International Standard

ISO/IEC 22460-2

First edition

Cards and security devices for personal identification — ISO UAS license and drone/UAS security module —

Part 2: Drone/UAS security module

Cartes et dispositifs de sécurité pour l'identification des personnes — Permis ISO de systèmes d'aéronefs sans équipage à bord et module de sécurité de drone/système d'aéronefs sans équipage à bord —

Partie 2: Module de sécurité de drone/système d'aéronefs sans équipage à bord

PROOF/ÉPREUVE

Reference number
ISO/IEC 22460-2:2024(en)

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

Published in Switzerland

Contents

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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC 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, ISO and IEC 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 www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and security devices for personal identification*.

A list of all parts in the ISO/IEC 22460 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

The ISO/IEC 22460 series consists of the following parts, under the general title *Cards and security devices for personal identification — UAS license and drone/UAS security module*:

- Part 1[1]: *Physical characteristics and basic data sets for UAS licence*. Part 1 describes the basic terms for the ISO/IEC 22460 series, including physical characteristics, basic data element set, visual layout, and physical security features.
- Part 2 (this document): *Drone/UAS security module*. This document describes data and cryptographic functions of the drone/UAS security module. The drone security module does not limit the types of data contained in this module and the cryptographic functions it provides.
- Part 3[2]: *Logical data structure, access control, authentication and integrity validation for drone license*. Part 3 describes guidelines for the design format and data content of a UAS license with regard to logical data structure, access control, authentication and integrity validation.

[1] Under development. Stage at the time of publication: ISO/IEC DIS 22460-1.

[2] Under development. Stage at the time of publication: ISO/IEC AWI 22460-3.

Cards and security devices for personal identification — ISO UAS license and drone/UAS security module —

Part 2: Drone/UAS security module

1 Scope

This document specifies cryptographic functions of the drone/unmanned aircraft system (UAS) security module. The drone/UAS security module is a security device that serves as a container for the drone/UAS pilot license, drone/UAS operator license, and other personal identification. It provides storage space for storing optional elements and has the capability of cryptographic functions including integrity validation, authentication and data encryption.

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 21384-4, *Unmanned aircraft systems — Part 4: Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 21384-4 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
drone security module
drone/unmanned aircraft system security module
drone/UAS security module
security device that serves as a container and cryptographic function provider for the drone pilot/operator license and other personal identification and for drone ID and flight permit ID, as optional elements

3.2
access entity
functional entity that can read, write and update data of the drone security module

3.3
drone security module issuer
authority, company or country issuing a drone security module, which applies a digital signature to a drone security module and is responsible for the associated key management

3.4
drone security module user
entity that writes data to the drone security module and reads data from the drone security module, but which cannot write or update data to be issued by the issuing authority

3.5
remote control station
control station that provides the facilities for the pilot control or automatic flight of an unmanned aircraft (UA)

3.6
unmanned aircraft
UA
aircraft which is intended to operate with no pilot on board

3.7
unmanned aircraft system
UAS
aircraft and its associated elements which are operated with no pilot on board

3.8
unmanned aircraft system management system
UAS management system
counterpart entity as a system responsible for the identification, authentication, registration, operation, flight-permit, and other management of an unmanned aircraft (UA)

4 Symbols and abbreviated terms

For the purposes of this document, the following symbols and abbreviated terms apply.

AAD	Additional Authentication Data
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
APDU	Application Protocol Data Unit
BCD	Binary Code Decimal
CA	Certification Authority
DER-TLV	Distinguished Encoding Rules – Tag Length Value
DH	Diffie-Hellman
EC	Elliptic Curve
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECKA-DH	Elliptic Curve Key Agreement Algorithm – Diffie-Hellman
eSIM	embedded Subscriber Identity Module
GCM	Galois/Counter Mode
HKDF	HMAC-based Extract-and-Expand Key Derivation Function
HMAC	Keyed-Hashing for Message Authentication Code
IV	Initial Vector
KDF	Key Derivation Function
MAC	Message Authentication Code

OID	Object identifier
SD	Secure Digital
SHA	Secure Hash Algorithm
SoC	System on Chip
SPI	Serial Peripheral Interface
TLS	Transport Layer Security
UA	Unmanned aircraft
UAS	Unmanned aircraft system
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module

5 Overview of a drone security module

5.1 General

A drone security module is a security device that serves as a container with personal identification for a drone.

A drone security module can contain the drone pilot/operator license and other personal identification data. However, these data are not mandatory data that should be included in the drone security module.

A drone security module shall provide storage space for storing optional elements such as user-specific data.

A drone security module shall provide cryptographic functions, including integrity validation, authentication and data encryption to protect personal identification data.

5.2 Form-factor of a drone security module

The form-factor of a drone security module is not limited to any specific hardware type. A drone security module is independent of physical interface technology. The physical form-factor of a drone security module may be, for example, an IC card, a universal subscriber identity module (USIM) card, a micro secure digital (SD) card, an embedded subscriber identity module (eSIM), or a module in system on chip (SoC).

Transmission protocols used to communicate between the drone security module and its access entity should be in accordance with ISO/IEC 7816-3 unless specified otherwise. Command-response pairs exchanged at the interface, namely a command application protocol data unit (APDU) followed by a response APDU in the opposite direction, should be in accordance with ISO/IEC 7816-4.

Other transmission protocols, such as serial peripheral interface (SPI) and universal serial bus (USB) may be used between the drone security module and its access entity according to the hardware type of drone security module.

This document does not limit transmission protocol between drone security module and its access entity.

5.3 Use of a drone security module

A drone security module is issued by a drone security module issuer. A UAS management system, aviation authorities or a drone service provider may be the drone security module issuer.

A drone security module is used by the drone security module user, e.g. UA, UA operator or UAS management system (when it is not an issuer). They may read data in the drone security module and write any data to the drone security module.

6 Data format of a drone security module

6.1 General

A drone security module contains data written by the issuer and the user.

There is no mandatory data that shall be issued by the drone security module issuer. Data to be written in the drone security module can be different according to the regulations of each country.

As shown in Figure 1, a drone security module contains a drone pilot/operator license and other personal identification data. A drone security module shall provide storage space for storing optional elements such as user-specific data.

This document does not specify data elements of each data in the drone security module. Detailed data elements follow each country's regulations.

NOTE See Annex A for the informative data examples.

The encoding of each data may be:

- packed BCD, if the value of data consists of only N characters;
- in accordance with ISO/IEC 8859-1, if the value of data includes any alphabetical or special characters;
- unpacked BCD, if the value denotes date.

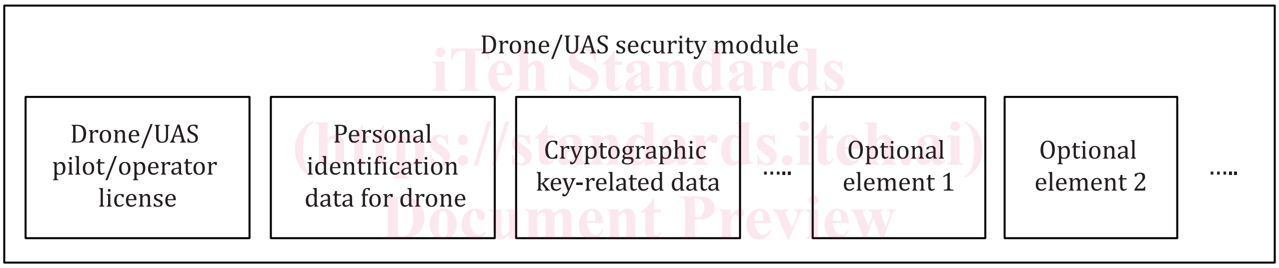
Drone/UAS security module
Drone/UAS pilot/operator license
Personal identification data for drone
Cryptographic key-related data
.....
Optional element 1
Optional element 2
.....

Figure 1 — Drone security module data

6.2 Drone pilot/operator license

A drone pilot/operator license can be contained in the drone security module.

This document does not specify the data elements and format of a drone pilot/operator license.

6.3 Personal identification data for a drone

The personal identification data for a drone can be contained in the drone security module.

This document does not specify the data elements and format of a personal identification data for a drone.

6.4 Cryptographic key-related data

Cryptographic key-related data is required to execute cryptographic functions and can be stored in the drone security module.

The digital certificate and identifier of a private key is cryptographic key-related data. Security requirements regarding storage and access of credential information, including private key, are out of scope of this document. It is the responsibility of the drone security module issuer to ensure that all data stored in the drone security module is stored securely.