Classification: **Public**

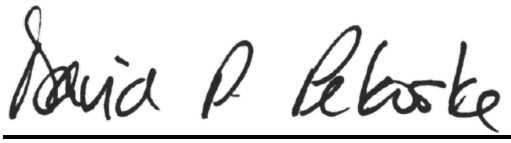
Open Architecture for Airport Security Systems

Endorsed by:

Prepared by the Joint Open Architecture Steering Group composed of leading regulators, airport operators, security equipment manufacturers and service providers

Name	Open Architecture for Airport Security Systems
Edition	2nd Edition
Version	1.00
Status	Approved
Date last updated	21st August 2023
Change Control Owner	ACI EUROPE

Approvals

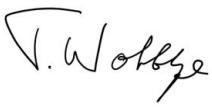


David P. Pekoske
Administrator Transportation Security Administration

Paolo Venturoni
CEO EOS

Olivier Jankovec
Director General ACI EUROPE

Abraham Foss
CEO Avinor



Thomas Woldbye
CEO Heathrow Airport

Contents

1. Change Control

Change History				
Version	**Status**	**Date**	**Summary of changes and contributors**	**Comments**
0.1	Draft	06/10/2022	Draft produced by ACI and EOS following reviews by Avinor, Heathrow, TSA and EOS	
0.21	Final Draft	30/01/2023	Final draft version following multiple reviews by JOASG	
0.3	Final Draft (all comments removed apart from Annex URL questions)	03/04/2023	Updated Final draft version following multiple reviews by JOASG	
0.9	Ready for approval and signature	17/07/2023	Final draft ready for approval and signature	
1.00	Approved	21/08/2023	Final approved and signed document	

2. Background

The original 2020 open architecture paper[1] acted as a catalyst and highlighted a desire for Open Architecture from end-users. The paper was published by ACI-Europe with contributions from the TSA[2], other national regulators, and airport operators but without the Original Equipment Manufacturers and technology stakeholder input. This revision represents a joint initiative across stakeholder communities, to include the OEMs and technology stakeholders, on the development of Open Architecture for aviation security. This new version aspires to reflect the outcome of many discussions that occurred over the past two years and is aimed to give both more detailed technical standards, that can be implemented by OEMs, and identifies the remaining issues and challenges around the successful deployment of solutions utilising Open Architecture.

[1] https://www.aci-europe.org/downloads/resources/Open%20Architecture%20for%20Airport%20Security%20Systems_1st%20Edition.pdf

[2] https://www.tsa.gov/

3. Executive Summary

This document defines the high-level scope and objectives of Open Architecture for Airport Security Systems and serves as a framework for implementable standards and detailed specifications. The Airport Operators, Regulators, Control Authorities, OEMs, and Industry Bodies mentioned herein have agreed upon the contents of this document. It is understood, that by the nature of local regulations and laws, there may be differences between the final implementations, but the definition of Open Architecture remains unequivocally endorsed. This document outlines:

- The broad concept of Open Architecture
- The intent of the signatories to move towards Open Architecture
- The work already performed to move collaboratively towards Open Architecture
- Stakeholder commitment and agreement to develop true open standards that will form the foundation of implementable Open Architecture initiatives and solutions

Following the publication of the 1st edition of Open Architecture for Airport Security Systems, Airports Council International (ACI) EUROPE, Transportation Security Administration (TSA) and EOS (European Organisation for Security)[3] formed the Joint Open Architecture Steering Group (JOASG). Under this working group sits the following three workstreams (these are discussed in greater detail in Section 5.1):

1. Technical Standards
2. Testing, Security and Certification
3. Commercial and Liability

The JOASG manages the three workstreams. It identifies and proposes standards, solutions, and guidelines to a wider plenary group of interested parties. A greater level of detail for the workstream products is provided in Annexes to this document which will be updated as activity progresses. Links to these Annexes are included at the end of this document.

> The contributors and endorsers of this paper pledge to continue to work together collaboratively and with an assumption of good faith to develop a workable and genuinely open architecture[4] based on agreed open standards for security equipment. They will also endeavour to respond to the challenges ahead and pledge to respect the investment to-date, intellectual property and the right to commercial viability of all parties.

[3] http://www.eos-eu.com/

[4] In the context of security equipment, in particular Airport Security Systems, Open Architecture refers to a software architecture that supports the integration, upgrading and ultimately interoperability of systems from multiple vendors.

4. Open Architecture - Definition and Benefits

The term Open Architecture may be familiar to the reader and is often understood to refer to physical and software architecture where interfaces[5], communication and protocols are appropriately available, well documented, and free to use. This greatly facilitates sharing data and adding, replacing and updating modules without unreasonable difficulties (commercial barriers, proprietary protocols, etc.).

For the purposes of Open Architecture for Airport Security Systems, we have identified 7 key areas which span across the workstreams' activities:

1. Accountability
2. Cybersecurity
3. User Administration
4. Security Equipment
5. Algorithms
6. Data Sharing
7. Security Equipment Control and Monitoring

These 7 key areas were factors in the development of the Annexes and will remain as drivers in their evolution.

The Airport Security Systems considered as being in scope for Open Architecture for Airport Security Examples of building blocks are shown below.

- **Hardware building blocks**
  - Security Scanner[6]
  - All X-Ray technology (e.g. Computed Tomography [CT], traditional 2D and diffraction)
  - ATRS[7] (Automated Tray Return Systems), Baggage Handling Systems (BHS) and conveyor systems that support and form part of the X-Ray technology
  - Shoe Metal Detection (SMD) and Shoe Explosive Detection (SED) equipment
  - Walk Through Metal Detectors (WTMD)
  - Explosives Trace Detection (ETD)
  - Other airport security technology, e.g. CCTV[8], optical trace detection, Liquid Explosive Detection Systems (LEDS), identity verification, access point control
  - Network devices
  - Mobile devices
- **Software and application building blocks**
  - Algorithms
  - Viewing Stations[9]/Common GUIs
  - Interfaces

[5] Consider interfaces as any point of data ingress or egress from the system(s).

[6] Security Scanners (EU term) are referred to as Advanced Imaging Technology (AIT) in the US market.

[7] Automatic Tray Return Systems (EU term) are referred to as Automatic Screening Lanes (ASL) in the US market.

[8] CCTV in this context refers to camera equipment specifically on a security lane rather than terminal wide.

[9] Similar to the solution developed by TSS for CT machines for Avinor but applicable across all devices.

- Image Distribution/Multiplexing
- Business Intelligence (BI) & Reporting
- Predictive maintenance
- Threat Image Projection (TIP)
- Management tools
- Data storage
- Secure applications

Technologies described above are representative and may not reflect the full list. Additionally, there are geographic and use case variations to consider.

This document does not attempt to standardise any elements of the physical devices, computer hardware architecture or physical architecture related to the actual airport security equipment itself, rather it describes the equipment that falls within the scope of Open Architecture for Airport Security Systems and those issues relevant to software architecture for Airport Security Systems and other screening applications.

This document is *not* intended to limit opportunities for innovation on the part of any OEM.

For a piece of security equipment to be identified as Open Architecture compliant it must support Open Architecture functions such as algorithms, data sharing, user management, system control and monitoring, and cybersecurity aspects described in the following sections. However, partial compliance is possible provided the level of compliance is identified. The Open Architecture is an answer to the security industry objectives and enables opportunities such as:

- **Objectives**
  - Flexibility - the ability to change system components as needs and/or technology evolve.
  - Choice - the ability to choose best of breed components. This prevents customers from being locked into a single OEM solution. This also opens potential new markets for OEMs and 3rd parties.
  - Efficient Lifecycle Management - the ability to replace or upgrade particular components in a modular fashion (as needed) without having to perform complete upgrades across the operating environment. This approach will require the establishment of robust configuration management policies, processes, and procedures, and possibly a transfer of liability responsibilities from equipment manufacturers to system integrators.
  - Operating Efficiency - the ability to implement real-time security management activities using multiple data sources.
  - Performance - the ability to ensure Key Performance Indicators (KPIs)[10] are met.
  - Scalability - the ability for customers to expand their system(s) efficiently and effectively with fewer limitations.
  - Checkpoint Management Systems and Business Intelligence Systems - all systems in scope will utilise these tools to simplify system management and reporting activities.
  - Common Viewing Station - system User Interface (UI) construction will be based on a standardised toolkit.

[10] The KPIs will need to be defined in the specifications to be written by the OEMs and agreed with the Airport Operators and Regulators. It is suggested the KPIs include (but not limited to) operational and functional requirements, fault tolerance, resilience, reactive behaviour, open documentation and maintainability.

  - Standards-Based/Non-Proprietary Solutions - will enable solutions to be globally deployed and fully interoperable at and between each location.
  - Cyber Security and Resilience - cyber security and resilience are critical components of Open Architecture implementation.
- **Opportunities**
  - Standardization and interoperability. Where Interoperability refers to the ability of equipment, products and systems from different vendors to seamlessly communicate, process data and operate in a way that requires the minimum of involvement from end-users.
  - Innovation and providing equipment purchasers with the ability to select from a broad range of systems and suppliers to meet operational requirements.
  - Enable airport operators to benefit from interoperable equipment when capacity needs increase. Open Architecture enables customers to rapidly deploy new interoperable equipment in a phased manner using more efficient incremental procurements vice large monolithic procurements.
  - Providing a more flexible means of adapting and responding to emerging threats and technological advances where requirements are clearly defined and testing/approval processes and regulation allows.
  - Improve operational, business, and procurement efficiencies - resulting from the step change in flexibility offered by Open Architecture.
  - Improve cyber security/resilience, and security collaboration, cooperation, and communication efforts between Airport Operators and Regulators. This will be achieved using standardised and interoperable interfaces across security systems and business management tools assuring data quality and routine testing methodologies by authorities and organisations, e.g. European Civil Aviation Conference (ECAC).
  - Information Sharing/Access - establish and implement an appropriate framework that allows data, data analytics, and machine learning/artificial intelligence information and applications to become more easily shared and accessible to authorised third parties. This approach is expected to improve the utilisation and optimisation of Airport Operator, Regulator, and customer corporate resources; and to improve the overall passenger experience.
  - Increase the ability to re-use images and data derived from outbound screening by inbound authorities or by airlines for applications such as the screening of dangerous goods or items prohibited by customs authorities.
  - Enable the use of innovative applications and data that have yet to be identified.

Adoption of Open Architecture for security equipment is intended to enable greater competition[11], whilst aiding continued innovation in Aviation Security systems.

[11] Competition in terms of both the commercial element and capability enhancements through continuous evolution of the systems and algorithms. The intention is to enable the market and open up opportunities for companies, both large and small, who may not have previously considered this market or been able to sell to this market. Most start-ups are software focused hence Open Architecture is a key component enabling their entry and creating new markets for software companies to develop and sell in to.

5. Introduction

This revised version of Open Architecture for Airport Security Systems reflects the output of the workstreams throughout 2021 and 2022. It provides an updated understanding of Open Architecture, reflecting the input from a wider range of key stakeholders. As with the previous version, the document defines what Open Architecture means in the context of security equipment. Many of the concepts contained in this document are applicable to other security environments as well as non-security environments such as customs, the detection of dangerous goods, and items of illegal wildlife trafficking. A wide range of international organisations, control authorities and regulators have reviewed the document, have given input, agreed on the content, and have consensus on the approach contained within.

This document sets out broad guidelines for how the equipment in scope will share data, not just between equipment deployed at the airport, but also with other applications, airports, and organisations.

Additionally, guidelines for user administration, algorithms, machine control and monitoring, cybersecurity, and most importantly - ownership of the data and accountability - will be introduced.

Industry stakeholders have unanimously agreed to define open standards as well as guidance which will better enable Systems of Systems that use Open Architecture to be realised.

We envisage that following the agreement, development and adoption of Open Standards and guidance material, there will be a need for ongoing engagement with the community to develop detailed specifications ensuring this Open Architecture definition is implemented uniformly across all equipment and associated systems and applications.

The scope of this Open Architecture definition covers all airport screening and other applications. The equipment and data for all these areas is fundamentally similar, however processes and procedures may vary and influence how Open Architecture is implemented in each area.

A key requirement is understanding the benefits of an *Interoperable* approach, rather than an *Integration* approach. An Interoperable approach offers the ability to connect and configure multiple, possibly disparate, components without the need for integration. A clear desire for the end-user is to move away from proprietary end-to-end systems integration, and instead favour interoperability across interfaces and system boundaries.

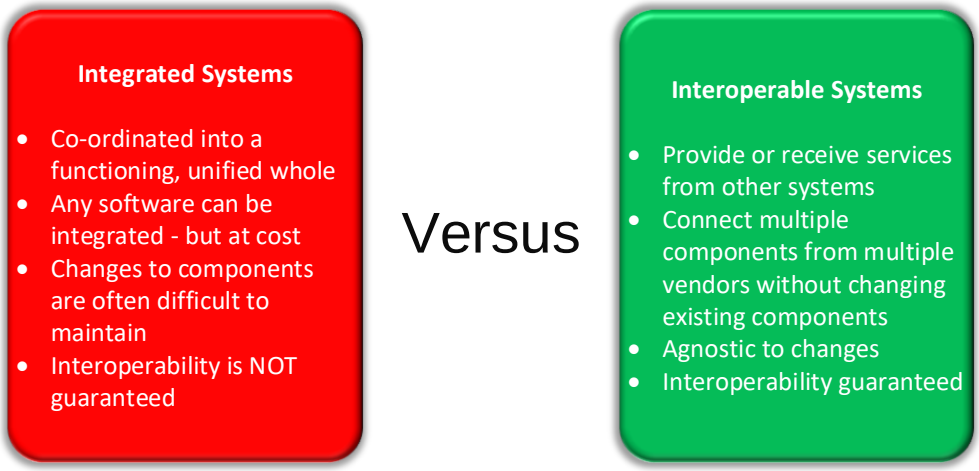


Figure 1 - Comparison of Integrated Systems versus Interoperable Systems

Integration costs can be high. It is expected that the use of standard interfaces and protocols will yield increased interoperability and reduced complexity and customisation[12]. The outcome is expected to result in lower costs, improved efficiencies and more flexible solutions.

The Cybersecurity requirements are published in Annex 3 as an annex to this Open Architecture due to its integral importance, however the scope of this annex is broader than Open Architecture for Airport Security Systems.

5.1. Summary of the 3 Workstreams

Workstream 1 - Technical Standards: Group formed of ACI members (airport operators), regulators (TSA), and representatives from EOS working towards the identification of key technical foundations for open architecture and providing guidelines for their implementation. The workstream has agreed on standardised formats and protocols. The key achievements of this workstream are summarised below:

- Unanimous agreement on the use of the Digital Imaging and Communication for Security (DICOS) format for security screening data (initially X-Ray but support for further screening modalities as the DICOS standard matures and is tested).
- Support and interest from all parties in the enhancement of Aviation Community Recommended Information Services (ACRIS)[13] semantic data model to provide a common data dictionary.
- Agreement and adoption of a common set of interfaces between security screening equipment must be achieved. The JOASG supports the development of both the Open Platform Software Library (OPSL) API and OEM API and recommends combining these approaches at an appropriate point in time and level of technical maturity.
- Differences in scenarios of use, timeline, technology, security issues, maintenance, performance and other factors may contribute to decisions regarding what approach to use, as well as future experience.

[12] https://www.nist.gov/publications/open-architecture-controls-key-interoperability

[13] https://acris.aero/

- Common protocols such as System for Cross-domain Identity Management (SCIM) and OpenIDConnect are recommended for component connectivity and enhanced user management.
- Best practices will be applied to ensure Cybersecurity is maintained and enhanced.

Workstream 2 - Testing, Security and Certification: Group formed of ACI members (airport operators), regulators (TSA) and representatives from EOS working towards the development of a common set of testing and certification processes. The key principles of Workstream 2 are:

- Open Architecture provides an opportunity to improve capabilities as well as processes. Current processes industry and regulators use to test, evaluate, approve, procure, and implement technologies will need to evolve to realize the full potential of Open Architecture. While the new processes must continue to ensure compliance with regulatory requirements and provide the necessary documentary evidence, they must also include details of new roles and responsibilities. Furthermore, they need to be tailored to support the advances this design and technology approach presents.
- The use of classified and commercial data/information is a necessity to support testing activities. All data/information used for the development of technology or generated by the security screening equipment must be protected in accordance with its classification level and authorised use. Any entity creating, handling, managing, or using data and information is responsible for obtaining the necessary approval or justification for its use prior to distribution/receipt and following the appropriate process to protect it.
    - Classified material has documented handling and storage requirements based on the level of classification. Strict compliance with these requirements is paramount to maintain an entity's access to material.
    - In the context of testing, IP, vendor proprietary documentation and test data (such as image data) should be considered the property or IP of the OEM and not shared without the permission of the OEM, which could be sought via the custodian or provided in advance.

Workstream 3 - Commercial and Liability: The Commercial, Liability and Intellectual Property Working Group was formed from a membership representing Airports from Europe and North America, TSA and several Equipment developers. Several core issues were identified that would need to be resolved when using Systems of Systems to deliver security screening equipment solutions. The key outcomes of Workstream 3 are summarised below:

- Currently when discrete screening solutions are deployed based on equipment by one supplier, the responsibility for many issues is very clear. For example, the responsible party for a given obligation (such as the purchaser, operator or supplier) is very clear for issues such as:
    - Who is liable for failing to prevent a terrorist event
    - Failing to meet approved detection performance levels
    - Meeting configuration management obligations
    - Protecting intellectual property or classified information
- Responsibilities for meeting maintenance and training obligations.
- However, with Systems of Systems there is a risk that responsibility is not clearly assigned, and this could mean that either there is doubt or confusion regarding who is responsible for a given obligation or there is a risk that parties may be held responsible for obligations they have not agreed to or are not even aware of.

- This working group identified the key areas of responsibility that need to be accounted for when deploying screening solutions using open architecture as well as suggesting how many of the potential problems can be resolved. This would typically be by assigning one party as responsible for delivery of the solution and outcome (often the prime integrator) and that party having responsibility for managing the agreed contractual responsibilities and obligations with the providers of subsystems. The findings and recommendations of this working group can be found in Annex 1 and may also have relevance to Annex 2 (Testing, Security and Certification) and Annex 6 (Roadmap).

6. Annexes

This document will serve as a framework and remain current and relevant to implementations of Open Architecture for Airport Security Systems. This framework refers to the annexes described below which provide a greater level of detail for the development of standards and specifications. As the combined understanding of all members and contributors increases and develops, the standards and specifications will evolve and be reflected in future versions of the annexes.

Under the JOASG, the three workstreams were formed with members from the airport operator, regulator, and OEM communities. Their aim is to identify and address those technical, regulatory, and commercial issues necessary to support the successful development and implementation of open architecture. The workstream members have collaborated to document the framework for implementable standards and specifications in the Annexes described below. These annexes are living documents that will continue to mature and evolve as work proceeds.

Annex 1. Commercial and Liability Framework

Objective: Create an accountability framework.

Focus areas:

- Protecting all Intellectual Property (IP) to allow connectivity and interoperability without exposing the underlying technology, solutions and innovations created by any OEM, airport operator or 3rd party.
- Defining terms related to a commercial and liability framework.

Introducing guidelines to consider when addressing commercial and liability issues.

Annex 2. Testing, Security and Certification

Objective: Provide insight and guidance on the elements of the testing process.

Focus areas:

- Providing an overview of the existing Testing & Evaluation (T&E) methodology
- Highlighting the needs of an Open Architecture T&E methodology
- Identifying considerations for the evolution of testing

Annex 3. Cybersecurity

Objective: Develop an IT security model that conforms to the approaches such as the Zero Trust model[14], requiring regular strict identity verification for every person and device trying to access resources on private networks, regardless of whether they are inside or outside the network perimeter. Develop steps and requirements that lead to meeting appropriate cybersecurity requirements, as an example the TSA ensure their Authority to Operate (ATO) aligns with the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF).

[14] https://www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles
https://github.com/ukncsc/zero-trust-architecture

Focus areas:

- **Secure the System** (Identify vulnerabilities, Manage vulnerabilities, Secure configurations)
- **Secure System Access** (Secure accounts and privileged users, strengthen and secure passwords, Logging)
- **Secure the Hardware** (Secure physical ports)
- **Secure the Network** (Separate the network, Encrypt the network, Restrict network services)

Annex 4. Use Cases

Objective: Establish use cases used to illustrate the application of Open Architecture and potential solutions to points of friction. (Note: The details of the use cases will not be made public, anyone wishing access to these should contact ACI EUROPE (or the standards body) requesting access.)

Focus areas:

- Ensure a complete list of use cases.
- Refine, verify and validate use cases.

Annex 5. Technical Standards

Objective: Identify common standards, definitions and interfaces to develop and implement Open Architecture.

Focus areas:

- Common definitions of terms
- Common definitions of data (data dictionaries/data domain models)
- Common protocols and formats for communication, data exchange, monitoring and maintenance, including image data
- Interoperability support.

Annex 6. Roadmap

Objective: Map out the future state of Open Architecture and translate the goals, objectives and actions to be achieved in the next two to five years into tangible deliverables.

Focus areas:

- Outline and prioritize key activities, milestones, and outcomes
- Determine roles and responsibilities of involved parties in implementing Open Architecture
- Determine critical paths and gate decisions
- Determine Use case prioritization.

Annex 7. Glossary of Terms

Objective: Maintain a glossary of common terms.

Focus areas:

- Incorporation of new terms and definitions resulting from documentation updates.

7. Conclusions

The contributors and endorsers of this paper pledge to continue to work together collaboratively and with an assumption of good faith to develop a workable and genuinely open architecture[15] based on agreed open standards for security equipment. They will also endeavour to respond to the challenges ahead and pledge to respect the investment to-date, intellectual property and the right to commercial viability of all parties.

- There has been unprecedented effort and collaboration from all relevant stakeholders across regulators, airport operators, and OEMs. This has provided all parties with improved insight into the complexities of this subject from perspectives other than their own.
- This has resulted in genuine progress towards implementable standards and ongoing efforts to realize Open Architecture for Airport Security Equipment.
- Workstreams were established to focus on 1. Technical Standards, 2. Testing, Security and Certification, and 3. Commercial and liability. Issues were identified and potential solutions proposed.
- The output of this initiative, is a set of annexes, presented to the reader in Section 6. These will evolve as the collective knowledge evolves and detailed specifications are written.

[15] In the context of security equipment, in particular Airport Security Systems, Open Architecture refers to a software architecture that supports the integration, upgrading and ultimately interoperability of systems from multiple vendors.