

# ISO/IEC 22460-2:2024-04 (E)

## Cards and security devices for personal identification - ISO UAS license and drone/UAS security module - Part 2: Drone/UAS security module

---

<b>Contents</b>		<b>Page</b>
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