

**OCF 2.0 Release Errata – Post-onboarding D2D connections and local credentials – Security
WG CR 2661**

Legal Disclaimer

THIS IS A DRAFT SPECIFICATION DOCUMENT ONLY AND HAS NOT BEEN ADOPTED BY THE OPEN CONNECTIVITY FOUNDATION. THIS DRAFT DOCUMENT MAY NOT BE RELIED UPON FOR ANY PURPOSE OTHER THAN REVIEW OF THE CURRENT STATE OF THE DEVELOPMENT OF THIS DRAFT DOCUMENT. THE OPEN CONNECTIVITY FOUNDATION AND ITS MEMBERS RESERVE THE RIGHT WITHOUT NOTICE TO YOU TO CHANGE ANY OR ALL PORTIONS HEREOF, DELETE PORTIONS HEREOF, MAKE ADDITIONS HERETO, DISCARD THIS DRAFT DOCUMENT IN ITS ENTIRETY OR OTHERWISE MODIFY THIS DRAFT DOCUMENT AT ANY TIME. YOU SHOULD NOT AND MAY NOT RELY UPON THIS DRAFT DOCUMENT IN ANY WAY, INCLUDING BUT NOT LIMITED TO THE DEVELOPMENT OF ANY PRODUCTS OR SERVICES. IMPLEMENTATION OF THIS DRAFT DOCUMENT IS DONE AT YOUR OWN RISK AMEND AND IT IS NOT SUBJECT TO ANY LICENSING GRANTS OR COMMITMENTS UNDER THE OPEN CONNECTIVITY FOUNDATION INTELLECTUAL PROPERTY RIGHTS POLICY OR OTHERWISE. IN CONSIDERATION OF THE OPEN CONNECTIVITY FOUNDATION GRANTING YOU ACCESS TO THIS DRAFT DOCUMENT, YOU DO HEREBY WAIVE ANY AND ALL CLAIMS ASSOCIATED HERewith INCLUDING BUT NOT LIMITED TO THOSE CLAIMS DISCUSSED BELOW, AS WELL AS CLAIMS OF DETRIMENTAL RELIANCE.

The OCF logo is a trademark of Open Connectivity Foundation, Inc. in the United States or other countries. *Other names and brands may be claimed as the property of others.

Copyright © 2019 Open Connectivity Foundation, Inc. All rights reserved.

Copying or other form of reproduction and/or distribution of these works are strictly prohibited.

***** Section 13.2.1.10 Credential Usage Device Authentication with Certificates *****

Credential Usage indicates to the Device the circumstances in which a credential should be used. Five values are defined:

- oic.sec.cred.trustca: This certificate is a trust anchor for the purposes of certificate chain validation, as defined in section 10.3. OCF Server SHALL remove any "/oic/sec/cred" entries with an "oic.sec.cred.trustca" credusage upon transitioning to RFOTM. OCF Servers SHALL use "/oic/sec/cred" entries that have an "oic.sec.cred.trustca" Value of "credusage" Property only as trust anchors for post-onboarding (D)TLS session establishment in RFNOP state; these entries are not to be used for onboarding (D)TLS sessions.
- oic.sec.cred.cert: This credusage is used for certificates for which the Device possesses the private key and uses it for identity authentication in a secure session, as defined in section 10.3.
- oic.sec.cred.rolecert: This credusage is used for certificates for which the Device possesses the private key and uses to assert one or more roles, as defined in section 10.3.1.
- oic.sec.cred.mfgtrustca: This certificate is a trust anchor for the purposes of the Manufacturer Certificate Based OTM as defined in section 7.3.6. OCF Servers SHALL use "/oic/sec/cred" entries that have an "oic.sec.cred.mfgtrustca" Value of "credusage" Property only as trust anchors for onboarding (D)TLS session establishment ; these entries are not to be used for post-onboarding (D)TLS sessions.
- oic.sec.cred.mfgcert: This certificate is used for certificates for which the Device possesses the private key and uses it for authentication in the Manufacturer Certificate Based OTM as defined in section 7.3.6.

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