

ER-013A

AERONAUTICAL INFORMATION SYSTEM SECURITY GLOSSARY

LEGAL NOTICE

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, hired, lent or exchanged outside your company. It may not be reproduced, in whole or in parts, without prior written permission by EUROCAE.

06/2021

FOREWORD

1. This document was developed jointly by EUROCAE Working Group 72 “Aeronautical Systems Security” and RTCA SC-216 “Aeronautical Systems Security” and approved on 11 June 2021.
2. This document supersedes ER-013 Aeronautical Information System Security Glossary (2015).

ER-013A reflects the updates of definitions in current and future WG-72 ED documents that have been approved after going through open consultation. As each ED document is published, ER-013 will be updated to reflect the current definitions of the ED documents.
3. This document is technically identical to RTCA Paper No. 120-21/PMC-2151.
4. EUROCAE, an international non-profit organisation, is the European leader in the development of worldwide recognised standards for aviation. This is achieved by utilising the expertise from our members and stakeholders across the global aviation community.
5. EUROCAE standards are developed following an open, transparent and consensus-based process, governed by process and quality management principles, which are clearly documented and is in line with the World Trade Organisation (WTO) Technical Barriers to Trade (TBT) Agreement, Annex 3 “Code of Good Practice for the Preparation, Adoption and Application of Standards”.
6. EUROCAE standards and other deliverables are recommendations and best industry practices. EUROCAE is not an official body of the European governments. EUROCAE standards are intended to complement and support the regulatory and certification framework.
7. Whilst efforts are made during the standards-development process to avoid the inclusion of proprietary information and material, some of the elements of this document may be the subject of patent, copyright or other proprietary rights. EUROCAE shall not be held responsible for identifying any such rights. Trade names and similar terms used within this document do not constitute an endorsement by EUROCAE thereof.
8. Copies of this document may be obtained from:

EUROCAE

9 – 23 rue Paul Lafargue
93200 Saint-Denis
France

Telephone: +33 1 49 46 19 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	34
IMPROVEMENT SUGGESTION FORM.....	38

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 and RTCA Documents:

- ED-201 *Aeronautical Information System Security (AISS) Framework Guidance* (2015)
- ED-202A/DO-326A *Airworthiness Security Process Specification* (2014)
- ED-203A /DO-356A *Airworthiness Security Methods and Considerations* (2015)
- ED-204/DO-355 *Information Security Guidance for Continuing Airworthiness* (2014)
- ED-204A/DO-355A *Information Security Guidance for Continuing Airworthiness* (2020)
- ED-205 *Process Specification for security Certification of Air Traffic Management/Air Navigation Services (ATM/ANS) Ground Systems* (2019)

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/non-RTCA 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-204A/DO-355A
Aeronautical Information System	The set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information involved in all aspects of aircraft operations. Note that this includes supplier's information systems supporting the development of onboard system software and data.	ED-202A/DO-326A adapted from: Title 44 U.S.C., §3502 (8)
Airborne Software	Airborne Software includes all programs and data that are included in an aircraft system safety assessment or requires flight operations approval or requires maintenance operations approval. Airborne software encompasses Aircraft Controlled Software (ACS, equivalent to Field Loadable Software (FLS)) and Hardware Controlled Software (HCS) as defined in ARINC 667-1 [Source: ARINC 667].	ARINC 667-1 ED-203A/DO-326A
	Airborne software encompasses Aircraft Controlled Software (ACS, equivalent to Field Loadable Software (FLS)), Hardware Controlled Software (HCS) and Firmware (configuration of FPGAs (Field Programmable Gate Arrays) and other complex electronic hardware).	ED-204A/DO-355A
Aircraft	An aircraft or "aeroplane" means an engine-driven fixed-wing aircraft heavier than air that is supported in flight by the dynamic reaction of the air against its wings" (from Regulation (EU) No 965/2012).	ED-204A/DO-355A
	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, 2 nd Ed., 2001

Term	Definition	Source
Aircraft Component	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"
	An aircraft component is a component approved for installation on a type-certified aircraft.	ED-204A/DO-355A
Aircraft Domain	see Domain (Aircraft).	
Aircraft Information Security Center	The Aircraft Information Security Center should act as the operator's point of contact for aircraft information security events from within and outside the operator's organization.	ED-204A/DO-355A
Aircraft Type Certification	Design approval of an aircraft establishing that it ensures compliance with the applicable airworthiness requirements.	ED-204A/DO-355A
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 15 th Ed., 2007
Airworthiness	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 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/DO-326A ED-204A/DO-355A
	The protection of the airworthiness of an aircraft from "intentional unauthorized electronic interaction.	ED-203A/DO-356A
Anonymity	The condition of an identity being unknown or concealed.	IETF RFC 4949

Term	Definition	Source
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
Appropriate authority	The entity to which Declaration is made or who certifies the system.	ED-205
Assessment	An evaluation based upon engineering judgment.	SAE ARP 4754A
Asset(s)	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/DO-326A
	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/IEC 27005:2011
Assumptions	Statements, principles, and/or premises offered without proof.	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.	
Attack	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.	ED-202A/DO-326A DO-204A/DO-355A Adapted from IETF RFC 2828 "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

Term	Definition	Source
Attack Path	The path, interface, and actions by which an attacker executes an attack.	ED-202A/DO-326A
Attack Vector	The means of access which an attacker used to begin an attack.	ED-202A/DO-326A
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-202A/DO-326A
Audit	Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. NOTE 1 TO ENTRY: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines). NOTE 3 TO ENTRY: “Audit evidence” and “audit criteria” are defined in ISO 19011.	ED-205 ISO/IEC 27000:2016
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, Rev 5
Availability	Security usage: Ensuring authorized users have access to information and associated assets when required	ED-203A/ED-205 ISO17799 (Withdrawn)
	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
Certificate (Digital)	See Digital Certificate.	

Term	Definition	Source
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 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-204A/DO-355A
	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 4754A
	Any form of recognition based on an appropriate assessment, that a legal or natural person, ATM/ANS system, ATM/ANS constituent complies with the applicable requirements, through the issuance of a certificate attesting such compliance	ED-205
	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
Claims	“Claim” is a shorthand notation for a “Security Conformance Claim”. It includes an identification of security requirements for which the conformance is claimed. It has a statement about the conformance or conditions influencing the claim. A rationale is provided that assists the evaluator in confirming if the claim is acceptable by checking whether it meets all requirements for content and presentation of evidence.	ED-205
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

Term	Definition	Source
	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	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.	ED-79A / ARP4754A No definition, paragraph extract Section 5.4.2(c)
Component	Any self-contained part, combination of parts, subassemblies or units, that perform a distinctive function necessary to the operation of the system.	ED-79A / ARP4754A
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	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.	ISO 27000:2018 ED-203A/DO-356A/ ED-205 refers to previous ISO 27000 2016 same definition
Consequence	Outcome of an event affecting objectives. NOTE 1 TO ENTRY: <i>An event can lead to a range of consequences.</i> NOTE 2 TO ENTRY: <i>A consequence can be certain or uncertain and, in the context of information security, is usually negative.</i> NOTE 3 TO ENTRY: <i>Consequences can be expressed qualitatively or quantitatively.</i> NOTE 4 TO ENTRY: <i>Initial consequences can escalate through knock-on effects.</i>	ISO/IEC 27000:2018 ED-205 refers to ISO 27000 2016 same definition

Term	Definition	Source
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-202A/DO-326A
Continued Airworthiness	All the actions associated with the upkeep of a type design and the associated approved data through life.	ED-204A/DO-355A
Continuing Airworthiness	All of the processes ensuring that, at any time in its operating life, the aircraft complies with the airworthiness requirements in force and is in a condition for safe operation.	ED-204A/DO-355A
Control (Security)	See Security Control.	
Correctness	The degree to which an individual requirement is unambiguous, verifiable, consistent with other requirements and necessary for the requirement set.	ED-79A / ARP4754A No definition, paragraph extract Section 5.4.2(c)
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

Term	Definition	Source
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. NOTE: <i>References to a type certificate includes supplemental type certificates unless noted otherwise.</i> 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 Authorization Holders and Type Certificate Holders [Source: FAA]	ED-204A/DO-355A
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-204A/DO-355A
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-204A/DO-355A
Declaration	Declaration' means any written statement made under the sole responsibility of a legal or natural person to confirm that the applicable requirements relating to a legal or natural person, ATM/ANS system, or ATM/ANS constituent are complied with.	ED-205
Defense in Depth	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-204A/DO-355A
Dependent System	An aircraft system that depends on an external system for correct function.	ED-202A/DO-326A
Development Error	A mistake in requirements determination, design or implementation.	ED-79A / ARP4754A

Term	Definition	Source
Digital Certificate	A digital representation of information which at least (a) identifies the certification authority issuing it, (b) names or identifies its subscriber, (c) contains the subscriber's public key, (d) identifies its operational period, and (e) is digitally signed by the certification authority issuing it. [Ed see also Public Key Certificate].	NIST SP800-32: "Certificate"
	The term digital certificate refers to the private key and the associated public key of the digital certificate. The sender's private key is used for signing and the receiver's private key for decrypting; the sender's public key is used to verify the signature and receiver's public key for encrypting.	ED-204A/DO-355A
	A certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object.	IETF RFC 4949
Digital Signature	A value computed with a cryptographic algorithm and associated with a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.	IETF RFC 2828, IETF RFC 4949
Discretionary Access Control (DAC)	An access control service that enforces a security policy based on the identity of system entities and their authorizations to access system resources.	IETF RFC 2828
	An access control service that (a) enforces a security policy based on the identity of system entities and the authorizations associated with the identities and (b) incorporates a concept of ownership in which access rights for a system resource may be granted and revoked by the entity that owns the resource.	IETF RFC 4949
Diversity	The differences presented when comparing two or more security measures, in terms of functionality, technology and code.	ED-203A/DO-356A
Domain (Aircraft)	A set of equipment and related networks that share common administrative, security, and functional attributes.	ARINC 664 P5
	Logical environment that allocates and separates resources for the simultaneous operation of the system and host platform.	ARINC 811
Elemental Analysis	Elemental analysis method provides a measurement of the verification process to support the determination of verification coverage and completeness. Every functional element within the FFP (Functional failure path) is identified and verified using verification test cases that meet the verification objectives.	ED-80/DO-254