Air Traffic Management - Information security for organisations supporting civil aviation operations

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 16495:2014 sisaldab Euroopa standardi EN 16495:2014 inglisekeelset teksti.	This Estonian standard EVS-EN 16495:2014 consists of the English text of the European standard EN 16495:2014.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 22.01.2014.	Date of Availability of the European standard is 22.01.2014.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 03.220.50, 35.040

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16495

January 2014

ICS 03.220.50; 35.040

English Version

Air Traffic Management - Information security for organisations supporting civil aviation operations

Gestion du trafic aérien - Sécurité de l'information pour les organismes assurant le soutien des opérations de l'aviation civile

Flugverkehrsmanagement - Informationssicherheit für Organisationen im Bereich der Zivilluftfahrt

This European Standard was approved by CEN on 9 November 2013.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 16495:2014 E

Contents

Page

Foreword 4

1 Scope 5

2 Normative references 5

3 Terms and definitions 5

4 Information security management in aviation 5
4.1 Structure of this European Standard 5
4.2 Information security management systems in aviation 6
4.3 Assessment of information security risks 6
4.4 Selecting controls 10
4.5 Levels of trust 10
4.6 Statement of applicability 12
4.7 Measurement and auditing of security 12

5 Security policy 12
5.1 Information security policy 12

6 Organisational security 13
6.1 Internal organisation 13
6.2 External parties 14

7 Asset management 15
7.1 Responsibility for assets 15
7.2 Information classification 15

8 Human resources security 16
8.1 Prior to employment 16
8.2 During employment 17
8.3 Termination or change of employment 17

9 Physical and environmental security 18
9.1 Secure areas 18
9.2 Equipment security 18

10 Communications and operations management 19
10.1 Operational procedures and responsibilities 19
10.2 Third party service delivery management 19
10.3 System planning and acceptance 20
10.4 Protection against malicious and mobile code 20
10.5 Back-up 20
10.6 Network security management 21
10.7 Media handling 21
10.8 Exchange of information 21
10.9 Electronic commerce services 22
10.10 Monitoring 22

11 Access control 23
11.1 Business requirement for access control 23
11.2 User access management 23
11.3 User responsibilities 25
11.4 Network access control 25
11.5 Operating system access control 26
11.6 Application and information access control 27
11.7 Mobile computing and teleworking 27

12 Information systems acquisition, development and maintenance 28
12.1 Security requirements of information systems 28
12.2 Correct processing in applications 28
12.3 Cryptographic controls 30
12.4 Security of system files 31
12.5 Security in development and support processes 31
12.6 Technical Vulnerability Management 31

13 Information security incident management 33
13.1 Reporting information security events and weaknesses 33
13.2 Management of information security incidents and improvements 34

14 Business continuity management 34
14.1 Information security aspects of business continuity management 34

15 Compliance 36
15.1 Compliance with legal requirements 36
15.2 Compliance with security policies and standards, and technical compliance 37
15.3 Information systems audit considerations 37

Annex A (informative) **Implementation examples 38**

A.1 General 38

A.2 Security of information in web applications and web services (LoT-A-WEB) 39
A.2.1 General 39
A.2.2 Parameters for the Level of Trust of a web application / web service 39
A.2.3 Determination of the web application / the web service (LoT-A-WEB) 39
A.2.4 Consequences 40

A.3 Connections between multiple organisations /external connections (LoT-A-NET) 40
A.3.1 Determination of the necessary protection controls 40
A.3.2 Effects of the coupling of networks 46

A.4 Certificates / Public Key Infrastructure (LoT-A-PKI) 47
A.4.1 Parameters for the Level of Trust of the certificate management 47
A.4.2 Determination of the Level of Trust of the certificate management (LoT-A-PKI) 47
A.4.3 Effects: Recognition of Certificates / PK 47

A.5 Identity Management (LoT-A-IDM) 48
A.5.1 Parameters for the Level of Trust of Identity Management 48
A.5.2 Determination of the Level of Trust of the Identity Management (LoT-A-IDM) 48
A.5.3 Effects: Recognition of identities 49

Annex B (informative) **Level of Trust – Implementation Example 50**

Bibliography 60

Foreword

This document (EN 16495:2014) has been prepared by Technical Committee CEN/TC 377 “Air Traffic Management”, the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by July 2014, and conflicting national standards shall be withdrawn at the latest by July 2014.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

1 Scope

This European Standard defines guidelines and general principles for the implementation of an information security management system in organisations supporting civil aviation operations.

Not included are activities of the organisations that do not have any impact on the security of civil aviation operations like for example airport retail and service business and corporate real estate management.

For the purpose of this European Standard, Air Traffic management is seen as functional expression covering responsibilities of all partners of the air traffic value chain. This includes but is not limited to airspace users, airports and air navigation service providers.

The basis of all requirements in this European Standard is trust and cooperation between the parties involved in Air Traffic Management.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000:2012, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security controls*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000:2012 and the following apply.

3.1
Air Traffic Management
aggregation of the airborne and ground-based functions (air traffic services, airspace management and air traffic flow management) required to ensure the safe and efficient movement of aircraft during all phases of operations

3.2
trust
situation where one party is willing to rely on the actions of another party

Note 1 to entry: Trust is more than what can be achieved by assurance. However, assurance represents a supporting instrument to trust building.

4 Information security management in aviation

4.1 Structure of this European Standard

This European Standard is structured in line with ISO/IEC 27002. ISO/IEC 27002 is merely referenced in all cases in which its measures can be applied without being amended or supplemented.

In all cases in which the implementation of ISO/IEC 27002 measures requires supplementation specific to aviation, this has been integrated directly in the respective section.