



The European Organisation for Civil Aviation Equipment
L'Organisation Européenne pour l'Équipement de l'Aviation Civile

INFORMATION SECURITY GUIDANCE FOR CONTINUING AIRWORTHINESS

This document is the exclusive intellectual and commercial property of EUROCAE.

It is presently commercialized by EUROCAE.

This electronic copy is delivered to your company/organization for internal use exclusively.

In no case it may be re-sold, or hired, lent or exchanged outside your company.

ED-204

June 2014

INFORMATION SECURITY GUIDANCE FOR CONTINUING AIRWORTHINESS

This document is the exclusive intellectual and commercial property of EUROCAE.

It is presently commercialized by EUROCAE.

This electronic copy is delivered to your company/organization for internal use exclusively.

In no case it may be re-sold, or hired, lent or exchanged outside your company.

ED-204

June 2014

FOREWORD

1. This document was prepared jointly by EUROCAE Working Group 72 “Aeronautical System Security” and RTCA Special Committee 216 “Aeronautical System Security” and was approved by the Council of EUROCAE on 16 June 2014.
2. EUROCAE is an international non-profit making organization in Europe. Membership is open to manufacturers and users of equipment for aeronautics, trade associations, national civil aviation administrations, and, under certain conditions, non-European organizations. Its work program is principally directed to the preparation of performance specifications and guidance documents for civil aviation equipment, for adoption and use at European and world-wide levels.
3. The findings of EUROCAE are resolved after discussion amongst Members of EUROCAE and in collaboration with RTCA Inc, Washington D.C., and/or the Society of Automotive Engineers (SAE), Warrendale PA, U.S.A., through their appropriate committees.
4. This document is technically identical to RTCA DO-355.
5. EUROCAE performance specifications and other documents are recommendations only. EUROCAE is not an official body of the European Governments. Its recommendations are valid as statements of official policy only when adopted by a particular government or conference of governments.
6. Copies of this document may be obtained from:

EUROCAE
102, rue Etienne Dolet
92240 MALAKOFF
France

Telephone: 33 1 40 92 79 30

Fax: 33 1 46 55 62 65

Email: eurocae@eurocae.net

Website: www.eurocae.net

TABLE OF CONTENTS

FOREWORD	I
TABLE OF CONTENTS.....	II
LIST OF FIGURES.....	V
CHAPTER 1 INTRODUCTION	1
1.1 PURPOSE	1
1.2 SCOPE	2
1.3 HOW TO USE THIS DOCUMENT	3
1.4 CONVENTIONS OF THIS DOCUMENT.....	3
1.5 RELATIONSHIP TO OTHER DOCUMENTS	3
1.6 GENERAL CONSIDERATIONS	4
1.6.1 Design Approval Holder (DAH)	4
1.6.2 Instructions for Continued Airworthiness (ICA)	4
1.6.3 Master Minimum Equipment List (MMEL)	5
1.6.4 Contracted Maintenance and Service Providers	5
CHAPTER 2 AIRBORNE SOFTWARE	6
2.1 GENERAL	6
2.2 OPERATIONAL SECURITY MEASURES	7
2.2.1 Reception	7
2.2.2 Creation/Modification	8
2.2.3 Storage	8
2.2.4 Media	8
2.2.5 Software Tools.....	8
2.2.6 Software Distribution	9
2.2.7 Data Loading	9
2.2.8 Confidentiality	9
2.2.9 Incident Managment	9
2.3 DAH RESPONSIBILITIES	9
2.4 OPERATOR RESPONSIBILITIES.....	10
CHAPTER 3 AIRCRAFT COMPONENTS.....	11
3.1 GENERAL	11
3.2 OPERATIONAL SECURITY MEASURES	11
3.2.1 Storage	11
3.2.2 Transport	11
3.2.3 Repair	11
3.2.4 Tools.....	11
3.2.5 Decommissioning	11
3.2.6 Incident Managment	11
3.3 DAH RESPONSIBILITIES	12
3.4 OPERATOR RESPONSIBILITIES.....	12

CHAPTER 4	AIRCRAFT NETWORK ACCESS POINTS	13
4.1	GENERAL	13
4.2	OPERATIONAL SECURITY MEASURES	13
4.3	DAH RESPONSIBILITIES	13
4.4	OPERATOR RESPONSIBILITIES.....	14
CHAPTER 5	GROUND SUPPORT EQUIPMENT (GSE).....	15
5.1	GENERAL	15
5.2	OPERATIONAL SECURITY MEASURES	15
5.2.1	Equipment Security and Operations Management	15
5.2.2	Access Control	16
5.2.3	Usage	16
5.2.4	Storage	16
5.2.5	Incident Management.....	17
5.3	DAH RESPONSIBILITIES	17
5.4	OPERATOR RESPONSIBILITIES.....	17
CHAPTER 6	GROUND SUPPORT INFORMATION SYSTEMS.....	18
6.1	GENERAL	18
6.2	OPERATIONAL SECURITY MEASURES	18
6.2.1	Connection	18
6.2.2	Access Control	18
6.2.3	Data Exchange	19
6.2.4	System Hardening Of Ground Support Information Systems	19
6.2.5	Repair	19
6.2.6	Decommissioning	19
6.2.7	Vulnerability Management.....	19
6.2.8	Incident Managment.....	19
6.3	DAH RESPONSIBILITIES	19
6.4	OPERATOR RESPONSIBILITIES.....	20
CHAPTER 7	DIGITAL CERTIFICATES	21
7.1	GENERAL	21
7.2	OPERATIONAL SECURITY MEASURES	21
7.3	DAH RESPONSIBILITIES	22
7.4	OPERATOR RESPONSIBILITIES.....	22

CHAPTER 8	AIRCRAFT INFORMATION SECURITY INCIDENT MANAGEMENT	23
8.1	GENERAL	23
8.2	OPERATIONAL SECURITY MEASURES	24
8.2.1	Plan And Prepare	25
8.2.2	Monitoring And Detection	25
8.2.3	Reporting	26
8.2.4	Analysis	26
8.2.5	Response	26
8.2.6	Lessons Learned	26
8.3	DAH RESPONSIBILITIES	27
8.4	OPERATOR RESPONSIBILITIES	27
CHAPTER 9	OPERATOR AIRCRAFT INFORMATION SECURITY PROGRAM	28
9.1	GENERAL	28
9.1.1	AISP Relation to ISMS	28
9.1.2	AISP Relation to Security Management System	29
9.2	OPERATIONAL SECURITY MEASURES	30
9.3	DAH RESPONSIBILITIES	30
9.4	OPERATOR RESPONSIBILITIES	30
CHAPTER 10	OPERATOR ORGANIZATION RISK ASSESSMENT	31
10.1	GENERAL	31
10.2	OPERATIONAL SECURITY MEASURES	31
10.3	DAH RESPONSIBILITIES	31
10.4	OPERATOR RESPONSIBILITIES	31
CHAPTER 11	OPERATOR PERSONNEL ROLES AND RESPONSIBILITIES	33
11.1	GENERAL	33
11.2	OPERATIONAL SECURITY MEASURES	33
11.2.1	Skills Required For Operator Information Security Management	33
11.2.2	Aircraft Information Security Specialist	33
11.2.3	Specific Task Skills	34
11.3	DAH RESPONSIBILITIES	34
11.4	OPERATOR RESPONSIBILITIES	35
11.4.1	General	35
11.4.2	Aircraft Information Security Center	35

CHAPTER 12	OPERATOR PERSONNEL TRAINING.....	36
12.1	GENERAL	36
12.2	OPERATIONAL SECURITY MEASURES	36
12.2.1	Training, Awareness, And Competence	36
12.2.2	Education And Certification	36
12.3	DAH RESPONSIBILITIES	36
12.4	OPERATOR RESPONSIBILITIES	36
12.4.1	Training Organization	36
12.4.2	Scope Of Training (General And Specific)	37
12.4.3	General Training.....	37
12.4.4	Specific Training	39
12.4.5	Training Records	40
12.4.6	Regulatory Requirements For Operator Training	41
12.4.7	Recurrent Training	41
12.4.8	Organizational Communication Regarding Aircraft Information Security	41
APPENDIX A	WG-72 / SC-216 MEMBERSHIP	42
APPENDIX B	GLOSSARY OF TERMS.....	47
APPENDIX C	ACRONYMS.....	51
APPENDIX D	REFERENCES.....	53
APPENDIX E	IMPROVEMENT SUGGESTION FORM	55

LIST OF FIGURES

FIGURE 1 – AIRCRAFT INFORMATION SECURITY GUIDANCE	2
FIGURE 2 – TERMS FOR AIRCRAFT SECURITY INCIDENT MANAGEMENT	24

CHAPTER 1

INTRODUCTION

This document is a joint product of two industry committees: the EUROCAE Working Group WG-72, titled "Aeronautical Systems Security" and the RTCA Special Committee SC-216, also titled "Aeronautical Systems Security". WG-72 was formed to address information security and the overall Aeronautical Information System Security (AISS) of airborne systems in conjunction with related ground systems and environment, while SC-216 was formed more specifically to address information security for certification and operation of aircraft and its systems. Both committees agreed that the guidance provided by this document and its companion documents constitute an acceptable means to address the increasing potential of information security threats against aircraft information systems.

This document provides guidance for the operation and maintenance of aircraft and for organizations and personnel involved in these tasks. It shall support the responsibilities of the Design Approval Holder (DAH) to obtain a valid airworthiness certificate and aircraft operators to maintain their aircraft to demonstrate that the effects on the safety of the aircraft of information security threats are confined within acceptable levels. As all information security threats may have an intentional origin, this document also covers electronic sabotage (as used in AMC 25.1309).

1.1

PURPOSE

This document is a resource for civil aviation authorities and the aviation industry when the operation and maintenance of aircraft and the effects of information security threats can affect aircraft safety. It deals with the activities that need to be performed in operation and maintenance of the aircraft related to information security threats.

This document gives also guidance that is related to operational and commercial effects (i.e. guidance that exceeds the safety-only effects). Thus, it also supports harmonizing security guidance documents among Design Approval Holders (DAH), which is deemed beneficial to DAHs, operators and civil aviation authorities.

ED-204 / DO-355 is a companion document¹ to ED-202A / DO-326A "Airworthiness Security Process Specification" that supports security in the development and modification part of the airworthiness process.

NOTE: *This document was developed in the European context of the European Aviation Safety Agency (EASA) Certification Specification CS-25 "Large Aeroplanes" and the American context of Title 14 Code of Federal Regulations (14CFR) Part 25 "Transport Category Aircraft". Tailoring of this guidance may be used in other regulatory contexts including but not limited to JAA JAR 25, CS-23, CS-27, CS-29, CS-E, Part 23, Part 27, Part 29, and Part 33.*

The most comprehensive possible area of the application of this guidance is deemed to be Large Transport Aircraft programs. However, this document does not make any assumptions about and is without prejudice to its applicability.

NOTE: *The measures proposed in this document are subject to commercial terms between DAH and operators. Especially for the service and support related topics mentioned in this document, it is up to the DAHs to integrate them in their commercial offers.*

¹ This document is also intended to be a companion to other documents being produced by EUROCAE WG-72 and RTCA SC-216 relating to Aeronautical Information System Security that were under development by the time this document was issued.

1.2

SCOPE

ED-202A / DO-326A provides guidance in addressing airworthiness security during the aircraft product life cycle from project initiation until the aircraft Type Certificate (Amended Type Certificate, Supplemental Type Certificate and Amended Supplemental Type Certificate) is issued for the aircraft type design. In addition, it includes the handover of information about the Type Design that is necessary to ensure continuing airworthiness with respect to possible information security threats.

ED-204 / DO-355 (this document) provides guidance for the following stages of the product life cycle: operation, support, maintenance, administration and deconstruction.

Where an organization subcontracts any activities in these stages, the organization still retains the responsibility for aircraft information security (for contracted maintenance providers, refer to section 1.6.4).

Topics in the scope of Type Certification activities that are related to operation and maintenance of the aircraft such as Instructions for Continued Airworthiness (ICA) and security guidance documents are introduced in ED-202A / DO-326A and detailed in ED-204 / DO-355. In such cases ED-202A / DO-326A provides references to ED-204 / DO-355.

This document addresses information security risks only. The security measures to mitigate these risks are not limited to information technology; they may also be physical or organizational.

Apart from the classical Instructions for Continued Airworthiness that are directly related to aircraft parts and systems, this document also provides guidance on Ground Support Equipment and Ground Support Information Systems that are related to the security of aircraft information systems and data networks as illustrated in FIGURE 1.

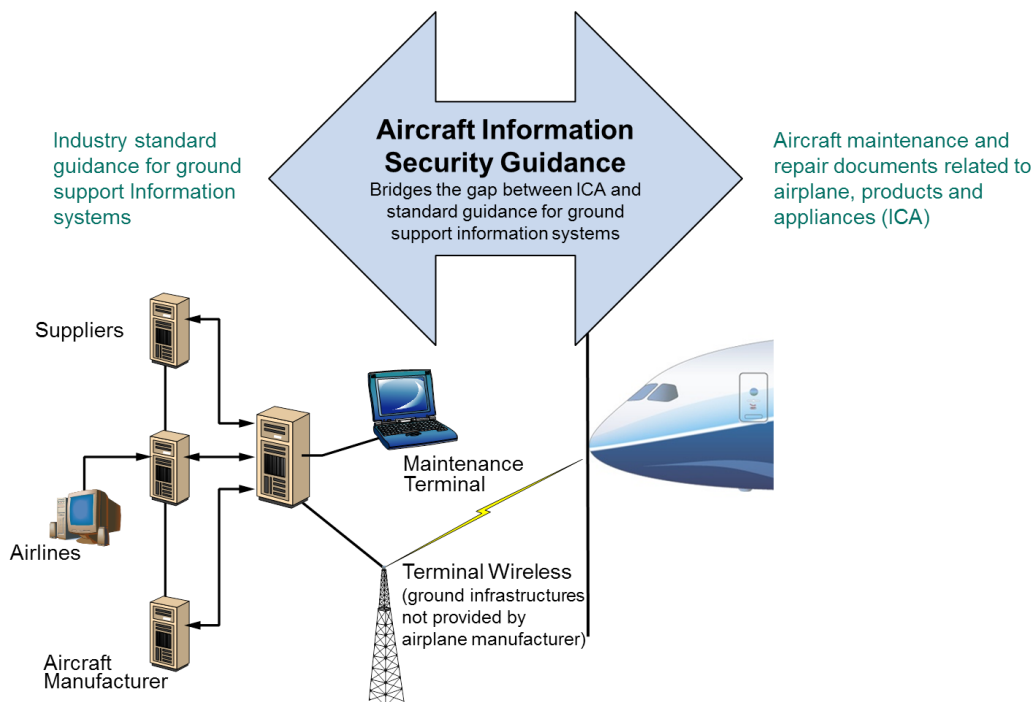


FIGURE 1: AIRCRAFT INFORMATION SECURITY GUIDANCE

NOTE: *The material in subsequent sections is only applicable if the aircraft and the operator use the features described.*

1.3 HOW TO USE THIS DOCUMENT

This document is organized in 12 chapters plus informative appendices.

- Chapter 1 introduces the document.

The remainder of this document is organized into the following chapters and appendices. The substructure of these chapters is harmonized as follows:

- Chapter X.1 gives **General** information to introduce and define the topic
- Chapter X.2 gives an overview of what **Operational Security Measures** can be taken to manage the topic
- Chapter X.3 lists the **Design Approval Holder (DAH) Responsibilities**
- Chapter X.4 lists the **Operator Responsibilities**

The following topics are addressed:

- Chapter 2 Airborne Software
- Chapter 3 Aircraft Components
- Chapter 4 Aircraft Network Access Points
- Chapter 5 Ground Support Equipment
- Chapter 6 Ground Support Information Systems
- Chapter 7 Digital Certificates
- Chapter 8 Aircraft Information Security Incident Management
- Chapter 9 Operator Aircraft Information Security Program
- Chapter 10 Operator Organization Risk Assessment
- Chapter 11 Operator Personnel Roles and Responsibilities
- Chapter 12 Operator Personnel Training
- Appendix A lists all members of the working groups that have been involved during the creation of this document.
- Appendix B contains an informal Glossary of Terms.
- Appendix C contains a list of acronyms.
- Appendix D contains a list of cited and relevant documents. This list is neither exhaustive nor does it characterize any of the documents therein to be applicable. However, these documents constitute a solid starting point when addressing the subject matter.
- Appendix E contains the improvement suggestion form.

1.4 CONVENTIONS OF THIS DOCUMENT

Within this document, “must” is used for requirements, “should” is used for recommendations, “may” and “need not” are used for permission, “can” and “might not” are used for possibility, and “cannot” is used for impossibility. Other terms that are not defined in APPENDIX B are intended to have their common dictionary meaning.

1.5 RELATIONSHIP TO OTHER DOCUMENTS

Any mention of other documents is for information only. Thus, it is expected that the cited documents are often used in the development and airworthiness certification of aircraft. A list of cited documents can be found in APPENDIX D.

1.6 GENERAL CONSIDERATIONS

1.6.1 Design Approval Holder (DAH)

A Design Approval Holder (DAH) is the holder of a type certificate, a Parts Manufacturer Approval (PMA) or a Technical Standard Order (TSO) authorization or the licensee of a Type Certificate (TC).

NOTE: *References to a type certificate includes supplemental type certificates unless noted otherwise. All design approval holders must:*

- *Report failures, malfunctions, and defects*
- *Make Instruction for Continued Airworthiness (including changes) available to each aircraft, aircraft engine or propeller owner*
- *Satisfy Additional Obligations for: Parts Manufacturer Approval Holder, Technical Standard Order.*

1.6.2 Instructions for Continued Airworthiness (ICA)

Instructions for Continued Airworthiness are the instructions and information that are necessary for the continued airworthiness of the aircraft, engine, propeller, parts and appliances, which must be developed and/or referenced by the Design Approval Holder in accordance with the applicable Certification Basis or Standard.

ICAs are not limited to the maintenance of the aircraft; they can also be operational instructions.

Specifically for maintenance, the regulatory requirements for “Instructions for Continued Airworthiness Responsibilities, Requirements, and Contents” can be found in documents provided by civil aviation regulatory systems. For example:

- EASA
 - EU 748/2012
 - Part 21, Section A
 - CS 25.1529 Instructions for Continued Airworthiness
 - CS 25, Book 1, Appendix H
- FAA
 - 14 CFR Part 25.1529
 - 14 CFR Part 25 Appendix H (25.1529 directs the reader to Appendix H)
 - 14 CFR Part 21.50
- TCCA
 - CAR 521.368 Instructions for Continuing Airworthiness
 - AWM Chapter 525.1529 Instructions for Continuing Airworthiness
 - AWM Chapter 525.1529 Appendix H

The term “Instructions for Continued Airworthiness” is defined and used in a very specific way within the applicable civil aviation regulatory systems. For the definition of the term ICA, refer to the glossary. Design Approval Holders negotiate the specific content of ICA packages with the regulatory authorities. For example within the FAA system, some ICA documents are approved by the Aircraft Certification Office, but all are submitted to the FAA Aircraft Evaluation Group for acceptance or approval prior to delivery of each aircraft to an operator.

The clear intent of ICA is to provide instructions for maintenance of the aircraft, to ensure that those instructions are available within the operator’s system and to ensure that the instructions are used by technicians who maintain the operator’s aircraft.

NOTE: *Whenever DAH applicants use commercial parts they should refer to the guidance in FAA AC 21-45 para.5.B Commercial Parts to satisfy the regulatory requirements of 14 CFR part 21 section 21.50c.*

1.6.2.1 ICA Related to Aircraft Information Security

ICA are written to allow maintenance technicians to perform their aircraft maintenance tasks and direct them to raise items of security concern to the appropriate area of the operator's organization. It is assumed that personnel implementing ICA are not information technology (IT) security specialists.

In addition to ICA, operators may also have extensive processes, tools, facilities and information technology systems that support aircraft maintenance. As shown in FIGURE 1, DAHs provide additional non-ICA guidance to support the security of Ground Support Equipment and Ground Support Information Systems whenever they contribute to information security of the aircraft.

1.6.2.2 Differences Between ICA and Non-ICA

To summarize the difference between ICA and non-ICA:

- ICA
 - Any required maintenance activity on the aircraft should be covered by an ICA
 - Affecting airworthiness and safety
 - ICA provide documentation of methods, inspections, processes, and procedures.
 - ICA Examples: Aircraft Maintenance Manual (AMM), Maintenance Review Board Report (MRBR), Fault Isolation Manual (FIM), Trouble Shooting Manual (TSM), Illustrated Parts Catalogue (IPC), Airworthiness Limitation Section (ALS).
 - ICA are required to maintain the continued airworthiness of the aircraft
- Non-ICA
 - Aircraft or ground operations related: Affecting operation (availability, commercial aspects).
 - Off-aircraft maintenance (e.g. Shop Maintenance) is not necessarily covered by ICA.
 - Non-ICA are recommended, but not required to maintain the continuous airworthiness of the aircraft.

1.6.3 **Master Minimum Equipment List (MMEL)**

The Master Minimum Equipment List (MMEL) is a list of aircraft instrument and equipment items which may be inoperative under certain operational conditions while maintaining the airworthiness of the aircraft along with an equivalent level of safety. It contains the conditions, limitations and procedures required for operating the aircraft with these items inoperative. This MMEL is used by the operator to create their customised MEL (Minimum Equipment List) applicable to each particular aircraft, which has to be approved by the competent authority.

If aircraft equipment is rendered inoperative due to failure, the MEL needs to be checked for dispatch. This also applies if aircraft equipment is inoperative due to an aircraft information security issue.

If Ground Support Equipment or Ground Support Information Systems contribute to safety, they shall be addressed by other documents to be agreed on with applicable civil aviation authorities.

1.6.4 **Contracted Maintenance and Service Providers**

Whenever there is an arrangement between an operator and a third party such as a Maintenance Repair and Overhaul organization (MRO) or an IT service provider, it is the responsibility of the operator to ensure that this third party complies with the operator's aircraft information security requirements.

CHAPTER 2

AIRBORNE SOFTWARE

2.1 GENERAL

The objective of this section is to give guidance to ensure the authenticity and integrity of Airborne Software is maintained during its reception, creation, modification, storage and distribution on the ground. Confidentiality and availability aspects are also considered if specifically required.

The creation of Supplier Controlled Software (SCS) is out of the scope of this document (it is covered as part of the TC, ATC, STC or TSO).

The term airborne software as used in this document encompasses Aircraft Controlled Software (ACS, equivalent to Field Loadable Software (FLS)) and Hardware Controlled Software (HCS).

New generation aircraft come with a large number of airborne software parts with most of them delivered in an electronic form. Operators use software tools to verify the integrity and authenticity of airborne software. Operators can deliver the software to the aircraft through several connectivity means (e.g. wired, wireless, USB-key). Operators should ensure that the airborne software delivered to the aircraft is authorized while maintaining its integrity and authenticity.

For legacy aircraft the number of airborne software parts may be lower and the variety of connectivity means may be less, nevertheless integrity and authenticity needs to be ensured as well.

Regardless of the aircraft type, operators are in transition from media-based airborne software distribution that depends on physical security measures to electronic airborne software distribution. The electronic distribution of software requires ground systems and processes that support information security.

Electronic airborne software distribution or Electronic Distribution of Software (EDS) is the process of moving software and data from one location to another location without the use of portable electronic media such as magnetic disks, optical disks, or flash drives. This classification of software distribution can make use of any data connectivity model such as wide area networks, local area networks, proprietary networks, and direct links. The connectivity method used within these models can be wired or wireless.

A common security methodology for electronic airborne software distribution is as follows.

- For electronic software distribution, security is implemented by using a means of attaching one or more cryptographic signatures to the files that use a public/private key encryption method. If required, the entire software data payload may be encrypted using a public/private key method.
- Before sending a software package, a cryptographic signature that can only be created by the sender using their private key is attached. The signature is created using the contents of software, the sender's identification information, and other related information. The recipient has the public key required to verify that the software data came from the identified sender and that nothing in the data has been altered in any way.
- Additionally, if the software needs to be encrypted, so only the recipient can interpret and use the software, then the sender uses a sender key to encrypt or conceal the software package data. Only the intended recipient with the receiver private key may decrypt and use the data. In order to ensure sender authentication as part of the encrypted distribution process, the sender key must be kept private and secure also.

Refer to ARINC 667-1 and ARINC 827 for specific information regarding electronic distribution of airborne software.

Refer to CHAPTER 7 for specific information regarding public/private keys and the handling and management of digital certificates.

Media-based airborne software distribution uses portable electronic media. Media such as magnetic and optical disks containing software and data are required to have a physical label attached that indicates the content information of the media.

A common security methodology for distribution of software stored on portable physical media is as follows.

- For media-based distribution, physical security is implemented by having trusted people in a physically secure environment with proper credentials prepare, label, package, and send physical media to the intended recipient.
- The media is received at the intended recipient location, checked, and processed by trusted people with proper credentials in a physically secure environment.

Refer to ARINC 667-1 for specific information regarding physical distribution of airborne software.

NOTE: *This section addresses on-aircraft loading as well as shop loading.*

Related ARINC documents are:

- *ARINC 667-1 Guidance for the Management of Field Loadable Software can provide guidance for handling of field loadable software (terms used in this section comply with ARINC 667-1). However, it does not cover the security of field loadable software and data.*
- *ARINC 827 Electronic Distribution of Software by Crate (EDS Crate) defines the industry standard method to be applied for electronic distribution of software.*
- *ARINC 835 Guidance for Security of Loadable Software Parts Using Digital Signatures.*

Airborne software distribution is a different process from data loading. Transferring airborne software from one location to another is software distribution. A location for distribution may include an onboard aircraft mass storage device (MSD) that is used to store software that may be loaded later. Moving airborne software into the actual onboard aircraft system components, other than a MSD, is data loading.

2.2 OPERATIONAL SECURITY MEASURES

The following subsections give an overview of what operational security measures can be taken for secure handling and managing of airborne software on the ground.

2.2.1 Reception

- Verify the authenticity and integrity of the software upon receiving. This can be done by verifying a digital signature, comparable methods, or a combination of measures to be agreed upon with the sender (aircraft manufacturer, supplier, etc.), using software tools that conform to the sender's specification.

NOTE: *A comparable method could be the usage of a sealed envelope in combination with a physical media.*

- Define actions to take when software reception is invalid or fails authentication. This would include notification to the software provider to resend the software or data. Also include actions to take for inter-company distribution and reception authentication failures).

NOTE: *Resolve any issues with receipt of loadable software when it is received, not when it is needed.*

2.2.2 Creation/Modification

- Develop a secure process and environment (personnel, tools and infrastructure) for creating and modifying User Modifiable Software (UMS) and User Certifiable Software (UCS).

2.2.3 Storage

- During storage of airborne software on the ground, implement physical, logical and organizational measures sufficient to prevent and detect unauthorized access in order to protect the integrity of the software (e.g. usage of digital signatures, locked rooms, passwords, defined roles and responsibilities, badges).
- Ensure procedures address the full life cycle of the physical storage device (e.g. aircraft server, maintenance laptop, data loader, development computer) and the airborne software stored on it.
- Address digital certificate expiration issues that might occur during storage

NOTE: *Depending on the way airborne software is packaged (e.g. with digital signatures) there may be no requirements on the storage. For additional guidance, refer to CHAPTER 6.*

2.2.4 Media

- If airborne software is stored on media:
 - Ensure that the media is free of malicious code before airborne software is stored on it.
 - Ensure that the media is protected from malicious code during its lifecycle.
 - Ensure that the airborne software maintains its integrity.
 - Consider various types of media available and the possible use restrictions and life cycle associated with each type and the possibilities of commercially installed software products (e.g. read-only media or USB mass storage devices with preinstalled applications).
 - Ensure that the media is appropriately labeled (e.g. part number, version, date).

NOTE: *Depending on the selected media type, be aware that each media type bears different risks and vulnerabilities that should be considered (e.g. USB mass storage device compared to read-only CD-ROM).*

2.2.5 Software Tools

- Use software tools for the purpose of ensuring the authenticity and integrity of airborne software as specified by the software supplier or DAH.
- These software tools include applications that run on equipment related to airborne software distribution and storage such as Portable Data Loaders (PDL's), office desktops, servers and maintenance laptops.
- Equipment running software tools should be kept secure and free of unauthorized code. The configuration of this equipment should also be controlled.
- Ensure software tools are not used for any other purpose or in any other way than that specified by the DAH or the software supplier.

NOTE: *For additional guidance, refer to CHAPTER 5 and CHAPTER 6.*

2.2.6 Software Distribution

- Perform transfer of airborne software only by personnel who are authorized by the operator to access, manage, and store software.

Examples of transfer within organizations:

- Software Vault to Data Loader, Data Loader to Aircraft, and Vault to Aircraft Mass Storage.

Examples of transfer between organizations:

- DAH to operator, suppliers/vendors to operator or operator to MRO.

- Ensure the integrity and authenticity of airborne software during transfer, both physical and logical, between entities (e.g. flight ops, engineering, aircraft, airport, shop).
- Implement a chain of custody for transporting airborne software (record keeping) to detect security events.

NOTE: *Airborne Software can be distributed on portable physical media or by electronic distribution. For additional guidance, refer to CHAPTER 6*

2.2.7 Data Loading

- Ensure that the authenticity and integrity of airborne software is verified and remains secure before data loading (e.g. after staging the software on the aircraft or in the shop).
 - Ensure that airborne software is loaded as per ICA or other applicable documentation such as Component Maintenance Manual (CMM) or Service Bulletin

2.2.8 Confidentiality

- Where required, ensure that confidentiality (e.g. of private keys for digital certificates) is maintained during the whole life-cycle of the airborne software (including decommissioning).

NOTE: *Unauthorized disclosure of airborne software could enable reverse engineering. So if airborne software is distributed over open networks like the internet, encryption techniques such as https should be used.*

2.2.9 Incident Management

- Report and investigate security issues (breaches and weaknesses) so safety impacts can be properly understood and security can be improved in the future. Refer to CHAPTER 8.

2.3 DAH Responsibilities

The DAH should provide guidance to the operators to establish policies and associated procedures for the handling and managing of airborne software.

The guidance should be based on

- The information security requirements that have been identified by the DAH through a process as specified in ED-202A / DO-326A
- The operational security measures listed above (in section 2.2)
- Applicable civil aviation regulations.

NOTE: *There may not be one solution that covers all cases. The level of guidance provided will vary depending on the capability, implementation type and complexity of the aircraft and the software tools.*

2.4 OPERATOR RESPONSIBILITIES

The operator should document and implement policies and procedures for handling and managing of airborne software regarding information security.

The policies and procedures should be based on:

- The operational security measures listed above (in section 2.2)
- The guidance provided by the DAH²
- Applicable civil aviation regulations
- The operational environment.

² Such as the Boeing Airplane Network Security Operator Guidance (ANSOG) or the Airbus Security Handbook

CHAPTER 3

AIRCRAFT COMPONENTS

3.1 GENERAL

Regulatory requirements exist to protect aircraft components during repair and maintenance. However, aircraft information security concerns may not have been fully addressed.

New generation aircraft are equipped with components that may require specific handling during transport, storage, repair and decommissioning, as these components can contain sensitive or confidential information such as private keys and personal data.

This section provides operational security measures to protect these components off-wing from unauthorized access.

3.2 OPERATIONAL SECURITY MEASURES

The following subsections provide an overview of what operational security measures can be taken for secure handling and managing of aircraft components.

3.2.1 Storage

- Ensure secure storage of aircraft components to prevent unauthorized access.

3.2.2 Transport

- Protect aircraft components and component interfaces against physical tampering.
- Verify protection means when the aircraft component enters trusted facilities.
- Use a chain of custody for transporting aircraft components (record keeping).

3.2.3 Repair

- Ensure a secure environment (personnel, tools and infrastructure) for repair of components.
- Ensure isolation from potentially malicious systems and storage media.

3.2.4 Tools

- Use only tools approved/recommended by the DAH or equivalent tools.
- Restrict usage of these tools to the intended purpose only.

3.2.5 Decommissioning

- Ensure that no confidential data such as access key codes and passwords can be recovered from aircraft components by unauthorized personnel.
- Comply with procedures for disposing of aircraft parts by following the Component Maintenance Manual (CMM) or applicable civil aviation regulations.

3.2.6 Incident Management

- Report and investigate security issues (breaches and weaknesses) so safety impacts can be properly understood and security can be improved in the future. Refer to CHAPTER 8.

3.3 DAH RESPONSIBILITIES

There are existing regulatory requirements for aircraft component handling and managing. However, the DAH should identify aircraft components that require specific handling and managing with regards to aircraft information security.

For these components, the DAH should provide guidance to assist operators to establish policies and associated procedures for the secure off-wing handling of these components.

The guidance should be based on:

- The information security requirements that have been identified by the DAH through a process as specified in ED-202A / DO-326A
- The operational security measures listed above (in section 3.2)
- Applicable civil aviation regulations.

3.4 OPERATOR RESPONSIBILITIES

The operator should document and implement policies and procedures for the off-wing handling of aircraft components regarding information security.

The policies and procedures should be based on:

- The operational security measures listed above (in section 3.2)
- The guidance provided by the DAH
- Applicable civil aviation regulations
- The information security aspects of contracts for parts pooling
- The operational environment.