA in the credential management service shall retrieve a device's public key and proof of possession of the private key, generate a device's certificate signed by this CA certificate, and then the credential management service shall transfer them to the device including its CA certificate chain.

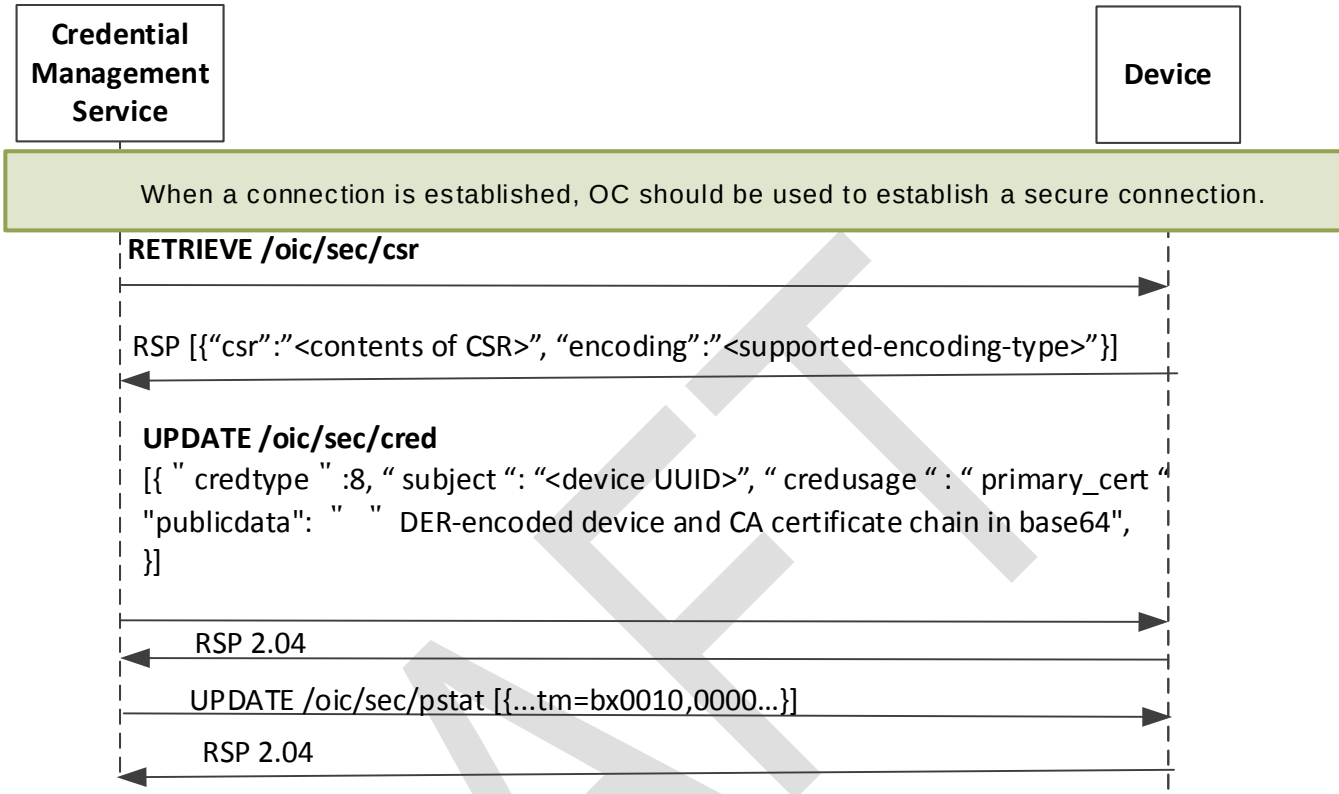
In the below sequence, the Certificate Signing Request is defined by PKCS#10 in RFC 2986, and is included here by reference.

The sequence flow of a certificate transfer for a Client-directed model is described in Figure 17.

1. The credential management service retrieves a Certificate Signing Request (CSR) from the device that requests a certificate. In this CSR, the Device shall place its requested UUID into the subject and its public key in the SubjectPublicKeyInfo. The Device determines the public key to present; this may be an already-provisioned key it has selected for use with authentication, or if none is present, it may generate a new key pair internally and provide the public part. The key pair shall be compatible with the allowed ciphersuites listed in section 9.3.2.2 and 11.2.3, since the certificate will be restricted for use in OCF authentication.

   If the Device does not have a pre-provisioned key pair and is unable to generate a key pair on its own, then it is not capable of using certificates. The Device shall advertise this fact both by setting the 0x8 bit position in the sct property of /oic/sec/doxm to 0, and return an error that the /oic/sec/csr resource does not exist.

2. The credential management service shall transfer the issued certificate and CA chain to the designated device using the same credid, to maintain the association with the private key.



3.

Figure 17 – Client-directed Certificate Transfer

13.8 Certificate Signing Request Resource (/oic/sec/csr)

The /oic/sec/csr resource is used by an OCF Device to provide its desired identity, public key to be certified, and a proof of possession of the corresponding private key in the form of a RFC 2986 PKCS#10 Certification Request. If the Device supports certificates (the sct property of /oic/sec/doxm has a 1 in the 0x8 bit position), the Device shall have an /oic/sec/csr resource.

Fixed URI	Resource Type Title	Resource Type ID ("rt" value)	Interfaces	Description	Related Functional Interaction
/oic/sec/csr	Certificate Signing Request	urn:oic.r.csr	baseline	The CSR resource contains a Certificate Signing Request for the device's public key.	Configuration

Table 1 – Definition of the oic.r.csr Resource

Property Title	Property Name	Value Type	Value Rule	Unit	Access Mode	Mandatory	Description
Certificate Signing Request	csr	String	-	-	R	Yes	Contains the signed CSR encoded according to the encoding property
Encoding	encoding	String	-	-	R	Yes	A string specifying the encoding format of the data contained in the csr property "oic.sec.encoding.pem" – Encoding for PEM-encoded certificate signing request "oic.sec.encoding.der" – Encoding for DER-encoded certificate signing request

Table 2 – Properties of the oic.r.csr Resource

The Device chooses which public key to use, and may optionally generate a new key pair for this purpose.

In the CSR, the Common Name component of the Subject Name shall contain a string of the format "uuid:X" where X is the device's requested UUID in the format defined by RFC 4122. The Common Name, and other components of the Subject Name, may contain other data. If the Device chooses to include additional information in the Common Name component, it shall delimit it from the UUID field by white space, a comma, or a semicolon.

If the Device does not have a pre-provisioned key pair to use, but is capable and willing to generate a new key pair, the Device may begin generation of a key pair as a result of a RETRIEVE of this resource. If the device cannot immediately respond to the RETRIEVE request due to time required to generate a key pair, the device shall return an "operation pending" error. This indicates to the Client that the device is not yet ready to respond, but will be able at a later time. The Cient should retry the request after a short delay.