International Standard

ISO/IEC 22460-2

First edition
2024-04

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

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

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.

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 22460-1:2023.

2) Under development. Stage at the time of publication: ISO/IEC AWI 22460-3:2024.

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.

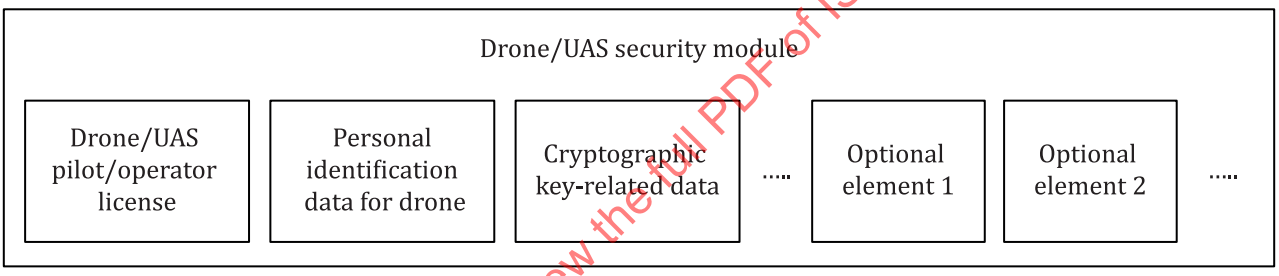


Figure 1 — Drone security module data

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.

A drone security module issuer may define the certificate profile. An example of a certificate profile is shown in Table 1. These are some of the most common fields in certificates. Other certificates can contain a number of fields not listed in Table 1.

Table 1 — Example of a certificate profile signed by a drone security module issuer (X.509 v3 certificate)

Field		Field type	Value, definition or explanation
Version		m	3 (0x2)
Serial number		m	Non-sequential positive, non-zero integer, minimum containing at least 63 bits of output from a CSPRNG, maximum 20 octets.
Signature algorithm		m	Value shall match the OID in signature algorithm.
Issuer		m	Country name(mandatory): ISO 3166-1 alph2 (e.g. US or KR) Organization(mandatory): name of root certificate issuer
Validity	Not before	m	The value of not before date shall not be later then issuance date of drone security module. See RFC 5280 for data type format.
	Not after	m	The value of not after date shall be later then expiry date of drone security module. See RFC 5280 for data type format.
Subject		m	Country code(mandatory): ISO 3166-1 alph2 (e.g. US or KR) Organization: name of drone security module signer
Subject public key info	Algorithm	m	OID of public key algorithm (Elliptic curve).
	Parameters	m	OID of curve identifier (e.g. P-256).
	Public key	m	Public key shall be encoded in uncompressed form.
Extensions		m	
Authority key identifier		m	Same value as subject key identifier of the drone security module CA certificate.
Subject key identifier		m	SHA1 value of the value as subject public key bit string.
Certificate signature algorithm		m	ECDSA-with SHA256 ECDSA-with SHA384 ECDSA-with SHA512
Certificate signature value		m	Value according to signature algorithm

6.5 Other data

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

The use of optional elements is determined by each country's regulations. Optional elements may or may not be used. The optional elements are related to users such as UA, UA operator or UAS management system.

7 Cryptographic functions of a drone security module

7.1 General

Cryptographic functions of the drone security module shall be used for security applications if the UA uses a drone security module to compute cryptographic functions.

A UA may be a user of the drone security module. A UAS management system may be a counterpart entity that communicates with the UA.

Communication between the UA and the UAS management system is divided into communication between the drone security module and the access entity of the drone security module, between the access entity and the UA, and between the UA and the UAS management system through wireless media.

A drone security module performs cryptographic functions on the request of a UA or other user of the drone security module.

Cryptographic functions implemented in the drone security module shall include integrity validation, authentication, data encryption and digital signature.

In addition, a Transport Layer Security (TLS) and a digital signature for drone flight data can be implemented in the drone security module according to each aviation authority's policy.

Each country can use different cryptographic functions for the different security applications based on the UA category, flight environment and other factors.

7.2 Integrity validation

7.2.1 Purpose and general

The purpose of integrity validation is to confirm that data that is written by a drone security module issuer, such as a drone pilot/operator license and personal identification data, have not been changed since the drone security module was issued.

However, a drone pilot/operator license and personal identification are not mandatory data. Therefore, no integrity validation is required if there is no data issued by the issuer.

Integrity validation is implemented by way of a digital signature over data written by the drone security module issuer, using a public-private (asymmetric) key pair.

Hash values of data written by the drone security module issuer are calculated and the values are then digitally signed using a private key and the digital signature is stored in the drone security module.

The public key belonging to the private key used for the digital signature is provided as part of the drone security module certificate. The drone security module issuer's CA root certificate is used to sign the drone security module certificate.

This document does not mandate both methods to obtain and to establish trust in a drone security module issuer's CA certificate. It is the responsibility of the person or organization responsible for the counterpart entity to either obtain or to establish trust or both, in the drone security module issuer's CA certificate used to verify a drone security module certificate. It is the responsibility of a drone security module issuer to ensure that keys are generated, administered and protected as necessary.

7.2.2 Hash function

A drone security module issuer may use one of the following digest algorithms: SHA-256, SHA-384 or SHA-512 specified in ISO/IEC 10118-3.

7.2.3 Digital signature

The digital signature value is generated over the concatenation of the hash values of each data written by the drone security module issuer and the value is stored in the drone security module.

A drone security module issuer may use ECDSA as specified in ANSI X9.62 as a digital signature algorithm. The elliptic curve domain parameters used to generate the ECDSA key pair may be described explicitly in the parameters of the public key, i.e. parameters may be of type ECParameters (no named curves, no implicit parameters) and may include the optional cofactor. ECPoints may be in uncompressed format. The minimum size for the base point order should be 224 bits.

For example, a digital signature value may be implemented as a SignedData Type, as specified in RFC 5652. The value may be encoded in DER-TLV format. Table 2 describes an example of SignedData Type.

Table 2 — SignedData type

Data element	m/o/c	Comments
Signed Data	m	
version	m	v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-mrtd-security-ldsSecurityObject
eContent	m	The encoded contents of digital signature value.
Certificates	o	
crls	x	
signerInfos	m	
SingerInfo	m	
Version	m	
sid	m	
issuerandSerialNumber	c	It is recommended that a drone security module issuer support this field over subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the hash value over encapsulatedContent and signedAttrs.
signedAttrs	o	The drone security module issuer may include additional attributes for inclusion in the signature.
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the signature value and any associated parameters.
Signature	m	The result of the signature generation process.
unsignedAttrs	o	The drone security module issuer may use this field.
Key m = mandatory (the field shall be present); x = do not use (the field shall not be populated); o = optional (the field may be present); c = choice (the field content is a choice from alternatives).		

7.3 Authentication

7.3.1 Purpose and general

The objective of drone security module authentication is to verify whether the drone security module is what it says it is. Another objective is to prevent cloning of the drone security module and to mitigate the man-in-the-middle attack.

The drone security module authentication key pair consists of a public and a private key. The drone security module private key is used to authenticate the drone security module. It is also used to authenticate the response data contained from the counterpart entity it communicates with. The drone security module public key is stored in the cryptographic key-related data.

In the security applications between UA and the counterpart entity, the counterpart entity assumes that the drone security module is authentic if the authentication signature or MAC is correct.

For example, the drone security module authentication key shall be used to authenticating the drone security module in one of two ways: ECDH-agreed MAC or ECDSA signature. A drone security module may choose

either approach, but shall choose only one of the two. A drone security module authentication key shall not be used to produce both MACs and signatures.

NOTE See Annex B and Annex C for the informative security protocol examples.

This document does not limit the use of any other authentication algorithms. In addition to the drone security module authentication methods of this document, each country and local authority can choose to implement commercial authentication methods according to their own security requirements.

7.3.2 Authentication by MAC

To authenticate the drone security module with MAC authentication, the drone security module computes the MAC with an ephemeral MAC key derived from the drone security module's private key, `SDimKey.Priv`, and the counterpart entity's public key, `EEntityKey.Pub`. The drone security module calculates this ephemeral MAC key, `EMacKey`, by computing the key derivation function KDF(ECDH*(*`SDimKey.Priv`, `EEntityKey.Pub`*)*) and the counterpart entity calculates this `EMacKey` by performing KDF(ECDH*(*`SDimKey.Pub`, `EEntityKey.Priv`*)*). The KDF and ECDH functions shall be the same on both the drone security module and the counterpart entity.

A drone security module shall generate the MAC to be sent to the counterpart entity and the drone security module shall verify the MAC received from the counterpart entity.

7.3.3 Authentication by signature

To authenticate the drone security module by digital signature, the drone security module shall generate the digital signature with the drone security module private key.

7.4 Data encryption

7.4.1 Purpose

The purpose of data encryption is to protect data sent out from the drone security module from eavesdropping and alteration.

In drone security applications, encrypting data between the drone security module and the counterpart entity with the session key protects data sent out from the drone security module from eavesdropping and alteration.

7.4.2 Procedure

For session encryption between the drone security module and the counterpart entity, the drone security module shall use ephemeral key ECDH and two exchanged random numbers to establish session keys for authenticated symmetric encryption. The following steps are performed in session encryption:

— Step 1: Ephemeral key pair generation. The drone security module generates an ephemeral key pair (`EDimKey.Priv`, `EDimKey.Pub`) and the drone security module generates a random number `Ra` and sends it to the counterpart entity.

— Step 2: Session establishment. The counterpart entity generates its ephemeral key pair (`EEntityKey.Priv`, `EEntityKey.Pub`) and the counterpart entity generates a random number `Rb` and sends it to the drone security module. Two session keys (`SKEntity`, `SKDim`) are derived independently by the drone security module and the counterpart entity and used to encrypt and decrypt messages during the remainder of the session. To compute the session keys (`SKEntity`, `SKDim`), the drone security module uses *KDF(ECDH(*`EDimKey.Priv`, `EEntityKey.Pub`*)*, `Ra`, `Rb`) and the counterpart entity uses *KDF(ECDH(*`EDimKey.Pub`, `EEntityKey.Priv`*)*, `Ra`, `Rb`). The counterpart entity encrypts the session data with `SKEntity` and sends it to the drone security module.

— Step 3 to Step *n:* Session data. The drone security module receives the data that is encrypted with `SKEntity`. The drone security module decrypts the encrypted session data with `SKDim` and encrypts data to be sent to the counterpart entity. Both `SKDim` and `SKEntity` shall be the same. The counterpart entity

and drone security module may optionally exchange additional messages. Each message is encrypted by the drone security module and counterpart entity using their respective session keys.

Another method of session encryption may use standard ephemeral key ECDH to establish session keys for authenticated symmetric encryption. The following steps are performed in session encryption:

— Step 1: Ephemeral key pair generation. The drone security module generates an ephemeral key pair (`EDimKey.Priv`, `EDimKey.Pub`).

— Step 2: Session establishment. The counterpart entity generates its ephemeral key pair (`EEntityKey.Priv`, `EEntityKey.Pub`). Two session keys (`SKEntity`, `SKDim`) are derived independently by the drone security module and the counterpart entity and used to encrypt and decrypt messages during the remainder of the session. To compute the session keys (`SKEntity`, `SKDim`), the drone security module uses *KDF(ECDH(*`EDimKey.Priv`, `EEntityKey.Pub`*))* and the counterpart entity uses *KDF(ECDH(*`EDimKey.Pub`, `EEntityKey.Priv`*))*. The counterpart entity encrypts the session data with `SKEntity` and sends it to the drone security module.

— Step 3 to Step *n:* Session data. The drone security module receives with the data that is encrypted with `SKEntity`. The drone security module decrypts the encrypted data with `SKDim` and encrypts data to be sent to the counterpart entity. Both `SKDim` and `SKEntity` shall be the same. The counterpart entity and drone security module may optionally exchange additional messages. Each message is encrypted by the drone security module and counterpart entity using their respective session keys.

Table 3 shows examples of the different methods used for the cryptographic operations.

— For ECDH, Elliptic Curve Key Agreement Algorithm – Diffie-Hellman (ECKA-DH) according to BSI TR-03111 should be used. The output of this function is the shared secret value `Zab`.

— The key derivation should use HKDF instantiated with SHA-256 as defined in RFC 5869.

— For encryption, AES-256-GCM should be used. The counterpart entity encrypts its messages with `SKEntity`, and the drone security module encrypts its messages with `SKDim`. Therefore, both the drone security module and the counterpart entity need to generate both session keys in order to be able to also decrypt the messages they receive. The nonce used for encryption is built up according to the following structure: identifier | counter. The identifier is an 8-byte value. The counterpart entity shall use the following identifier: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00. The drone security module shall use the following identifier: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x01. Each session key has its own counter value. The counter value is an unsigned integer. The first encryption with a key shall use a counter value of 1. For each following encryption, the counter value shall be increased by 1. The counter value shall be formatted as a 4 byte big endian value. A counter value shall never be reused in any future encryption using the same key. For the encryption, the IV is the nonce value and the AAD is an empty string. The format of the encrypted message is the ciphertext, followed by 16 bytes of the tag.

Table 3 — Example of cipher suites

Operation	Definition	Specification
ECDH	ECKA-DH	BSI TR-03111
KDF	HKDF-SHA-256	RFC 5869
Encrypt	AES-256-GCM	NIST SP 800-38D
MAC	HMAC-SHA-256	RFC 2104

This document recommends the use of cipher suites (shown in Table 3), but each drone security module issuer/user or aviation authority can use other cipher suites..

7.5 Transport layer security (TLS)

Communication between the drone security module and the counterpart entity may use TLS.

The drone security module may support TLS version 1.2 specified in RFC 5246 and may support TLS version 1.3 specified in RFC 8446.

The TLS connection should use one of the cipher suites listed in Table 4.

Table 4 — TLS cipher suites

Cipher suite	Reference
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	RFC 8422
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	RFC 8422

The key exchange should use one of the elliptic curves listed in Table 5.

Table 5 — Elliptic curves for the TLS key exchange

Elliptic curve	Reference
P-256	FIPS PUB 186-4
P-384	FIPS PUB 186-4
P-512	FIPS PUB 186-4

The TLS cipher suites in Table 4 are recommended, but other cipher suites can be used according to regulations and policy. The elliptic curve in Table 5 is recommended, but other elliptic curves can be used.

7.6 Digital signature

A drone security module may generate a digital signature for some data that a drone security module user, such as UA, requests.

In this case, a digital certificate and private key shall be provided by the drone security module user and may be contained in the module as optional elements. Security requirements regarding storage and access of credential information, including the drone security module private key, is out of scope of this document.

Annex A
(informative)

Data examples of a drone security module

A.1 General principles

Containing optional data in the drone security module is not mandatory.

However, the drone security module does not limit types of data that can be contained in the module because the module acts as a security container.

A.2 Example 1: Drone ID

A UA carries the drone ID information required by the national government in which it is being operated and in accordance with local aviation authority requirements.

If the UA uses the drone security module, the drone ID can be stored in the drone security module. Selection of a drone ID is at the discretion of the issuer or user.

Table A.1 shows examples of drone IDs that can be contained in the drone security module as optional elements.

Table A.1 — Example of drone IDs

Drone ID	Format
Remote ID (ISO 23629-8)	See ISO 23629-8
Remote ID (ASTM F3411-19)	See ASTM F3411-19
Remote ID (ASD-STAN prEN 4709-002)	See ASD-STAN prEN 4709-002

A.3 Example 2: Drone registration data

A drone security module should contain the following drone registration data. Any or all data of the below candidate should be present for a particular implementation.

— operating organization;

— operator(pilot)'s name;

— operator's address;

— operator's e-mail address;

— operator's telephone number;

— operator's license number;

— pilot registration number of registration authority.

NOTE Local regulations can apply to the selection and format of drone registration data.

Annex B
(informative)

Mutual authentication between a drone security module and a counterpart entity

B.1 General

Mutual authentication between a drone security module and a counterpart entity is a bi-directional protocol that the drone security module authenticates the counterpart entity to prevent access by an unauthorized entity and the counterpart entity authenticates the drone security module to prevent access by an unauthorized drone security module.

In this case, UA may be the drone security module user and the UAS management system may be the counterpart entity.

For mutual authentication, both drone security module authentication and counterpart entity authentication should be implemented using the same authentication method.

For details, see Annex C.

B.2 Drone security module authentication

See 7.3.

B.3 Counterpart entity authentication

Counterpart entity authentication uses information stored in the counterpart entity to confirm that the counterpart entity and the counterpart entity message are authenticated.

The counterpart entity authentication method should be the same as the drone security module authentication method.

Annex C
(informative)

Security applications — Use cases

C.1 Overview

This annex specifies use case security applications between a drone security module and a counterpart entity.

In this case, the access entity of the drone security module is in the UA. The access entity can read drone security module data and request to perform security mechanisms. A UAS management system or a remote control station can be a counterpart entity.

Communications between the UA and the UAS management system are divided into:

— communication between the drone security module and the access entity of the drone security module,

— communication between the access entity and the UA, and

— communication between the UA and the UAS management system through wireless media.

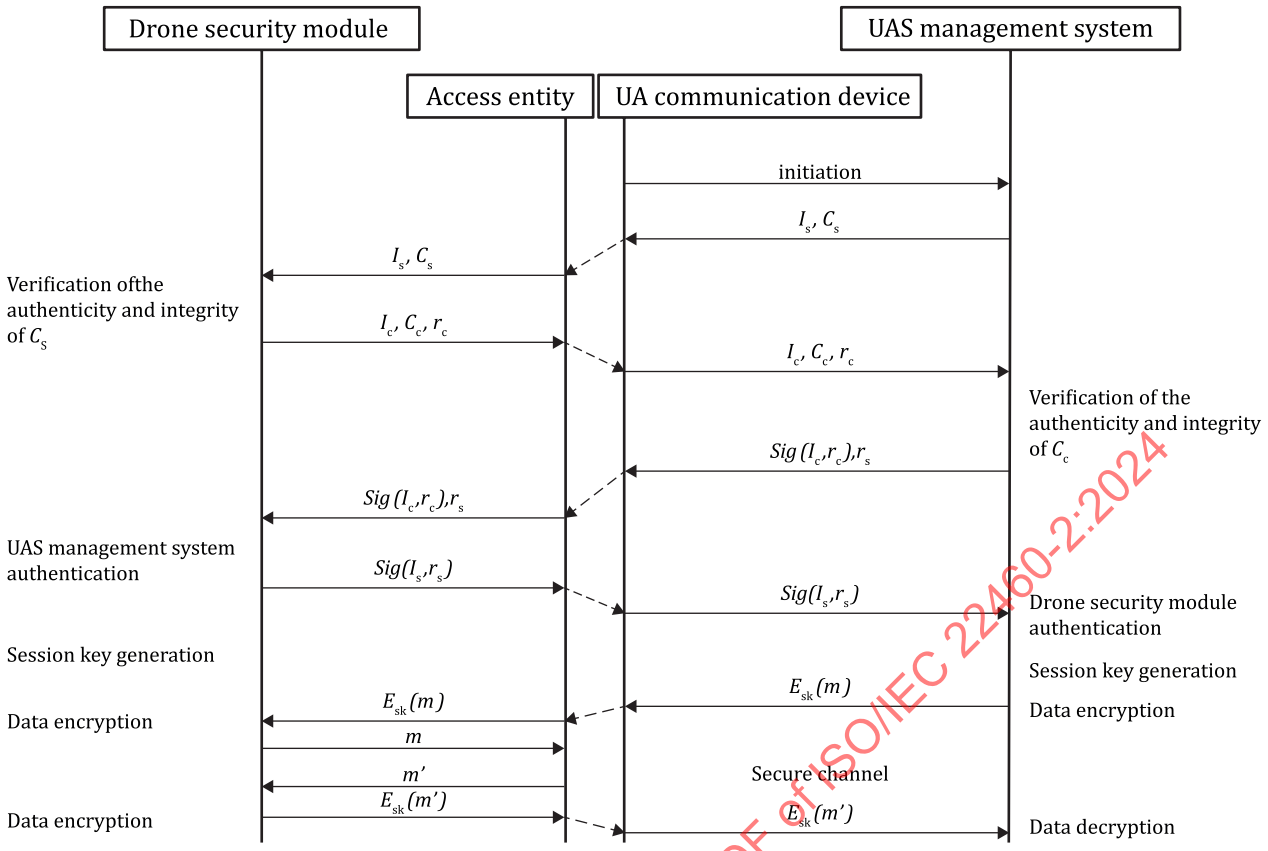
This document does not cover the implementation of security applications.

C.2 Use case 1: AKA based on ECDSA authentication

This application describes ECDSA-based mutual authentication between the drone security module and the UAS management system and data encryption between them.

The UA conceptually consists of a drone security module, an access entity of the drone security module and UA communication device. Wireless communication between the UA and the UAS management system is not covered in this document. Data exchange between the access entity of the drone security module and UA communication device is also out of scope of this document.

Before running the use case 1, it is assumed that the drone security module has its private key `EDimKey.Priv`(d_c) and certificate(C_c), and the drone security module issuer CA's certificate(C_{CA}). Likewise, the UAS management system has its private key `EEntityKey.Priv` (d_s) and certificate(C_s), and the management system CA's certificate(C_{CA}). C_c is issued by the drone security module issuer CA and signed by the drone security module issuer CA's private key using the ECDSA algorithm. C_s are issued by the UAS management system CA and signed by the UAS management system CA's private key using the ECDSA algorithm. The issuing certificate is out of scope of this document because it is different depending on each country's regulatory requirements.



Key

I_C Drone identification data
C_C drone security module certificate
r_C drone security module random number
I_S UAS management system identification data
C_S UAS management system certificate
r_S UAS management system random number
m message

Figure C.1 — ECDSA-based mutual authentication and data encryption between drone security module and UAS management system

The protocol in Figure C.1 works as follows:

a) [Initiation] The UA is a drone security module user. The UA initiates protocol either before or just after UA take-off.

b) [Certification request] The UAS management system sends the UAS management system's ID(I_s) and certificate(C_s) to the UA and the UA transmits I_s and C_s to the drone security module through the access entity of the drone security module.

c) [Verification of authenticity and integrity of UAS management system's certificate] The drone security module verifies the authenticity and integrity of the C_s using C_{CA}. According to the result, the drone security module chooses one of the following two cases:

   1) If the verification is successful, the drone security module ensures that C_s has really been issued for the UAS management system. Therefore, the drone security module sends a random number(r_c) to the UAS management system through the access entity of the drone security module.

2) If the verification fails, the protocol is terminated.

d) [Certification response] The drone security module transmits its ID(I_c) and certificate(C_c) with r_c, where I_c is a drone identification data.

e) [Verification of authenticity and integrity of drone security module certificate] The UAS management system verifies the authenticity and integrity of C_c using C_{CA}. According to the result, the UAS management system chooses one of the following two actions:

1) If the verification is successful, the UAS management system signs I_c and r_c with the private key `EEntityKey.Priv`(d_s) that corresponds to C_s. Then, the UAS management system ensures that C_c has really been issued for the drone security module. Next, the UAS management system sends a random number(r_s) with the signed value, $Sig(I_c, r_c)$, to the drone security module.

2) If the verification fails, the protocol is terminated.

f) [UAS management system authentication based on ECDSA] The drone security module verifies $Sig(I_c, r_c)$ with the public key `EEntityKey.Pub`(Q_s) which is included in C_s. According to the result, the drone security module chooses one of the following two actions:

1) For a positive result, the drone security module decides the UAS management system possesses the right certificate private key `EEntityKey.Priv`(d_s), i.e. the drone security module authenticates UAS management system. Then, the drone security module signs I_s and r_s with the private key `EDimKey.Priv`(d_c) that corresponds to C_c and sends the signed value, $Sig(I_s, r_s)$, to the UAS management system.

2) For a negative result, the protocol is terminated.

g) [Drone security module authentication based on ECDSA] The UAS management system verifies $Sig(I_s, r_s)$ with the public key `EDimKey.Pub` (Q_c). According to the result, the UAS management system chooses one of the following two actions:

1) For a positive result, the UAS management system decides that the drone security module possesses the right certificate private key `EDimKey.Priv` (d_c), i.e. the UAS management system authenticates the drone security module. In this step, mutual authentication procedure is completed.

2) For a negative result, the protocol is terminated.

h) [Key agreement for session encryption] After successful mutual authentication between the drone security module and the UAS management system, both the drone security module and the UAS management system computes the same session key from their own private key, the public key of the other one and exchanged random numbers. Finally, a secure channel is established between the drone security module and the UAS management system.

1) Session key generation at the drone security module:

i) The drone security module obtains the public key of the UAS management system $Q_s=d_sP$ from C_s.

ii) The drone security module derives a session key $sk = d_cQ_sr_cr_s = d_cd_sr_cr_sP$ from its own private key(d_c), UAS management system's public key(Q_s) and two exchanged random numbers(r_c, r_s).

2) Session key generation at the UAS management system

i) The UAS management system obtains public key of the drone security module $Q_c=d_cP$ from C_c.

ii) The UAS management system derives a session key $sk = d_sQ_cr_cr_s = d_sd_cr_cr_sP$ from its own private key(d_s), drone security module's public key(Q_c) and two exchanged random numbers(r_c, r_s).

i) [Data encryption and decryption] After mutual AKA, both the drone security module and the UAS management system establish a secure channel using the common session key. This session key ensures

the strong encryption of data during the further communication between the drone security module and UAS management system.

1) Decryption

   i) The UA receives encrypted data $E_{sk}(m)$ from the UAS management system over secure channel.

   ii) The drone security module receives the encrypted data $E_{sk}(m)$ through the access entity of the drone security module.

   iii) The drone security module recovers original data m using the session key sk, and returns m back to the access entity of the drone security module.

2) Encryption

   i) The drone security module receives data m' through the access entity of the drone security module.

   ii) The drone security module encrypts m' using the session key sk and returns encrypted data $E_{sk}(m')$ back to the access entity of the drone security module.

   iii) The UA sends $E_{sk}(m')$ to the UAS management system over secure channel.

C.3 Use case 2: AKA based on MAC authentication

This application describes MAC-based mutual authentication between the drone security module and the UAS management system and data encryption between them.

This application assumes that the drone security module has d_c, C_c and C_{CA}. Also, the UAS management system has d_s, C_s, and C_{CA}.