ISO/IEC TS 30168

Edition 1.0 2024-05

TECHNICAL SPECIFICATION

colour inside

Internet of Things (IoT) – Generic trust anchor application programming interface for industrial IoT devices

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 35.020

ISBN 978-2-8322-8518-3

CONTENTS

INTERNET OF THINGS (IoT) – GENERIC TRUST ANCHOR APPLICATION PROGRAMMING INTERFACE FOR INDUSTRIAL IoT DEVICES

FOREWORD

1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.
2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO National bodies.
3) IEC and ISO documents have the form of recommendations for international use and are accepted by IEC and ISO National bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC and ISO documents is accurate, IEC and ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC and ISO National bodies undertake to apply IEC and ISO documents transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC and ISO document and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC and ISO do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC and ISO marks of conformity. IEC and ISO are not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this document.
7) No liability shall attach to IEC and ISO or their directors, employees, servants or agents including individual experts and members of its technical committees and IEC and ISO National bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this ISO/IEC document or any other IEC and ISO documents.
8) Attention is drawn to the Normative references cited in this document. Use of the referenced publications is indispensable for the correct application of this document.
9) IEC and ISO draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC and ISO take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC and ISO had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch and www.iso.org/patents. IEC and ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TS 30168 has been prepared by subcommittee 41: Internet of Things and Digital Twin, of IEC technical committee JTC 1: Information technology. It is a Technical Specification.

This document contains attached files in the form of GTA API C header files and a secure element provider template that are cited in Annex A and Clause G.6. These files are intended to be used as a complement and do not form an integral part of the publication.

The text of this Technical Specification is based on the following documents:

Draft	Report on voting
JTC1-SC41/388/DTS	JTC1-SC41/413/RVDTS

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this Technical Specification is English.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Industrial Internet of Things (IIoT) devices face increasing security requirements. This insight is especially important as more and more devices become connected directly or indirectly to the Internet. It is essential that IIoT devices are prepared to perform secure communications for service interaction, monitoring, and control.

However, security is often still observed as rather complex by implementers and integrators. This perception often results in realization obstacles when the integration and use of security mechanisms and secure elements (SE) is wanted.

This document provides a versatile application programming interface (API) for security to allow a generic integration of SEs into IIoT devices. The API is vendor independent and also independent regarding the SE technology being deployed. This approach simplifies redesign for different SEs and supports software-hardware co-design for security. SEs offering different security properties facilitate the selection of an SE according to the intended use, protection goals, and other boundary conditions. The API aims at achieving high-level abstraction profiles for security services and mechanisms to avoid typical low-level interoperability complexity and implementation failures. Requirements and architectural constraints from IIoT applications shape the final design of the API and its usability.

The resulting API facilitates the security-by-design defined integration of security components within IIoT components on a large scale. The time-to-market for secured devices is accelerated. Stakeholders will benefit from higher security levels being available for lower prices. Application of updates and continuous improvements of security along the lifecycle of products and systems are facilitated.

The following stakeholders and their corresponding interests play a role for the generic trust anchor application programming interface (GTA API) definition:

- Manufacturers and users of industrial equipment

  Scalable use of adequate (hardware-based) security technologies depending on required security, multivendor support, migration strategy, or long-term suitability.

- Software developers

  Increased robustness due to use of a unified API.
  Ease of use for developers without dedicated security expertise.

- Manufacturers of security ICs or ICs offering security functions

  Promote use of hardware-based trust anchor technologies for IIoT devices.

- Conformity Assessment Bodies

INTERNET OF THINGS (IoT) – GENERIC TRUST ANCHOR APPLICATION PROGRAMMING INTERFACE FOR INDUSTRIAL IoT DEVICES

1 Scope

This document specifies a generic application programming interface (API) for the integration of SEs within Industrial Internet of Things (IIoT) devices. It considers needs from industrial usage scenarios and applications. This document also provides guidance for implementation, testing, and conformity validation.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEEE Std 802-2014, *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*

IETF RFC 1035, P. Mockapetris, "Domain names – implementation and specification", November 1987, available at https://www.rfc-editor.org/info/rfc1035 [viewed 2023-08-29]

IETF RFC 1779, S. Kille, "A String Representation of Distinguished Names", March 1995, available at https://www.rfc-editor.org/info/rfc1779 [viewed 2023-08-29]

IETF RFC 4122, P. Leach, M. Mealling, and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", July 2005, available at https://www.rfc-editor.org/info/rfc4122 [viewed 2023-08-29]

IETF RFC 8446, E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3", August 2018, available at https://www.rfc-editor.org/info/rfc8446 [viewed 2023-08-29]