



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

AERONAUTICAL INFORMATION SYSTEM SECURITY GLOSSARY

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

It is presently commercialised by EUROCAE.

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

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

ER-013

December 2015

AERONAUTICAL INFORMATION SYSTEM SECURITY GLOSSARY

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

It is presently commercialised by EUROCAE.

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

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

ER-013

December 2015

FOREWORD

1. This document was prepared by EUROCAE Working Group 72 "Aeronautical Systems Security".
2. EUROCAE is an international non-profit making organisation 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 organisations. Its work programme 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. 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.
4. 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
CHAPTER 1	INTRODUCTION.....	1
CHAPTER 2	DEFINITIONS AND REFERENCES	2
APPENDIX A	WG-72 MEMBERSHIP.....	30
IMPROVEMENT SUGGESTION FORM.....		33

CHAPTER 1

INTRODUCTION

This document is concerned with providing a glossary of terms for Aeronautical Information Systems Security (AISS). This Glossary is primarily intended to provide assistance to the users of the following EUROCAE Documents:

- ED-201 *Aeronautical Information System Security (AISS) Framework Guidance* (2015)
- ED-202A *Airworthiness Security Process Specification* (2014)
- ED-203 *Airworthiness Security Methods and Considerations* (2015)
- ED-204 *Information Security Guidance for Continuing Airworthiness* (2014).

The definitions represent the meanings understood and shared by the Aeronautical Information System Security Community and each Term in the Glossary definitions has a cross reference to the information source.

CHAPTER 2

DEFINITIONS AND REFERENCES

This chapter provides for the Definitions of Terms in Table 1 and for References to non-Eurocae documents, from which definitions have been adopted.

TABLE 1: DEFINITION OF TERMS

Term	Definition	Source
Access Control	Security service that controls the use of resources and the disclosure and modification of data.	NIAP CIM-BRE
Accountability	Property that allows activities in an IT system to be traced to the entity responsible for the activity.	NIAP CIM-BRE
Activity	Tasks that provide a means of meeting the objectives	ED-202
Aeronautical Information System	The <i>set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information</i> involved in all aspects of aircraft operations. Note that this includes supplier's information systems supporting the development of onboard system software and data.	adapted from: Title 44 U.S.C., §3502 (8)
Airborne Software	Airborne software encompasses Aircraft Controlled Software (ACS, equivalent to Field Loadable Software (FLS)) and Hardware Controlled Software (HCS) as defined in ARINC 667-1	Arinc 667-1
Aircraft	An aircraft is a machine that is able to fly by gaining support from the air, or, in general, the atmosphere of a planet. It counters the force of gravity by using either static lift or by using the dynamic lift of an airfoil, or in a few cases the downward thrust from jet engines	ED-204
	Any machine that can derive support in the atmosphere from the reactions of the air other than the reactions of the air against the earth's surface.	ICAO Doc 9713, 2nd Ed., 2001
Aircraft Component	An aircraft component is a component approved for installation on a type-certificated aircraft.	ED-204
	Any self-contained part, combination of parts, subassemblies or units, that perform a distinctive function necessary to the operation of the system.	SAE ARP 4754A, "Component"
Aircraft Domain	see Domain (Aircraft)	

Term	Definition	Source
Aircraft Information Security Center	The Aircraft Information Security Center should act as the operator's point of contact for aircraft information security issues from within and outside the operator's organization.	ED-204
Aircraft Type Certification	The legal recognition that a product, service, organization or person complies with the applicable requirements. Such certification comprises the activity of technically checking the product, service, organization or person, and the formal recognition of compliance with the applicable requirements by issue of a certificate, license, approval or other document as required by national laws and procedures. In particular, certification of a product involves: a. The process of assessing the design of a product to ensure that it complies with a set of standards applicable to that type of product so as to demonstrate an acceptable level of safety. b. The process of assessing an individual product to ensure that it conforms with the certified type design. c. The issue of any certificate required by national laws to declare that compliance or conformity has been found with applicable standards in accordance with paragraph (a) or (b) above.	SAE ARP 4754, "Certification"
	The legal recognition that a product, service, organization or person complies with the applicable requirements. Such certification comprises the activity of technically checking the product, service, organization or person, and the formal recognition of compliance with the applicable requirements by issue of a certificate, license, approval or other document as required by national laws and procedures.	SAE ARP 4754A, "Certification"
Air Gap	<i>An interface between two systems at which they are not connected physically, electrically or electro-magnetically (incl. optically)</i>	inspired by IETF RFC 4949
Air Traffic Management (ATM)	The dynamic, integrated management of air traffic and airspace including air traffic services, airspace management and air traffic flow management — safely, economically and efficiently — through the provision of facilities and seamless services in collaboration with all parties and involving airborne and ground-based functions.	ICAO Doc 4444 15th Ed., 2007
Airworthiness	The condition of an item (aircraft, aircraft system, or part) in which that item operates in a safe manner to accomplish its intended function.	SAE ARP 4754
	The condition of an aircraft, aircraft system, or component in which it operates in a safe manner to accomplish its intended function.	SAE ARP 4754A
Airworthiness Security (AWS)	The protection of the airworthiness of an aircraft and its occupants from the information security threat: harm due to human action (intentional or unintentional) using access, use, disclosure, disruption, modification, or destruction of data and/or data interfaces. This also includes the consequences of malware and forged data and of access of other systems to aircraft systems.	ED-202

Term	Definition	Source
	The protection of the airworthiness of an aircraft from intentional unauthorized electronic interaction: harm due to human action (intentional or unintentional) using access, use, disclosure, disruption, modification, or destruction of data and/or data interfaces. This also includes the consequences of malware and forged data and of access of other systems to aircraft systems.	ED-202A
Anonymity	The condition of an identity being unknown or concealed.	IETF RFC 4949
Anonymous	An application may require security services that maintain anonymity of users or other system entities, perhaps to preserve their privacy or hide them from attack. To hide an entity's real name, an alias may be used. For example, a financial institution may assign an account number. Parties to a transaction can thus remain relatively anonymous, but can also accept the transaction as legitimate. Real names of the parties cannot be easily determined by observers of the transaction, but an authorized third party may be able to map an alias to a real name, such as by presenting the institution with a court order. In other applications, anonymous entities may be completely untraceable.	IETF RFC 2828
Assessment	A systematic evaluation of an aircraft/ aircraft system/ item and its requirements.	SAE ARP 4754
	An evaluation based upon engineering judgment.	SAE ARP 4754A
Asset(s)	Resources of the aircraft and systems which are subject to attack or may be used as part of an attack, including functions, systems, items, equipment, data, interfaces, and information.	ED-202
	The logical and physical resources of the aircraft which contribute to the airworthiness of the aircraft, including functions, systems, items, data, interfaces, processes and information	ED-202A
	What has value to the organization and which therefore requires protection. Note: Assets can have (for example) a financial, operational or intellectual property value.	ISO 27005:2011
Assumptions	Statements, principles, and/or premises offered without proof.	SAE ARP 4754, SAE ARP 4754A
Assurance	The planned and systematic actions necessary to provide adequate confidence that a product or process satisfies given requirements.	ED-12B/DO-178B, ED-12C/DO-178C
Assurance (Information)	See Information Assurance.	

Term	Definition	Source
Attack	An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.	IETF RFC 2828
	An assault on a system that derives from an ... act that is an attempt to violate the security policy of a system. This includes intentional and unintentional acts.	adapted from IETF RFC 2828 "attack"
Attacker	The entity that initiates and directs an attack. This includes intelligent attacker as well the automatic actions of attack code such as a bot or worm, as well as the authors of such code.	ED-202
Attack Path	The path, interface, and actions by which an attacker executes an attack.	ED-202A
Attack Vector	The path, interface, and actions by which an attacker executes an attack.	ED-202
	The means of access which an attacker used to begin an attack	ED-202A
Audit (Security)	See Security Audit.	
Audit Trail (Security)	See Security Audit Trail.	
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.	NIST SP800-53, Feb 2005
Availability	Security usage: Ensuring authorized users have access to information and associated assets when required	ISO 17799
	Safety Usage: Probability that an item is in a functioning state at a given point in time.	SAE ARP 4754
	Safety Usage: Qualitative or quantitative attribute that a system or item is in a functioning state at a given point in time. It is sometimes expressed in terms of the probability of the system (item) not providing its output(s) (i.e. unavailability).	SAE ARP 4754A
Biometrics	An automatic identification process for identity verification of individuals based on unique behavioral or physiological characteristics. These are unique things that we do or unique physical characteristics that we have. Behavioral biometrics include voice, signature, and keyboard typing technique. Physical biometrics include fingerprint, hand geometry, facial recognition, and iris and retinal scan.	GSA GSCH, 2004

Term	Definition	Source
Certificate (Digital)	See Digital Certificate.	
Certificate (Public Key)	See Digital Certificate.	
Certificate Authority (CA)	A component of the Public Key Infrastructure. The CA is responsible for issuing and verifying digital certificates.	GSA GSCH, 2004
	Synonym for “certification authority”. Deprecated Term: IDOCs SHOULD NOT use this term; it suggests careless use of the term “certification authority”, which is preferred in PKI standards (e.g., [X509, R3280])	IETF RFC 4949
Certificate Blacklist (CBL)	A computer file that lists all digital certificates that have the access to certain system or protocol denied.	ED-204
Certificate Revocation List (CRL)	A computer file that contains the list of all digital certificates that is revoked and thus is no longer valid and reliable.	ED-204
	A periodically issued list, digitally signed by a CA, of identified certificates that have been suspended or revoked prior to their expiration dates.	GSA GSCH, 2004
	A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire. (See: certificate expiration, delta CRL, X.509 certificate revocation list.)	IETF RFC 4949
Certification	Aeronautical usage: see Aircraft Type Certification	SAE ARP 4754
	Information system usage: Comprehensive evaluation (usually made in support of an accreditation action) of an information system's technical security features and other safeguards to establish the extent to which the system's design and implementation meet specified security requirements.	IETF RFC 4949

Term	Definition	Source
Common Criteria	“The Common Criteria” is a standard for evaluating information technology products and systems, such as operating systems, computer networks, distributed systems, and applications. It states requirements for security functions and for assurance measures.	IETF RFC 2828
	A standard for evaluating information technology (IT) products and systems. It states requirements for security functions and for assurance measures.	IETF RFC 4949
	The CC permits comparability between the results of independent security evaluations. The CC does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation.	Common Criteria, Part 1, version 3.1, Rev 4
Completeness	<i>Completeness of a requirement statement means that no attributes have been omitted and that those stated are essential.</i> Completeness with respect to another requirement statement means completeness within the scope and attributes of the other statement.	adapted from: SAE ARP 4754
	Completeness is the degree to which a set of correct requirements, when met by a system, satisfy the interests of customers, users, maintainers, certification authorities as well as aircraft, system and item developers under all modes of operation and lifecycle phases for the defined operating environment.	SAE ARP 4754A
Complex System (Aircraft)	A system whose safety cannot be shown solely by test and whose logic is difficult to comprehend without the aid of analytical tools.	adapted from: SAE ARP 4754, Scope
Compromise	Data usage: A security incident in which information is exposed to potential unauthorized access, such that unauthorized disclosure, alteration, or use of the information might have occurred.	IETF RFC 2828 IETF RFC 4949
	Security usage: A security violation in which a system resource is exposed, or is potentially exposed, to unauthorized access.	IETF RFC 2828 IETF RFC 4949
Confidentiality	Ensuring that information is accessible only to those authorized to have access	ISO 17799
	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes	ISO 27000, 2012
Consistent	Consistency between requirements statements means the attributes are in agreement within the scope of the intended purposes. A design specification is consistent with the requirements if neither contradicts the other. A power budget summary is consistent with a design specification if a quantity in the budget that refers to the design specification is equal to the quantity implied by the design specification.	ED-202

Term	Definition	Source
Control (Security)	See Security Control.	
Correctness	Correctness of a requirement statement means the absence of ambiguity or error in its attributes.	SAE ARP 4754
	The degree to which an individual requirement is unambiguous, verifiable, consistent with other requirements and necessary for the requirement set.	SAE ARP 4754A
Crate	Digital container for aircraft software parts and related digital products used for electronic distribution between aerospace business partners.	Arinc 827
Cryptographic Key (Key)	Usually shortened to just “key”. An input parameter that varies the transformation performed by a cryptographic algorithm.	IETF RFC 2828, IETF RFC 4949
Design Approval Holder (DAH)	A design approval holder is the holder of a type certificate, a Parts Manufacturer Approval or a Technical Standard Order authorization or the licensee of a Type Certificate.	FAA
Data	Physical phenomena chosen by convention to represent certain aspects of our conceptual and real world.	Hansen, 1973
Data distribution	The ground based process of moving airborne software and data from a source location to a destination location and the process of storing software and data at each location. Examples of source and destination locations are software vaults, airborne software servers, Aircraft on-board mass storage, and OEM software distribution systems.	ED-204
Data Loading	The process of moving airborne software and data from a storage source into the active executable memory of aircraft systems. Examples of storage sources are aircraft on-board mass storage, Portable Data Loader (PDL) mass storage or media, Aircraft Data Loader (ADL) mass storage or media, and software vault servers.	ED-204
Defense in Depth	An architectural feature in which a security function is accomplished by more than one countermeasure such that an attack would require vulnerabilities in multiple countermeasures.	ED-202
	An architectural strategy in which more than one security measure is used such that a successful attack would require vulnerabilities in multiple security measures.	ED-204
Dependent System	An aircraft system that depends on an external system for correct function.	ED-202