# Secure Video Streaming for the Aviation Industry

## The Brief

Linaro has deep knowledge and long-established expertise in security consultancy in the Arm ecosystem. This expertise covers TrustZone, secure boot, secure update and DRM enablement for secure video streaming. In this case study, Linaro partnered with industry experts in digital aircraft cabins for an in-seat display (ISD) system to support Google WideVine L1 Certified DRM for secure video streaming in an aviation context.

Linaro worked across the engineering lifecycle for this project from security design, development, through certification consultancy and secure manufacturing process planning. Certification work was carried out for both Google WideVine L1 DRM and FAA/EASA Airworthiness Type Certification. In this use case Linaro leveraged secure-by-design principles to meet the security requirements.

The work was carried out on the customer's specified NXP iMX8 processor and leveraged the security features of that device.

## The Challenges of Secure Boot and Update in an Aviation Context

Secure boot and secure over-the-network update are vital requirements for the latest embedded system deployments. These functions are often implemented in the embedded firmware. In the case of aviation system components, any certified resident firmware forms part of the definition of the component's hardware P/N, and any change to this resident firmware requires a change request to the P/N and triggers a re-certification of the appropriate aviation standards. Hence Linaro needed to:

- identify the smallest secure boot immutable code base as part of hardware P/N for type certification. Ideally the customer doesn't want to lose the capability of mutable boot code upgrading at least CVE updating over its 10 years product lifecycle.
- provide platform root-of-trust of establishing Trusted Execution Environment (TEE) to satisfy WideVine L1 certifiable DRM's mandate.

- run-time system configurability without modifying immutable P/N code.
- Integrate compatibly with existing customer BSP boot flow and updating scheme.

## How Linaro's Expertise Addressed the Challenges

Deep understanding of NXP SoC hardware assistant security technologies, ARM TrustFirmware & secure boot flow and applicable certification requirements, as well as following secure-by-design principles are key factors ensuring project success in the first place.

- Understand the compliance requirements of WideVine L1 DRM certification and EASA/FAA Part-25 P/N qualification process then produce GAP analysis against existing BSP.
- Perform threat model to establish compliant security architecture, identify threat agents and corresponding mitigations for runtime secure streaming services and device provisioning.
- Customize secure boot flow and minimize immutable P/N firmware's SBOM & footprint.
- Follow OSS best practices & design patterns and abstract config parameters (eg. hardware firewall settings) away from business logic to improve P/N firmware's configurability.

## Outcome for the Customer

1. Via secure-by-design principles, the solution complies with applicable requirements defined by WideVine L1 certification and EASA/FAA Part-25 P/N qualification from the starting day of development life cycle.
2. The ISD customized secure boot scheme as part of L1 DRM content protection system passed P/N qualification and WideVine L1 Certification successfully as per project plan.
3. The entire ISD display system and in-cabinet server infrastructure were successfully deployed and EASA type certified on A320 aircraft

## Feature Set at a Glance

- Aircraft in-seat display(ISD) built on NXP iMX processor with secure video streaming H.265 content @ 60fps with 4K screen.
- Updateability and configurability during runtime discovery.
- Customized secure boot flow qualified with FAA/EASA airworthiness "Type Certification"
- Google WideVine L1 certified Linux DRM solution.
- NXP iMX8's HAB4 based secure boot flow to take advantage of accelerated crypto operations
- Seamless integration with customer's existing boot scheme with ease of maintenance and flexibility.
- Two tiers of image packaging and signing scheme, including two tiers of boot authentication keys, providing flexibility of key revocation and reduce attack surface of leaking device root keys.
- Hardware assisted memory protection, secure storage and cryptographic service in TEE

## Working with Linaro

Linaro has some of the world's leading Arm Software experts. This expertise and experience is made available to you for your project. Linaro has specialists in security on Arm, we leverage open source to ensure you benefit from the latest upstream features and security fixes. Linaro hosts and maintains the OP-TEE (Open source Portable TEE) and TrustFirmware for the Arm ecosystem. We support every aspect of product delivery, from building secure board support packages (BSPs), product validation, compliance assessment, secure manufacture planning and long-term maintenance - we help you to grow your business by getting your products to market faster.

Contact Linaro to discuss how we can help you to build, test, deploy and maintain great highly secure products on Arm.

**Get in touch with our experts at linaro.org/contact**

Metadata:

Broad keywords:"Secure video streaming", "secure boot", "WideVine DRM", "WideVine Certification", "Cybersecurity Resilience Act",TEE, TrustZone, Yocto, GStreamer

Platform-specific keywords: "NXP iMX8", "NXP hardware firewall", HAB4

Narrow keywords: "FAA/EASA", "EASA Part-25", "Line replaceable Unit", LRU, "in-seat display", ISD, airworthiness, "type certification", IFE,

Linaro USPs showcased: Security, OP-TEE, TrustFirmware

Lifecycle stages covered: Secure by Design, Develop, Test, Compliance, Secure manufacturing plan, Deployment