INTERNATIONAL STANDARD

ISO/IEC 20248

First edition
2018-03

Information technology — Automatic identification and data capture techniques — Data structures — Digital signature meta structure

Technologies de l'information — Techniques d'identification automatique et de capture de données — Structures de données — Méta-structure de signature numérique

Reference number
ISO/IEC 20248:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

Introduction

This document specifies a “language” which is used to specify data constructs with; how the data constructs can be read from one or more AIDC; and how to decode and verify such data.

This document is an ISO/IEC 9594-8 (Public Key Infrastructure: digital signatures and certificates) application specification for automated identification services. Data capacity and/or data transfer capacity of Automated Identification Data Carriers are limited. This restricts the normal use of a digital signature as specified in ISO/IEC 9594-8 within automated identification services.

This document specifies an effective and interoperable method to specify, read, decode and verify data stored in automated identification data carriers, independent from real-time remote control. Meta parameters included in a digital certificate are used to achieve

— offline integrity verification of the data source and data originality,

— a verifiable data structure description to enable interoperability of deployment, domain authority and automated identification data carriers,

— a verifiable data encoding method to achieve compact data to be stored in data constrained automated identification data carriers (the JSON data format is used for both input and output of the encoder and decoder),

— a verifiable automated identification data carrier read method description allowing for the data of a read event to be distributed over more than one carrier of the same and of different technologies, and

— a verifiable method to support key management of cryptographically enabled automated identification data carriers.

The user of this document may use any suitable hashing and asymmetric cryptography method. The choice of cryptography method should be considered carefully and it is advised that only internationally recognized or standardized methods, for example FIPS PUB 186-4 and IEEE P1363, be used.

This document should be used in conjunction with standard risk assessments of the use case and environment.

NOTE Many transport applications rely on a secure non-transferable unique identifier to ensure that the data are bound to the tag and/or the vehicle. For such functionality, please refer to ISO/IEC 29167. This specification provides a mechanism to ensure the integrity and authenticity of the data themselves in order to protect against alterations or insertion of false data into the system. It does not provide any means to defend against replay attacks. Including the secure non-transferable unique identifier of a tag, as signed data, allows for the unrefutable link between the tag and the data and provides a means to determine if the data were read from the tag. The reader can place the read DigSig in another DigSig, effectively signing the read transaction. A third party can then verify that the read transaction happened at a given place and time, as well as the data read.

Information technology — Automatic identification and data capture techniques — Data structures — Digital signature meta structure

1 Scope

This document is an ISO/IEC 9594-8 (Public Key Infrastructure: digital signatures and certificates) application specification for automated identification services. It specifies a method whereby data stored within a barcode and/or RFID tag are structured, encoded and digitally signed. ISO/IEC 9594-8 is used to provide a standard method for key and data description management and distribution. It is worth noting that the data capacity and/or data transfer capacity of Automated Identification Data Carriers are restricted. This restricts the normal use of a Digital Signature as specified in ISO/IEC 9594-8 within automated identification services.

The purpose of this document is to provide an open and interoperable method, between automated identification services and data carriers, to read data, verify data originality and data integrity in an offline use case.

This document specifies

— the meta data structure, the DigSig, which contains the Digital Signature and encoded structured data,

— the public key certificate parameter and extension use, the DigSig Certificate, which contains the certified associated public key, the structured data description, the read methods and private containers,

— the method to specify, read, describe, sign, verify, encode and decode the structured data, the DigSig Data Description,

— the DigSig EncoderGenerator which generates the relevant asymmetric key pairs, keeps the Private Key secret and generates the DigSigs, and

— the DigSig DecoderVerifier which, by using to the DigSig Certificate, reads the DigSig from the set of Data Carriers, verifies the DigSig and extracts the structured data from the DigSig.

A successful verification of the DigSig signifies the following:

— the data was not tampered with;

— the source of the data is as indicated on the DigSig Certificate used to verify the DigSig with;

— if a secured identifier of the data carrier is included in the DigSig it contains, then the data stored on the data carrier can be considered as the original issued copy of the data; the secure identifier will be able to guarantee that the data carrier is authentic.

This document does not specify

— cryptographic methods, nor

— key management methods.

This document is used in conjunction with standard risk assessments of the use environment.

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.

ISO/IEC 8824-1[1)], *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1*

ISO/IEC 9594-1[2)], *Information technology — Open Systems Interconnection — The Directory — Part 1: Overview of concepts, models and services*

ISO/IEC 9594-8[3)], *Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks*

ISO/IEC 9899, *Information technology — Programming languages — C*

ISO/IEC 18004, *Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification*

ISO/IEC IEEE 9945, *Information technology — Portable Operating System Interface (POSIX®) Base Specifications, Issue 7*

IETF 3986, *Uniform Resource Identifier (URI): Generic Syntax*

IETF RFC 5646[4)], *Tags for Identifying Languages*

1) ITU-T X.680 is equivalent to ISO/IEC 8824-1.

2) ITU X.500 is equivalent to ISO/IEC 9594-1, and is the commonly used reference for standard and terminology.

3) ITU X.509 is equivalent to ISO/IEC 9594-8, and is the commonly used reference for standard and terminology.

4) IEFT RFC 5646 is the reference specification of the IETF BCP 47.