



FSS Secure3D

Win Customer Trust With
Adaptive Authentication

Need for Intelligent Authentication

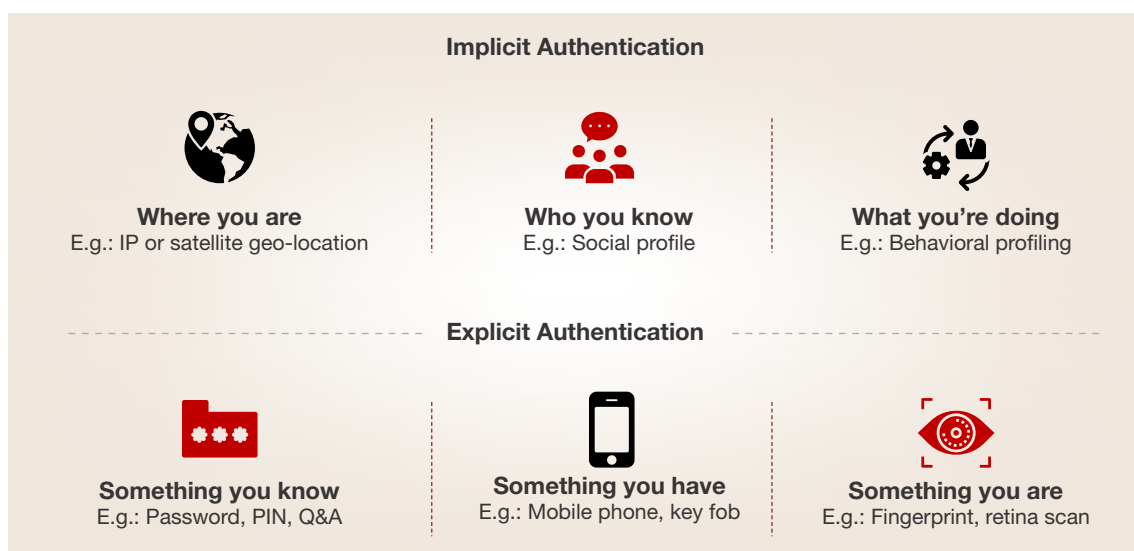
Poorly designed authentication experiences to counter fraud have an adverse impact on customer engagement, fraud mitigation, and operational efficiency. The current 3D Secure (3DS) protocol, where transactions are authenticated through a static password or a one-time passcode (OTP), has inherent limitations. The additional step during the checkout process results in high cart abandonment among customers. The user experience impact is especially pronounced in mobile apps, where applying 3D Secure may redirect customers out of the native app and onto a bank’s website that isn’t optimized for mobile devices.

Driven by regulatory requirements and the need for an intelligent authentication strategy, issuers are adopting the new global EMVCO 3DS 2.0 standard. The specification enhances security for online payments whilst providing a faster checkout experience across devices.

FSS Secure3D

FSS award-winning Secure3D, a real-time, risk-based authentication solution, compliant with EMVCO 3D Secure 2.0 guidelines, provides a comprehensive approach to secure card not present transactions. Deployed by 15+ banks and securing 200M+ authentication requests annually, FSS Secure3D is a proven solution to strengthen online transaction security and encourage the growth of e-commerce transactions.

FSS Secure3D supports explicit and implicit cardholder authentication. At the heart of the FSS Secure3D solution is an Adaptive Authentication Engine. Issuers can exploit a wide set of parameters - cardholder, device, location and merchant - to determine if transactions were initiated by legitimate cardholders. Based on these and other contextual variables, the solution generates a risk score. Suspect transactions with a high risk score are automatically stepped up for additional verification such as a one-time-passcode. This renders 100 per cent challenge rates obsolete whilst assuring protection against fraud, increasing completed sales, and delivering a better transaction experience for cardholders.



Why FSS Secure3D?

AI and ML-Driven Risk Decisioning

The Secure3D Adaptive Authentication Engine deploys sophisticated machine learning algorithms to detect fraud and lower false positives without compromising the customer journey. An advanced AI and ML-driven rule engine provides issuers the flexibility to create a custom set of policies and actions for cardholder verification. The rules are dynamically adjusted based on emergent user behavioral patterns.

Use Cases

- Implausible travel velocity (a user logs in from Cape Town, South Africa within 10 minutes of the same user logging into London, UK.)
- Mismatch between home and shipping address
- Activity from rogue or high-risk countries
- Same device making repeated attempts to log into multiple sites
- Suspicious combinations of locale settings on a computer (e.g., a browser's locale is set to the US while the OS locale points to a South Asian country and the device's IP address is physically located in South America)
- Customer buying schema - merchandise they buy, stores they frequently visit, times they shop, channel through which they shop are out of sync with normative patterns

Deploys Clear Box Approach to Authentication

FSS Secure3D analyses dynamic user behavior to build accurate data models using standard data elements prescribed by EMVCO for risk-scoring cardholders and transactions. A white-box approach provides transparency into each risk rule decision and outcome, with the flexibility to continually fine-tune the approach and improve decision making without human intervention.

Authenticates Payment and Non-Payment Transactions

FSS Secure3D supports app and browser-based implementations and enables a low-friction customer authentication process for payment as well as non-payment transactions such as verifying cardholder identity when signing up for a mobile wallet.

Flexible Step-Up Authentication Options

Issuers can set different step-up authentication methods, including biometrics or out-of-band verification methods such as push notification and OTP that can be enforced centrally in a cost-effective manner.

Support for 3DS 1.0 and 2.0 Protocols

FSS supports EMVCO 3DS 1.0 and the 2.0 protocols. For customers with existing implementations, FSS extends support for both versions and ensures a seamless migration experience, with minimal implementation and maintenance overheads.

Simplifies Enrollment for Quicker Service Adoption

FSS Secure3D supports bulk enrollment of eligible card members. In line with EMVCO mandates issuers can automatically provision customers for the service rather than during shopping. Pre-enrollment of card members eliminates the additional steps related to registration during shopping and improves services adoption rate.

Protects Customer Privacy

FSS Secure3D is compliant with data security, maintenance and privacy norms governing each region as well as regulatory reporting requirements in event of data breaches.

Richer Insights for Improved Fraud Prevention

Rich operational and business dashboards aid in identifying fraud-trends and fine-tuning fraud performance across all channels. In addition, FSS Secure3D ensures compliance with regional regulatory mandates related to reporting.

FSS Secure3D As-a-Service

FSS offers Secure3D As-a-Service on FSSNeT, FSS private cloud, exposing APIs to acquirers to connect to the platform. A multi-tenanted solution harnesses collective intelligence and brings data richness as evolving fraud patterns are shared across customers.

Further, issuers benefit as FSS assumes the mantle of responsibility for risk-assessment, reducing upfront investments and ongoing IT costs.

Specifically, the FSS Secure3D As-a-Service model:

- Lowers burden of compliance for regulatory and interchange related mandates
- Future protects issuers with seamless access to latest functional innovations and upgrades with zero services disruption
- Assures security as FSSNeT is PADSS 3.2 certified, limiting exposure to threats and data breaches
- Supports seamless vertical and horizontal scaling to accommodate increased transaction workloads
- Offers services reliability with multiple geographic regions and availability zones enabling issuers to remain resilient in the face of most failure modes, including system failures or natural disasters
- Guarantees high uptime with AI-based monitoring tools to predict and proactively troubleshoot performance issues
- Continuous access to operational and technical acumen with a dedicated team of experts
- Deploys analytic-driven billing processes for improved accuracy

Benefits to Issuers

Boosts Transaction Volumes

Transparent risk verification boosts transaction volumes by reducing stepped-up authentication requests for good customers, optimizing the checkout process and overall transaction completion rates.

Generates Cost-Efficiencies

FSS Secure3D As-a-Service unites applications, infrastructure, technical and business processes to provide issuers with a scalable, consumption-based service model that improves time to market and generates significant cost efficiencies.

Lowers Cost of Fraud

FSS Secure3D reduces the potential for data breaches and ensures risk is within an acceptable limit. A lower incidence of card not present fraud further translates into reduced costs due to lower chargeback volumes and fewer inbound calls related to fraud and false declines.

Strengthens Risk Governance

Strengthens risk governance and allows the issuer's risk management teams to focus on transactions that truly demand closer investigation.

Reduces Certification and Compliance-related Labor

Issuers can meet regional regulatory mandates and industry guidelines for stronger authentication compliance with regional regulatory mandates including SCA and PSD2.

Benefits to Merchants

Maximizes Revenues

By optimizing the customer experience and enabling effortless payments, merchants can improve conversions and overall basket size per transaction. This translates into improved revenues.

Secures Omni-Channel Shopping Experience

With an evolving e-commerce digital landscape, merchants are assured of a secure and more consistent user-experience across multiple touchpoints, including mobile, web, in-app and digital wallets.

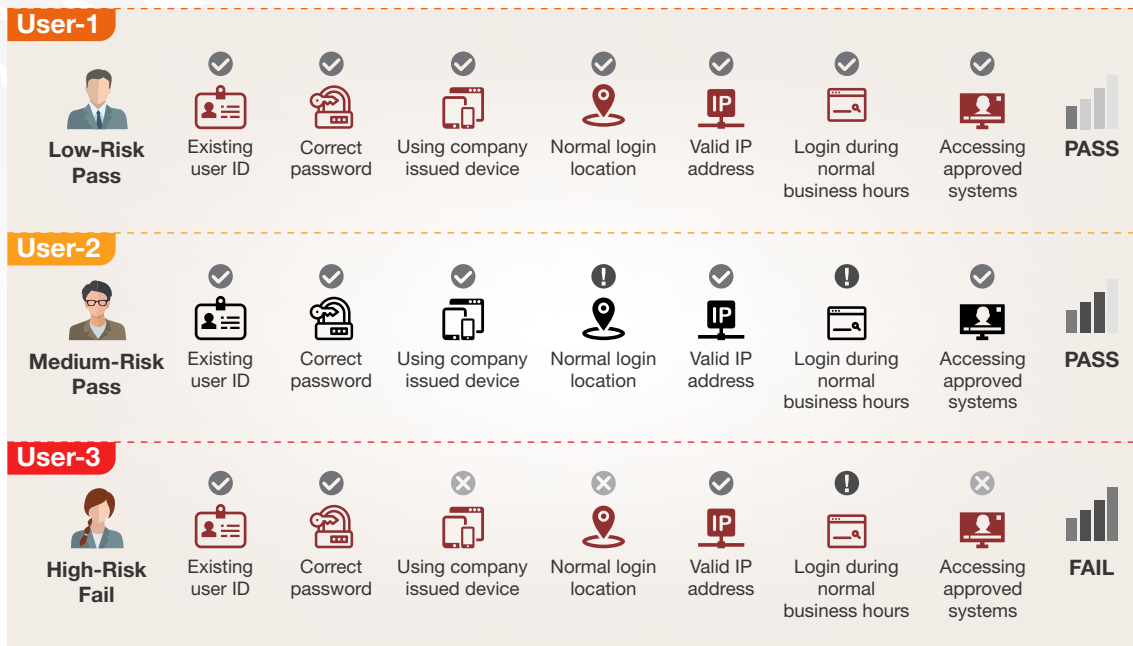
Lowers Risk

Merchants enabling Secure3D benefit from a liability shift to card issuers, which reduces their risk for non-authenticated transactions and associated refunds and lost revenue.

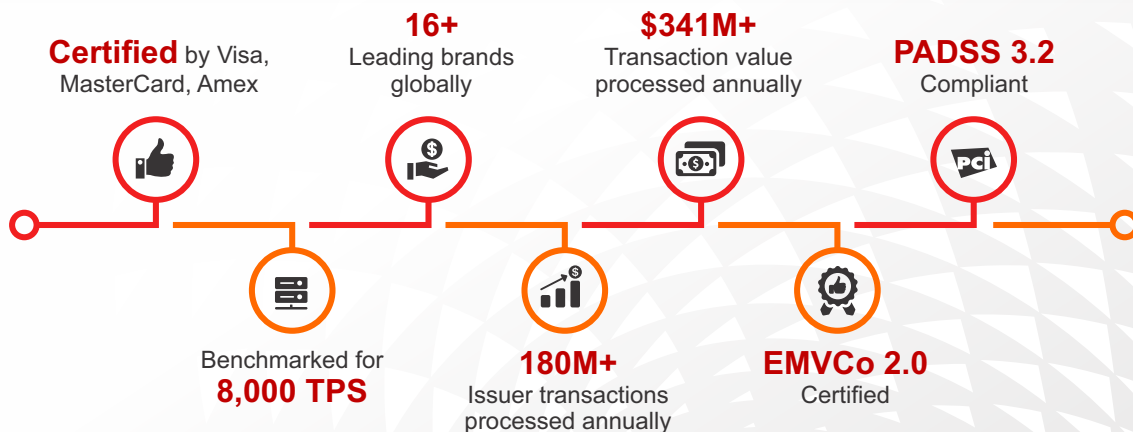
Uplifts Authorization Rates

FSS Secure 3D improves authorization rates between 10% and 15%, with no perceivable change to the checkout flow by customers.

Intelligent Risk-Based Authentication



Our Credentials



About FSS

Financial Software and Systems (FSS) is a leader in payments technology and transaction processing. The company offers a diversified portfolio of software products, hosted payment services and software solutions built over 25+ years of experience.

FSS, end-to-end payments suite, powers retail delivery channels including ATM, POS, Internet and Mobile as well as critical back-end functions including cards management, reconciliation, settlement, merchant management and device monitoring. Headquartered in Chennai, India, FSS services leading global banks, financial institutions, processors, central regulators and governments across North America, UK/Europe, ME/Africa and APAC and has 2,500 experts on-board.

For more information, write to products@fsstech.com