entersekt

The Financial Authentication Company.

3-D Secure ACS Buyer's Guide

entersekt.com

info@entersekt.com

Contents

Introduction

Payment fraud has evolved drastically over the last decade. With the ubiquitous distribution of EMV chip cards, card-not-present (CNP) fraud has become a massive target for bad actors, and the annual global increases in CNP fraud losses and share of all payment fraud bear this out. And as artificial intelligence (AI) and machine learning (ML) skills develop, and tools become widely available to fraudsters, financial institutions (FIs) become even more vulnerable as the targets of their efforts.

As a result, fraud prevention must also evolve to address accelerated and innovative threats, but without negatively impacting the customer experience.

This guide serves as a resource for issuers and processors to evaluate providers of 3-D Secure Access Control Servers (3DS ACS). It provides an overview of the payments threat landscape, addresses modern approaches to ensure a secure, user-friendly 3DS solution, and delves into capabilities that will best achieve fraud prevention and customer satisfaction objectives. It concludes with an evaluation checklist to aid your evaluation process when selecting a 3DS ACS provider with information about Entersekt's capabilities and a place for you to capture how an alternate provider addresses each requirement.

We hope this guide simplifies your 3DS ACS selection process and enables you to better protect your customers from evolving CNP payment fraud risks.

Evolving fraud and the authentication landscape

It is no secret that FIs are the most attractive target for the efforts of fraudsters, intent on emptying the bank accounts or lining their pockets with the spoils of stolen payment cards. Fraudsters have grown more industrious and sophisticated, adapting their strategies to exploit changes in technology and banking practices. It comes as no surprise then that **57% of fraud executives are concerned about consumer scam attacks**, according to leading analysts at Datos Insights.

Every day, cybercriminals demonstrate their ability to easily defeat one-time passcodes (OTPs) with scams that convince unsuspecting cardholders to share their OTP or find other ways to intercept them. In fact, even two-factor authentication (2FA) methods that rely on browser communications are vulnerable.

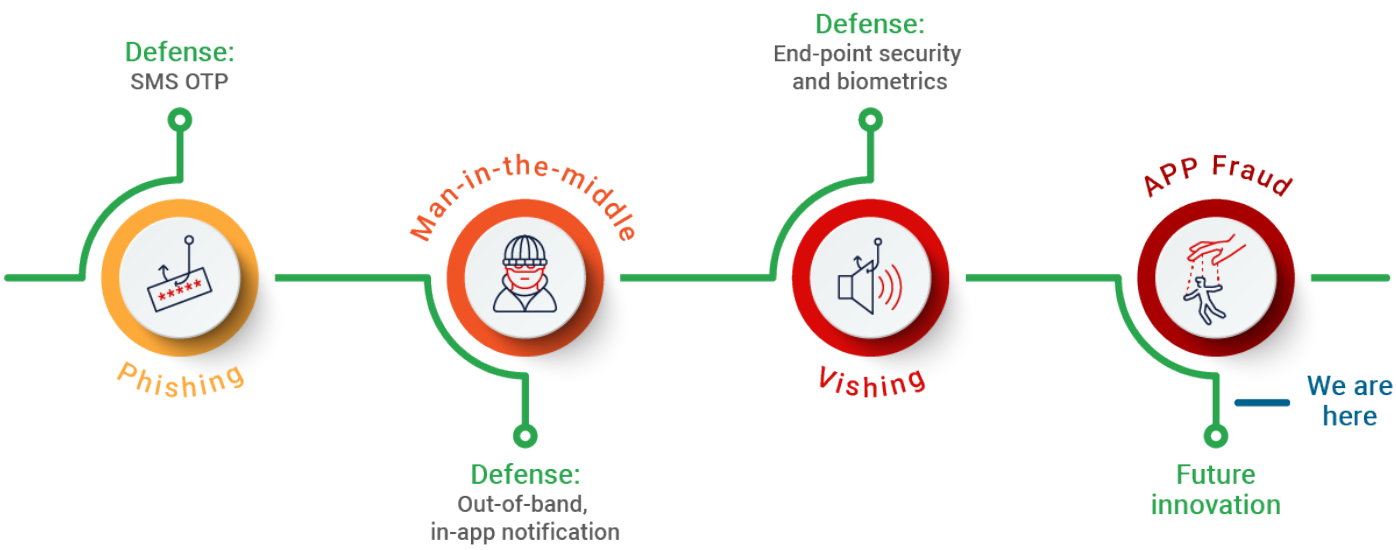
> "Anything that goes through a browser can be compromised by a Trojan."
>
> – Avivah Litan, Vice President and distinguished analyst at Gartner.

A Trojan or Trojan horse is a type of malware that downloads onto a browser, hiding its true content and fooling a victim into thinking it's a harmless file, when in fact, it gives backdoor access to a malicious actor.

Man-in-the-middle browser attacks circumvent the security expected from OTPs. The legitimate parties are unaware of the hacker's presence, enabling the fraudster to act as a proxy or "man-in-the-middle." In some cases, the malware copies the user's OTP and immediately uses it to expand their attack. In other cases, malware overwrites legitimate user transactions with fraudulent ones, unbeknownst to the user or to the bank. A strong defense system operates beyond OTPs and is comprised of multiple layers of security.

How fraud has evolved over the years

And will continue to evolve towards the weakest link, with more involvement every time from the end customer.



From phishing to more advanced forms of attacks, fraud will continue to evolve towards the weakest link, with more involvement every time from the end customer.

As scams evolve, issuers must move past OTPs. They can also no longer rely on a single authentication tactic. Industry experts and an increasing number of regulatory bodies recommend multiple layers of security and the most effective strategies include risk data and silent authenticators, which are simultaneously smarter than fraudsters and do not disrupt the customer checkout experience.

Selecting the right 3DS provider

Selecting the right 3DS provider is a crucial decision for issuers looking to optimize their fraud prevention, operational costs, and customer experience strategies. The true value of 3DS lies in choosing a partner with deep 3DS and authentication expertise, advanced ACS capabilities, and a commitment to continuous investment in new capabilities and modern, customer-friendly authentication options that take advantage of emerging technologies to address endlessly evolving scams.

The right 3DS provider can make a difference to your bottom line in three key ways:

Increases transaction success by recognizing your customer using reliable data and "silent" authentication that minimizes the need for challenges and false declines.

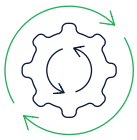
Reduces chargebacks and financial losses due to third-party fraud by preventing fraudulent transactions: reduced fraud reimbursement and operational costs associated with the dispute process.

Reduces chargebacks due to first-party fraud by providing easy access to proof of indisputable legitimate customer authentication.

Enhancing fraud prevention and customer experience:

A key differentiator of an effective 3DS solution is its ability to leverage data to inform authentication decisioning. The real power emerges when advanced data science and historic transaction data, enriched with global consortium data, are applied and can:

Take into consideration the context of a transaction in assessing risk --- a risky transaction for one cardholder might be typical for another.



Adapt risk rules over time – in contrast to static rules that are sitting ducks for fraudsters to learn and circumvent.

> "Risk intelligence that utilizes advanced data sources, context, and adaptive rules significantly enhances the solution's performance in terms of both fraud prevention and seamless customer experiences."

What to look for in a 3DS provider

Modern authentication methods, including active and silent methods are essential to a successful 3DS program. Biometric authentication is becoming pervasive and preferred, as customers use it on their devices and in all their daily digital interactions with Amazon, Google and more.

Out-of-band notifications from within your banking app, is an option that is far more secure than OTPs.

Silent authentication using cryptographic keys is another modern tool that is uniquely reliable, and frictionless during a transaction.

With the right 3DS provider that has deep expertise in authentication methods easily accessible to the ACS, your institution can add the latest authentication options to stay ahead of the fraudsters, as well as to offer a range of options to enable customer choice.

Flexibility is another cornerstone of a strong 3DS solution. A one-size-fits-all model doesn't address the diverse needs of processors and issuers. The optimal balance between fraud detection, customer experience, operational efficiency, and budgetary considerations varies for each client, often influenced by their unique business priorities and regulatory influences.

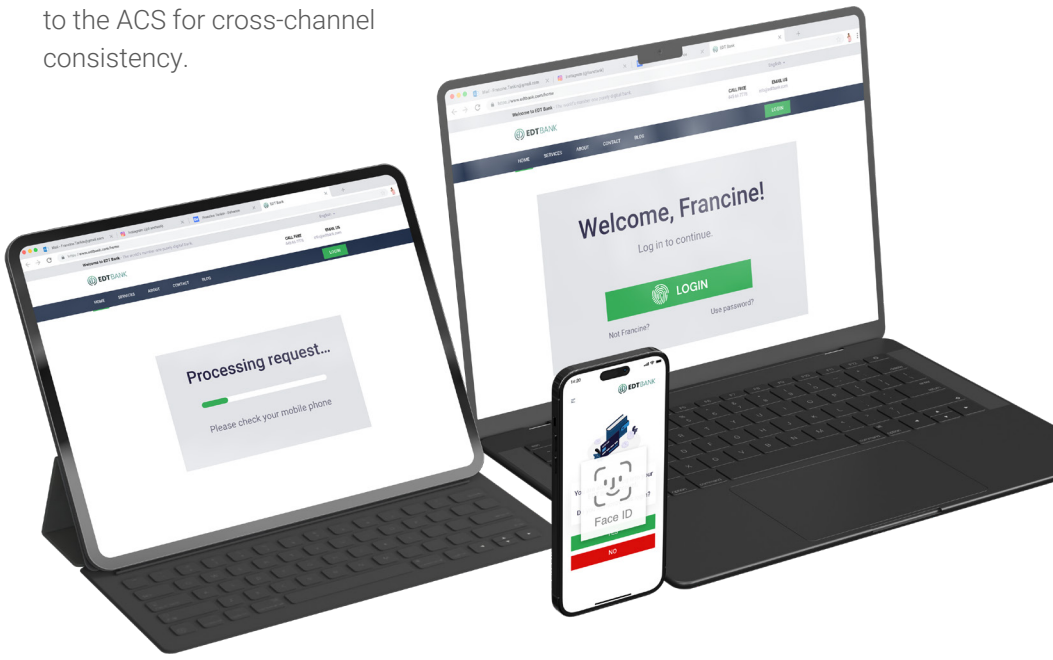
Solutions need to be adaptable, allowing for tailored configurations and preferred risk tools that allow issuers to exert control to manage their 3DS program in line with their risk appetite and customer journey priorities.

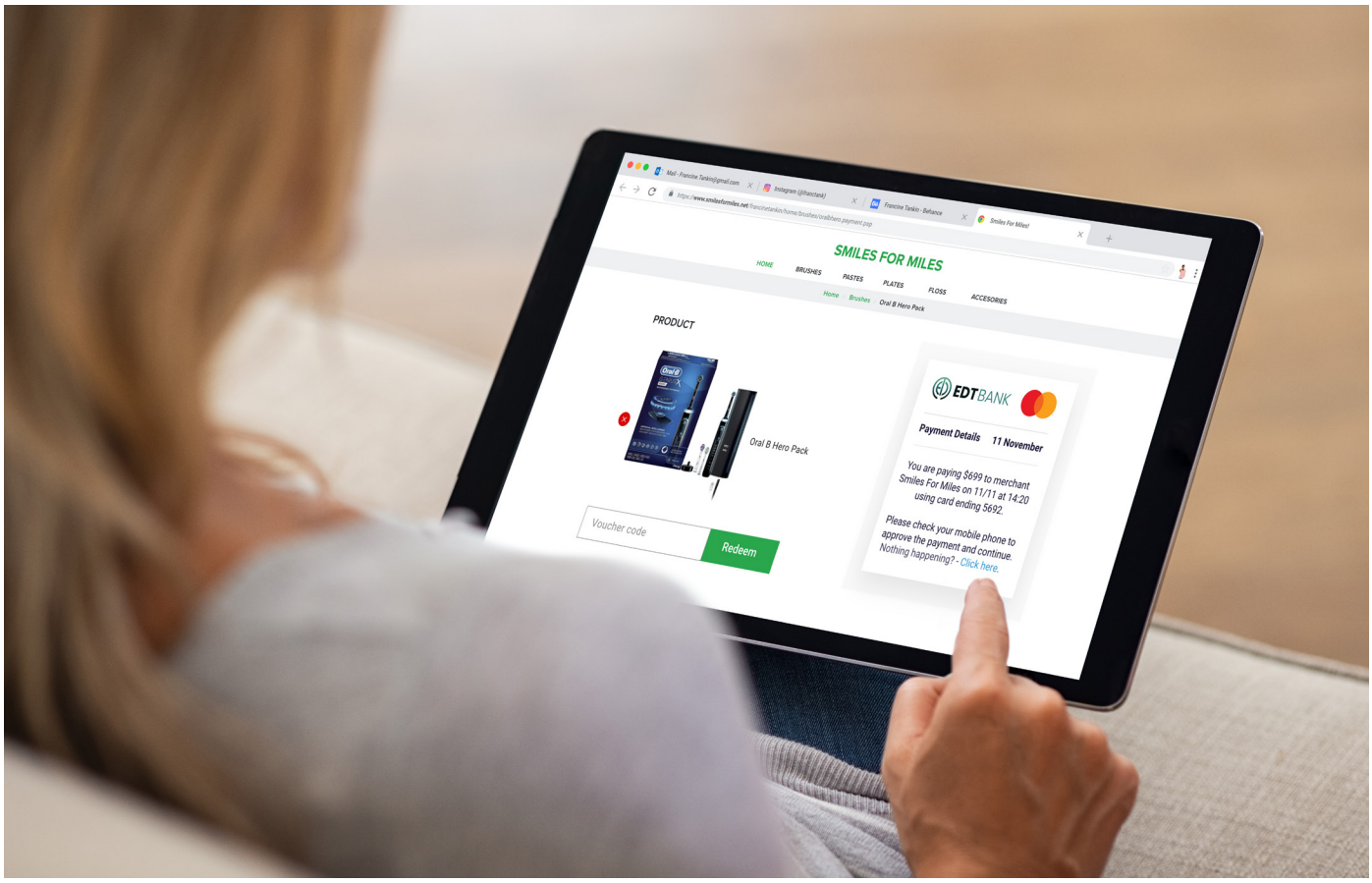
Cross-channel authentication is beginning to be recognized by financial institutions as a crucial pillar in a holistic fraud prevention strategy, rather than protecting each customer interaction channel in silos.

To support a holistic approach that closes gaps vulnerable to fraudsters, an effective 3DS provider should offer fraud prevention that is capable of supporting a unified solution protecting banking and payments channels, or at the very least, allows you to use your own risk engine integrated to the ACS for cross-channel consistency.

Proactive anticipation of the evolving regulatory landscape and technological advancements is essential for a 3DS provider to support issuers and processors to win the war against fraud. A provider needs to proactively update their solutions to ensure immediate compliance with new regulations. Beyond mere compliance, the provider should actively engage with standards bodies and card networks to both understand diverse options to address the 3DS protocol, and to influence the future direction of the protocol.

Continuous investment in emerging risk and authentication technologies is the only way to keep pace with emerging threats.





Optimal criteria for a modern authentication solution

In today's dynamic digital environment, FIs must move beyond outdated security measures, like OTPs and static risk rules, to protect themselves and their customers while delivering seamless experiences.

A modern authentication solution should prioritize strong, yet user-friendly, methods like biometrics and out-of-band verification, complemented by adaptive risk-based authentication (RBA) that dynamically assesses transaction risk using contextual, historical and consortium data to minimize fraud and friction.

An optimal solution will enable a frictionless authentication journey for trusted users across all digital channels, enhancing customer loyalty and increasing deposits.

Furthermore, it should streamline operations by offering self-management of rules and branding, reduce chargebacks through effective fraud prevention and provide valuable transaction authentication tracking data.

> "Enhanced reporting and analytics, including real-time compliance monitoring, are essential for gaining deeper insights, achieving KPIs and proactively meeting card brand compliance requirements."

Considerations for EU and regulated markets

The digital payment landscape has been reshaped by the need for strong fraud prevention and robust consumer protection. For FIs operating in or facilitating payments in Europe and other regulated regions, navigating this evolving environment demands a strategic approach to authentication that balances security with a seamless user experience.

This section discusses the role of the 3DS ACS in achieving compliance and the importance of the right 3DS provider with advanced risk insights and authentication capabilities in optimizing transaction success and reducing fraud.

The imperative of Strong Customer Authentication

Regulations such as the Revised Payment Services Directive (PSD2) in Europe, and its upcoming iteration, PSD3, mandate Strong Customer Authentication (SCA) for most electronic payments. When indicated, SCA requires multi-factor authentication, that is, at least two independent authentication elements from three categories:

Knowledge: Something only the user knows (e.g., password, PIN).

Possession: Something only the user possesses (e.g., mobile phone, hardware token).

Inherence: Something the user is (e.g., fingerprint, facial recognition).

While crucial for fraud prevention, SCA implementation creates difficulties for issuers. The goal is to apply these stringent authentication requirements without introducing excessive friction that leads to transaction abandonment and a degraded customer experience.

With the right ACS provider, issuers can get support to identify transactions eligible for exemptions (like Transaction Risk Analysis or TRA), and they can use advanced risk insights and silent authenticators to further reduce the need for friction whenever possible.

The right 3DS ACS: A gateway to secure, seamless compliance

The right 3DS ACS is more than just a compliance tool; it's a strategic asset designed to empower issuers with the agility, security, and user-centricity needed to thrive in regulated markets. A modern ACS fortified with dynamic risk insights and advanced authentication methods serves as the issuer's decision-making engine, determining whether a transaction can be approved frictionlessly, or requires authentication and, if so, how that authentication should be performed.

Here's how the right solution delivers strategic value:

1. Future-proofing regulatory compliance (PSD2, PSD3, and beyond)

The right ACS is built with regulatory compliance as a cornerstone:

- **Reliable SCA enforcement**: A high-quality ACS meticulously evaluates the 3DS data and supplements with broader data insights to determine if SCA is required, triggering appropriate authentication flows in real-time.
- **Dynamic exemption management:** The ACS must be equipped to recognize criteria for exemptions by accurately assessing risk and exempting low-risk transactions from authentication as defined in the PSD2 requirements. Taking full advantage of exemptions is essential to providing a high rate of frictionless transactions, vital for maximizing conversion rates.
- **Preparation for PSD3:** A flexible, API-driven architecture allows for rapid adaptation to future mandates, ensuring issuers remain ahead of the regulatory curve without major system overhauls.
- **Investment in ACS capabilities:** A 3DS provider must be committed to investing in enhancements to the ACS as new payment scams emerge, new authentication and risk technologies develop, and as regulatory compliance requirements evolve.

2. Advanced authentication for superior security and cardholder experience

Beyond basic compliance, the right 3DS ACS elevates authentication through advanced methods:

- **Biometric authentication:** Leveraging inherence factors, the right ACS facilitates secure, user-friendly biometric authentication (e.g., fingerprint, facial recognition) without relying on third party providers to provide updates and enhancements.
- **Out-of-band authentication:** The best solutions support out-of-band authentication via secure push notifications to registered mobile devices. This method provides possession-based security and is resistant to common phishing attacks.
- **Device-bound security:** By binding cryptographic keys to the user's mobile device and/or browser, a strong ACS enhances security, making it difficult for fraudsters to compromise accounts. Browser ID and Device ID can be used as a possession factor for silent authentication, with no added friction.

3. Optimized user experience and reduced abandonment

The right ACS directly addresses the balance between security and convenience:

- **Frictionless flows:** Through intelligent transaction risk analysis (TRA) and "silent authentication" (where the ACS authenticates in the background), many transactions can be completed without a visible challenge, paramount for customer satisfaction.
- **Preferred customer journey:** A modern ACS provider gives the issuer the ability to enable the ACS to intelligently select the least intrusive yet most secure authentication method based on risk, device capabilities, and customer preferences.
- **More agility and control for the issuer:** With the right ACS, the issuer can self-manage and test changes to risk rules and user messaging for more flexibility and agility without new fees for every change. They should also be able to easily upgrade to newer authentication and risk technologies as compliance requirements, market demands and threats change.

Choosing the right 3DS ACS vendor is a critical decision for financial institutions navigating the complexities of regulated digital payments. The regulatory requirements will certainly evolve as fraudsters innovate and utilize new technologies to stay ahead of FIs, so alignment with an ACS provider with a history of proactive investment in fraud prevention and authentication is not only valuable to maintaining compliance, but also crucial to protecting FIs and their cardholders.

Vendor selection checklist

Processors and issuers can use the list below to guide their 3DS ACS evaluation process. Entersekt capabilities are noted, and the Vendor #2 column is provided for you to add your findings for an alternate vendor.

ACS essentials		
Feature	**Entersekt**	**Vendor #2**
Certified for all major card brands	Entersekt is certified for all major card brands including: Mastercard, Visa, American Express, Discover, Diners Club, UnionPay, JCB	
Ease of certification to additional regional and local card schemes	Entersekt can certify to nearly any local and regional brand with ease and speed.	
Highest standards of cloud delivery	Entersekt has geographically dispersed hosting centers in the United States, Norway, and South Africa ensuring strong signals and reduced latency. For all hosting centers, clients can count on continuous compliance to all required standards, and multiple layers of security, monitoring and protection.	
Multi-tenant architecture	Processors and FI groups can host and manage multiple entities on a single server, with the ability to provide entities with visibility to only their data, and to combine entities for visibility by parent organizations. There is significant time and operational savings during month-end reporting and invoicing. Parent organizations can run invoicing reports by a single entity or in defined groupings without requiring manual efforts to segregate the data and calculate each entity's share.	

ACS essentials		
Feature	**Entersekt**	**Vendor #2**
Remote access Admin Portal	Ease of administration, configuration, and reporting. Diverse user roles supported to ensure hierarchical access to data only for those who should have it. Option for SSO security.	
Support for card scheme compliance	Entersekt provides reports that show real-time data that tracks metrics associated with Mastercard Edits and other card scheme performance requirements. Issuers can analyze the data to determine which rules can be adjusted to drive changes that meet the requirements and avoid non-compliance penalties.	
Fully customizable user journeys	Issuer can curate user journeys down to "per card" level. What-if scenarios can be tested using the ACS Rule Simulator using actual historic data, allowing issuers to pre-assess the impact of rule changes on their portfolio. This provides unique control to achieve your frictionless transaction benchmarks and similar KPIs.	
Effective testing prior to rollout of changes	Entersekt provides an end-to-end test environment with an EMVCo-certified Directory Server and Demo Merchant for full transaction testing. As one of the only ACS providers with EMVCo-certified components in all three domains, Entersekt clients can simulate a more real-world test transaction, which yields fewer errors or surprises when changes to rules or user journeys are pushed to the live environment.	

Strong authentication methods		
Feature	**Entersekt**	**Vendor #2**
Customer-preferred authentication methods	Entersekt's challenge methods use capabilities consumers have already widely adopted with their other smartphone apps, such as using biometric authentication.	
Passwordless options	Entersekt offers modern passwordless options, like biometrics and passkeys, to replace outdated and unsafe OTP measures. We also offer silent authentication options including Browser ID and Device ID that take advantage of highly secure cryptographic keys.	
Secure technology, less friction	Entersekt's options include biometrics, out-of-band (OOB) verification via mobile apps, and silent cryptographic authenticators. These methods are strong, more reliable than OTPs, and not as easy for fraudsters to intercept.	
Single provider with multiple authentication methods seamlessly integrated to ACS	Entersekt makes it easy to change or add authentication methods, since we are the authentication provider and do not rely on third-party integrations. A menu of authentication options can be enabled, which allows cardholders to select their preferred method.	
Adaptive risk-based authentication	Entersekt's intelligent risk engine leverages historic activity and global consortium data to dynamically assess transaction risk in real-time, minimizing false declines and reliably detecting fraud. In contrast to static risk rules, adaptive scoring enables rules to adjust according to historic activity, and specific cardholder activity, thereby preventing fraudsters from learning your static rules and submitting transactions just under your thresholds.	

Strong authentication methods		
Feature	**Entersekt**	**Vendor #2**
Futureproof technology through continuous innovation and investment	Entersekt is committed to anticipating emerging threats, continuously investing in development of patented fraud prevention and the most customer-friendly authentication capabilities. This is a core competency along with 3DS expertise, as evidenced by 120 patents for authentication and payments capabilities.	
Frictionless authentication	Entersekt reduces cart abandonment and improves approval rates by offering frictionless options with cryptographic Device ID and Browser ID, as well as intelligent risk assessment that minimizes steps for trusted users and low-risk transactions.	
Consistent customer experience	Entersekt provides a seamless and consistent authentication experience across all digital banking and payments channels, fostering customer loyalty that leads to increased deposits.	
Personalization	Entersekt gives the FI comprehensive control of rules and customer journey parameters, for instance, determining when a step-up challenge is needed. Customers can also be offered the option to select their preferred challenge method.	

Operational and cost savings		
Feature	**Entersekt**	**Vendor #2**
Agility and control	Entersekt's ACS enables self-management of changes to rules, messages, logos, and more, without requiring a support ticket or services fees. No waiting for others to implement.	
Chargebacks reduction	Entersekt's ACS provides proof of genuine cardholder authentication, reducing first-party chargebacks, and provides more effective fraud prevention reducing third-party chargebacks.	
ACS Rule Simulator for effective KPI management	By using Entersekt's Rule Simulator to test what-if scenarios and measure predicted impact based on your historic transactions, data-driven rule changes can reliably achieve KPI objectives.	
Comprehensive and easy-to-access reporting	Remote access to the Admin Portal enables convenient access to comprehensive reporting that provides deeper insights into transaction patterns. Issuers can also integrate the reporting API to retrieve data in their own systems.	
Card brand compliance support	Entersekt's reporting supports compliance to card brand requirements – access your compliance report that provides real-time status against Mastercard Edits with the ability to dissect performance and assess which rules to adjust so as to achieve benchmark requirements.	
24/7 Support	Entersekt offers 24/7 follow-the-sun support, enabling access to live support for urgent issues when you need it.	
3DS implementation and migration support	Entersekt's team of experienced solution, architect and project experts are always on standby to assist an FI in transitioning to the new solution. The client success model includes experts in delivery, support, and monitoring.	

Measuring your return on investment

Convincing your organization to invest for the first time or migrate your ACS solution can be a challenging task, in competition for resources with other unrelated priorities. However, the benefits of an effective 3DS program can extend across many divisions of the FI and yield gains to the overall bottom line. These include reducing direct financial losses due to fraud and the operational costs of fraud, as well as improved customer relationships that can lead to increased card usage and deposits in your broader banking relationships.

The areas that most issuers focus on to demonstrate return on investment (ROI) include direct and speculative areas of the business, primarily cost savings and customer satisfaction.

Factors impacting your bottom line

Direct costs of fraud: The out-of-pocket cost of reimbursing customer losses.

- **Reduced chargebacks due to first-party fraud:** Utilize the transaction audit trail to prove authentication occurred on the cardholder's frequently used device.
- **Reduced chargebacks due to third-party fraud:** Prevent fraud before it happens with more effective rule setting and risk advice.

Operational costs: A range of operational costs are associated with receiving cardholder disputes and researching their validity. Entersekt provides:

- **Reduced call center demand:** When you reduce the occurrence of third-party fraud, there are fewer calls to the call center.
- **Reduced fraud research resources:** Entersekt provides easy access to transaction tracking that supports the dispute research process. Issuers can reduce first-party fraud with cryptographic proof that the legitimate cardholder used their trusted device to authenticate the transaction.

Higher transaction success rates:

- Advanced risk insights: When using more effective risk insights that consider context such as an individual cardholder's typical behavior, false declines are greatly reduced.
- Advanced, customer-friendly authentication methods: More reliable, customer-friendly and silent authentication methods mean less friction in the checkout process and higher checkout conversions.

Non-compliance costs: Entersekt provides reporting that enables issuers to proactively prevent non-compliance to card brand requirement, such as Mastercard Edits, and other regulatory standards.

> FIs that use Entersekt as a single vendor for risk engine, authentication methods, 3DS authentication and digital banking security can reduce maintenance costs and enhance customer experience

Utilizing Entersekt across channels allows you to recognize your customer across these same channels, reducing friction and providing a consistent authentication experience. Similarly, fraudulent attempts can be shared in real-time across channels, closing gaps in your fraud defenses, especially needed when a fraudster uses the latest technology to launch rapid attacks against multiple channels simultaneously.

Evaluating Entersekt's financial authentication solutions

A multi-layered defense approach with a relentless focus on user-friendliness:

1. Tapping into advanced endpoint signals, flagging device anomalies, and ensuring the authentication channel is not compromised.
2. Leveraging silent authentication, which acts as an invisible layer of identifiers and signals — adding an additional layer of security without causing unnecessary friction.
3. Using risk-based decisioning, evaluating multi-faceted transaction risk data to prevent fraud.
4. Using MFA methods to secure high-risk transactions, while still delivering optimal user experiences. These include measures such as out-of-band push notifications to a trusted device, passkeys leveraging biometrics, and silent authentication measures.
5. Providing powerful user experience controls, ensuring consistent and optimal experiences throughout all user journeys.

Why choose Entersekt?

The implementation of a 3DS solution is not a static event but the beginning of an ongoing process. The fraud landscape is constantly shifting, with fraudsters continuously developing new tactics. Customer expectations evolve, regulations change, and competition intensifies. Entersekt is dedicated to continuous investment to ensure our 3DS solution not only meets current needs but is also futureproof and capable of adapting to changing market influences.

To support rapid time to value and a seamless onboarding experience, Entersekt offers a proven, well-defined implementation methodology built upon our extensive experience. Our end-to-end process covers all stages, from initial planning to testing and go-live support. Moreover, our approach is flexible, adapting to each FI's specific timelines, resources, and priorities.

Switching 3DS providers needn't be a challenging endeavor either. Entersekt tailors its methodologies and onboarding processes to the unique needs of each new customer, leveraging our best practices accumulated over years to deliver maximum value, quickly and cost-effectively. We assign an experienced project lead to guide clients through the entire process, actively listening to and considering their individual priorities, timelines, and resources. Close collaboration and expert guidance based on our deep understanding are central to our onboarding philosophy.

Success goes beyond implementation; a strong partnership is the key. Even after implementation, our customer success team remains engaged with our clients to help optimize their 3DS programs and any ongoing needs and enhancements.

Your partner now and in the future

As you navigate your 3DS ACS evaluation process, Entersekt stands ready to provide the expertise and support needed to assess and select a partner for the long haul, one that will evolve and keep pace with the dynamic future of digital payments and emerging fraud.

Ready to take the next step in your ACS journey?

Book a demo

V01_202506_MKT7469