EBA — SECUREPAY COMPLIANCE GUIDE

Entrust Datacard™

+1-888-690-2424 | entrust.com

Table of contents

Introduction to Today's Consumer

Today's consumer lives under the constant threat of identity theft, worrying that attackers will steal their money from their bank or credit card account. Depending on the liability policy in effect for the specific crime, anyone, consumer, retailer or bank alike, could be held accountable for the loss.

Online attacks on banking and e-commerce organizations erode customer trust. Breaches lead to negative impact on the bank or e-commerce brand, which can result in loss of customers. Therefore, security risks and erosion of trust emerge as major concerns even though moving services online provides great opportunities for financial and retail organizations to grow their revenues and customer base.

Security risk types that threaten businesses and promise to destroy customer trust include:

- **Card Not Present (CNP)/Online Fraud** - The attacker uses a copy of the consumer card number, expiry date and CVV to make an on-line purchase of goods. This is CNP fraud. In 2013, the European Central Bank identified that this type of attack increased by 24.7%, resulting in fraud that totaled 958 million euros for the year.[1]

  Hackers aren't deterred by advances in security measures. Instead, they adapt to these security advancements by evolving themselves. With the introduction of Europay, Mastercard and Visa (EMV) cards, card skimming attacks have become significantly harder for cyber criminals to carry out, particularly in-store. However, as CSO points out, the switch to EMV cards will cause merchants to implement fraud resistant chip point of sale devices in their brick and mortar stores, leaving them open to online attacks and liable (as well as the banks that fund their store cards) for losses resulting in fraudulent use.[2]

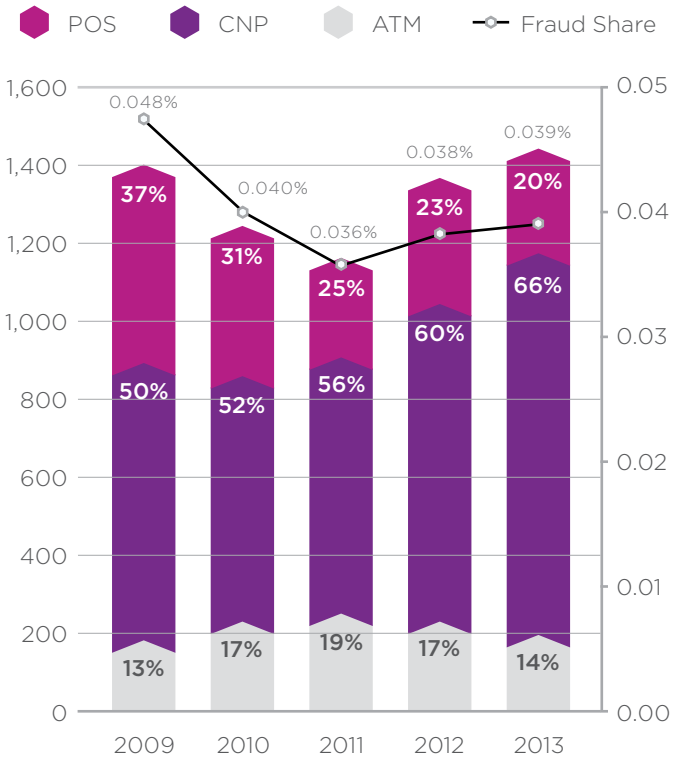
- **Man-in-the-Browser (MITB)** - MITB attacks, as TechTarget explained, transpire when criminals commandeer a user's Web transactions in real-time via a Trojan horse.[3] This type of attack is particularly concerning because it can appear that transactions are happening as they should, when, in fact, an intrusion is occurring.

- **Magnetic Stripe Cloning** - In countries where EMV cards and readers are deployed, it is near impossible to clone the chip, so the attacker must clone the magnetic stripe and take the attack to a country where they have not yet deployed credit card chip readers. The attack would be on an ATM or point of sale device which still uses magnetic stripe for the transaction. This type of attack, while not related to card not present fraud, can be prevented through the same Transaction Approval solution proposed for CNP when implemented by the card issuing bank.

When taking these facts into account, it becomes clear that a solution that helps secure online channels without placing huge demands on the consumer is required.

1 https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf
2 http://www.csoonline.com/article/2134340/malware-cybercrime/shift-to-emv-cards-expected-to-increase-online-fraud.html
3 http://searchsecurity.techtarget.com/definition/man-in-the-browser

Figure 1 Card Not Present Attacks on the Rise



On December 19, 2014, the European Banking Authority (EBA) published its final guidelines regarding the security of Internet payments.[4] All but three of the 28 European countries that make up the European Union have agreed to institute laws for compliance with these guidelines to fight Card Not Present fraud (The UK, Estonia, Slovakia opted out).[5]

Millions of dollars are spent annually on identifying whether transactions are being made by cardholders or by impersonators. And, while defeating fraud is a top concern, and regulatory guidelines help protect the consumer, there is a need for a more balanced approach – one that takes both the user experience and security into account.

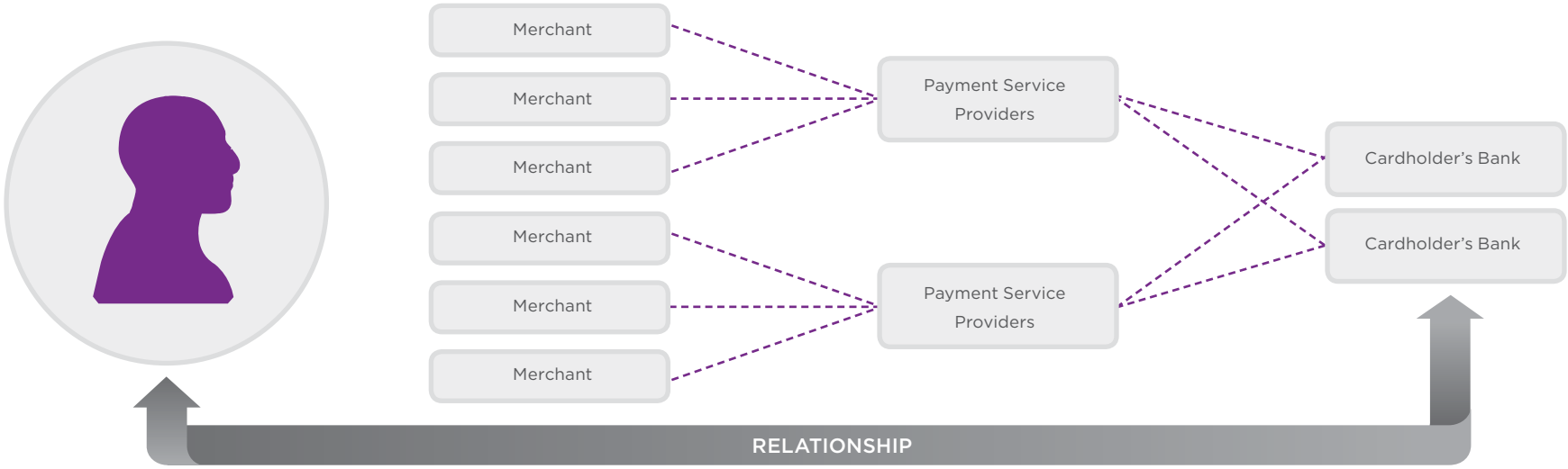
Today's always-connected, mobile, security conscious consumer has the potential to change how transactions are made. User experience is paramount to customer satisfaction — and no one is willing to deal with a clunky security solution. If security introduces too much friction, this leads to abandoned shopping carts and online transactions as users get frustrated and go elsewhere to spend their money. As service providers migrate more services to the online channel, they must balance security with user experience. A bad user experience and too much security interference and customers will become frustrated. But absent robust security, patrons won't trust your business. It's a vital balancing act, and if an enterprise gets it wrong, the customer will look elsewhere.

4 Legislative https://frederikmennes.wordpress.com/2015/02/04/security-of-internet-payments-legislative-developments-in-europe/
5 http://www.finextra.com/News/fullstory.aspx?newsitemid=27389&topic=payments

Overview of Payment Network

The Security of Internet Payments guide allows for any of the three participants in the payment transaction shown in the diagram below to authenticate transactions. Some of the security challenges and solutions facing these participants are:

Figure 2 The Payment Transaction



- **Merchant:** The merchant has an existing relationship with their consumers, which enables the merchant to request the transaction to be approved by the consumer through strong authentication. This will reduce the merchant's cost of fraud and improve their confidence in that merchant leading to more purchases. From the consumer viewpoint they will still experience fraudulent transactions as the counterfeit card will be used to make purchases in a country or merchant that does not require strong authentication. As well, each merchant bears the additional cost of compliance, which is passed onto the consumer as higher prices.
- **Payment Service Providers:** The payment service providers do not have a direct relationship with the consumer. The merchant must share their consumer relationship with their PSP to allow for a common solution, where the transaction is sent to the consumer for approval by strong authentication. Care must be taken within a region to prevent the consumer from being inundated with disparate authentication schemes across several PSPs. This could be achieved by PSPs within a region sharing a common framework for consumer transaction approval.
- **Card Issuing Bank:** The consumer's bank is in a very good position to implement strong authentication to its existing customers, as they have the existing consumer relationship + all payment requests, regardless of where it originates, is sent to the bank for approval. On receipt of a payment request, the card issuing bank needs to implement transaction verification, so that regardless of where the transaction originates, it will always end up with the consumer for approval. The bank no longer needs to rely solely on complex fraud detection to look for purchase irregularities.

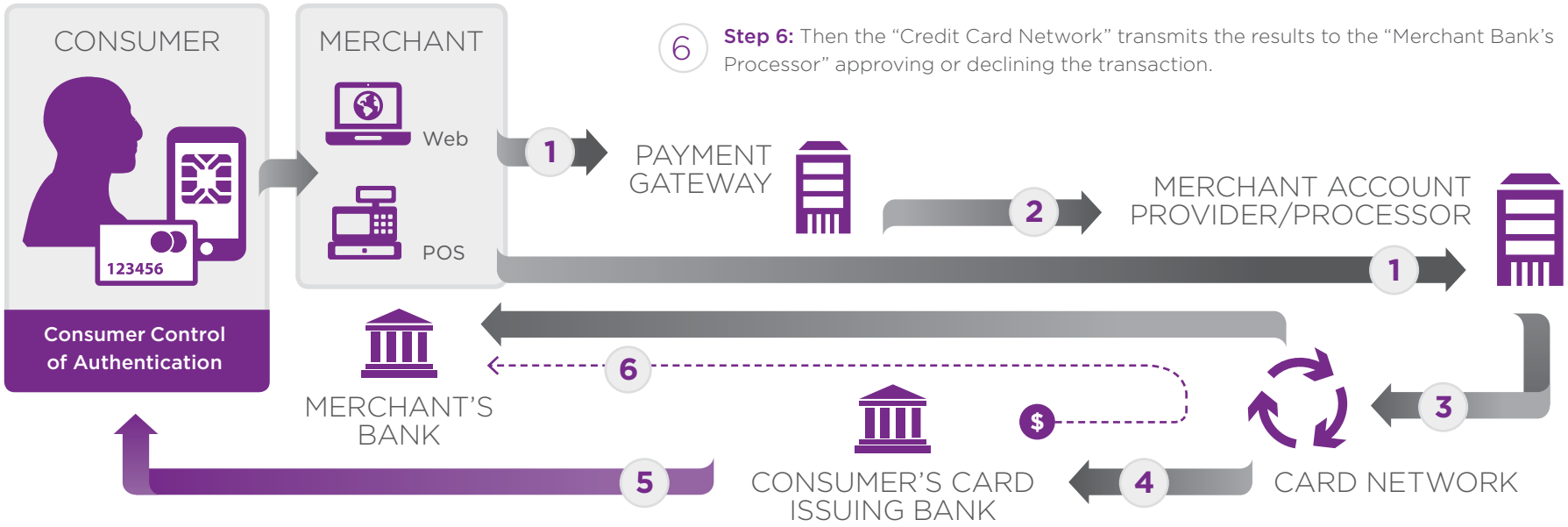
Entrust Datacard's Solution for Securing Internet Payments

Entrust Datacard provides a broad range of transaction verification and authentication solutions to help secure Internet payments. Our most popular method makes use of consumer mobile devices as the means to approve transactions.

When a new transaction is initiated received on Entrust's Authentication platform, it can be sent "out of band" to the user's mobile device for verification and confirmation, providing a simple, yet secure way to mitigate the threat of account takeover attacks. The following sequence of events maps out the process from transaction initiation to final completion using Entrust IdentityGuard as the internet payment solution:

1. **Step 1:** The merchant's website sends a credit card transaction to a "Payment Gateway" via a secure site connection.
2. **Step 2:** The "Payment Gateway" receives the credit card transaction request. If the choice has been made for the payment gateway to perform the authentication, then the transaction is sent to the consumer for approval. The transaction is then sent to the "Merchant Bank's Processor" using a secure connection.
3. **Step 3 :** The "Merchant Bank's Processor" sends the complete transaction request to the "Credit Card Network" (financial system network that is used to process CC transactions).
4. **Step 4:** The "Credit Card Network" forwards the complete transaction to the "Customer's Credit Card Issuing Bank."
5. **Step 5:** The cardholder or customer approves the transaction. The Customer's "Card Issuing Bank" accepts or refuses the transaction depending on the customer's available funds and sends back the results to the "Credit Card Network."
6. **Step 6:** Then the "Credit Card Network" transmits the results to the "Merchant Bank's Processor" approving or declining the transaction.

Figure 3 The Entrust Internet Payment Solution



A better approach to securing the payments channel

There are clearly many different approaches to securing e-commerce transactions. But what businesses must consider is how the secure approach directly impacts the integration efforts and deployment complexity of the solution.

Implementing transaction verification at the card issuing bank means you implement the solution one time and that the cardholder is covered, regardless of where the purchase or payment originated. And, because you are implementing the transaction verification, you have increased control while simultaneously ensuring a positive customer experience, gaining the opportunity to introduce new services that can drive increased customer stickiness and revenue down the road.

Figure 4 Reviewing and Approving Transactions

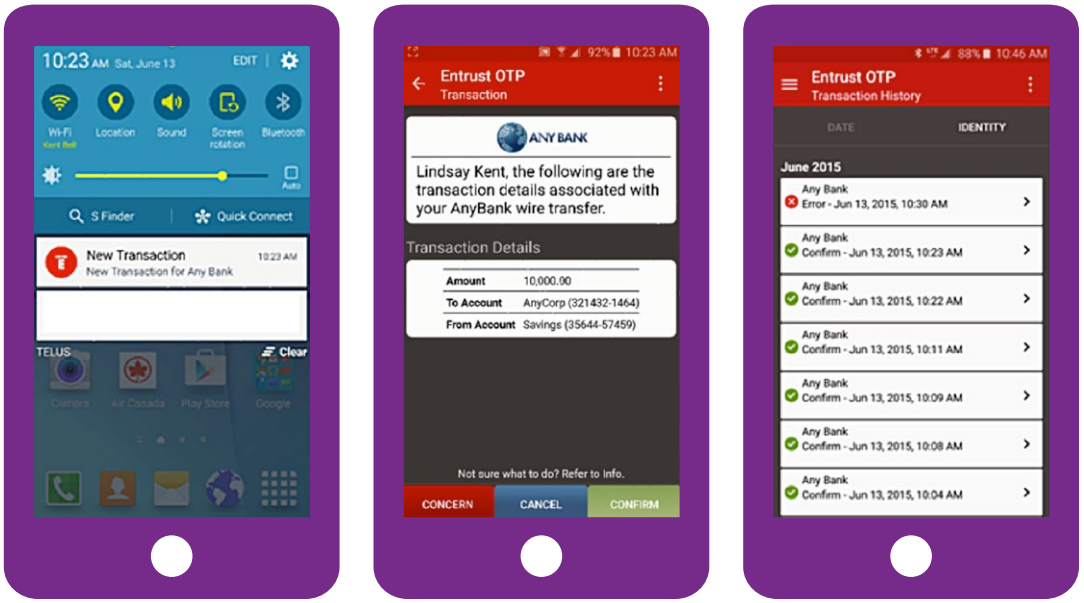


Figure 5 The Self-Service Web Page

The consumer uses a self-service web page augmented into the existing bank web portal to stay in control of the transactions sent for approval. This web page allows the consumer to reduce the number of transactions sent to their mobile device.

The Implementation Process

The implementation of the Entrust IdentityGuard Transaction Signing Solution begins with the integration of a mobile toolkit within the institution's payment application, merging the security approach of an EMV credit card with the convenience of a mobile device.

The toolkit includes either a PKI or OATH one-time-password consumer digital identity. The digital identity can be protected from theft either in the software or by the mobile device's inherent hardware; i.e. Samsung Knox and Apple Secure Enclave. A device fingerprint is recorded during issuance, which will identify when/if the digital identity is ever moved to another device for transaction approval (authentication). The cardholder's fingerprint or PIN is utilized to ensure the cardholder is the person who is in possession of the device.

Each payment transaction is sent as a notification to the mobile device, similar to a notification from Facebook. The consumer simply clicks the notification to bring up the banking application, and reviews the transaction, either approving or rejecting it. The cardholder can review all the past transactions, to compare to their monthly bank statement, as shown below.

Even if the payment transaction was originated on the same mobile device which contains your digital ID, the transaction will always sent "out-of-band" in a separate secure communications channel from that which was used for the purchase. The transaction is then processed by a different mobile application with a separate digital ID in a separate secured location. In the event a higher assurance level is required, the solution may be complemented by alternatives from the Entrust IdentityGuard platform.

A key challenge to any deployment is to ensure the credential used in all the payment approvals, is owned and under the control of the rightful owner. The Entrust IdentityGuard solution has the ability to authenticate with an existing authenticator prior to the issuance of the mobile digital identity. Options include: Question and Answer, National ID card, Credit Card, one-time-password and fingerprints. We can help you identify the right approach for a given deployment scenario.

The Transaction will always be completed

Figure 6 QR Code Security Challenge

In the event the card issuing bank cannot reach the consumer's mobile device to approve the transaction, the Entrust toolkit within the banking institution's banking application can still digitally sign the transaction presented on the Web page. An encrypted QR code will be displayed within the online merchant's browser, which can be scanned by the mobile application and the 8-digit digital signature entered into the merchant's system. This simple integration at the merchant, payment service provider or card-issuing bank allows for the transaction to be completed securely.

Unlike the 3D secure approach, which has seen consumers getting confused, encountering poor experiences, and forgetting their passwords, the Entrust Solution presents an experience similar to viewing a Facebook post or approving a Linkedin post, and supplies security without a password, meaning there is nothing for the user to forget.

The data shows us that customers who are presented with the 3D Secure screen when making a payment are five times less likely to go through with the payment than those who do not see the 3D Secure page. Only 14% of our sample actually persisted with the transaction when 3D Secure was enabled. Of those that continue with the 3D secure authentication, 17% are declined due the wrong password.[7]

7 http://hub.judopay.com/cart-abandonment-rates-and-3d-secure/

Augment your existing authentication solution

Entrust realizes that existing bank systems can be expensive to replace, so, with Entrust IdentityGuard, we provide the option of invoking a transaction request from either an existing authentication product or from an existing payment system using an Application Program Interface (API). The products will collaborate to use an existing authenticator to personalize the mobile toolkit embedded into the banking application.

In the event that the bank does not have an existing authentication server, then Entrust IdentityGuard also has a package that provides for a full authentication server.

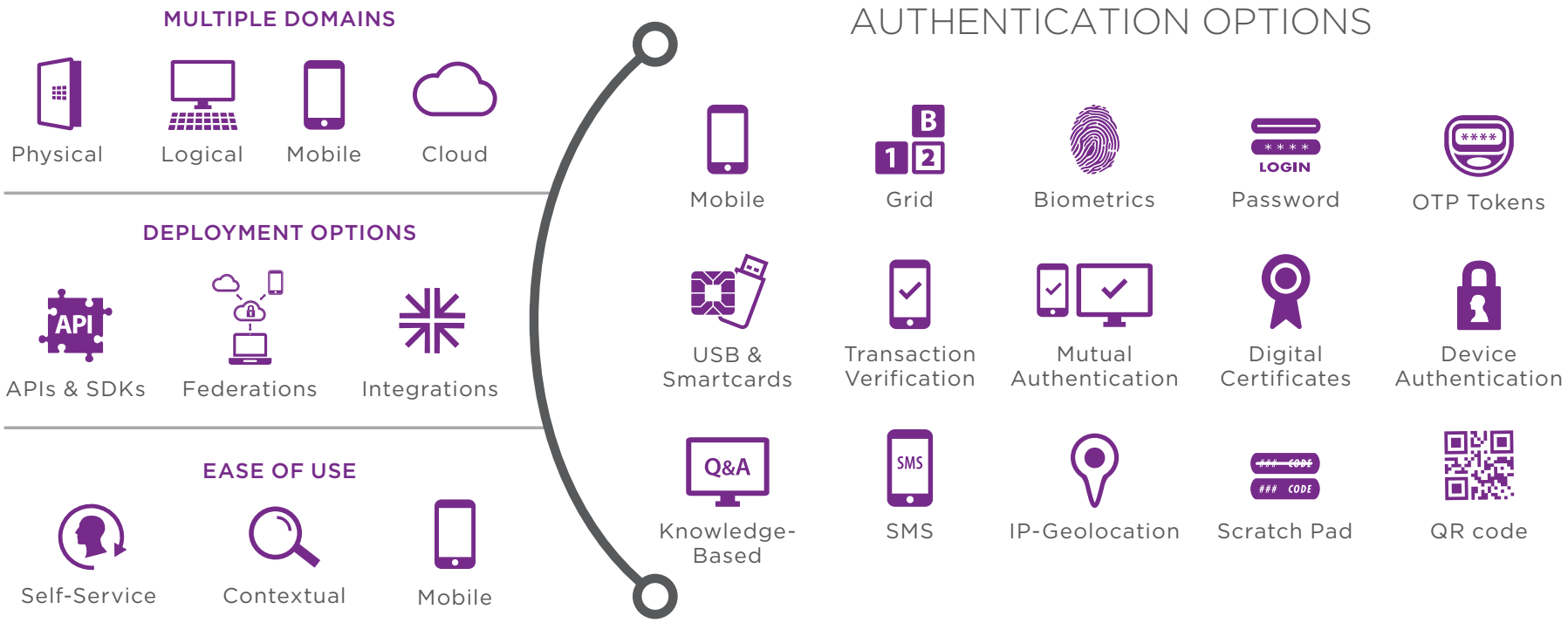
Once personalized, the mobile credential is ready for immediate use without any changes to merchants, ATMs or point of sale systems.

Entrust IdentityGuard: The Flexible Authentication Platform

Entrust IdentityGuard is a next-generation identity-based security framework that serves as the foundation for your current and evolving digital identity needs. With rich, contextual policy management, security can automatically adapt according to access requirements or the risk in a given transaction, across diverse users and applications.

Entrust's software authentication platform does not impact normal user behavior or back-end applications, speeding deployment and helping to save money. Entrust IdentityGuard affords the flexibility for specific authenticators to be defined per application and/or group so you can tailor your security to the use case and risk situation. Simple policy change can seamlessly adjust the authentication behavior of all applications virtually instantly and without have to re-architect applications, giving you the flexibility to protect what matters most proactively.

Software Authentication Platform



Entrust's management framework is unique in the market and drives significant value for today's connected enterprise. The solution enables organizations to deploy strong, risk-based authentication to properly secure employee access, privileged user accounts and even customer and partner access to company portals.

- Deploys to a single server
- Co-deploy with existing authentication solutions for smooth migration
- Simple integration and easy-to-use APIs
- Mobile, physical and logical authentication
- Federate internal and cloud-based applications (e.g., Salesforce.com, Microsoft 365)
- Reduce cost and maximize staff efficiency with an intuitive self-service module

Compliance with "Assessment Guide for the Security of Internet Payments"

Entrust IdentityGuard is compliant with the European Central Bank Assessment Guide for the Security of Internet.

European Central Bank Assessment	Entrust Datacard Solution
7.0.1 Does the authentication procedure make use of two or more elements to prove the authenticity of the user?	The authentication procedure utilizes a digital identity within the device representing the user and is protected from unauthorized use via a user PIN or biometric.
7.0.2 For ownership and inherence elements: Did independent and competent third parties certify or evaluate that the level of security for these devices is sound and that they are tamper-resistant?	The Entrust IdentityGuard cryptography is FIPS-140 certified. The Certificate Authority is Common Criteria certified. Entrust products are utilized in government and bank security worldwide.
7.0.3 Have the security features of the solution been properly defined and implemented (e.g. algorithm specs, key length, information entropy22)? • The security features follow publicly available and recognised standards. • For one-time passwords (OTPs): Is the password value generated using secure devices and procedures based on publicly available and recognised standards? The procedures generate sufficiently complex passwords; the knowledge of one password value does not assist in deriving subsequent values.	The Entrust solution uses open standards: • X.509 certificates with RSA 2048 or Elliptic Curve P256 keys • OATH one-time-password and challenge response • PIN policy is set by the bank and enforced by the Entrust mobile toolkit • AES 256 keys • Global Platform secure channel • TLS 1.2

European Central Bank Assessment	Entrust Datacard Solution
7.0.4 If a multi-purpose device (e.g. mobile phone or tablet) is used as the ownership element (e.g. to receive or generate a one-time password or initiate a drop call mechanism), does the PSP apply measures to mitigate the risk of it being used to initiate a fraudulent internet payment at the same time (e.g. via viruses/internet attacks)? o Do the security features follow recommendations contained in publicly available and recognised standards? o Is the payment itself initiated via a separate/independent channel?	The Entrust toolkit incorporates a device fingerprint and risk score to identify whether a digital identity has been compromised. The risk score will include several aspects of the mobile device including whether known malware is on the device or if the device was jail broken. Regardless of the device the transaction originated on, the transaction authentication is sent in a separate TLS channel to the user's mobile device.
7.0.5 Are the secrets used for the knowledge element based on an appropriate security policy? o Is there a password policy (information entropy, complexity, length, expiration time, number of characters that cannot be repeated, not guessable)? If so, is it enforced? o If a non-password-based procedure is adopted, is it ensured that the likelihood of a false positive is comparable or less than the case of a (sound) password?	The PIN, PIN unblock, symmetric and asymmetric key, OATH seed lengths are set by the bank policy configured into Entrust IdentityGuard and enforced in the Entrust mobile toolkit.
7.0.6 Are the procedure and the chosen elements designed to ensure independence, e.g. in terms of the technology used, algorithms and parameters? o The breach of one authentication element leaves the protection offered by the other elements unaffected (e.g. in the case of knowledge + ownership, the theft/misappropriation of one element leaves the effort necessary for the attacker to breach/bypass the other unchanged). o Alternatively, in the case of co-dependence (e.g. where a PIN is used to initiate the generation of an OTP for a device) the risks are appropriately mitigated, taking the following into consideration: **a)** specific security measures to avoid PIN guessing or retrieval from the device; **b)** anti-cloning features of the device (e.g. smart card, token, SIM); **c)** particularly strong security features of the OTP generated (length, information entropy, random algorithms).	There are several aspects of the security. Each is independent of the other, but all must be accepted when the transaction signature is validated: o The cardholder PIN or fingerprint. o The consumer's digital identity in the form of an RSA2048 or P256 key or OATH seed value. The identity is encapsulated within an applet which protects the identity from theft, it only replies with proof of possession when presented with a PIN or fingerprint. o Where available, the applet with identity are protected in the Apple Secure Enclave or Samsung Knox. o The mobile device fingerprint recorded at the time of enrollment is checked and assessed for risk on each transaction o Velocity, geo-location checks are factored into a risk score.

European Central Bank Assessment	Entrust Datacard Solution
7.0.7 Does the strong customer authentication procedure operate in such a way that: • the customer has to input all the credentials before receiving a positive or negative result; • in cases of denied authentication, no information is given about which was the incorrect piece of data input (user ID, first element, second elements, etc.)?	The consumer must input all credential information during the transaction approval, the user is not told which of the checks failed.
7.0.8 Does at least one of the selected elements fall into the inherence category or is it/are they non-reusable and non-replicable? • Authentication codes are not replicable since authenticator values6 are accepted only once by the authentication system, allowing the user to perform only a specific operation. • It is not feasible to forge/clone an exploitable copy of the element (except for inherence), even having the element in availability, and it is also not feasible to steal related confidential information (e.g. cryptographic keys, sensitive software or private keys for digital signatures) via the Internet, including when not performing a payment-related transaction (e.g. via malware or advanced persistent threats – APTs).	Each transaction sent to the cardholder is digitally signed by the cardholder, resulting in a unique authentication not reusable by other transactions – real or malicious. The cryptographic keys are protected from malicious use, and when stored in the Trusted Execution Environment of an Android or Apple device, comparable to the protection offered by a smart card.
7.0.9 Is the confidentiality of the authentication value protected from the moment it is generated to its verification by the authentication server?	In the event the PKI option is utilized, the private key is generated on the device, within the applet and never leaves the applet. In the event the OATH OTP option is utilized, the seed value is: (Samsung Knox) generated by the server and sent encrypted to the Samsung Knox container. (others) the seed is generated by a shared secret only the Entrust toolkit and server know. The seed does not leave the toolkit or server once created.

About Entrust Datacard

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide. For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Company Facts
Website: entrust.com
Employees: 359
Customers: 5,000
Offices: 10 globally

Headquarters
Three Lincoln Centre
5430 LBJ Freeway,
Suite 1250
Dallas, TX 75240 USA

Twitter Facebook Youtube LinkedIn Google+ RSS

Entrust Datacard™

30110-1-0915