

PUBLIC

JULY 2023

IL Strings usage

60802-related proposal

ABB

Agenda

- 01.** IDevIDs of IEEE 802.1AR
- 02.** ILStrings of IEC 61406-2 Ed1
- 03.** 60802 current D2.0 status
- 04.** Proposal for 60802

IDevId

Short description

- A DevID (IEEE 802.1AR) which usually comprise
 - An IETF RFC 5280 conformant X.509 certificate that identifies the subject device
 - Can include authorization information signed by the certificate's issuer
 - A secret private key that corresponds to the certificate's subject public key
 - Any certificate chain required to facilitate the certificate's use
- IDevIDs are provided by device suppliers
- Should be globally unique
- subjectAltName may be included
 - A HardwareModuleName should be included following IETF [RFC 4108](#) which says
 - The hardware module name is composed of an object identifier (hwType) and an octet string (hwSerialNumber) which uniquely identify the hardware module
 - hwType is a unique object identifier that names a hardware model and revision
 - hwSerialNumber is the serial number of the hardware module

ILStrings

Short description

- IEC 61406 Ed1 – 2022 defined the IL (Identification Link) string as a globally unique string assigned to only one physical object
- Such an IL string would provide access to
 - information from the manufacturer such as operating instructions, drawings, spare parts lists and calibration records
 - operating data such as speeds, power consumption and pressures
 - models such as function and simulation models
 - maintenance and inventory management data
- IEC 61406 Ed2 went on and describes an Annex F (informative) on a proposal on how IL strings should be embedded to DevIDs, as a cryptographic binding between the device and the respective IL string
- In this context, IL strings should be defined following the ABNF notation (IETF [RFC 5234](#))

60802

Current D2.0

- Both IEEE 802.1AR in conjunction with IETF RFC 4108 (subjectAltName HardwareModuleName) and IEC 61406 IL-Strings in conjunction with IETF RFC 3986 propose mechanisms of uniquely identifying a physical object
- The IEC 61406/RFC 5234 method is more comprehensive (based on URIs) and a larger adoption, while the IEEE 802.1AR/IETF RFC 4108 one has a somewhat limited semantic
 - IEC 61406 for this purpose used in [Digital Data Chain](#) by [several companies](#)
- Both specs (IEC 61406/RFC 5234 and IEEE 802.1AR/IETF RFC 4108) should remain as they are
- In 60802 D2.0, 4.8.6.3.6 Device Identity Representation in IDevID and LDevID credentials, there are several forms of bindings for verifiable device identity information (items that encode device naming information appear in the subjectAltName extension)
 - By-value: for an IDevID, the product serialNumber in IDevID credentials
 - By-ref: the verifiable device identity information is represented by a reference inside the IDevID (the actual value may be provided by the device itself or by a device-external source)
 - If unprotected information object: the reference object should include a digest value

60802

Proposal

- **Proposal, add also this fourth bullet at 60802 4.8.6.3.6**
- *by-IL-String: the verifiable device identity information is represented by an IL-String, an URI following the requirements of the IEC 61406-2 and with the URI syntax with ABNF notation, described in IETF RFC 5234*

Examples:

Example 1:

- *IL string: `https://www.domain-abc.com/? .1P=1A2B3C&.S=sd09fqw4hrdfj0as89u7`*
- *Resulting URI: `ilstring:http://www.domain-abc.com/? .1P=1A2B3C&.S=sd09fqw4hrdfj0as89u7`*

Example 2:

- *IL string: `https://www.domain-abc.com/sd09fqw4hrdfj0as89u7`*
- *Resulting URI: `ilstring:https://www.domain-abc.com/sd09fqw4hrdfj0as89u7`*

ABB