# Open Architecture for Airport Security Systems

**Prepared by:**

Avinor AS
Oslo Atrium
Dronning Eufemias gate 6
0191
OSLO
Norway

Heathrow Airport Limited
The Compass Centre
Nelson Road
Hounslow
Middlesex
TW6 2GW
United Kingdom

**Endorsed by**:

ACI EUROPE, US Transportation Security Administration, UK Department for Transport, UK Civil Aviation Authority, Canadian Air Transport Security Authority, German Federal Police, Heathrow Airport Limited, Swedavia Airports, Avinor AS, Amsterdam Schiphol Airport, Groupe ADP, Manchester Airport Group, Geneva Airport, Dublin Airport Authority, Birmingham Airport, AVSEC New Zealand, Copenhagen Airports A/S, Munich Airport, Dubai Airports, Changi Airport

**Contributions from**:

Heathrow Airport Limited, Avinor AS, Amsterdam Schiphol, ACI EUROPE, daa (Dublin Airport Authority), UK CAA, UK DfT, AVSEC New Zealand, Copenhagen Airports A/S and TSA.

| | |
|---|---|
| Name | Open Architecture for Airport Security Systems |
| Version | 2.0 |
| Status | Final |
| Date last updated | 16.07.2020 |
| Authors | E Kramer, R Dempers, J Paulshus |
| Change Control Owner | ACI EUROPE |

# Contents

# 1. Change Control

| | Name | Role | Organisation |
|---|---|---|---|
| Prepared by: | John Christian Paulshus | IT Application Portfolio Management, Architecture and Technology | Avinor |
| | Eugene Kramer | Head of Cybersecurity for Passenger, AVSEC and Borders | Heathrow |
| | Dr Richard Dempers | Sponsoring Solution Architect, Cabin Baggage Security | Heathrow |
| Assured by: | | | |

| Change History | | | | |
|---|---|---|---|---|
| **Version** | **Status** | **Date** | **Summary of changes and contributors** | **Approver** |
| 0.1 | Draft | 15/01/2020 | Initial template by John Christian Paulshus | |
| 0.2 | Draft | 20/01/2020 | Updated by Richard Dempers and Eugene Kramer | |
| 0.3 | Draft | 21/01/2020 | Updated by Richard Dempers following call with Avinor (and Paul Evans and Eugene) | |
| 0.31 | Draft | 31/01/2020 | Updated by Richard Dempers following initial review by Marc Reitman | |
| 0.32 | Draft | 03/02/2020 | Incorporated feedback from David Ryder | |
| 0.33 | Draft | 06/02/2020 | Updates following internal Heathrow review | |
| 1.0 | Draft | 06/02/2020 | Published internally within Heathrow | |
| 1.1 | Draft | 13/02/2020 | Accountability section added | |
| 1.2 | Draft | 13/03/2020 | Updated following ACI EUROPE meeting 10/03-11/03, includes comments from Jérôme Morandière and wider community | |
| 1.3 | Draft (for comment) | 13/03/2020 | Changes accepted and new draft issued for formal review by Airport Operator and Regulator community | |
| 1.4 | Draft (for comment) | 03/04/2020 | Comments incorporated from Ben Wong (UK CAA), Ben Jones and Anthony Parker (DfT), Ole Folkestad (Avinor), and ACI EUROPE | |
| 1.5 | Draft (for comment) | 08/04/2020 | Updated following review by Daiga Dege and David Ryder (ACI EUROPE) | |
| 1.6 | Draft (for comment) | 21/04/2020 | Updated to incorporate feedback from the TSA (Jeff Quinones et al) | |
| 1.7 | Draft (for final review) | 27/04/2020 | Updated to incorporate comments from Avinor and UK CAA Cyber Security Team | |

| | | | | |
|---|---|---|---|---|
| 1.8 | Draft (v1.7 changes accepted) | 13/05/2020 | Changes from previous version accepted to make document readable for AVSEC NZ - existing comments still need to be addressed/confirmed | |
| 1.9 | Draft | 22/05/2020 | Comments from AVSEC NZ and Copenhagen incorporated together with input from ACI EUROPE and TSA | |
| 1.9 | Draft | 11/06/2020 | Foreword and Introduction inserted | |
| 2.00 | Final | 16/06/2002 | Updated TSA Administrator title and included Dubai and Changi to list of supporters/endorsers | |

# 2. Foreword

As world leaders in aviation security we continually look for innovative ways to strengthen aviation security levels and raise the global baseline.

A safe and secure aviation system underpins the global economy; but the threat to this system is real and persistent; and technology is changing the way the world and our adversaries operate.

Key to our success is the shared ability to collaborate across the public, private and academic sectors. It is through these partnerships that we bring the best technologies and brightest minds together and rise to the collective challenge of outmatching a dynamic threat.

We are pleased to support the Open Architecture for Airport Security Systems initiative. Through this initiative we commit to working with our partners to open our hardware and in doing so, broaden the market and safely provide new entry paths for collaborators.

Today, we welcome a new class of partner; tomorrows software developers to join us in the development and delivery of world leading threat detection software and help us defeat terrorism.

| | | |
|---|---|---|
| David P Pekoske | John Holland-K | |
| **David Pekoske** | **John Holland-Kaye** | **Olivier Jankovec** |
| **TSA Administrator** | **CEO, Heathrow Airport** | **Director General, ACI EUROPE** |

# 3. Introduction

The following document defines what Open Architecture means in the context of airport security equipment.  The concepts contained herein can also be applied to other capabilities and areas. It has been reviewed by a wide range of international organisations, control authorities and regulators, all of whom have given input, agree 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 in the security lane but also with other applications, airports and organisations.

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

The regulators and airport operators that have endorsed this document have collectively agreed on this approach with support from ACI EUROPE.

We envisage the next steps in this process will be to engage with the manufacturers to create a community to develop, adopt and maintain detailed specifications ensuring this Open Architecture definition is implemented uniformly across all equipment.

We therefore urge you to see this as an opportunity to embark on the development of Open Architecture across security equipment.  Members of the aviation community are closely following Heathrow's approach to the procurement and implementation of security equipment. Your involvement and adoption of Open Architecture would be beneficial to the industry and provide you with a competitive advantage in future procurements as you will be seen to be innovative and pro-active, whilst offering customers choice and value.

# 4. Abstract

The term Open Architecture may be familiar to the reader and is often understood to refer to physical and software architecture where interfaces[1], communication and protocols are publicly 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).

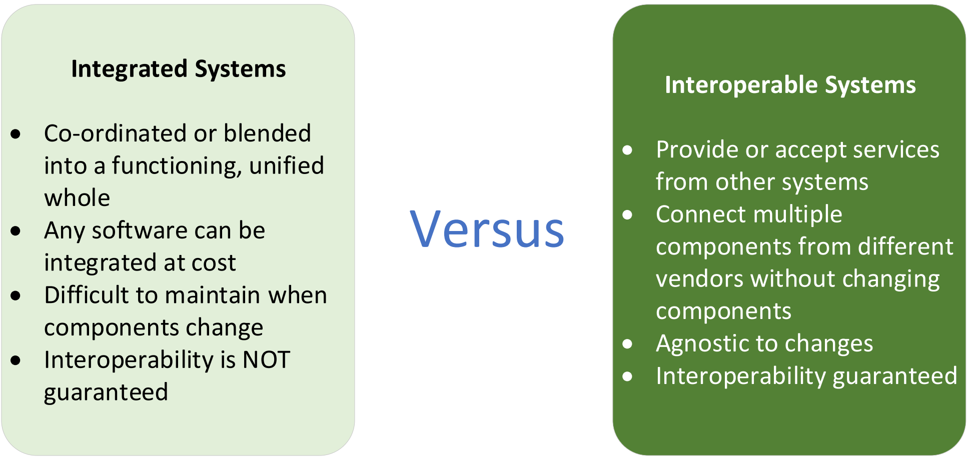
This document describes the Open Architecture issues relevant to software architecture for Airport Security Systems. It does not include standards for physical devices or computer hardware architecture or physical architecture related to the actual airport security equipment. The Open Architecture being proposed here offers the airport industry the following advantages:

- Improve standardisation and interoperability;
- Opportunity for increased innovation and providing operators with the ability to select from a far broader range of systems from a broader range of suppliers to meet operational requirements;
- Faster, more efficient & more flexible means of adapting and responding to emerging threats and technological advances;
- Improve operational, business and procurement efficiencies, resulting from the step change in flexibility offered by Open Architecture allowing rapid changes to screening equipment, aligning with the threat landscape and demands on resources;
- Improve security and cooperation between Airport Operators and Regulators, this will be enabled by standardised and interoperable interfaces across security systems and business management tools assuring data quality and common testing methodologies by authorities and organisations, e.g. ECAC;
- Reduce through-life costs associated with complex system integrations due to existing bespoke solutions;
- Implement the necessary foundations for data and outputs to become more easily accessible and supply data analytics and machine learning/artificial intelligence applications. These methods are expected to improve the utilisation and optimisation of corporate resources to assist Airport Operators and Regulators, customers and improve passenger experience.

The areas of Open Architecture in this context include readily sharing data, monitoring of security screening equipment, end-user administration and cybersecurity.

For an open software architecture, these areas should be possible to implement without additional fees or license costs. 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 objective for the industry is to move away from proprietary end-to-end systems integration, and instead favour interoperability across interfaces and system boundaries.

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



**Integrated Systems**

- Co-ordinated or blended into a functioning, unified whole
- Any software can be integrated at cost
- Difficult to maintain when components change
- Interoperability is NOT guaranteed

Versus

**Interoperable Systems**

- Provide or accept services from other systems
- Connect multiple components from different vendors without changing components
- Agnostic to changes
- Interoperability guaranteed

*Figure 1 - Comparison of Integrated Systems versus Interoperable Systems*

Integration costs often far outweigh the costs of hardware purchase, this is undesirable and is a driver for the adoption of Open Architecture[2]. Interoperability, where appropriate, is the key, e.g. not necessarily connecting every device, only connecting those that provide real benefits.

The remaining requirements for Open Architecture can be summarised as:

- Flexibility, the ability to change system components as either needs or technology evolve;
- Choice, ability to choose best of breed components allowing customers to not be locked in with one Vendor;
- Lifecycle Management, no need for complete upgrades across the environment, components can be replaced or upgraded as needed;
- Operating Efficiency, real-time security management provided from multiple sources of data;
- Performance, ensuring KPIs are met[3];
- Scalability, no limitations for the customer when it comes to expanding their system(s);
- Resource Management, a Common Viewing Station based on a toolkit for User Interface (UI) construction. This will be applicable to all systems in scope and simplify system management;
- Standards Compliant, non-proprietary allowing global deployment and interoperability at and between each location. This will include image data format, Programmable Logic Controllers (PLCs) and provide adaptability for future sensor levels and Corrected Data Interfaces (CDI) for pixel corrected raw data[4], Transformed Data Interfaces (TDI) for reconstructed images and Inspection Data Interfaces (IDI) for images displayed to operators;
- Security; maintains or improves cyber security and resilience.

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

[3] The KPIs will need to be defined in the specifications to be written by the Vendors 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.

[4] Raw data is the linear attenuation coefficient measurements from the X-ray detectors that is used for the reconstruction of the high and low energy images (or any other intermediate energy images). This data includes, but is not limited to, the raw data from the X-ray detectors, calibration data from the X-ray detectors and other signal or image processing information required to process the data from the X-ray detectors into the linear coefficients. This data is used to determine effective atomic number ($Z_{eff}$) and X-ray density ($\rho$). Image data is any image information generated after raw X-ray data has been processed for display to an operator or usage in a system to support Automated Threat Detection algorithms.

Adoption of Open Architecture for security equipment is intended to deliver greater and more diverse competition[5] and innovation to Aviation Security systems.

A standard Systems Compliance template will be provided for Vendors to populate with their responses to this document.

This document outlines the definition of Open Architecture and high-level requirements for Open Architecture including Cybersecurity requirements. The contents have been agreed by the Airport Operators, Regulators, Control Authorities and Industry Bodies mentioned herein. 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.

[5] Competition in terms of both the commercial element and capability enhancements through continuous evolution of the systems and algorithms. The intention is to stimulate 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. Key Concepts and Areas of Interest

## 5.1. Security Equipment in Scope for Open Architecture

The following table defines the security equipment that Open Architecture will include for Airport Operators and Regulators:

| Security Equipment | Algorithms | Data | External Interfaces |
|---|---|---|---|
| Security Scanner[6] | In scope | In scope | In scope |
| X-ray technology (e.g. Computed Tomography [CT], traditional 2D and diffraction) | In scope | In scope | In scope |
| ATRS[7] | In scope | In scope | In scope |
| Shoe Metal Detection (SMD) and Shoe Explosive Detection (SED) equipment | tbc | In scope | In scope |
| Explosive Trace Detection (ETD) | tbc | In scope | In scope |
| Walk Through Metal Detectors (WTMD) | tbc | In scope | In scope |
| Common Viewing Station[8] | In scope | In scope | In scope |
| Other technology, e.g. CCTV[9], optical trace detection, Liquid Explosive Detection Systems (LEDS) | tbc | tbc | tbc |

*Table 1 - Security Equipment in Scope for Open Architecture*[10]

Note, the list in the table above is not exhaustive.

## 5.2. Algorithms

Three use cases for algorithms for imaging devices (such as 2D, CT and diffraction X-ray technology and Security Scanners) have been identified as being pertinent to Open Architecture:

1. Application of different detection algorithms provided by the device manufacturer on the OEM hardware itself and extracting the data;
   - Switching between algorithms provided by the device manufacturer;
2. Application of 3rd party algorithms not provided by the device manufacturer on the OEM hardware itself and extracting the raw data to run against the algorithm;
   - Switching between algorithms provided by the device manufacturer and a 3rd party;
3. Extracting the raw data off the device and applying 3rd party algorithms in a separate system;
   - The output from the 3rd party algorithm will be fed back to the screening device. The screening device in this context can be thought of as an edge device or

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

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

[10] The definition and expected operational performance for each piece of equipment will be defined in the detailed specifications and by the Airport Operators and Regulators during requirements capture prior to design and implementation.

cloud-based device where the data will need to be secured both in transit and at rest.

The ability to dynamically switch[11] from one detection algorithm to another is highly desirable to enable the detection of different threats and items of interest to other agencies, e.g. for the detection of drugs, currency and wildlife. For example, the X-ray machine must be capable of running a 3rd party weapons detection algorithm concurrently with the OEM explosive detection algorithm. The combined result then being sent to the ATRS for tray diversion as required.

The hardware (both OEM and 3rd party) and software must be compatible with the running of multiple algorithms. This may occur sequentially or concurrently depending on the operator's implementation.

All algorithms must be approved by the appropriate regulatory bodies and authorities to assure compatibility with different configurations of hardware, software and compatibility with other algorithms which may be running concurrently or sequentially[12]. The process for approval and assurance must be defined and agreed with Airport Operators and Regulators.[13]

OEMs and 3rd parties will implement an Open Platform Software Library (OPSL) to provide inputs and outputs to their algorithms. This will act as a wrapper and enable communication between one OPSL wrapped algorithm and any other OPSL wrapped algorithm or software component.

## 5.3. Data Sharing

In the context of security equipment (see Table 1), Open Architectures must conform to the following requirements and include image data, data for condition-based monitoring, telemetry, analytics and the storage of data over configurable time periods (for forensics, predictive maintenance etc):

- A defined interface and data model must be available. This should support standardised non-proprietary formats, e.g. Delimited text files such as Comma Separated Value (CSV) or similar. Where this is not possible, (and only permissible with a waiver) documentation of Vendor specific formats must be provided, e.g. A data dictionary containing common meta-data. The data should be available in Vendor independent storage such as a data-lake and visualised via a Head System (or similar).

  The data model must be accepted as an industry standard (an independent industry body such as ACI EUROPE is the custodian), such that any change(s) go through approvals[14] and the data model is updated once the change(s) are approved[15];

- Any Application Programming Interfaces (API) must be based on Open Systems Interconnect (OSI – see Appendix – OSI Model) Model Protocol Layers and support communication between the application software, platform and external environment.

[11] As opposed to manually selecting the algorithm and, in some cases, having to restart the machine

[12] ECAC and the Airport Operators and Regulators must decide how best to approach this subject. The CEP is a lengthy process and may not be a suitable mechanism for the approval of rapidly developed 3rd party algorithms. A possible solution may involve a paradigm shift in the CEP and the wider AVSEC community. This is something which will require careful consideration by the ECAC TTF.

[13] Regulators such as the TSA, DfT and ECAC will need to assess the critical paths for algorithms in the equipment's architecture. Robust configuration management will be needed to ensure integrity is not compromised.

[14] It is suggested that ACI EUROPE's Security Technical Panel manage updates to this definition and subsequent standards. Additionally, the Vendors have an important role in shaping Open Architecture.

[15] Database definitions and report definitions should be part of the functional requirement documentation and include the format and capability for export and transmission.

Additionally, as indicated in the previous section the APIs will constitute an OPSL[16]. The APIs can be summarised as:

  - **User** - Interfaces intended to provide access from the software with the user defining the service(s) available to the applications for information exchange with the user;
  - **Communication** - Interfaces defining services available to the application software to exchange state and information with the application platform(s) and/or other application software and hardware such as the security equipment listed in Table 1, testing infrastructure, enterprise infrastructure, airport facilities and infrastructure;
  - **Information** - Interfaces providing non-communications services to exchange state and information with the application platform(s) and/or other application software such as the security equipment listed in Table 1, testing infrastructure, enterprise infrastructure, airport facilities and infrastructure;
  - **System services** - Interfaces defining language services available internally to the application platform(s) for interoperability with other application software or platforms such as the security equipment listed in Table 1, testing infrastructure, enterprise infrastructure, airport facilities and infrastructure;
  - **Primary Scan Acquisition** - interfaces to retrieve data from the security equipment listed in Table 1;
  - **Analysis** - Interfaces to provide input and output from algorithms running on OEM or 3rd party platforms.
- All Vendors are to work to these API standards that will also support:
  - Interfaces for physical access between the device(s) and human operators providing the look and feel of the User Interface[17] (UI) with the application platform(s);
  - Interfaces providing IT language services for connectivity and protocols for state and data interchange;
  - Interfaces providing IT language services using physical and logical file structures;
- Communication will be based on publicly known and secure protocols;
- Authentication and authorisation will follow valid cybersecurity principles (see section 5.6.1);
- Adoption of the Digital Imaging and Communications in Security (DICOS) standard[18] (latest published version) and compliance with the DICOS Toolkit, to ensure all parties are implementing the same interpretation of the DICOS standard, for all X-ray (2D and

[16] An OPSL can be utilised in three ways:

- Adapter - Separate server;
- Static - usually installed on a scanning device but can be on a separate server;
- Dynamic - Installed on a scanning device and fully integrated into the OEM's platform.

[17] The expectation is that a toolkit will be provided for the construction of the UI according to the specifications of each Airport Operator or Regulator.

[18] The Universal File Format (UFF) may be considered as an alternative to DICOS offering opportunities for commonality across Hold Baggage and Cargo. The TSA has advised that UFF is less mature than DICOS and focussed on Non-Intrusive Imaging (NII) of shipping containers, vehicles and trailers, as well as freight and parcels. Introduction of UFF may add complexity and implementation issues. The wider scope of UFF is expected to be included in the next DICOS version that will add air cargo to its scope. Exploration of formats for generalised line-scan imagery versus X-ray imagery should be explored.

CT) images and passive/active millimetre wave images is expected from all Vendors[19] including the raw image data in a common format. DICOS is suitable for image reconstruction but there are concerns with its use when transferring images due to time constraints related to transmission and file size, however it must be noted that DICOS is an evolving standard. This should use the recommended network protocol however Vendors may suggest alternatives to this provided there is a valid reason[20]. The data formats must be standardised based on the source systems and all participants in related work must ensure this format is standardised in terms of DICOS objects. Building systems based on defined DICOS Information Object Definitions (IOD) formats and services will assist Vendors and serve as shared requirements across the wider airport community;

  - Additionally, Vendors must be compliant with the latest published version of DICOS and update their compliance based on the DICOS revision cycle;
  - Current Security Scanner technology deletes the millimetre wave images immediately after the algorithms have been run. Options to allow the running of different algorithms (if the risk analysis requires) need to be considered. In addition, a means to link the millimetre wave image to the person without privacy implications must be found;

- The network requirements and expectations of airports producing high volumes of image data must be understood. Achieving this will greatly assist solutions from different Vendors interacting with each other in standard formats;
- The concept of Open Architecture must include methods of data extraction;
- Data ownership must be addressed. Is the data collected by security systems owned by the airport, control authorities or some other organisation? It should *not under any circumstances* be owned by the Vendor(s), i.e. the customer (Airport Operator or Regulator) should own the data. Data access is covered by the Cybersecurity Requirements (see section 5.6.1). This includes the ability to link image data to identifiable persons (as with Data Driven Differentiated Screening [3DS]) and share this with Control Authorities and Airport Operators due to capacity constraints and/or intelligence based operational requirements. This applies to all data generated from the equipment in scope (see Table 1);
- Airport Operators and Regulators base decisions on information rather than data, i.e. data from one or more sources presented in a defined manner via an approved user interface. Therefore, the Vendors will ensure the raw image and component data is available for extraction to enable 3rd party algorithm development and support the operation of these in production environments. Consensus between the Airport Operators and Regulators and Vendors needs to be achieved on:
  - Data ownership, governance and sharing frameworks to address the legal aspects of data sharing to cover bilateral agreements and ensure anonymisation and privacy where appropriate;
  - Challenges linked to the gathering of large amounts of data such as:
    - Protection of Intellectual Property (IP) such as control over stored and processed data and associated decisions on who is permitted access;
    - Quality and relevance of the data;
    - Validation and verification of the data and related device(s) to ensure integrity and cybersecurity - this includes confidentiality integrity and availability;
    - How best to anonymise data without rendering the data unusable;

[19] Unlike DICOS this Open Architecture standard for Security Equipment should be freely available for all those with a legitimate reason for access, however the risk of the standard getting into the hands of uncontrolled users must be balanced by recovering the costs of developing the OA standard itself.

[20] Airport Operators and Regulators must be clear in identifying the reasons why a particular protocol is unsuitable.

  - Infrastructure, capacity and system availability including computational power to process data in real-time (or near real-time);
  - Increased threat - Access to large datasets is known to be a motivation for cyber compromise;
- Consideration should be given to the use of Geneva Airport's Information Security and Data Privacy (ISDP) concept[21]. This concept may aid Airport Operators and Regulators and Vendors to identify threats related to a given information system, propose measures likely to mitigate risks associated with those threats and evaluate residual risks. An example Target of Evaluation (ToE) is included in Example ToE model;
- Consideration should be given to the introduction of a universal clock in an integrated and interoperable system. This will greatly assist the synchronisation of data from multiple sources, e.g. Reconciliation of timings from X-ray machine Threat Image Projection (TIP) logs with the ATRS TIP decision logs, this is of particular importance in a high-volume Centralised Image Processing (CIP) environment.

## 5.4. Security Equipment Control and Monitoring

The following requirements for agent free data retrieval must be met:

- Equipment status and maintenance data should be available through Simple Network Management Protocol (SNMP), service ports or Web Services/APIs for device alerts at network level, device log data or system data respectively. The precise format will drive whether alarm acknowledgement will be sent back to the source system and/or management system. A decision is required whether alarm feeds should be brokered centrally. Where do airports want to see this information? Do airports want to automate processes within systems, e.g. AODB, based on the alerts?
- Equipment status and maintenance data should be available through standard agents, e.g. NSClient[22].
- Provision must be made for not just monitoring but active control of equipment from a remote application or system. Industrial Internet of Things (IIoT) technologies and protocols such as MQ Telemetry Transport (MQTT) should be considered.

A suggested list of data points that Airport Operators and Regulators would expect from Vendors supplying X-ray machines, including CT machines and ATRS is available in Cabin Screening Data Requirements. These data points should be useful in any future SCADA system and during commissioning, testing, validation during rollout and ongoing support.

The data collected will support Remote Monitoring and Maintenance (RMM) and Maintenance Ticketing Applications (MTA). Ultimately, the data will be used to train Predictive Maintenance algorithms and feed into these in a production environment to deliver operational benefits and cost efficiencies.

## 5.5. User Administration

User administration is important because many airports use contractors to perform security procedures, such as handling passenger security screening.

The Open Architecture must support integration with external Identity Providers and support the adoption of common frameworks for password rules and expiry, particularly if user identities are synchronised.

[21] Refer to Geneva Airport's ISDP concept document

[22] NSClient is an agent originally designed to work with Nagios but has evolved into a monitoring agent which can be used with monitoring tools such as like Icinga, Naemon, OP5, NetEye, Opsview etc

- As Airport Operators and Regulators and Vendors move to Cloud based Identity Providers it is important to include Security Assertion Mark-up Language (SAML) and OAuth for access and authentication.
- Systems should be built on Role Based Access Control (RBAC) to support Single Sign-On (SSO)[23]. The RBAC will be granular allowing permissions to be set appropriate to each Airport Operator and Regulator, e.g. one airport may want screeners to run reports while another airport may not want screeners to have access to reports.
- Multi-Factor Authentication should be considered based on system capability. Where SSO is correctly implemented this requirement can be built into the Identity Provider rather than the Vendor's application(s).
- Remote access will require security controls:
    1. Network based controls, e.g. IP limiting based on source IP addresses;
    2. Possible requirement for VPN/secure communication channels;
    3. A web layer could be presented externally if the underlying systems are correctly architected
- Integration to training systems(s) for training and alerting when certifications are about to expire;
- Support for certificates to allow secure communication between equipment.
- User and device authentication

## 5.6. Cybersecurity

The long-term goal for cybersecurity should be conforming to the Zero Trust model[24]. This is an IT security model 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.

In terms of network security, the Zone Model is viewed as desirable, however alignment of components of Vendor systems needs to be investigated. Data classification should be looked at and mapped to relevant zones, likewise for user roles within each system, e.g. RBAC as discussed in section 5.5.

Airports currently have their own standards that if implemented properly would meet many of the security standards suggested in the joint TSA/ACI Cyber Requirements (see section 5.6.1), however they do not operate single systems to govern these, e.g. vulnerability scanning, anti-virus, SIEM. Each of these systems provides IT security with a view of environment security from different perspectives and does not necessarily provide overarching coverage.

### 5.6.1. Cybersecurity Requirements

The following 18 requirements were agreed and defined in a series of workshops and meetings involving ACI EUROPE and its members (which includes Heathrow, Amsterdam Schiphol, Avinor, MAG and other European Airport Operators) and European Regulators and TSA.

These serve as a minimum baseline for Vendors to ensure safeguards are in place to protect data and reduce the risk of compromise when developing new innovations and when proposing technology for screening purposes. These requirements are included here to provide a fundamental building block upon which Open Architecture can be delivered. Where

[23] From the market's perspective SSO coupled with RBAC must be the goal for vendors to achieve, however it is acknowledged that individual Airport Operators and Regulators may wish to implement SSO or RBAC rather than together due to legacy identity access management dependencies.

[24] https://www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles

https://github.com/ukncsc/zero-trust-architecture requirements have been met, the vendor must provide the steps required for verification to certification bodies. The vendor must also provide evidence of these requirements being met to the operator and instructions for the continued maintenance of the cybersecurity posture of the equipment/software. Where a specific requirement cannot be met the supplier must state clearly why this is so and how the impact(s) can be mitigated.

**Secure the System** (Identify vulnerabilities, Manage vulnerabilities, Secure configurations)

1. **Audit and Accountability** - Vendors must ensure capabilities are in place to audit events and configuration changes, conduct analysis and reporting, and monitor for appropriate information disclosure. Enable logging and the ability to forward to SIEM (Security Information and Event Management) solutions e.g. Splunk, QRadar. Include the ability to send security audit logging information to a SOC (Security Operations Centre) for security analysis.
2. **Protected Sensitive Screening Algorithms** - Vendors must ensure adequate system protections are employed to protect any sensitive screening algorithms from compromise or modification that would render the Security Equipment inoperable (i.e. fault). Vendors must also provide an immediate alerting mechanism for access to, or modification of, the algorithms and prevent any removal from the Security Equipment, with full activity logs provided to a SOC for security analysis.
    - Logs should cover access, change, ingress, egress and location.
3. **Configuration Management** - Vendors must employ automated measures to store and maintain baseline configurations and ensure adequate system protections are employed to protect baseline configuration from compromise, modification, and render the Security Equipment inoperable (i.e. fault) and provide an immediate alerting mechanism for when the baseline configurations have been accessed, and/or modified. Vendors must adhere to or utilize industry best practice's standard configuration guides. Information Technology and Cybersecurity personnel maintain and provide periodic updates to ensure configurations are consistently applied to Security Equipment
4. **System and Information Integrity** - Vendors must address and implement methods to update Security Equipment affected by software flaws including potential vulnerabilities resulting from those flaws. This involves security-relevant software updates to include, for example, patches, service packs, hot fixes, and anti-virus signatures. Vendors must provide a managed process to periodically provide software and configuration updates for the Security Equipment while maintaining the on-going effectiveness of screening capabilities. Systems should provide an endpoint control mechanism to reduce the likelihood of system compromise between software updates (i.e. endpoint protection/anti-virus, firewall, application whitelisting).

    Vendors must provide a configuration verification hash to assist with ensuring the correct configuration is used. The hash will also assist in the detection of tampering. The following is not exhaustive but the hash must include all peripherals and workstations and switches and servers.

5. **Security Assurance Scanning/Testing** - Vendors must ensure that security assessment tools can be externally run (by the operators) against the Security Equipment to ensure appropriate configuration (e.g. hardening), patch levels, and that there are no Indicators of Compromise (IOC) present on Security Equipment that may impact the system integrity of the screening processes. The vendor must define the types and methods permitted for independent security assurance testing but should aim to minimise restrictions imposed on the types and methods. This includes all peripherals and workstations encompassing switches and servers. All external devices used to connect to security equipment for any purpose must be scanned by an appropriate anti-virus capability prior to and after each system connection.

6. **Cyber Intelligence** - Vendors must demonstrate the ability to update equipment design and capabilities to align with changing cyber intelligence and threat reporting.
7. **Supported Systems** - Vendors must ensure full Security Equipment hardware, software, and operating system support to remediate any identified vulnerabilities with the Security Equipment or supporting systems (Patching). Systems must be supported by the OEM vendor during the useful life of the equipment or appropriate upgrades must be performed

**Secure System Access** (Secure accounts and privileged users, strengthen and secure passwords, Logging)

1. **Access Control (A)** - Vendors must implement adequate access control and account management practices. This allows bespoke changes by the airport operator to enable, disable, remove, and monitor user and privileged accounts and maintain controlled access to Security Equipment. On-Site Vendor Support personnel must integrate into the Access Control mechanism for the Security Equipment including system and account monitoring for activities performed locally to the Security Equipment.
2. **Access Control (B)** - Vendors must implement a capability to enable multi-level access to equipment resources and enable the ability to restrict users to only the level of access required. Access by privileged accounts / super-users / admin user must be separated from other regular users.
3. **Password Control** - Vendors must implement and provide the capability for the airport operator to change system level passwords periodically. Password use should be minimised wherever possible and replaced by other more secure multifactor technologies - where system passwords must be used, an audited and automated password change process should be leveraged. Specifically, the system must support this by limiting the time accounts / passwords may be used, including warnings and messages to users to take action. Vendor must also provide the capability for the airport operator to change built-in super administrator and administrator user accounts periodically.
4. **Identification and Authentication** - Vendors must ensure unique identification of individuals, individual activity, or access to the Security Equipment. Vendors should employ multifactor authentication for identification and authentication into the Security Equipment and controlled through the customer/stakeholders' identity management system.

**Secure the Hardware** (Secure physical ports)

1. **Physical and Environment Protection** - Vendors must ensure physical security measures are in place to prohibit unauthorised access to Security Equipment (ensure USB ports are securely covered or disabled, access to ports, cables, and other peripherals are protected from unauthorised use). Physical protection is robust enough to ensure system security and integrity when the equipment is physically unmonitored. This includes all peripherals and workstations encompassing switches and servers.
2. **Personnel Security** - All maintenance personnel either performing work locally or remotely must be vetted by the local or country authority to include appropriate background checks. This applies both to vendors' employees, nominated subcontractors, and any other associated third parties.

**Secure the Network** (Separate the network, Encrypt the network, Restrict network services)

1. **Data at Rest Encryption** - Vendors must ensure that all Data at Rest on the Security Equipment fully utilise an approved encryption method and digital signature. This guarantees confidentiality and integrity of the Data at Rest. This also includes archived images, TIP image libraries and user account information. Vendors must ensure that

encryption method does not negatively impact the performance of the Security Equipment.

2. **Systems and Communications Protections** - Vendors must ensure the system:
    - Adequately manages any internal and external interfaces;
    - Encrypts ingress and egress traffic with industry standard cybersecurity technology;
    - Separates user functionality from physical and logical information system management functionality;
    - Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.
3. **Supply Chain Management** - (Best effort) Vendors must provide a comprehensive list of all software and hardware (Bill of Materials) that comprise a Security Equipment offering. Each item should identify part or component name, manufacturer, supplier and/or integrator (with complete addresses). This includes all peripherals and workstations which encompasses switches and servers.
4. **Vendor Cybersecurity culture** - Vendors must adopt a culture of "cybersecurity by design" for Security Equipment, the vendor should demonstrate how this culture has been achieved. The use of ISO 27001/2013 framework should be considered. Information Technology and Cybersecurity professionals are integral to the continued operations and maintenance and on-going cybersecurity issue remediation with Security Equipment.
5. **Incident Response** - Share your organisation's critical vulnerability response approach in your specification, including but not limited to how would you handle a widespread cyber-incident across multiple airports (e.g. ransomware, emergency security patch)?

The TSA have published these requirements below (except for "Incident Response"):

https://beta.sam.gov/opp/fdc87793ced04442b8a34cd6a913749f/view

## 5.7. Accountability

The accountability for making changes to the devices will be against the Vendor and/or 3rd party provider(s) and not the Airport Operators or Regulators.[25]

Furthermore, concerning changes made to 3rd party algorithms, the Vendors will ensure the system will not breach accreditation/certification/compliance measures stipulated by relevant control authorities. These changes must not affect OEM warranties.

The URL below provides details of all equipment that has met ECAC/EU Common Evaluation Process (CEP) performance standards. The reader is advised that the evaluations made, and the performance standards attributed to each piece of equipment are only valid for the configurations described. The evaluation does not constitute approval or certification by ECAC, this is the responsibility of the European Union or the appropriate authority for aviation security in each ECAC member state.

https://www.ecac-ceac.org/cep

Accountability extends to cover contractual issues that Airport Operators and Regulators may face when adopting Open Architecture, e.g. Staff re-allocation, re-deployment and automated decision making which includes decisions based on 3rd party software.

[25] Each organisation will determine their own position with respect to accountability.

# 6. Proposed Features of Open Architecture for Airport Security Systems

- **Requirements Architecture** - An architecture prepared in accordance with this standard can be tailored for design implementation based on actual system requirements.
- **Critical Interfaces** - An architecture prepared in accordance with this standard shall provide detection, image, security (user access and usage), security incident alerting and system health (condition-based monitoring) functionality and interfaces.
- **Service Interfaces** - An architecture prepared in accordance with this standard shall provide non-critical support functions and interfaces such as data access, training and simulation.
- **Resource Control** - An architecture prepared in accordance with this standard shall provide for control of system resources used for control and information processing by system services software as requested by application software through a standard interface.
- **Commonality** - The architecture shall be comprised of common hardware and software components to the maximum extent possible[26]. Non-common components or non-standard interfaces shall require a waiver from the working group/responsible authority (ACI EUROPE will chair this body and act as the custodian).
- **Interface Standardisation** - An architecture prepared in accordance with this standard shall provide standard interfaces and allow user definable interfaces where no standards exist or are not applicable. Where such an architecture incorporates implementation specific[27] components these must be justified and well documented, this also applies to any layers of abstraction. Should interface profiles be implemented, these must be understood by all parties to refer to a set of one (or more) interface standards defining specific subsets (and potentially extensions) of these standards.

  Compliance with the same interfaces or interface profiles promotes:

  1. Intraoperability between two system-internal components, and;
  2. Interoperability between a system-internal component and an external system.

  Any use of proprietary or vendor-specific profiles should only be used where necessary and be justified, abstracted and well documented. If for any reason, the Vendor is unable to provide an open standard for connectivity, integration or availability of a service they must ensure this can be achieved via a layer of abstraction.

  Interfaces between hardware[28] and other hardware entities shall be based on publicly accepted and open standards[29]. Interfaces between hardware and software shall be based on standards. Interfaces between system services software and applications software shall be based on standards. Interfaces prohibited in an architecture compliant with this standard shall include:

  - Direct, non-service task to task communications;
  - Applications to applications direct information exchanges, which bypass use of system services;
  - These interfaces will be provided in the form of APIs as indicated in section 5.3.

[26] Common and non-common components will be defined during the writing of the specifications.

[27] Specific in relation to the Airport Operator or Regulator

[28] Hardware in this context refers to the devices in Table 1

[29] These standards will be identified and if necessary, developed during the writing of the specifications

- **Modularity** - An architecture prepared in accordance with this standard shall be modular. The modularity of such an architecture is dependent upon the degree to which it consists of components with the following properties:
    - Architecture-level (individual components are themselves architecture-level sub-systems);
    - Single abstraction - this is the principle of having at most a single layer of abstraction between two interfaces;
    - High cohesion - this is the relationship within each component;
    - Low coupling - this is the relationship between components;
    - High encapsulation - such that access to a component is limited.

    The degree of modularity will be determined when writing the detailed specifications.

- **Interoperability** - An architecture prepared in accordance with this standard shall support interoperability by providing standard interfaces between multiple systems:
    - No longer a single manufacturer environment, multiple manufacturers each with a solution – customers want “best of breed”;
    - Shift to IP networks, IT demands “plug and secure”[30];
    - Rapid technology growth, multiple devices and ultimately IoT connectivity;
    - Volatility of security equipment market, acquisitions result in competition and support issues;
    - True Open Architectures provide:
        - Forward and limited backward compatibility[31];
        - Freedom of choice;
        - Reliable interoperability;
        - Proactive management;
- **Cyber resilience** - an architecture prepared in accordance with this standard shall implement Secure by Design principles, the Zero Trust Model and aim to be cyber resilient.

The following diagram provides a high-level logical view of Open Architecture.

[30] Refer to secure devices, e.g. certificates

[31] Backwards compatibility must be limited to ensure that out-of-date and unsupportable hardware, software and operating systems is refreshed with supportable equivalents that are compliant with all other requirements

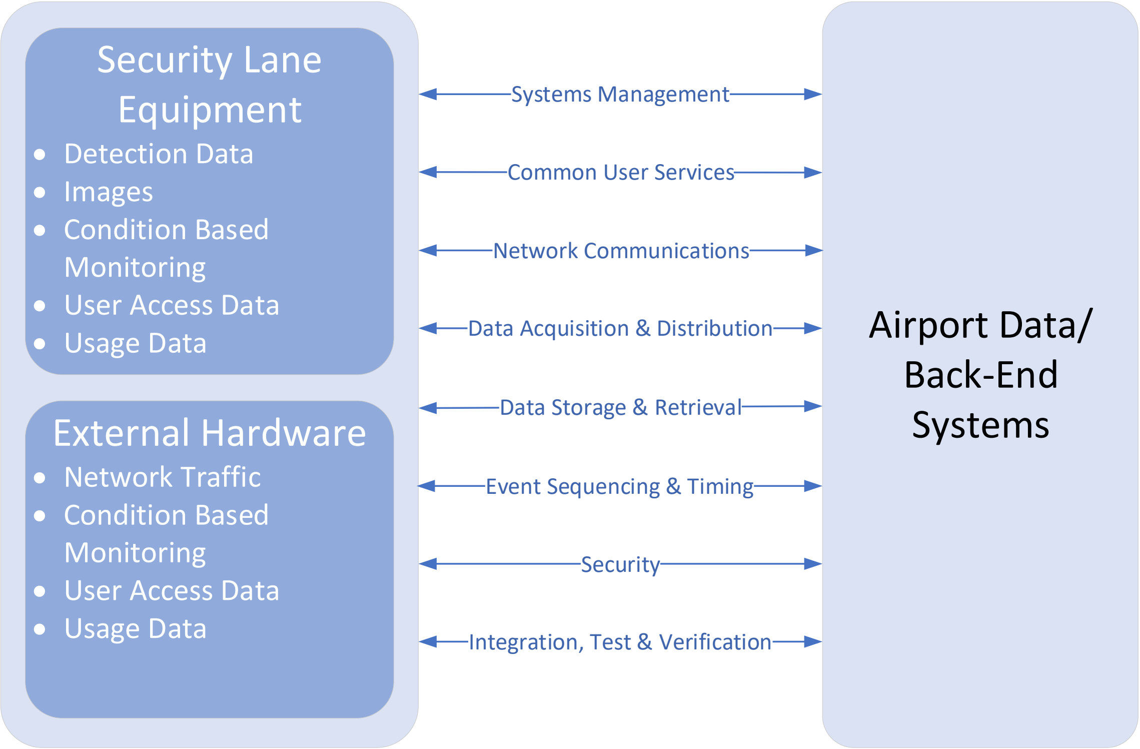


*Figure 2 - Proposed high level features of Security Equipment Open Architecture*

Successful adoption of Open Architecture for Security Systems will require a regulatory certification process to be in place to support, for example the running of a particular algorithm in a particular system environment. This process needs to be defined with boundaries and limitations documented.[32]

The certification process(es) must verify that the cybersecurity requirements within this document have been met to ensure the continued secure operation of the security equipment.

[32] Refer to footnote 10 on page 7

# Annex A Examples of Open Architectures in Other Industries

Before writing the detailed specifications for the Open Architecture for Security Equipment the Vendor is advised to review similar specifications in other industries. Examples are given below, along with URLs where appropriate:

- **DICOM** - Imaging standard for medical CT scanners (DICOS evolved from this);
- **FACE** - The Open Group Future Airborne Capability Environment Consortium is a government and industry partnership to define an open avionics environment for all military airborne platform types. The FACE Consortium is a vendor-neutral forum that provides standardized approaches for using open standards with avionics systems;

  https://www.opengroup.org/face

  https://www.adacore.com/industries/defense/face

  https://publications.opengroup.org/c17c

  https://www.curtisswrightds.com/technologies/open-architecture/face.html

  https://en.wikipedia.org/wiki/Future_Airborne_Capability_Environment

  https://upload.wikimedia.org/wikipedia/commons/b/be/FACE_Reference_Architecture.png

  https://astronautics.com/technology/aerospace/

  https://dl.acm.org/doi/abs/10.1145/3092893.3092897

  FACE is designed to:

  - Standardise approaches and process models within the Astronautics systems;
  - Lower implementation costs of future applications in Astronautics FACE conformant systems;
  - Conform to standards that support a robust architecture and quality software;
  - Define interoperability within FACE systems and components;
  - Develop portable applications across multiple FACE systems;
  - Select FACE conforming ARINC-653 RTOS products.

  The above bullet points are very similar to the desired features of Open Architecture for Airport Security Systems.

- **NIST Enterprise Architecture** - Relates an enterprise's business, information and technology environments.

  https://www.nist.gov/publications/architecture-semantic-enterprise-application-integration-standards

  https://www.gao.gov/assets/590/588407.pdf

  Each layer in this model covers a specific area:

  - Business Architecture level: This level can picture the total or a subunit of any corporation, which are in contact with external organisations;
  - Information architecture level: This level specifies types of content, presentation forms, and format of the information required;
  - Information systems architecture level: Specifications for automated and procedure-oriented information systems;

- Data Architecture level: Framework for maintenance, access and use of data, with data dictionary and other naming conventions;
- Data Delivery Systems level: Technical implementation level of software, hardware, and communications that support the data architecture.

https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=821656

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

- **ACRIS** - A standard for information and data exchange across commercial aviation. Aspects of this may be re-usable.

  https://aci.aero/about-aci/priorities/airport-it/acris/

- **OSA** - Developed by the US Navy this supports modular, interoperable systems which support component addition, modification, or replacement by different vendors throughout the lifecycle, driving opportunities for enhanced competition and innovation. OSA is composed of five fundamental principles:
  1. Modular designs based on standards, with loose coupling and high cohesion, that allow for independent acquisition of system components;
  2. Enterprise investment strategies, based on collaboration and trust, that maximize reuse of proven hardware system designs and ensure we spend the least to get the best;
  3. Transformation of the life cycle sustainment strategies for software intensive systems through proven technology insertion and software product upgrade techniques;
  4. Dramatically lower development risk through transparency of system designs, continuous design disclosure, and Government, academia, and industry peer reviews;
  5. Strategic use of data rights to ensure a level competitive playing field and access to alternative solutions and sources, across the life cycle.

  https://www.navy.mil/navydata/fact_display.asp?cid=2100&tid=450&ct=2

  https://dl.acm.org/doi/abs/10.1145/3092893.3092897

- **Avionics and Aerospace Computer Systems Open Architecture** proposals

  https://www.defensedaily.com/collins-wants-bring-open-architecture-military-avionics/air-force/

  https://www.aviationtoday.com/2018/09/11/can-open-architecture-model-enable-plug-fly-avionics/

  https://ieeexplore.ieee.org/abstract/document/282135/metrics#metrics

  http://mil-embedded.com/articles/open-architecture-role-in-avionics-and-electronic-warfare-designs/

- **IOA** - whitepaper discussing the benefits of an Interoperable Open Architecture over an Open Architecture

  https://www.rti.com/ioa-wp

- **Open Banking** - numerous examples have been designed to bring more competition and innovation to financial services.

  https://github.com/OpenBankProject/OBP-API/wiki/Open-Bank-Project-Architecture

  https://www.openbankproject.com/

https://www.forgerock.com/industries/financial-services/open-banking/UK-Spec

- **Rail Industry**

  https://www.railwaygazette.com/europe/sbb-joins-openetcs-foundation/48098.article

  https://catalogues.rssb.co.uk/library/research-development-and-innovation/research-brief-T912.pdf

# Annex B Organisations supporting, endorsing or contributing to this document

The definition of Open Architecture for Security Equipment has been an international collaborative effort and was initiated by Avinor.

The following table lists all those organisations and people who have contributed or support this document.

| Organisation | Contributors |
|---|---|
| Avinor* | John Christian Paulshus<br>Ole Folkestad |
| Heathrow* | Eugene Kramer<br>Dr Richard Dempers<br>Paul Evans<br>Russell Watkinson<br>Dan Haines<br>David Kitchen<br>Daniel Ginn |
| TSA* | Russell Roberts<br>Paul Morris<br>Jeff Quinones |
| Schiphol* | Marc Reitman<br>Wil Weterings |
| ADP | Eric Vautier |
| CATSA* | Denis Perron |
| MAG | Alcus Erasmus |
| Geneva* | Charles Badjaksezian |
| ACI EUROPE* | David Ryder<br>Jérôme Morandière<br>Daiga Dege |
| Dublin | Dave Weir |
| Birmingham | Wayne Smith<br>Sarah Kent |
| UK CAA* | Dr Ben Wong<br>Nicky Keeley<br>Sabrina Brookfield |
| DfT* | Dr Ben Jones<br>Anthony Parker<br>Dr Paul Redfern |
| German Federal Police | Frank Koussen |
| Swedavia* | Thorbjorn Henningsson |
| Copenhagen Airports A/S* | Brian Cilinder-Hansen |
| AVSEC New Zealand* | Ben Smith<br>Andrew Jones |
| Munich Airport | Mandy Drohm<br>Robert Goetze |
| Dubai Airports | Buti Qurwash<br>Georgios Makrogiorgos |
| Changi Airport | Alan Tan |

*Table 2 - List of contributors and partners involved in defining Open Architecture for Airport Security Equipment (* comments and feedback received in person or via email)*

# Annex C Non-Functional Data Attributes and Data Definitions

| Data Quality Attribute | Definition | Example questions | Trend required for zero defects |
|---|---|---|---|
| Timeliness/ latency | The elapsed time from the business event occurring to when the processing system is notified of the state update | How soon are material changes communicated? Is good data available during the Airport Operator's (and Regulator's) planning windows? | As soon as new information becomes available, the dissemination to all interested parties shall be notified immediately, without batching delay |
| Accuracy of forecast | The measured error between an estimated value at a pre-determined interval prior to the business event occurring, and the known fact of the value that occurred. | What "actuals" were output and at which time windows were estimates most reliably predicting the correct outcome (e.g. missed TIP images, operator performance?) | Data feeds that are statistically no better than static schedules shall never be used. Demonstrating increasing certainty before system implementation through Proof-of-Value demonstration is expected prior to G3 implementation, and ongoing monitoring through-life is mandatory |
| Stability | The number of changes that are applied to a value over its lifetime | What is the frequency of change, is there any jitter? (small updates)<br>Do large changes get notified too late to allow teams to re-assign to other useful tasks? | Spurious or minor data changes are a distraction, and require defensive coding to detect and clean for consumption by users; minimising unnecessary noise must be demonstrated and show required trending over time |
| Precision | The refinement in a measurement, calculation, or specification, especially as represented by the number of digits given. This covers data representing actual events and can be used to prove that a log event is related to the correct event in the physical world | Are schedule times in 5 minute increments? | Raw data should be retained to avoid downstream "rounding" losing fidelity and missing undiscovered insight |
| Reference timestamps | The computer-generated logging of events as they are ingested by systems, processed to give new insight and notified to downstream systems | Are all system-generated event timestamps referenced to UTC? | Millisecond accuracy to UTC as per SQL server/UNIX capabilities is essential. Data scientists must not spend inordinate time identifying and correcting clock-drift in data sources. |

| Data Quality Attribute | Definition | Example questions | Trend required for zero defects |
|---|---|---|---|
| Completeness/ Compliance | The adherence to interface specification of all data items expected that conform to semantic and syntactic checks | Are all data items expected present? Are the fields populated in accordance with compatibility/interoperability standards?<br>Is the expected data fully qualified in accordance with a schema?<br>Is data integrity checking performed? | Data that is missing or incomplete must be logged and problem-reported and not discarded. The trend shall be that all data received is industry schema-compliant (e.g. ACRIS) and capable of being processed |
| Coverage | The data set boundary of known inclusions and explicit exclusions. | Are all security operators included in the reports? What time period does the data cover? | Reducing the number of interfaces removes complex rule processing required when “gap-filling”. Data feeds shall provide maximum coverage, and where possible, re-contracting shall reduce the number of discrete reference sources |
| Correctness | The measured rate of error-free delivery over a given sample window | Are there credible errors in the data that require manual correction by operators? | The trend shall be towards zero repeat Problem Reports generated by service desk relating to data errors |
| Availability | The capability to interrogate the data at given times of published serviceability | Are the feeds architected for high availability service, backed by a service level commitment?<br>When will the service be unavailable due to planned maintenance? | Internet-only data driven organisations now trend towards zero-downtime, with continuous integration and deployment methods allowing non-stop services with no maintenance windows. |
| Reliability | The likelihood that the data set is available at published times expressed as a percentage over a given timeframe. | Are there any system issues that cause unplanned downtime?<br>Are all potential failure modes understood and either acceptable or mitigated? | Trend towards 100% uptime; aviation is a complex system-of-systems and any weakness in data chains results in a multiplier effect that means disrupted journeys for some or all passengers |
| Confidentiality | The potential for the data to cause harm, loss of business, reputational damage or incur payment of fines for deliberate or inadvertent release to unauthorised actors. | Are there any special considerations with the data that would require special handling? Any Personally Identifiable Information?<br>Any licence restrictions for downstream use?<br>Any potential use of the data for anti-competitive practices? | Full audit logs of downstream consumption by systems and users will provide assurance that confidentiality obligations are respected |
| Veracity/ Lineage | The confidence that users can place in data that can avoid the need for cross-checking or validation through triangulation as origination and tamper resistance measures are engineered into the systems. | How certain is it possible to be that the information is from the credible source claimed?<br>Has the originator maintained an adequate cyber-security regime to prevent subversion?<br>Is the data item calculated? If so, how? | Digitally signed data fields with certificates attributed to originators from credible certificate authorities can provide technical reassurance where mission-critical decisions could be being made<br>Frequent 3rd party audits shall reveal any vulnerabilities left unaddressed<br>Inherited precision offsets must be captured and understood |

| Data Quality Attribute | Definition | Example questions | Trend required for zero defects |
|---|---|---|---|
| Longevity/ Expiry | The useful lifetime of the data and any limitations on when the data should no longer be used for real-time operations or post operation analysis | How useful is the data after receiving? How long should it be retained? Is there a legal maximum retention period, e.g. DfT regulations for TIP. | Data shall be retained as long as is allowed, and all data categorised with an expiration timeframe that informs real-time user or data scientist alike |
| Calibration or correction factor source | The reference source of known accuracy used in setting up the data-producing device | Is the data item referenced as absolute or relative?<br>When was the device last calibrated? | Identifying the datum or yardstick used ensures maximum transparency |
| Commercial | The business considerations of cost of ownership, value, sales revenue, risk avoidance, regulatory compliance etc. | Are costs of acquisition, storage, data feed monitoring and management understood?<br>Does the nominated business owner know the impact if data is unavailable? | Traceability of cost/value stream is essential to ensure correct prime P&L, cross-charges are agreed or overhead allocation set. |
| Changelog | The history of when the data item was updated, detailing the authorised updater, and with a reason for the update | Are all updates logged and traced back to an originator?<br>Can authorised and authenticated user updates be back-traced for audit?<br>Are logs uneditable and immutable? | Changelogs shall inform all users of provenance |
| Integrity | The validity of data across the relationships to ensure that all data in a database can be traced and connected to other data. | Ask yourself: Is there are any data missing important relationship linkages?<br>For example, in a customer database, there should be a valid customer, addresses and relationship between them. If there is an address relationship data without a customer then that data is not valid and is considered an orphaned record. | The ability to link related records together reduces the risk of duplicate records across systems, or perpetuation of siloed and unexposed/undocumented business processes |
| Consistency | A measure of the degree to which a valid value in a field or column is consistent with valid values in other fields, columns, tables or data sets. | Are the data values consistent with an expected derivation of a realistic and achievable outcome? | Avoiding un-credible corruption of data (e.g. unachievable turnaround times) means that derived metrics and business decisions can be made with greater confidence |
| Redundancy | The extent to which the data item appears to be mastered from many diverse source systems | If the data item master system is unavailable, can the same data be sourced from a secondary provider or system? | Supplier redundancy can ensure that unacceptable reliability challenges can be addressed. This approach should be used with caution, as complexity to de-duplicate or re-synchronise is likely to be introduced. |

| Data Quality Attribute | Definition | Example questions | Trend required for zero defects |
|---|---|---|---|
| Stewardship | The ability to pinpoint a business area and appointed data steward for the data item | Who is the prime business user of the data item?<br>Which business processes are impacted if the data item is corrupted, lost or unavailable? (integrity, confidentiality, availability) | No data items are orphaned nor are there multiple “owners” claiming responsibility |

*Table 3 - Illustration of non-functional data attributes, definitions and example questions*

# Annex D OSI Model

| Layer | Description |
|---|---|
| 1 | Connection to the transmission medium, handling the transmission and reception of raw bits across the medium. |
| 2 | Interface between the OSI hardware and software layers. |
| 3 | Software layer that accepts packets of data from the transport layer (software) and routes them to their destination over all necessary links and immediate systems as necessary. |
| 4 | Software layer that provides reliable data flow between a sender and a receiver while relieving these entities of the need for detailed knowledge of the actual transport mechanism. |
| 5 | Software layer that establishes communications paths between systems and terminates them upon completion of transmissions. |
| 6 | Software layer that performs translation functions to convert messages from native format(s) to international standard format(s) for transmission and from international format(s) to native format(s) upon receipt. The international format is a transfer syntax, a set of rules for data representation while in transit between two entities. The translation is performed by network services on network data only and not application data. |
| 7 | Interface between the application software and the network. |

*Table 4 - OSI Model*[33]

[33] https://www.iso.org/standard/18824.html

# Annex E Example ToE model[34]

The example presented below represents airport security equipment comprising an X-ray machine and ATRS. This methodology comprises 4 steps as summarised below:

| | | |
|---|---|---|
| 1 | Identification of critical information assets processed by the system | Target of Evaluation characterisation |
| 2 | Description of the system's characteristics | |
| 3 | Inventory of applicable threats | Threats and Security Controls |
| 4 | Deduction of applicable security controls | |

*Table 5 - Steps comprising the ISDP concept (the proposed security controls will be based on ISO27002:2103)*

Following this approach and considering appropriate security controls, description of information assets to be processed, threat agents and technical (and non-technical) problems allows the construction of a graphical representation of the ToE and associated data flows. An example of this is shown below.

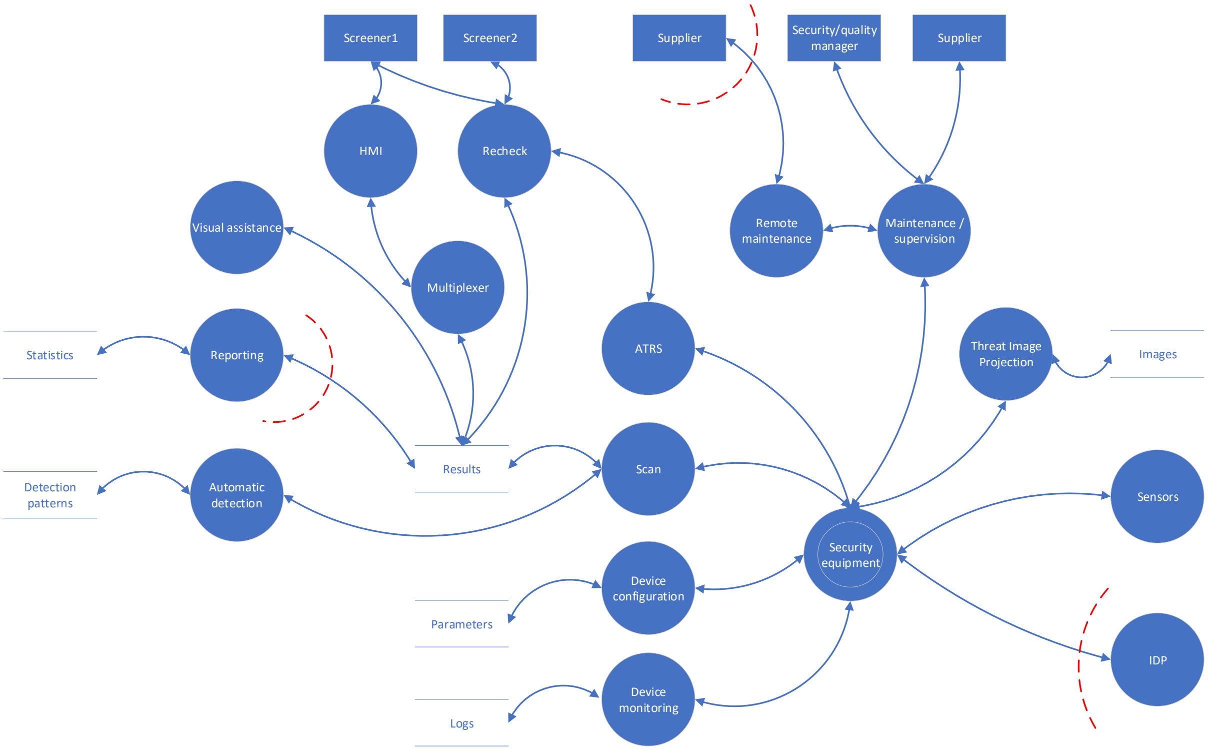


*Figure 3 - Graphical representation of ToE for an X-ray machine and ATRS*

The components of the ToE in Figure 3 are listed below.

[34] Further details on ISDP and ToE analysis and design can be found in Geneva Airport's ISDP Concept document

| Component | Description |
|---|---|
| ATRS | The Automatic Tray Return System (ATRS) manages the flow of trays, whose content is scanned by the security equipment. Its proper functioning is necessary to guarantee the throughput of the screening process. It is also in charge of isolating items for which the automatic detection process has raised an alert. Its accidental or intentional disruption may therefore impact the whole threat identification process |
| Automatic detection | This component analyses the scans generated by the security equipment for automatic threat detection (Diagnostic Aid), based on detection patterns. Altering those patterns or the algorithm performing the analysis may result in false negatives (impact on people’s security) or false positives (impact on productivity) |
| Device configuration | This component enables the parametrization of the security equipment. Modifying the parameters may alter the efficiency of the equipment, or even lead to denial of service |
| Device monitoring | This component is in charge of collecting logs of relevant events affecting the security equipment. The integrity and availability of those logs is paramount for traceability and investigation purposes |
| HMI | Human-Machine Interface, allowing the interaction of users with the security equipment |
| IDP | The IDP (Identity Provider) is in charge of managing the Authentication, Authorisation and Accounting (AAA) processes relating to the identities, which interact with the security equipment. Its compromising may lead to identity spoofing and unauthorised access |
| Maintenance/supervision | Maintenance and supervision operations performed by the suppliers on the security equipment. This process is performed using elevated privileges on the equipment’s software components, which makes it a valuable entry point for a malicious actor |
| Multiplexer | The multiplexer allows scan results from multiple sources to be analysed from a central location. It constitutes a potential target for an attacker to alter scan results |
| Recheck | The process allows an item, which has been flagged as suspicious, to be authenticated and isolated for physical control by a screener |
| Remote maintenance | Process allowing the remote maintenance of the security equipment by the suppliers |
| Reporting | This process consists in generating statistics linked to the operation of the security equipment |
| Security equipment | The hardware and software allowing to interconnect all the modules that constitutes the security equipment |
| Sensors | All the hardware sensors in charge of the accurate production of scans (X-ray sensors, ATRS sensors, etc.) |

# Annex F Example Open Architecture Controls

Open Security Architecture provide example controls, these cover such areas as Access Control Policy and Procedure, Account Management, Access Enforcement, Information Flow Enforcement and Use of External Information Systems. The full list of controls, together with a brief description of each is available at the following URL:

http://www.opensecurityarchitecture.org/cms/library/0802control-catalogue/255-13-05-all-controls

# Annex G Cabin Screening Data Requirements

These requirements align closely with the data required to assess X-ray machines and ATRS for compliance with the DfT's 3PI approach. Note these cabin baggage screening data requirements can be adapted to Hold Baggage Systems (HBS) data requirements.

The associated requirements for the logging and secure storage of data will be covered in the detailed specifications and will be dependent on local regulations. The Cybersecurity Requirements described in section 5.6.1 will be applied.

| **Before Trigger:** | **What do you want to know about the tray before it begins the process?** |
|---|---|
| | What is the equipment ID (lane/EDS) |

| **During the Processing:** | **What do you want to know about the tray through the process?** |
|---|---|
| | Why did the tray route to the search lane? - Output from the system and the level because they are unclear.<br>Which terminal is the tray being screened?<br>What time did the tray exit the EDS?<br>What time did the tray enter the EDS?<br>What time did the machine make a decision?<br>What time did the image arrive at an operator workstation?<br>What time did the operator make their decision?<br>Which workstation was the tray presented to?<br>Which operator viewed and made a decision on the image?<br>What time did the tray arrive at each decision point?<br>What was the status of the tray at each decision point? (Clear, reject, pending, mis-track, etc)<br>Was the tray scanned successfully / image created? (tray not analysed, tray chopped, etc)<br>How far behind / in front is the next / previous tray?<br>Did the tray successfully track through the EDS?<br>How many threats were in the tray?<br>How many operators where online at the time of screening?<br>What was the trayID received by the EDS?<br>What was the TrayID when RFID'ed? At exit and entry<br>What was the TrayID received by the EDS? |

| **During the Processing:** | **What do you want to know about the tray through the process?** |
|---|---|
| | How are results handled that are out of range, e.g. A tray spacing diagnostic that alerts when the tray spacing has changed or an alert when a change is detected in an algorithm's integrity?<br>What was the result of recal (found/not found /error /etc)?<br>What was the decision on exit of the EDS?<br>What was the final decision from the EDS?<br>Did the tray stop whilst in the screening process?  If so, what points and for how long?<br>How long is the tray measured by the EDS?<br>How many times has a tray been cycled?<br>If timeout, what level did it reach<br>What time was the image recalled at Remote Work/Analyst Station (RWS)?<br>What was the RFID of tray at RWS?<br>How long was the image on the RWS?<br>Who recalled the image at the RWS?<br>What was the location of RWS?<br>What time was the tray divert to the High Threat Alarm/Alert (HTA)?<br>What time was the overhead photo taken?<br>What time was the door opened on HTA?<br>What time was the HTA reset?<br>What was the RWS decision?<br>What was the RWS decision time?<br>What was status of the tray at re-input? (Empty, not empty?)<br>What time of each status of the tray?<br>Was a tray removed or lost?<br>What time did an operator log-in / log-out?<br>Which work-station did the operator log-in to?<br>What time was a TIP image sent to a work-station?<br>What was the TIP decision?<br>What are the TIP settings? |

| **During the Processing:** | **What do you want to know about the tray through the process?** |
|---|---|
| | What TIP category was sent to the screener?<br>What time was an aborted TIP sent to the screener?<br>Is the full TIP data analysis available as a set of data fields which can be easily exported (e.g. CSV format)? |

| **After Processing:** | **What do you want to know about the tray after completing the process?** |
|---|---|
| | How long was the tray in the Screening process? |

| **X-ray machine:** | **What do you want to know about the X-ray machine?** |
|---|---|
| | What state is it in?  (fault, start-up, ready, etc)<br>What time did the state change?<br>What was the time of each sensor state change?<br>What was the time of each motor state change?<br>What was the time of tray insertion?<br>What state in the EDS in?<br>What time did the EDS go into fault?<br>What is the error code of the EDS fault?<br>What time was an e-stop pressed?<br>What e-stop was pressed?<br>What is the comms status of all devices?<br>What time did the X-rays change state?<br>The image for each tray |

| **Lane:** | **What do you want to know about the Lane?** |
|---|---|
| | What state is it in?  (fault, start-up, ready, etc)<br>What time did the state change?<br>What was the time of each sensor state change?<br>What was the time of each motor state change?<br>Where was the tray inserted?  Which input? |

| **Lane:** | **What do you want to know about the Lane?** |
|---|---|
| | What was the time of tray insertion?<br>What state in the lane in?<br>What time did the lane go into fault?<br>What is the error code of the lane fault?<br>What time was an e-stop pressed?<br>What e-stop was pressed?<br>What is the comms status of all devices? |

# Glossary

| Term | Definition |
|---|---|
| 3DS | Data Driven Differentiated Screening (DfT programme) |
| ACI | Airports Council International |
| ACRIS | Aviation Community Recommended Information Services |
| ADP | Groupe ADP (formerly Aéroports de Paris) |
| AIT | Advanced Imaging Technology (US terminology for Security Scanners) |
| AODB | Airport Operational Data Base |
| API | Application Programming Interface(s) |
| ASL | Automatic Screening Lanes (US terminology for ATRS) |
| ATRS | Automated Tray Return Systems |
| Avinor | Avinor AS, state-owned limited company operating most of the civil airports in Norway |
| CDI | Corrected Data Interface |
| CATSA | Canadian Air Transport Security Authority |
| CEP | Common Evaluation Process (of Security) - laboratory testing of security equipment against EU/ECAC performance standards |
| CSV | Comma Separated Variable (file format) |
| CT | Computed Tomography |
| DfT | Department for Transport (UK Government department) |
| DICOM | Digital Imaging and COmmunications in Medicine |
| DICOS | Digital Imaging and COmmunications in Security |
| ECAC | European Civil Aviation Conference |
| EDS | Explosive Detection Systems |
| ETD | Explosive Trace Detection |
| EU | European Union |
| FACE | Future Airborne Capability Environment |
| HBS | Hold Baggage Systems |
| IDI | Inspection Data Interface |
| IIoT | Industrial Internet of Things |
| IOA | Interoperable Open Architecture |
| IOD | Information Object Definitions (DICOS component) |
| IP | Intellectual Property |
| ISDP | Information Security and Data Privacy |
| KPI | Key Performance Indicator |
| LEDS | Liquid Explosive Detection Systems |
| MAG | Manchester Airports Group |
| MTA | Maintenance Ticketing Application |
| MQTT | MQ Telemetry Transport (an open standard lightweight, publish-subscribe network protocol that transports messages between devices) |
| NII | Non-Intrusive Imaging |
| NIST | National Institute of Standards and Technology |
| OAuth | Open standard for access delegation, commonly used to grant applications access to their information on other systems without giving them the passwords |

| | |
|---|---|
| OEM | Original Equipment Manufacturer |
| OPSL | Open Platform Software Library |
| OSA | Open Systems Architecture |
| OSI | Open Systems Interconnect |
| PLC | Programmable Logic Controller |
| RBAC | Role Based Access Control |
| RMM | Remote Monitoring and Maintenance |
| SAML | Security Assertion Mark-up Language |
| SCADA | Supervisory Control and Data Acquisition |
| SED | Shoe Explosive Detection |
| SIEM | Security Information and Event Monitoring |
| SMD | Shoe Metal Detection |
| SOC | Security Operations Centre |
| SNMP | Simple Network Management Protocol |
| SSO | Single Sign-On |
| TDI | Transformed Data Interface |
| TIP | Threat Image Projection |
| ToE | Target of Evaluation (systems in scope for ISDP analysis) |
| TSA | (the) Transportation Security Administration (agency of the U.S. Department of Homeland Security) |
| TTF | Technical Task Force (run by ECAC) |
| UFF | Universal File Format |
| UI | User Interface |
| USB | Universal Serial Bus |
| VPN | Virtual Private Network |
| WTMD | Walk Through Metal Detector (sometimes referred to as a AMD, Archway Metal Detector) |