EOS POSITION PAPER ON OPEN ARCHITECTURE FOR SECURITY SCREENING SYSTEMS

IN BRIEF

EOS security screening technology manufacturers recognise the important role that open architecture (OA) will play in the future evolution of security screening systems and have been actively engaged in identifying the requirements and technical standards needed to facilitate OA. We urge regulators and interested stakeholders to continue collaborative efforts to create an effective, compliant, and secure framework for OA and facilitate further innovation in security screening, including a more efficient approval process for new technologies and capabilities.

EOS & Open Architecture

Open architecture provides one way to deliver the security screening innovations and process improvements needed for security screening. OA requires a clear framework for implementation that is effective, compliant, and secure. Manufacturers from the European Organisation for Security (EOS) have dedicated several years to working with airports, regulators, and other aviation industry stakeholders to highlight the potential for OA for security screening and define the requirements and technical standards for its implementation. Alongside ACI-Europe and other stakeholders, EOS manufacturers contributed to the joint OA Working Group, and delivered solutions to the challenges being addressed in its three workstreams. These include:

✓ Technical Workstream

The technical workstream was set up to review the standards for interfacing and data required to be shared through open architecture. EOS manufacturers fully support the definition of standards that are open and can be freely implemented in any system architecture or software ecosystem. This workstream will continue to work on technical requirements as OA evolves.

✓ Certification, Classified Information and Cyber security Workstream

This workstream identified the issues to be addressed to test, evaluate and approve systems of systems that meet security and detection performance standards. One of its key outcomes was that a single organisation or entity should accept responsibility for issues such as data ownership (including funding its generation), protection of classified information, configuration management, ensuring cyber security solutions, etc. and have clear contractual responsibilities. Further engagement with regulators and testing houses is foreseen to adapt approvals processes and methodologies to accommodate more complex OA system configurations.

✓ Commercial Liability and Intellectual Property workstream

This workstream identifies potential challenges to OA aviation security systems of systems, and proposes solutions to how they may be resolved. These challenges include liability, safety, the meeting of key performance indicators, and the protection of individual suppliers' intellectual property, which could potentially hinder or stop OA deployments. However, stakeholder discussions during workstream meetings over the past two years have shown that many of these problems can be circumvented if a prime integrator takes responsibility for the entire system.

The OA initiative for security screening is in the early stages of being translated into a framework, which has agreed technical specifications and commercial arrangements. The supplier and user communities are working together to rapidly complete this framework and enable the design of solutions that deliver the promise of OA. Until this work is complete, OA based solutions will likely be proof of concepts to test this framework and ensure reliable, secure, and compliant solutions are available.

Future Commitment to OA

The results of current OA efforts are emerging in a joint paper with ACI-E and other stakeholders that defines OA in the context of security equipment. The successful rollout of OA requires backing from regulators, airports, manufacturers and third-party developers to provide the foundation for an effective, compliant, and secure framework for OA in aviation security screening. EOS manufacturers encourage all stakeholders to:

1. Develop, collaboratively and in good faith, mutually agreeable, open standards for OA for security screening technology that can be implemented uniformly across all equipment.
2. Implement detailed specifications for OA for images, threat data, metadata, system status, interfaces and protocols, etc. to allow data to be transmitted and shared securely
3. Support the generation and implementation of guidelines for issues and topics such as user administration, algorithm use, machine control and monitoring, cybersecurity, ownership of data, and importantly to understand and recognise where accountability resides in the chain of implementation.
4. Identify workable approvals processes and methodologies to accommodate more complex OA system configurations
5. Endeavour to respond to the challenges ahead and respect the investment to-date and intellectual property of each party, as the joint development of OA architectures are implemented across the industry.

EOS Contact Point

Lorraine Wilkinson
EOS Security Screening and Detection Technology Working Group Coordinator
E-mail: Lorraine.Wilkinson@eos-eu.com