



BSI Standards Publication

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

Part 2: Drone/UAS security module

National foreword

This British Standard is the UK implementation of ISO/IEC 22460-2:2024.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and security devices for personal identification.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 25154 8

ICS 35.240.15

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2024.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------



International
Standard

ISO/IEC 22460-2

**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*

**First edition
2024-04**



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	2
5 Overview of a drone security module	3
5.1 General	3
5.2 Form-factor of a drone security module	3
5.3 Use of a drone security module	3
6 Data format of a drone security module	4
6.1 General	4
6.2 Drone pilot/operator license	4
6.3 Personal identification data for a drone	4
6.4 Cryptographic key-related data	4
6.5 Other data	5
7 Cryptographic functions of a drone security module	5
7.1 General	5
7.2 Integrity validation	6
7.2.1 Purpose and general	6
7.2.2 Hash function	6
7.2.3 Digital signature	6
7.3 Authentication	7
7.3.1 Purpose and general	7
7.3.2 Authentication by MAC	8
7.3.3 Authentication by signature	8
7.4 Data encryption	8
7.4.1 Purpose	8
7.4.2 Procedure	8
7.5 Transport layer security (TLS)	9
7.6 Digital signature	10
Annex A (informative) Data examples of a drone security module	11
Annex B (informative) Mutual authentication between a drone security module and a counterpart entity	12
Annex C (informative) Security applications — Use cases	13
Bibliography	21

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 1¹⁾: *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 3²⁾: *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