PICS Proforma for IEEE 802.1AR

1. Implementation identification

Supplier	Axis Communications AB
Contact point for queries about the PICS	support-pki@axis.com
Implementation Name(s) and Version(s)	Axis Device ID
Other information necessary for full identification – e.g., name(s) and version(s) of machines and/or operating system names	In hardware devices with support for AXIS Edge Vault
NOTE – The terms Name and Version should be interpreted appropriately to correspond with a supplier's terminology (e.g., Type, Series, Model).	

2. Protocol summary, IEEE Std 802.1AR-2018

Identification of protocol specification	IEEE Std 802.1AR-2018, IEEE Standard for Local and Metropolitan Area Networks—Secure Device Identity
Identification of amendments and corrigenda to the PICS proforma that have been completed as part of the PICS	Amd: N/A Corr: Amd: N/A Corr:
Have any Exception items been required? **(See A.3.3: The answer Yes means that the implementation does not conform to IEEE Std 802.1AR-2018.)**	No

Date of Statement	December 15th, 2022

3. Major capabilities and options

Item	Feature	Status	References	Support

Does the DevID module:				
RSA	Support the RSA-2048/SHA-256 signature suite	O.1	5.3, 9.1, A.10	Yes [x]
ECDSA256	Support the ECDSA256/SHA-256 signature suite	O.1	5.3, 9.2, A.11	Yes [x]
ECDSA384	Support the ECDSA384/SHA-384 signature suite	O.1	5.3, 9.3, A.12	Yes [ ]
IDEVID	Contain an Initial Device Identifier (IDevID) for each of the supported signature suites	M	5.3a), Clause 6	Yes [x]
IDSECRET	Contain an IDevID secret for each IDevID	M	5.3a), 6.1	Yes [x]
IDCERT	Contain an IDevID certificate for each IDevID	M	5.3a), 6.2	Yes [x]
IDCHAIN	Contain an IDevID certificate chain for each IDevID	M	5.3a), 6.3	Yes [x]
STOR	Store DevID secrets as specified in	M	5.3b), 7.1	Yes [x]
SI	Support the mandatory service interface operations for each supported signature suite	M	5.3c), 7.1, A.6	Yes [ ]
ICERTF	Include all mandatory fields in IDevID certificates	M	5.3d), A.8 Clause 8	Yes [x]
ICHAINF	Include all mandatory fields in IDevID intermediate certificates	M	5.3d), A.8 Clause 8	Yes [x]
XSNMP	Restrict SNMP access as specified	M	5.3f)	Yes [x]
RNG	Generate random numbers for key generation or use by other protocol entities	SI-9:M O	5.3, 7.1.3, 5.4d), A.7	Yes [x] No [ ]
RNGSS	Use an RNG with the required security strength	M	5.3g) 7.1.3	Yes [x]
XSIGN	Permit remote access to signing operations	X	5.3h)	No [x]
XCERTF	Include any prohibited field in an IDevID certificate or intermediate certificate	X	5.3i), 8.10, Clause 8	No [x]
LDEVID	Support the use of at least one LDevID certificate	O	5.4a), 7.2, A.6	Yes [ ] No [x]

ZKEY	Zeroize cryptographically when deleting keys	O	5.4c), 7.2.10	Yes [ ] No [x]
ZCERT	Zeroize cryptographically when deleting certificates	O	5.4c), 7.2.13	Yes [ ] No [x]
ZCHAIN	Zeroize cryptographically when deleting cert chains	O	5.4c), 7.2.14	Yes [ ] No [x]
MIB	Support access to the DevID MIB using SNMP	MGT:O	5.4e), 7.3, Clause 10	Yes [ ] No [x]

4. DevID Service Interface

Item	**Feature**	**Status**	**References**	**Support**
Does the DevID module implement the following operations:				
SI-I	Initialization	M	7.2.1	Yes [x]
SI-KN	DevID public key enumeration	M	7.2.2	Yes [x]
SI-CN	DevID certificate enumeration	M	7.2.3	Yes [x]
SI-CHN	DevID certificate chain enumeration	M	7.2.4	Yes [x]
SI-S	Signing	M	7.2.5	Yes [x]
SI-CE	DevID certificate enable/disable	M	7.2.6	Yes [ ]
SI-KE	DevID key enable/disable	M	7.2.7	Yes [ ]
SI-KG	LDevID key generate	LDEVID:O	7.2.8	Yes [ ] N/A [x]
SI-KI	LDevID key insert	LDEVID:O	7.2.9	Yes [ ] N/A [x]
SI-KD	LDevID key delete	SI-9:M SI-10:M	7.2.10	Yes [ ] N/A [x]
SI-CI	LDevID certificate insert	LDEVID:M	7.2.11	Yes [ ] N/A [x]
SI-CHI	LDevID certificate chain insert	LDEVID:M	7.2.12	Yes [ ] N/A [x]

SI-CD	LDevID certificate delete	LDEVID:M	7.2.13	Yes [ ] N/A [x]
SI-CCD	LDevID certificate chain delete	LDEVID:M	7.2.14	Yes [ ] N/A [x]
SI-RNT	Addition of RNG entropy	RNG:O	7.2.15	Yes [ ] No [x]

5. DevID Random number generation

Item	**Feature**	**Status**	**References**	**Support**
Does the DevID module:				
RNG-N	Use a non-deterministic RNG	RNG:O2	5.4d), 7.1.3	Yes [ ]
RNG-D	Use a deterministic RNG	RNG:O2	5.4d), 7.1.3	Yes [x]
DRBG	Use an SP 800-90A Revision 1 DRBG for the RNG	RNG-D:O	5.4d), 1), 7.1.3	A_ the Hardware module IoT Applet provides random numbers using an AIS20 compliant pseudorandom number generator (PRNG) with class DRG.3 generator initialized by a TRNG compliant to AIS31 class PTG.2. The PRNG is implemented according to NISTSP800-90A.
RNTRP	Support addition of RNG entropy	RNG-D:O SI-RNT:M	5.4d), 2), 7.1.3	Yes [ ]

6. A.6 DevID Certificate fields and extensions

Item	**Feature**	**Status**	**References**	**Support**
Does each IDevID certificate in the DevID module:				
NAME	Have a subject name that has not been and will not be issued to any other device by the CA issuing the certificate	M	5.3a), 6.1	Yes [x]
DNAME	Have an X.500 DN in the subject field.	M	5.3e), 8.6	Yes [x] No [ ]

SNAME	Include a unique device serialNumber in the subject field of each IDevID certificate.	O	5.4b), 8.6	Yes [x] No [ ]
ALTNAME	Include the subjectAltName in each IDevID certificate.	O	5.4f), 8.10.4	Yes [x] No [ ]
HWNAME	Include the device HardwareModuleName in the subjectAltName of each IDevID certificate.	O	5.4g), 8.10.4	Yes [x] No [ ]
CERTF1	Contain the subjectKeyIdentifier	O	8.10.2	No [x] Yes [ ]
Does each IDevID certificate and intermediate certificate in the DevID module:				
CERTF2	Contain the version, serialNumber, signature, issuer, validity, subjectPublicKeyInfo, signatureAlgorithm, and signatureValue, and authorityKeyIdentifier as specified in Clause 8.	M	5.3d), 8.1, 8.2, 8.3, 8.4, 8.5, 8.7, 8.8, 8.9, 8.10.1	Yes [x]
Does each intermediate certificate in the DevID module:				
CERTF3	Contain the subjectKeyIdentifier	M	8.10.2	Yes [x]

7. DevID Supplier Information

Item	Feature	Status	References	Support
ESTOR	What encryption mechanism is used if external storage is supported?	O M	6.2.5	S_External storage is not supported
KEYEXP	What notification method will be used if a credential signing key is suspected of being compromised?	M	6.6.1	S_Notification via Axis Security Notification Service
KEYGEN	What are the key generation mechanisms and associated IDevID signing mechanisms for the IDevID credential?	M	6.5.1	S_Key generation and signing mechanisms described in the Axis Edge Vault CPS.
ISSUER	What is the basis for the belief that the issuer name is unique?	M	7.2.4	S_Issuing CA is managed by Axis and named after the Axis-specific product terminology for the implementation.

CPS	What is the CA's CPS?	O	6.5	S_Axis Edge Vault CPS.
AUTH	What distinguished subject name fields contain identifiers appropriate for authorization, auditing, or other purposes? How are these parsed?	M	Clause 6	S_subject formatted as: axis_X520SerialNumber_cryptosuite. SubjectAltName contains the HardwareModuleName (OID) and unique serial number.

8. RSA-2048/SHA-256 Signature Suite

Item	Feature	Status	References	Support
S1-A	Does the DevID module support RSA-2048/SHA-256 with the algorithms and parameter types specified?	RSA:M	9.1.1	Yes [x]
S1-KS	Do any keys generated by the DevID module for this signature suite have the specified strength?	RSA:M	9.1.2	Yes [x]
S1-CSA	Are signatureAlgorithm values in DevID certificates and intermediate certificates as specified for this suite?	RSA:M	9.1.3	Yes [x]
S1-CPK	Are signatureAlgorithm values in DevID certificates and intermediate certificates as specified for this suite?	RSA:M	9.1.4	Yes [x]
S1-CSV	Are the signatureValue values in DevID certificates and intermediate certificates as specified for this suite?	RSA:M	9.1.5	Yes [x]

9. DSA P-256/SHA-256 Signature Suite

Item	Feature	Status	References	Support
S2-A	Does the DevID module support ECDSA P-256/SHA-256 with the algorithms and parameter types specified?	ECDSA256:M	9.2.1	Yes [x]
S2-KS	Do any keys generated by the DevID module for this signature suite have the specified strength?	ECDSA256:M	9.2.2	Yes [x]
S2-CSA	Are signatureAlgorithm values in DevID certificates and intermediate certificates as specified for this suite?	ECDSA256:M	9.2.3	Yes [x]

S2-CPK	Are signatureAlgorithm values in DevID certificates and intermediate certificates as specified for this suite?	ECDSA256:M	9.2.4	Yes [x]
S2-CSV	Are the signatureValue values in DevID certificates and intermediate certificates as specified for this suite?	ECDSA256:M	9.2.5	Yes [x]

10. ECDSA P-384/SHA-384 Signature Suite

Item	**Feature**	**Status**	**References**	**Support**
S3-A	Does the DevID module support ECDSA P-384/SHA-384 with the algorithms and parameter types specified?	ECDSA384:M	9.3.1	Yes [ ]
S3-KS	Do any keys generated by the DevID module for this signature suite have the specified strength?	ECDSA384:M	9.3.2	Yes [ ]
S3-CSA	Are signatureAlgorithm values in DevID certificates and intermediate certificates as specified for this suite?	ECDSA384:M	9.3.3	Yes [ ]
S3-CPK	Are signatureAlgorithm values in DevID certificates and intermediate certificates as specified for this suite?	ECDSA384:M	93.4	Yes [ ]
S3-CSV	Are the signatureValue values in DevID certificates and intermediate certificates as specified for this suite?	ECDSA384:M	9.3.5	Yes [ ]