ENTRUST

SECURING A WORLD IN MOTION

ebook

Entrust Solutions for Financial Institutions

State-of-the-art issuance and security for trusted identities, data, and payments

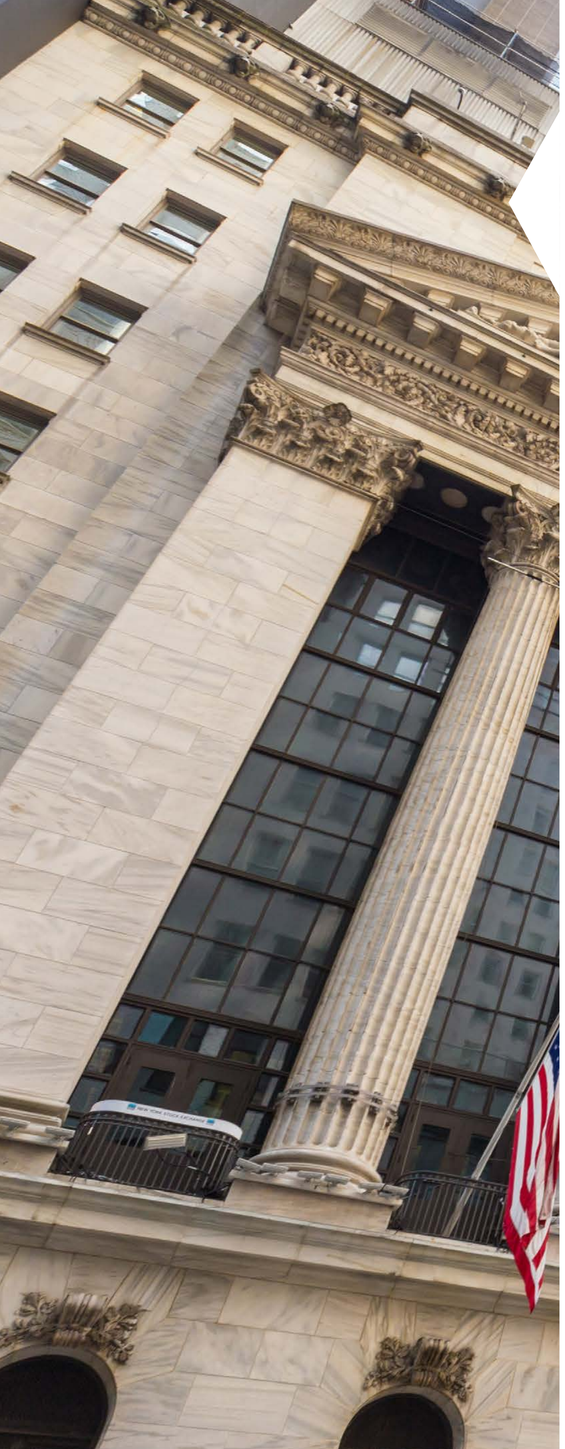
FINANCIAL SERVICES ARE BEING REDEFINED

> By the end of 2023, 10% of banks will use consumer digital identities to drive new, innovative business models creating new sources of revenue.
>
> By 2022, 40% of in-branch transactions will be initiated as prestaged transactions or appointments for specialists that start on digital platforms and fulfilled on bank-owned technology and locations.

– IDC FutureScape: Worldwide Financial Services 2021 Predictions Report

Table of contents

ADDRESS TODAY'S KEY SECURITY CHALLENGES AND ISSUANCE REQUIREMENTS, AND DELIVER ON HEIGHTENED CONSUMER EXPECTATIONS.



Embrace the future of financial services

The value of financial data puts a target on all financial institutions (FIs). From procuring and handling transactions, funds, and data, FIs are in the middle of a hostile battleground surrounded by the world's most sophisticated cybercrime cartels and nation-state hackers.

In 2021, destructive cyberattacks against FIs rose to 54% of all companies, a 118% increase from the previous year.[1] Not only is this increase in volume concerning, but also the methods being used to defraud FIs demonstrate a deep understanding of the financial sector, market strategies, and institutional interdependencies.

In order to thrive against such constant threats, FIs require a full complement of digital and physical solutions to address today's key security challenges and issuance requirements, deliver on heightened consumer expectations, and realize digital transformation initiatives.

Today's key financial services security challenges and risks:

- Protecting consumer data and fighting fraud
- Meeting compliance mandates like GDPR, PSD2, KYC/AML, etc.
- Improving the consumer experience
- Securing financial services infrastructure
- Enabling a secure, productive workforce
- Ensuring a secure, scalable card issuance operation
- Safeguarding financial service delivery, transactions, and payments

» 54%

of financial institutions experienced destructive attacks[1]

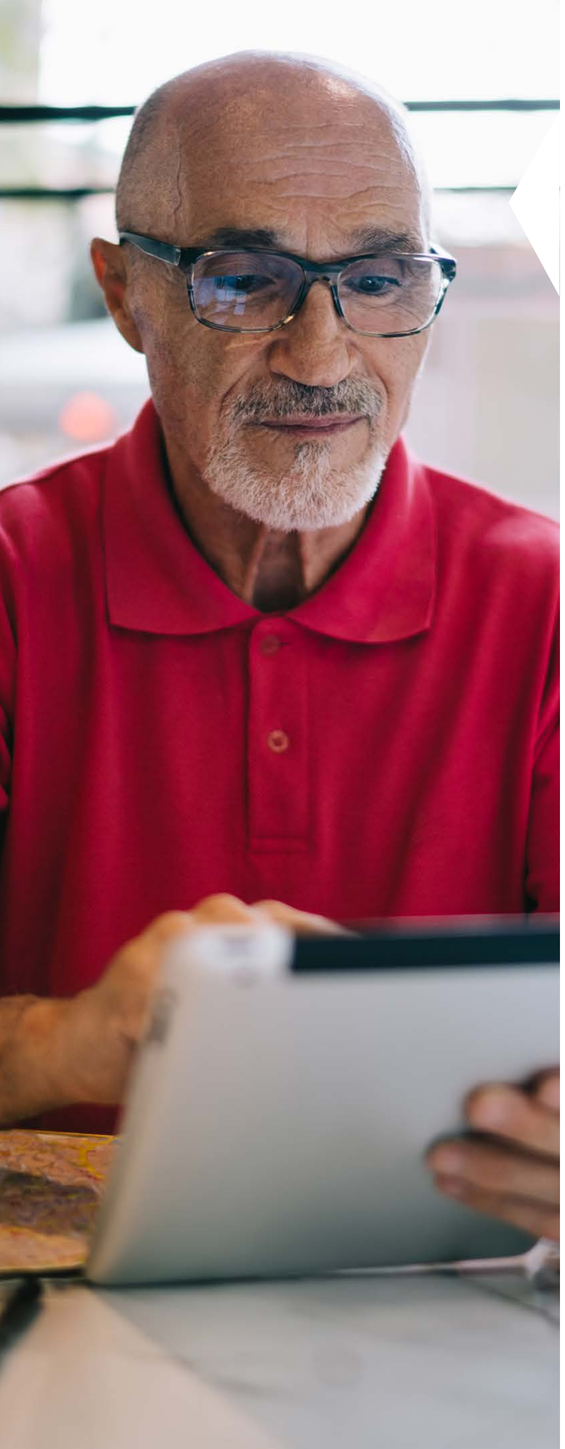
» 41%

of respondents saw attackers attempt to manipulate timestamps[1]

» 51%

of financial institutions experienced attacks that targeted their nonpublic information and market strategies[1]

[1] https://www.carbonblack.com/resources/modern-bank-heists-2021/



Protect consumer data and fight fraud

At $18.3 million per year, per company, the cost of cyberattacks is highest in finance.[2] Plus, the explosion in e-commerce means an equivalent increase in card-not-present (CNP) transactions, which have a higher fraud risk.

Protect consumers from identity theft and fraud with identity proofing, MFA, adaptive risk-based authentication, 3DS compliance for CNP transactions, document signing, and transaction signing and verification. As well, consumer banking data should be encrypted or tokenized for strong data protection and accessible only by authorized users.

When financial information needs to be shared with financial partners, any personal data should be tokenized to protect consumer privacy. As well, any electronic document containing client data should be digitally signed or sealed to ensure content integrity and authenticity, and to clearly identify the financial professional or institution that owns the document to help prevent document fraud and forgery.

« Cryptography with strong key management is the critical infrastructure that underpins the adoption of these new digital practices and associated transformation. »

Resources to help you protect consumer data and fight fraud:

IAM Solutions for Banks ebook

Mitigating Fraud Risk with 3DS Solution Brief

nShield General Purpose HSMs Brochure

Entrust Cryptographic Center of Excellence Data Sheet

Signing Automation Service Data Sheet

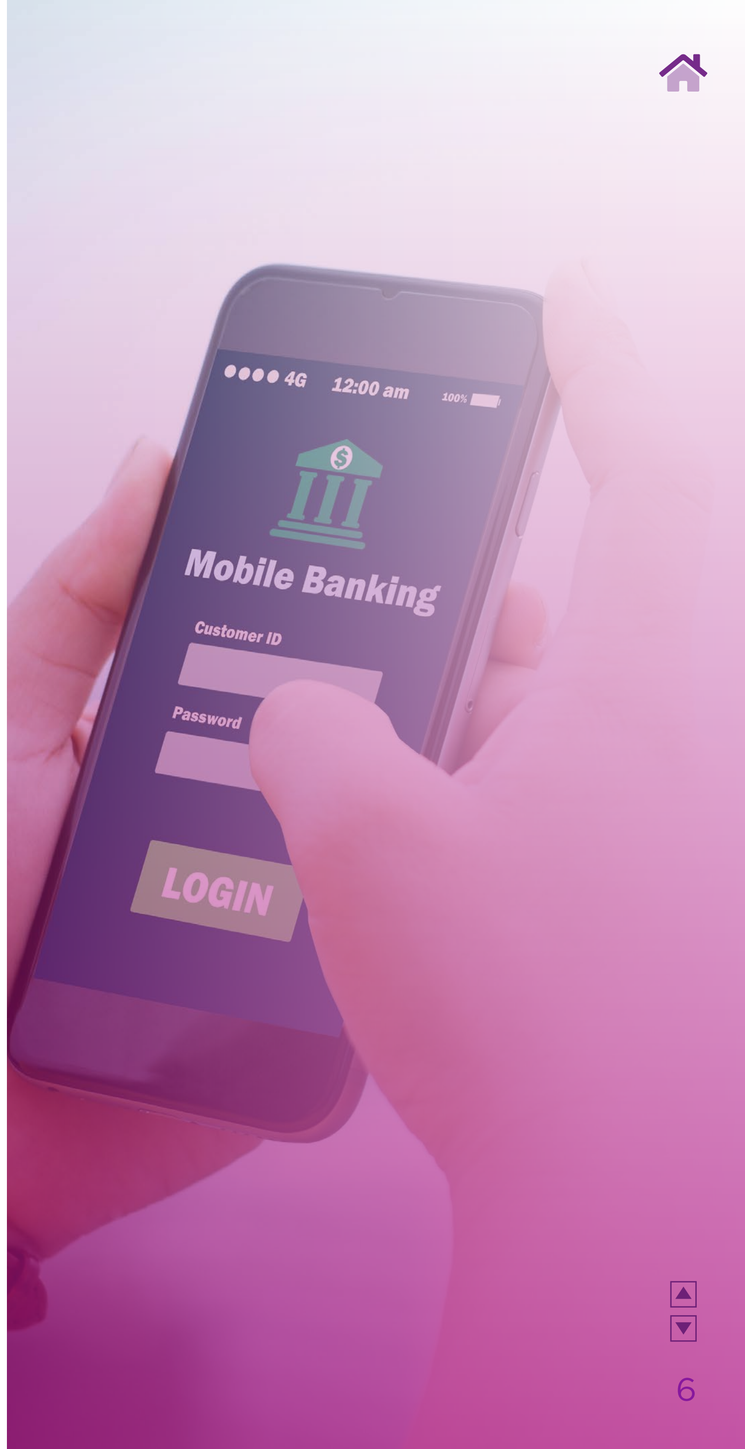
[2] https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/?sh=d83ab506e906

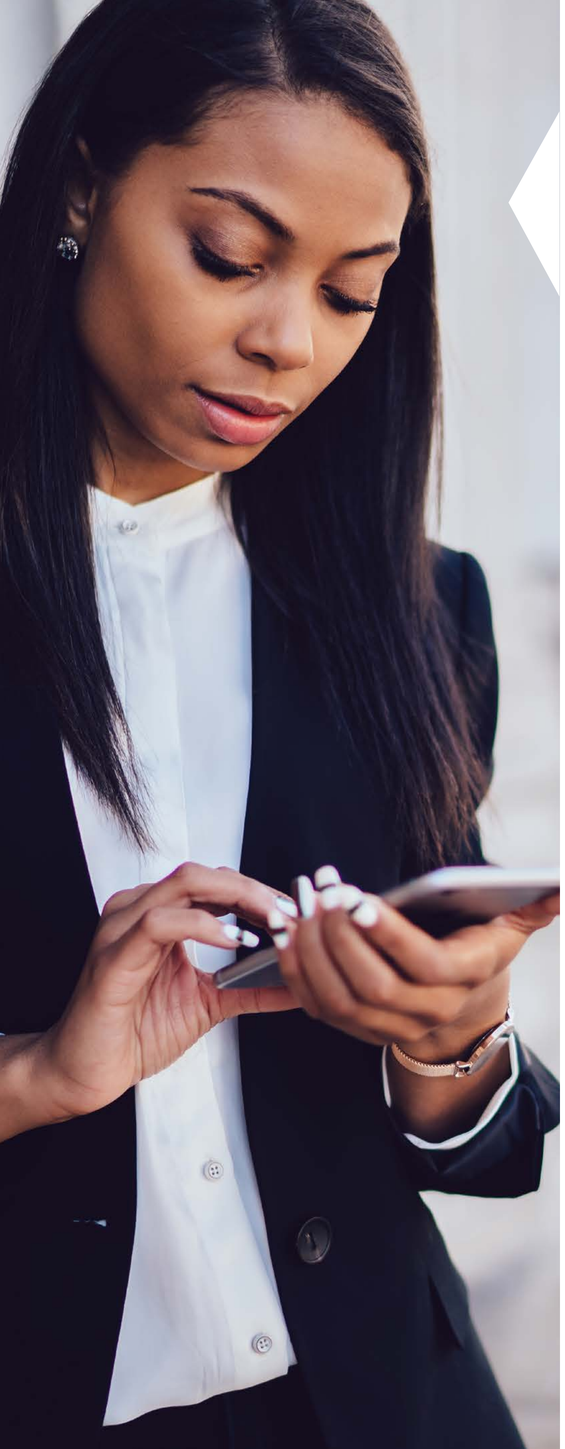
Help meet compliance mandates

Knowing the relevant data privacy, open banking, and anti-money laundering regulations across jurisdictions is one thing; meeting them is another.

The ability to adhere to data privacy regulations, including GDPR, CCPA, and eIDAS, requires an understanding of what these regulations mean as well as the ability to follow policies for collecting, processing, and securing personal data to specific financial records.

Complying with open banking regulations, such as PSD2 in Europe, also has requirements for strong customer authentication (SCA), transaction risk analysis, dynamic linking, and app hardening. As well, adhering to know your customer regulations (KYC), demands that financial institutions make efforts to verify customer identity and risks involved with maintaining business relationships.





Help meet compliance mandates

Know your compliance mandates and customer regulations:

GDPR: EU
The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy in the European Union.

eIDAS
Electronic Identification, Authentication, and Trust Services is an EU regulation on electronic identification and trust services for electronic transactions in the European Union.

PSD2
The Revised Payment Services Directive is a European Union directive to regulate payment services and payment service providers throughout the EU.

CCPA
The California Consumer Privacy Act is a state statute intended to enhance privacy rights and consumer protection for residents of California.

KYC
Know your customer guidelines require that financial institutions make an effort to verify the identity, suitability, and risks involved with maintaining a business relationship.

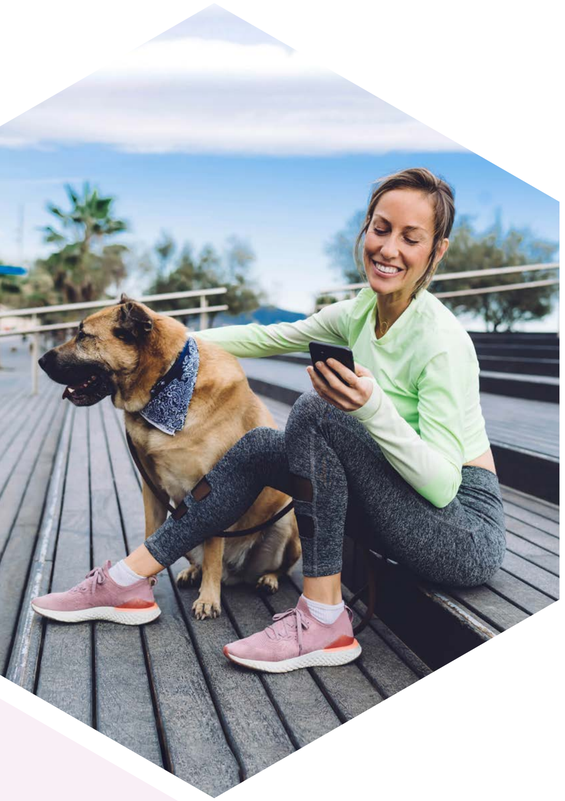
Resources to help you meet compliance mandates:

Payment Services Directive 2 (PSD2) White Paper

eIDAS Regulation for Dummies ebook

European Data Protection Board GDPR Guidelines

CCPA Webpage



Improve the consumer experience

Limiting consumer friction and avoiding abandoned financial applications requires a number of tools that allow consumers to access services themselves, anytime, anywhere, including the ability to onboard for new accounts.

Providing seamless experiences while continuing to ensure only authorized users gain access to financial information is a major challenge. To ensure the surging demand for mobile banking can be met securely, FIs must depend on trusted identity solutions like identity proofing and device reputation, along with intelligent authenticators like biometrics and adaptive risk-based authentication, to provide an added, yet invisible layer of security.

Additionally, instant issuance, whether digital or physical, delivers on consumer expectations of real-time access while also aligning with the high degree of security and trust required to ensure improved experiences.

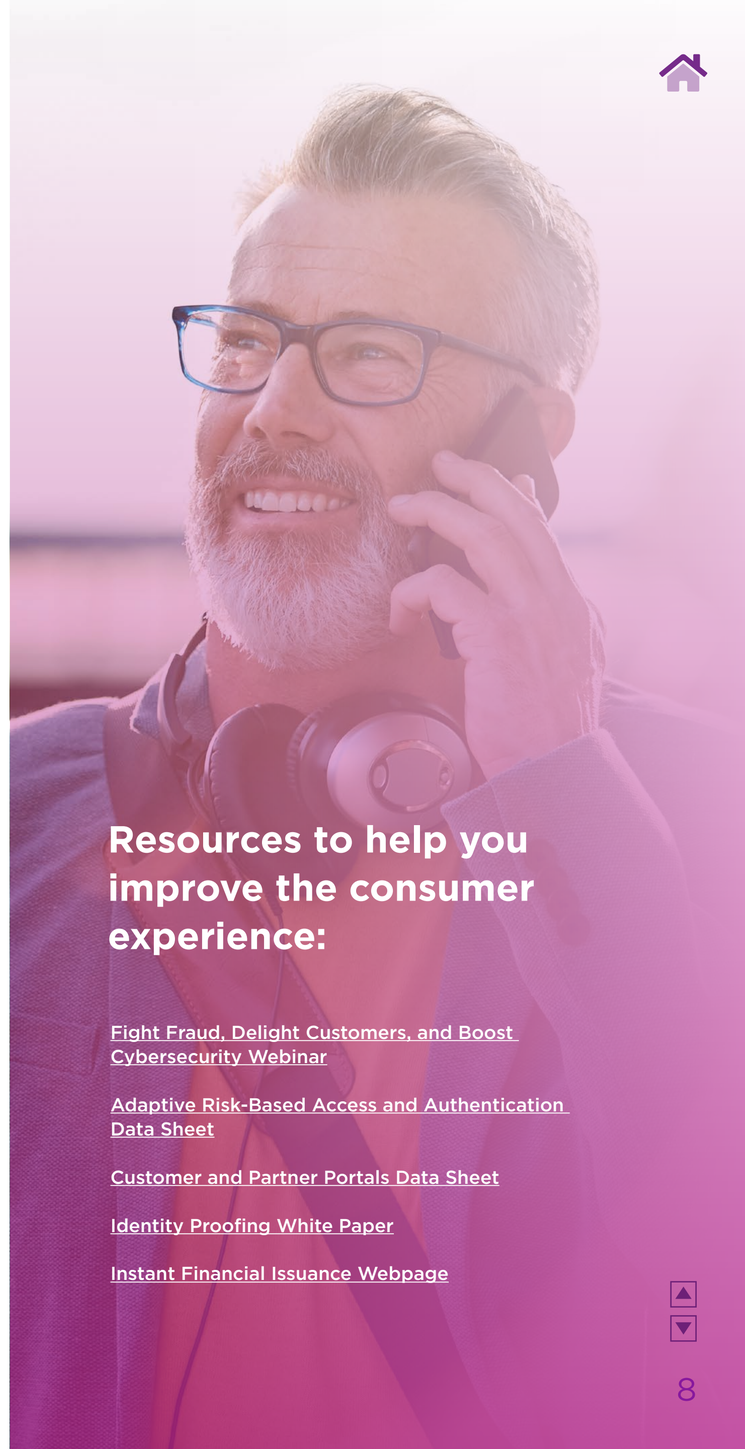
Improve the consumer experience with...

Identity proofing

Device reputation

Biometric

Risk-based authentication



Resources to help you improve the consumer experience:

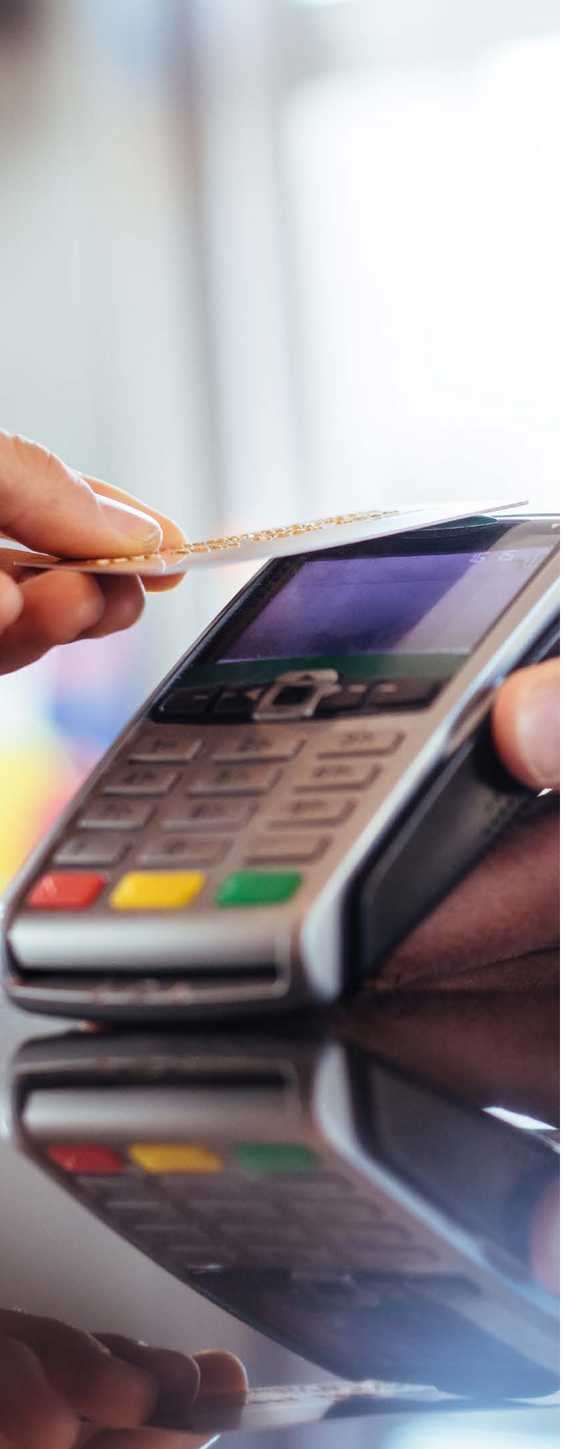
Fight Fraud, Delight Customers, and Boost Cybersecurity Webinar

Adaptive Risk-Based Access and Authentication Data Sheet

Customer and Partner Portals Data Sheet

Identity Proofing White Paper

Instant Financial Issuance Webpage



Secure your financial infrastructure

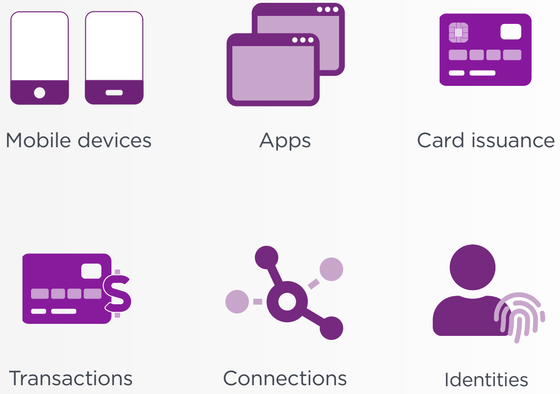
Mobile devices, apps, card issuance, transactions, and connections must all be secure to protect the integrity of financial services provided and ultimately, the safety of consumers.

Device reputation establishes trust in the device first. Run-time application self-protection (RASP) and code signing help keep mobile apps secure, while TLS certificates, including qualified website authentication certificates (QWACs), create trusted connections and provable ownership.

Securing the authenticity of card issuance systems needs to be done at the manufacturing level via code signing and key/certificate injection, ensuring the security of data collection and communication needs to occur at the operator level with encryption and authentication. As well, HSMs protect your certificate infrastructure.

Seamless card issuance across your financial network, either in-branch desktop card issuance systems or centrally from a bureau with high-volume central issuance systems, depends on ensuring security across your entire financial infrastructure.

All must be secure to protect your financial infrastructure:



Resources to help you secure your financial infrastructure:

Mobile App Protection – RASP & Code Hardening Data Sheet

Importance of Code Signing White Paper

nShield Issuance HSM Data Sheet

Issue Cards at the Speed of Life eBook

Enable a secure, productive workforce

People are always your largest attack surface. It's no different in banking, where 27% of cyberattacks originate with bank staff.[3] Keys and certificates issued by a public key infrastructure (PKI) offer the highest levels of security and enable use cases such as secure email, file encryption, and non-repudiable digital signatures.

Multiple login credentials to different systems frustrate users, which can also lead to poor password hygiene. High assurance credential-based authentication with single sign-on (SSO) remedies these concerns. Better yet, take your workforce passwordless with credential-based authentication that transforms their mobile devices into their trusted digital workplace identities.

Faced with hybrid and multi-cloud environments including legacy apps, many financial institutions are forced to rely on manual user provisioning and de-provisioning, which adds cost and risk. This complexity can be removed with an identity and access management (IAM) solution that provides workflow orchestration.

[3]Verizon, 2020 Data Breach Investigations Report

Keep workers secure and productive with...

- High assurance credential-based authentication
- Passwordless access
- Single sign-on
- Secure email, file encryption, and signing

Resources to help you enable a secure, productive workforce:

- Passwordless Solution Selection Guide
- Identity for Workforce Brochure
- Consolidated Bank of Kenya Case Study
- Entrust Mobile Device Management (MDM) Integration Solution Brochure

Issue cards securely at scale

Creating a strong line of defense for high-volume card issuance requires a number of different disciplines and tools.

Card issuance operators need to restrict access to controllers, ports, CD/DVD drives, and network connections. Systems should also be able to control operator access based on roles to ensure that data directories and write devices are secure.

To help mitigate security risks, card issuance operators need equipment that provides strong lines of defense for data at rest, data in transit, and data in use. This includes encrypting data throughout the personalization process. As well, operators need to destroy sensitive customer data left behind on supplies.

Integrating delivery and insertion systems with your high-volume card issuance solution will help you realize further efficiencies and provide high-impact messaging opportunities for card carriers.

Ensure a scalable card issuance operation with:

Role-based access

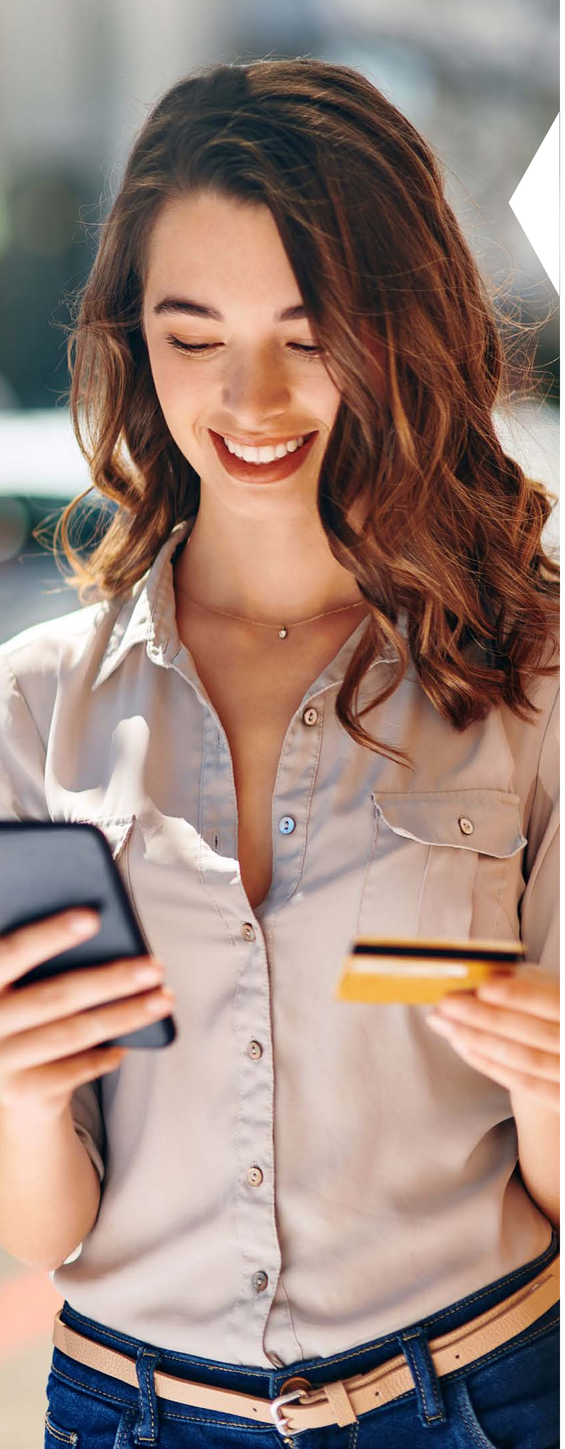
Encryption

Delivery and insertion systems

Resources to help you ensure a scalable card issuance operation:

Central Financial Card Issuance Webpage

Inline Delivery and Insertion Systems Webpage



Safeguard financial service delivery and transactions

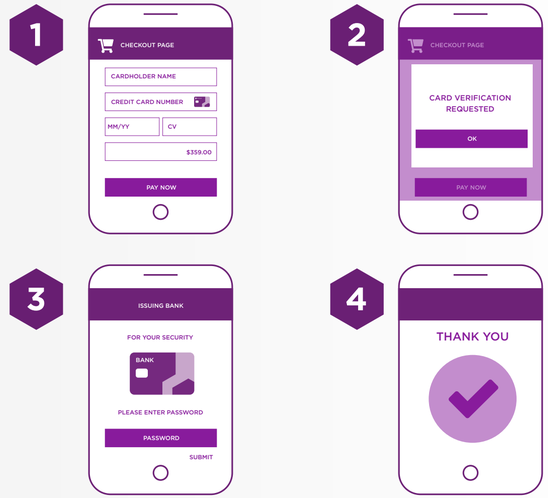
Digital transformation has significant security implications for financial institutions, their service partners, and consumers.

Financial institutions need to continually invest to stay ahead of bad actors, securely engage with customers, and digitally deliver financial services. This starts with digital identity proofing for secure self-service client identity verification and onboarding. Once a customer is authenticated, secure credentials can be issued.

These physical and digital credentials can be issued en masse from a central location. Alternatively, instantly activated physical and digital credentials can be generated from any distributed site connected to the financial institution's secure network.

Financial institutions, third-party payment providers, and merchants need to be able to ensure the authenticity of financial transactions performed remotely. 3-Domain Secure (3DS) compliance for CNP transactions, transaction signing and verification with mobile push, and digital document signing improve efficiency, security, and traceability.

How does 3DS work?



Resources to help you safeguard financial service delivery and transactions:

Identity Proofing Data Sheet

Instant ID Issuance Data Sheet

Identity Enterprise Transaction Signing Solution Brochure

Stop CNP Fraud while Complying with PSD2 Webinar

Advance the adoption of emerging banking technologies

The adoption of digital currencies, blockchain, and distributed ledger technologies (DLTs) depends on trust – more specifically establishing a strong root of trust to ensure these are protected.

Cryptographic keys and processes provide the foundation of digital currencies. HSMs deliver FIPS- and Common Criteria-certified key generation and protection, and high performance to handle escalating numbers of transactions.

As with any crypto-based infrastructure, protecting keys is paramount to ensuring a blockchain system's security. HSMs offer the scalability and flexibility a decentralized blockchain model requires.

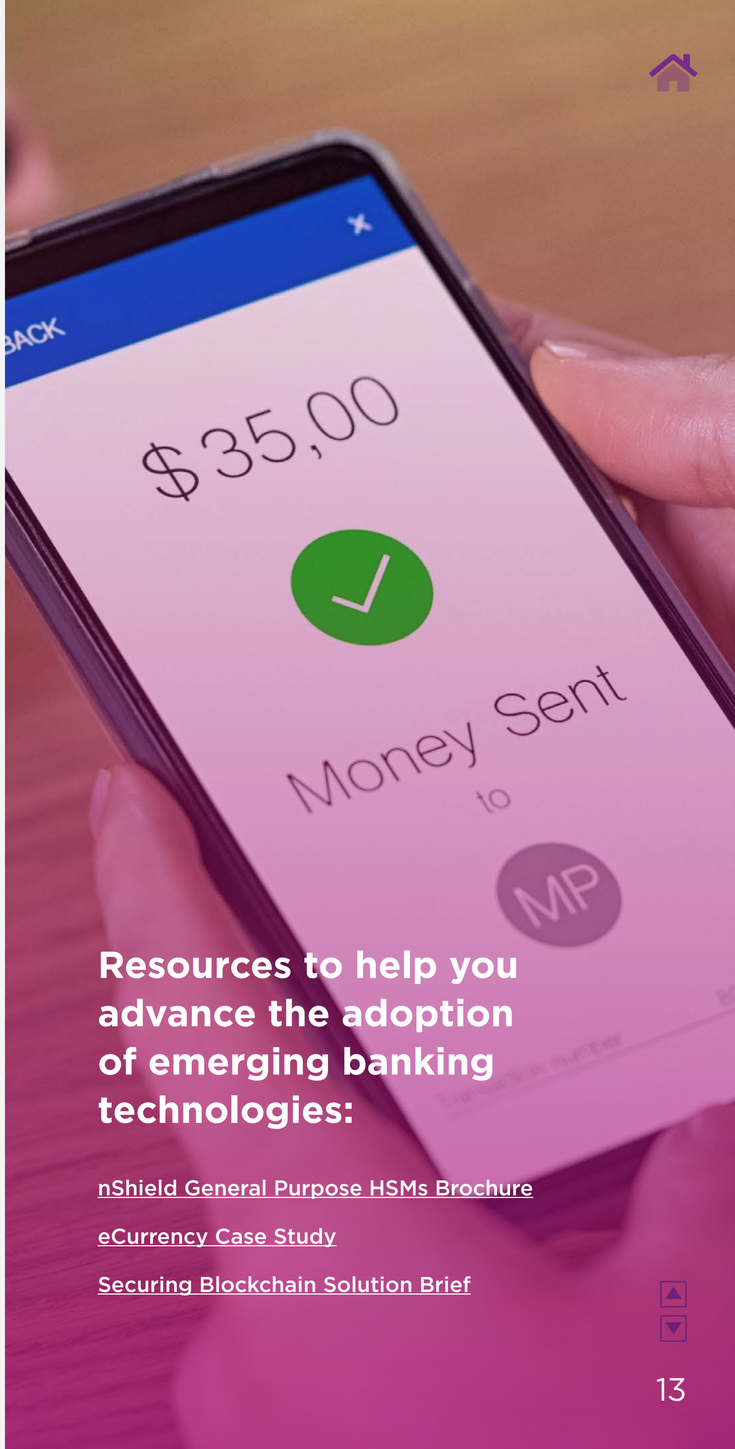
The consensus logic underpinning blockchains and DLTs must be fully safeguarded. The tamper-resistant HSM execution environment protects sensitive signing processes with support for the latest elliptic curves.

The emerging technologies you will be protecting:

Digital currencies

Blockchain

Distributed ledger technologies



Resources to help you advance the adoption of emerging banking technologies:

nShield General Purpose HSMs Brochure

eCurrency Case Study

Securing Blockchain Solution Brief

For more information

888.690.2424
+1 952 933 1223
info@entrust.com

entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com entrust.com/contact