

Dear Reviewer

The ESTA Control Protocols Working Group is pleased to present this draft of BSR E1.88 (FENCE) for public review.

You may notice that this document is entering the public review process earlier in its development lifecycle than is typical for ESTA standards. This early release is entirely intentional.

FENCE represents a paradigm shift for our industry. For decades, entertainment control networks have operated on an "Open by Default" perimeter-defense model. Impending global cybersecurity regulations (such as the EU Cyber Resilience Act) and the increasing integration of production networks dictate that our industry must transition to a "Secure by Default" architecture.

Because FENCE fundamentally changes how devices communicate, authenticate, and authorize control data, we want to ensure industry-wide alignment on the core architecture before finalizing the technical subtleties. Your feedback at this stage is critical to ensuring the standard is robust, implementable, and practical for both live production environments and architectural installations.

This document covers the security framework that allows the 'secure pipe' to be setup. Additional documents, defining how DMX style level data is delivered, are in development and will follow soon.

This draft introduces numerous concepts designed to balance state-of-the-art security with the low-latency, high-reliability needs of live entertainment:

- Zero Trust Architecture: Security is bound cryptographically to the data itself at the application layer, rather than relying on network boundaries or VLANs.
- Native Air-Gapped operation: FENCE does not require Internet connectivity to function in a show setting. It is designed to provide full cryptographic security in completely isolated, air-gapped environments.
- IoT Foundations: Rather than inventing bespoke cryptography, FENCE uses modern, highly efficient IETF standards designed for constrained devices, including EDHOC, CoAP, OSCORE, and Group OSCORE.
- Decoupled Trust Models: We have separated Manufacturing Attestation (proving a device is genuine hardware) from Operational Trust (granting a device permission to control Universe 1 on your local network).

The FENCE task group recognizes that the concept of onboarding will be new to many and any additional steps that add to the show setup workflow come at a cost. Onboarding is the process by which all equipment introduced to the network, security checked and allocated its list authorized tasks. We recognize the prospect of managing certificates, passwords, and cryptographic keys on a dark stage at 2:00 AM is daunting.

However, the task group approached FENCE's onboarding process not just as a security requirement, but as an opportunity to modernize system deployment.

FENCE introduces a unified, operator-initiated onboarding workflow relying on Out-of-Band (OOB) credentials, such as scanning a QR code or RFID tag on the device. This "new onboarding thing" is actually designed to make load-in faster and more accurate than it is today.

Imagine a workflow where a technician simply powers on a fixture and scans its QR code with a tablet. Behind the scenes, FENCE automates the rest:

- The device automatically discovers the network's Guardian (the network security manager, and the core of FENCE).
- The Guardian cryptographically verifies it is talking to the exact physical fixture that was scanned.
- The device proves its factory identity.

- The device is instantly issued its access tokens, security groups, and operational scope.
- No typing IP addresses. No default passwords to change. No manually mapping MAC addresses. What was once a tedious, error-prone manual setup becomes an automated, cryptographically secure handshake that simultaneously verifies your hardware inventory and locks down your network.

While some sections of this document are still under construction, the core cryptographic architecture, the onboarding flow, and the data-plane encapsulation are fully defined.

We are asking manufacturers, software developers, system integrators, and network engineers to review this draft with the following questions in mind:

- Does the dual key-pair (Onboarding vs. Identity) factory provisioning model work for your hardware manufacturing pipelines?
- Are the profiles for EDHOC and Group OSCORE clear enough for your engineering teams to begin prototyping?
- Does the Access Token and Authorization Assertion (AA) model provide the right balance of granular control and low-latency performance for responders?

Thank you for your time, your expertise, and your commitment to securing the future of entertainment control. We look forward to your feedback.

Sincerely,

The ESTA Control Protocols Working Group