Contributors
Pfaff, Oliver <oliver.pfaff@siemens.com>
Pössler, Thomas <Thomas.poessler@siemens.com>
Steindl, Günter <guenter.steindl@siemens.com>

Log
v0.1 2021-11-08 Initial version

IEEE 802.1AR Adoption by IEC/IEEE 60802

5.5.4 Common Requirements for Security
Bridge and end station implementations of any conformance classes for which a claim of
conformance to this document is made shall support the following requirements as specified in
6.3:

Note to editor: the text that follows shall become part of chapter “5.5.4 Common
Requirements for Security”. The item a) is a replacement for the text of the already existing
security requirements item 5.5.4 a) in D1.3. The items b)-g) present additional requirements
that shall be added before the current items 5.5.4 b)-d) in D1.3

a) Support the implementation of a Secure Device Identity as specified in chapter 5.3
“Required capabilities” of IEEE Std 802.1AR-2018 a), b), c), d), e), g), h) and i).
- Note for f) in 5.3 of IEEE Std 802.1AR-2018: this profile does not utilize SNMP
for remotely managing DevID modules or DevID trust anchor stores.

b) Support the implementation of a Secure Device Identity as specified in chapter 5.4
“Optional capabilities” of IEEE Std 802.1AR-2018 a), b), c), d), f), g).
- Note for a) in 5.4 of IEEE Std 802.1AR-2018: one LDevID is required that
fulfills the requirements for NETCONF-over-TLS (in NETCONF resp. TLS
server role). Remark: this LDevID is not present in factory default state.
- Note for e) in 5.4 of IEEE Std 802.1AR-2018: this profile does not utilize
SNMP for remotely managing DevID modules or DevID trust anchor stores.

c) Support the implementation of a Secure Device Identity as specified in chapter 5.5
“Supplier information” of IEEE Std 802.1AR-2018 a), b), c), d), e), g), h) and i).

d) Implement remote management for the contents of DevID modules and DevID trust
anchor stores (that belong to the LDevID-class of identifiers and trust anchors) by
means of NETCONF-over-TLS according to a TLS cipher suite identified by 5.5.4 h)
or 5.6.3 c). The remote management of DevID module and DevID trust anchor store
contents shall be access controlled by means of a NACM module using following
roles: KeystoreAdminRole, TruststoreAdminRole.

e) Implement DevID modules using the information model provided by the YANG
module ietf-keystore. This module shall support a DevID signature suite that allows to
implement the TLS cipher suite TLS_ECDHE_ECDSA_WITH_AES_128_GCM_
SHA256 based on the elliptic curve Curve25519.

Editor’s note: a contribution is invited that describes a DevID signature suite (see chapter 9 in
f) Implement DevID trust anchor stores using the information model provided by the YANG module ietf-truststore.

g) Possess IDevID EE certificates whose contents comply with the profile for IDevID EE certificates provided by this standard.

Editor’s note: a contribution is invited that describes a profile for IDevID EE certificates in industrial automation. This is supposed to profile clause c) in 5.5 of IEEE Std 802.1AR-2018 according to common conventions in TSN-based industrial automation. Rationale: to fulfill use cases in industrial automation, IA-station naming and property information beyond “serialNumber” and “HardwareModuleName” need to be expressed in IDevID EE certificates.