

What is an ACS in the 3DS Ecosystem?

In today's rapidly evolving digital landscape, online card-not-present (CNP) fraud remains a persistent challenge for financial institutions and merchants alike. **3D Secure** (3DS), particularly its modern iteration, **EMV 3-D Secure** (3DS 2.x), stands as the industry's answer to this threat. This sophisticated security protocol introduces an essential layer of authentication for online credit and debit card transactions, aiming to drastically reduce fraud while simultaneously improving the customer experience.

ACS in the 3DS Ecosystem

The "3D" in 3DS refers to the three interconnected domains:

- Acquirer Domain: Encompassing the merchant and their acquiring bank, which processes card payments.
- Issuer Domain: Representing the cardholder's issuing bank, responsible for the card itself.
- Interoperability Domain: The underlying infrastructure and systems that facilitate seamless communication between the acquirer and issuer during a transaction.

At the heart of the Issuer Domain lies the **Access Control Server** (ACS). This is the technology that Verestro has now secured EMVCo approval for. The ACS is the brain behind the cardholder's authentication experience, operating in real-time to assess transaction risk and, when necessary, challenge the cardholder for verification.

Why Choose the Verestro ACS?

Building and certifying your own ACS can take over a year and cost upwards of €100,000.

Verestro ACS provides a ready-to-use, fully certified solution that eliminates these barriers - offering rapid deployment, reduced costs, and full compliance.

Core functions of Verestro ACS

- Verifying whether a card number is eligible for 3-D Secure authentication
- Determining if the consumer's device type supports 3-D Secure
- Authenticating the cardholder or confirming account information during transactions

Benefits of Verestro ACS

- Enhanced Customer Experience: Offer a fast, intuitive, and secure checkout process - reducing cart abandonment and improving satisfaction.
- Optimized Authentication Performance: Benefit from fast, reliable authentication flows that minimize delays and reduce failed transactions.
- Device-Agnostic Compatibility: Ensure seamless operation across all channels - web, mobile browsers, and mobile apps.
- Frictionless and Low-Friction Authentication: Support risk-based authentication and modern low-friction methods like biometrics, helping reduce step-up challenges.
- Higher Approval Rates with Lower Fraud: Improve authorization rates by up while maintaining high security standards. Reduce fraud on 3DS-enabled transactions compared to non-3DS transactions.
- Regulatory Compliance Made Easy: Stay fully aligned with evolving EMV® 3-D Secure standards and PSD2 SCA requirements - no additional development needed.
- Faster Time-to-Market: Avoid long certification cycles and heavy infrastructure costs.

Key Features

- EMVCo Certified
- SaaS Model: Scalable, reliable, and maintenance-free
- Simple API Integration: Fast time-to-market
- Powerful Admin Panel
 - Browse and review authentication events in detail
 - Manage challenge screens and user flows via a flexible UI builder
 - Define custom rules with a highly configurable Rule Engine
 - Dashboard providing insights and key statistics at a glance

Authentication Flows

Frictionless Flow

- The cardholder is authenticated without any additional input, based on a real-time risk assessment using data such as transaction history, device information, and behavioral analytics.
- *Best for low-risk transactions* – no user disruption.

Challenge Flow

- The cardholder is required to complete a step-up authentication, such as entering a one-time passcode (OTP) or using biometrics.
- Used for higher-risk or non-recognized transactions.

3RI (Three Requestor Initiated)

- Authentication initiated by the merchant or payment service provider without the cardholder actively being involved (e.g., for subscriptions or card-on-file payments).
- Enables secure recurring or delayed transactions.

SPC (Secure Payment Confirmation)

A new flow supported by some browsers (notably in the EU), using WebAuthn and device biometrics to allow strong customer authentication in a streamlined, secure manner.

Combines strong security with an excellent user experience.

Authentication methods

- One-time passcode (OTP) sent via SMS
- Out-of-band verification through a mobile app
- Decoupled authentication
- Biometric authentication
- Other methods supported by EMV® 3-D Secure 2.3.1 and EMV® 3-D Secure 2.2.0

Device Channels

- App-based
- Browser-based

Regulatory Compliance

Verestro ACS is fully compliant with major standards and certifications, including:

- EMV® 3-D Secure 2.3.1
- EMV® 3-D Secure 2.2.0
- PCI-DSS
- PCI 3DS

Verestro is excited to continue empowering the future of payments by providing our clients with the cutting-edge technology - Access Control Server. This milestone reinforces Verestro's position as a trusted innovator, dedicated to making online transactions safer, smarter, and more seamless for everyone. If you are interested in our solution, don't hesitate to [contact us](#).

Revision #1

Created 6 June 2025 09:25:09 by Justyna Mazurek

Updated 6 June 2025 09:51:50 by Justyna Mazurek