

Introduction

Verestro Access Control Server (ACS) Overview

The **Verestro Access Control Server (ACS)** is an EMVCo-certified software component located within the **Issuer Domain** of the 3-D Secure ecosystem. It functions as the authoritative system for authenticating cardholders during Card-Not-Present (CNP) transactions.

As a fully managed SaaS solution, the Verestro ACS processes authentication requests (AReq) from the Directory Server (DS) and 3DS Server, applies risk logic, and returns the appropriate authentication response (ARes) to the acquirer.

Technical Scope & Functionality

The ACS is responsible for the complete lifecycle of a 3-D Secure transaction on the issuer side. Its primary technical functions include:

- **Protocol Version Negotiation:** Automatically determines the highest common version of the EMV 3-D Secure protocol (2.1.0, 2.2.0, 2.3.1) supported by both the issuer and the merchant's 3DS Server.
- **Card Eligibility Validation:** Queries the card range and BIN configurations to confirm if a specific PAN is enrolled in the 3-D Secure program.
- **Device Info Analysis:** Ingests device telemetry and browser data to determine if the consumer's endpoint (User Interface) supports the required security method.
- **Risk-Based Authentication (RBA):** Evaluates transaction data against a configured rule set to determine the authentication method (Frictionless vs. Challenge).
- **Challenge Orchestration:** Manages the step-up authentication interface and logic, including OTP generation/validation, Biometric prompts, and Out-of-Band (OOB) verification.

Supported Authentication Flows

The Verestro ACS supports the full range of EMV 3-D Secure transaction flows:

- **Frictionless Flow:** The ACS assesses the transaction risk as low based on historical data and rules. Access is granted without user interaction.
- **Challenge Flow:** The ACS mandates user interaction via a UI Challenge. Supported methods include SMS OTP, Mobile App OOB, and Biometrics.
- **3RI (Three Requestor Initiated):** Asynchronous authentication initiated by the merchant for recurring billing or installments, without active user participation.
- **SPC (Secure Payment Confirmation):** Leveraging FIDO/WebAuthn standards for cryptographically secure authentication via browser-based biometrics.

System Architecture & Integration

The solution is architected as a cloud-native SaaS platform, ensuring high availability and compliance without local infrastructure management.

Rule Engine & Administration

The ACS includes a granular **Rule Engine** allowing administrators to define logic for risk assessment. Authentication decisions are available in the **Admin Panel**, providing detailed audit trails for every transaction (AReq/ARes pairs, Challenge results, and error codes).

Integration Interface

Integration is achieved via the flexible REST APIs or Verestro LC API.

Compliance & Security Standards

The platform is certified and compliant with the following specifications:

- **EMV® 3-D Secure:** Versions 2.2.0 and 2.3.1
- **Security:** PCI-DSS and PCI 3DS Core Security Standard
- **Regulatory:** PSD2 SCA (Strong Customer Authentication) compliant

Revision #1

Created 24 November 2025 16:07:31

Updated 24 November 2025 16:23:02