Industrial Ethernet Security Harmonization Group

_____

WHITEPAPER ON A HARMONIZED IDEVID PROFILE FOR INDUSTRIAL AUTOMATION DEVICES

4.422

Version 1.00 | August 12th, 2025

Disclaimer

Prepared by Industrial Ethernet Security Harmonization Group, consisting of the Standards Developing Organizations (SDOs):

- FCG (FieldComm Group)
- ODVA, Inc.
- OPC Foundation
- PI (PROFIBUS & PROFINET International)

Core group members contributing (alphabetic order):

Andreas Walz (PI)
Dominik Ziegler (PI)
Frank Fengler (FCG)
Jack Visoky (ODVA)
Joakim Wiberg (ODVA)
Randy Armstrong (OPC Foundation)
Simon Merklin (PI)
Stephen Mitschke (FCG)

Comments to be submitted to working group editor: simon.merklin@endress.com

1 Executive Summary

IDevIDs, standardized in IEEE 802.1AR, are secure identifiers for devices. This whitepaper proposes a profile for IDevIDs for devices in the *Industrial Automation* (IA) domain (IA devices). The profile intends to facilitate an interoperable use of IDevIDs across different IA device manufacturers, different standards development organizations (SDOs), different solution providers, and for different use cases. Concretely, the proposed profile:

- recommends IL Strings (in accordance with IEC 61406) as a **common, instance-specific, and globally unique device identity** in IDevIDs, and
- provides a **shortlist of asymmetric cryptographic algorithms** for IDevIDs, seeking to minimize mismatches in algorithm support between devices possessing IDevIDs and verifying entities.

The whitepaper is the result of a harmonization effort between FieldComm Group, ODVA, OPC Foundation, and PROFIBUS & PROFINET International. The proposed profile is applicable for device manufacturers and solution provides in the IA domain that hold, use, and/or process IDevIDs in their products.

2 Background

IEEE 802.1AR is a standard that specifies *Secure Device Identifiers* (DevIDs). DevIDs are designed to be used as interoperable secure device authentication credentials. A DevID comes in the form of a X.509 v3 certificate as profiled by RFC 5280. Devices possessing DevIDs must store them in a way that protects them from modification and illegitimate use [IEEE 802.1AR].

A common use case for DevIDs is the *Extensible Authentication Protocol* (EAP), but other industry standard authentication and provisioning protocols make use of DevIDs, too.

A device with DevID capability incorporates a single, globally unique, and manufacturer-provided *Initial Device Identifier* (IDevID). An IDevID is the secure reflection of a device's permanent identity as assigned and attested by its manufacturer.

One of the main motivations for equipping devices with IDevIDs is that IDevIDs can support a secure onboarding process. During onboarding, a device is equipped with locally significant, i.e., installation-specific, credentials. IDevIDs allow identification and authentication of the device prior to onboarding. This step may be used to inform the decision whether to allow an onboarding of the device. Details of the decision-making process are specific to the use case and the environment; it is considered out-of-scope for this whitepaper. However, the decision is commonly going to consider the identity of the device that is to be onboarded. To allow an unattended secure onboarding of devices (i.e., without human intervention), the decision-making process must be automatable.

Having said that, the IEEE 802.1AR standard does not define an identity model for devices. As a result, different device manufacturers use different device identity models and identity encodings in IDevIDs. In practice, this situation prohibits the interoperable and automated use of device identities from IDevIDs.

IEC 61406 is a standard that specifies *Identification Link (IL) Strings* [IEC 61406-1, IEC 61406-2]. An IL String is a globally unique identifier of a physical object, which can also serve as the address to a web page providing digital information related to the object. An IL String comes in the form of a URL using the manufacturer's DNS name. Each device must not have more than one IL String.

IEC 61406 further specifies the use of 2D symbols (e.g., QR Codes) and NFC tags to carry an object's IL String. Attached to the object's nameplate, it facilitates automated work processes

through machine-readability. With a device's IL String used as a URL, users (e.g., owners, operators) can easily find manufacturer-specific information about the object, such as drawings, operating instructions, and spare parts.

IL Strings are defined in two different flavours. IEC 61406-1 defines IL Strings as transparent identifiers, which do not allow to extract individual device identity attributes [IEC 61406-1]. Other than being used as a URL, the only reasonably possible operation with transparent IL Strings is a comparison of two instances. IEC 61406-2 provides a definition of *structured* IL Strings, which additionally allow a standardized encoding and extraction of individual data elements as key-value pairs [IEC 61406-2]. As keys, IEC 61406-2 allows data identifiers defined by IEC 15418 [IEC 15418].

3 Proposed IDevID Profile for the IA Domain

The IDevID profile proposed herein comprises the following two requirements, which apply if a device possesses an IDevID.

1. **Globally unique device identity**: If a device has an IDevID and an IL String assigned by its manufacturer, the IDevID's end entity certificate(s) shall embed the assigned IL String as described by IEC 61406-2, Annex F.

   Background and rationale: Embedding the IL String assigned to a device in the device's IDevID provides a cryptographic binding between the device and the IL String that is attested by the device manufacturer. It allows a device to cryptographically prove through protocol interactions that it has been assigned the embedded IL String. The obvious prerequisite is that the verifying entity has a trust relation to the device manufacturer (e.g., in the form of an IDevID CA certificate used as trust anchor).

   IEC 61406-2 states that an IL String shall be embedded in a DevID certificate by adding it as a distinct entry of type `uniformResourceIdentifier` (URI) to the *Subject Alternative Name* extension. The URI is formed by prefixing the string "`ilstring:`" to the IL String. This construction ensures smooth coexistence with other URI/URL entries while ensuring deterministic recognizability/distinguishability (i.e., avoiding mistaking an arbitrary other URL for an IL String).

   Example: Consider a device which has been assigned the following example IL String

   "`http://www.domain-abc.com/series/model/serialnumber`".

   The corresponding URI entry to be added to the *Subject Alternative Name* extension of the device's IDevID end-entity certificate then is

   "`ilstring:http://www.domain-abc.com/series/model/serialnumber`".

   Note: This whitepaper does not put forth any recommendations for or limitations of the rules that IA device manufacturers can or should use to build IL Strings for their devices. The rules of IEC 61406 apply without changes or additions.

   Disclaimer: Note that the URI scheme registration for "`ilstring`" at IANA[1] has the status "*provisional*", which means that it "*... can be removed by the experts if – in consultation with the community – the experts find that they are not in use*" [RFC 8615]. Expert review, as required for a "permanent" registration, has not taken place.

   Fallback: If the device does not have an IL string in accordance with IEC 61406 assigned, then a URI representing a globally unique identifier for the device shall be embedded instead. This generic URI shall be added to the *Subject Alternative Name*

[1] Internet Assigned Numbers Authority; see https://www.iana.org/assignments/uri-schemes/uri-schemes.xhtml.

extension of the IDevID end entity certificate(s). Case-sensitive string comparison shall be used to check for equivalence of two such URIs.

Note: If a generic URI is used as fallback, then it may not be possible to determine deterministically which URI in the *Subject Alternative Name* extension is the globally unique identifier for the device (in case multiple URI entries exist).

2. **Cryptographic algorithms**: A device should be able to offer an IDevID certificate chain whose:
    a. end-entity certificate contains a **public key** that corresponds to one of the following elliptic curves
        - NIST P-256
        - NIST P-384
        - NIST P-521
        - Curve 25519
        - Curve 448
    b. and that can be verified (up to a trusted CA) using only the following **signature algorithms**
        - ECDSA P-256 with SHA-256 [IEEE 802.1AR]
        - ECDSA P-384 with SHA-384 [IEEE 802.1AR]
        - ECDSA P-521 with SHA-512 [NIST FIPS 186-5]
        - Ed25519 [RFC 8032]
        - Ed448 [RFC 8032].

ECDSA P-256 with SHA-256 and ECDSA P-384 with SHA-384 are defined by IEEE 802.1AR as possible signature algorithms for DevIDs. ECDSA P-521 with SHA-512, Ed25519, and Ed448 are proposed herein as additional options.

Background and rationale: A device may hold multiple IDevID certificate chains with identical subject identity but using different cryptographic algorithms. IA devices equipped with IDevIDs shall be able to offer at least one IDevID certificate chain that only uses cryptographic algorithms from the above list. The list puts a focus on elliptic curve cryptography (ECC), as it is widely used, state-of-the-art, and provides for small keys and efficient computations. The list comprises both NIST-defined and Edwards curves to offer options from independent sources. Other algorithms or algorithm combinations that are not listed above may nevertheless additionally be offered/supported (i.e., this profile does *not* intend to deprecate the use of certain algorithms or algorithm combinations).

Note: As a result of the anticipated long running use of devices in the IA domain, the selection of cryptographic algorithms for IDevIDs requires device manufacturers to make a critical forward-looking decision. It should be made with care and in consideration of pertinent recommendations and guidelines (e.g., [NIST SP 800-57])[2]. In addition, the private key corresponding to an IDevID is highly sensitive information. The use of dedicated hardware (e.g., a “secure element”) that never exposes the private key of an IDevID is highly recommended.

[2] An overview of recommendations from different bodies can be found under https://www.keylength.com/.

4 Miscellaneous

a. References

[IEC 15418]	ISO/IEC 15418:2016: Information technology — Automatic identification and data capture techniques — GS1 Application Identifiers and ASC MH10 Data Identifiers and maintenance
[IEC 61406-1]	IEC 61406-1:2022: Identification Link - Part 1: General requirements
[IEC 61406-2]	IEC 61406-2 ED1: Identification Link - Part 2: Types/Models, Lots/Batches, Items and Characteristics
[IEEE 802.1AR]	IEEE 802.1AR: IEEE Standard for Local and metropolitan area networks–Secure Device Identity
[NIST FIPS 186-5]	National Institute of Standards and Technology (NIST), Digital Signature Standard (DSS). (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 186-5. https://doi.org/10.6028/NIST.FIPS.186-5
[NIST SP 800-57]	National Institute of Standards and Technology (NIST), Recommendation for Key Management, NIST SP 800-57. https://doi.org/10.6028/NIST.SP.800-57pt1r5
[RFC 8615]	RFC 8615: Well-Known Uniform Resource Identifiers (URIs)
[RFC 8032]	RFC 8032: Edwards-Curve Digital Signature Algorithm (EdDSA)

b. Version History

Version	Date	Changes
Version 1.0	12.08.2025	Release of first version

FieldComm Group

http://go.fieldcommgroup.org

ODVA

www.odva.org

OPC Foundation

www.opcfoundation.org

Profibus and Profinet International (PI)

www.profibus.com