

ISO/IEC/IEEE 8802-1AR:2020-03 (E)

Telecommunications and exchange between information technology systems - Requirements for local and metropolitan area networks - Part 1AR: Secure device identity

Contents	Page
1. Overview.....	13
1.1 Scope.....	14
1.2 Purpose.....	14
1.3 Relationship to other standards.....	14
2. Normative references.....	15
3. Definitions.....	17
4. Acronyms and abbreviations.....	20
5. Conformance.....	22
5.1 Requirements terminology.....	22
5.2 Protocol Implementation Conformance Statement.....	22
5.3 Required capabilities.....	22
5.4 Optional capabilities.....	23
5.5 Supplier information.....	23
6. Secure Device Identifiers (DevIDs) and their use.....	25
6.1 DevID secrets.....	26
6.2 DevID certificates.....	26
6.3 DevID certificate chains.....	28
6.4 DevID Trust Model.....	28
6.5 Privacy considerations.....	30
7. DevID Modules.....	31
7.1 DevID module functionality.....	31
7.2 DevID Service Interface.....	33
7.3 DevID Management Interface.....	37
8. DevID certificate fields and extensions.....	38
8.1 version.....	39
8.2 serialNumber.....	39
8.3 signature.....	39
8.4 issuer.....	39
8.5 validity.....	39
8.6 subject.....	40
8.7 subjectPublicKeyInfo.....	40
8.8 signatureAlgorithm.....	40
8.9 signatureValue.....	40
8.10 extensions.....	40
9. DevID signature suites.....	42
9.1 RSA-2048/SHA-256.....	43
9.2 ECDSA P-256/SHA-256.....	44
9.3 ECDSA P-384/SHA-384.....	45
10. DevID MIB.....	46
10.1 Internet-Standard Management Framework.....	46
10.2 Relationship to other MIB modules.....	46
10.3 Structure of the MIB module.....	46
10.4 Security considerations.....	47

10.5	Definitions for Secure Device Identifier MIB	48
Annex A (normative)	PICS proforma.....	60
A.1	Introduction.....	60
A.2	Abbreviations and special symbols.....	60
A.3	Instructions for completing the PICS proforma.....	61
A.4	PICS proforma for IEEE 802.1AR	63
A.5	Major capabilities and options	64
A.6	DevID Service Interface	65
A.7	DevID Random number generation.....	65
A.9	DevID Supplier Information.....	66
A.8	DevID Certificate fields and extensions	66
A.10	RSA-2048/SHA-256 Signature Suite	67
A.11	ECDSA P-256/SHA-256 Signature Suite.....	67
A.12	ECDSA P-384/SHA-384 Signature Suite.....	67
Annex B (informative)	Scenarios for DevID.....	68
B.1	DevID use in EAP-TLS	68
B.2	DevID uses in consumer devices	69
B.3	DevID uses in enterprise devices.....	70
Annex C (informative)	Bibliography.....	71

Figures

Figure 6-1	DevID trust hierarchy	28
Figure 7-1	DevID functionality.....	31
Figure B-1	Example EAP-TLS exchange.....	69

Tables

Table 7-1	DevID storage examples.....	32
Table 8-1	DevID certificate and intermediate certificate fields.....	38
Table 8-2	DevID certificate and intermediate certificate extensions	38
Table 10-1	DevID managed objects.....	48