White Paper

Card Issuance at the Speed of Life

Securing In-Branch Issuance Technology

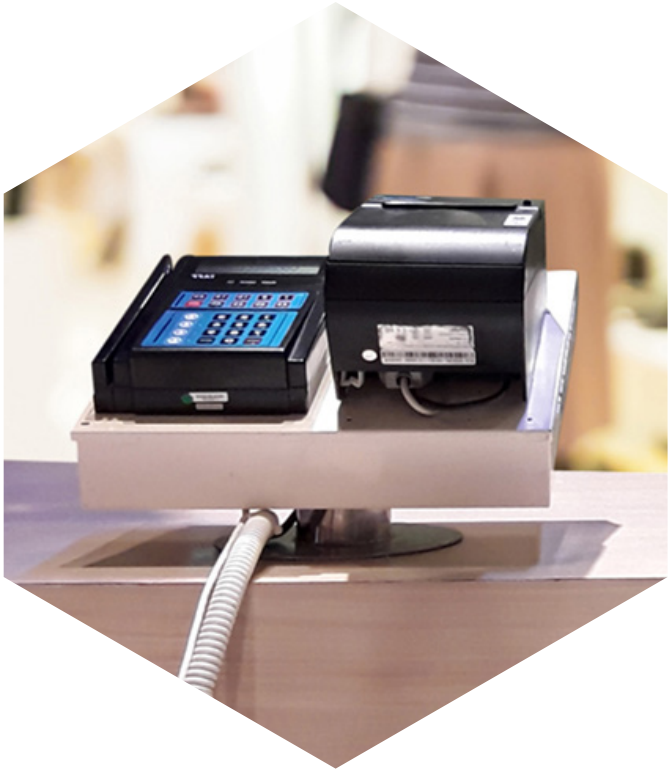
ENTRUST

SECURING A WORLD IN MOTION

This white paper is one in a three-part series focused on providing a more secure solution for instant card issuance. This series discusses three aspects of secure instant card issuance: hardware, software, and hosted services.

Card issuance in "real-time" at the branch is a service every cardholder desires. As securing data is critically important for financial services firms, they too often choose security over the customer or member experience and the ability to deliver services and products in a streamlined and on-demand fashion. Some interactions are more difficult and frustrating than they should be but that's beginning to change as financial institutions revolutionize their branch experience and upgrade their mobile touch points.

An excellent example of this evolution in action is debit and credit card issuance. Other industries have shown consumers that waiting times for services and products can be reduced dramatically, and increasingly banks and credit unions are leveraging in-branch card issuance to provide one of their most popular products, the debit card, the instant it's needed.



« Increasingly banks and credit unions are leveraging in-branch card issuance to provide one of their most popular products, the debit card, the instant it's needed. »

The technology for instant card issuance has existed for some time, but now improvements in security are making the technology more attractive to financial institutions that are wary of accepting the risk inherent in legacy systems and on-premises hosting. One important change is that new solutions are being designed with enhanced security at the very foundation of the solution. The includes critical security technologies such as Trusted Platform Modules (TPM) and Secure Boot start-up processes to better protect the end-to-end solution. These technologies satisfy financial firms' security requirements while causing no negative impact on the branch or cardholder experience. In addition, cyber-security professionals have improved their understanding of the threat landscape giving them greater awareness of where cyber threats are coming from and the technologies they can develop to stop them.

Although financial card numbers will remain a primary target of cyber-theft, new solutions that better secure the sensitive cardholder information at the point of issuance are making it possible to meet cardholder demand for immediate permanent card issuance while reducing risk and complexity.

The security of instant card issuance has improved to the extent that some financial institutions are now using it as a competitive advantage, touting instant card issuance in television commercials and other marketing material as a reason to change banks.

Instant Card Issuance Is a Major Improvement to the Cardholder Experience

One of the changes driven by recent events is a movement away from cash and toward payment cards of all types (debit and credit; EMV chip and contactless). With greater use comes more frequent need for card issuance and heightened awareness among consumers about the way in which they receive their card. With these options in mind, the legacy process of waiting two weeks for a card to arrive in the mail before it can be manually activated means a cardholder must resort to a different form of payment while they wait for your product to arrive – having a negative impact on activation, usage, and 'top of wallet' status in day-to-day transactions.

Instant card issuance is what consumers want, but financial institutions won't implement it if they feel the end-to-end solution is not secure and easy to support. There is good news. The security of instant card issuance has improved to the extent that some financial institutions are now using it as a competitive advantage, touting instant card issuance in television commercials and other marketing material as a reason to change banks. That demonstrates that financial firms understand that this service has a very high perceived value among cardholders, and creates an unmatched experience for new and existing clients alike.

Beyond just handing over a card to a consumer in need of a new or replacement card, it's important that the product provided meets their full expectations of what a secure payment card should be. Some financial institutions issue temporary cards, with only substandard security features like magstripe and no personalization. While "instant" in nature, the product doesn't "check the boxes" if it cannot leverage the latest security or be easily leveraged in ecommerce or card-on-file transactions. To realize the full lift of an instantly issued payment card, it's been proven that the following items are critical:

- **The card should match or be similar in look and feel to centrally issued cards.** This includes logos, personalization, and other features that the cardholder expects to see. This means that a firm that regularly embosses its cards will likely want to do the same with its instantly issued cards.
- **Instant activation is essential.** Providing immediate access to funds and purchasing power is the only way to create a "top of wallet" experience between your card and your customer or member. The ability to transact instantly is what sets an instantly issued card apart; however, not all instant issuance providers offer immediate card activation.
- **Touchless issuance options are highly valued during the pandemic,** and instant issuance can further enable the issuance of contactless cards through drive-up or drive-through issuance models.
- **Offering your institution's full card portfolio.** When instantly issuing cards from the branch, enabling the service for as many clients as possible offers a clear benefit. Having multi-hopper or blank card printing options as a part of an instant issuance solution means you can create a great experience for everyone.

« Providing immediate access to funds and purchasing power is the only way to create a "top of wallet" experience between your card and your cardholder. »

Providing Improved Hardware Security for Instant Card Issuance

In the past, concerns about securing the hardware used for instant card issuance caused some financial institutions to forgo offering this highly desirable service to their customer or member base. However, new hardware security measures have been implemented in the latest offerings, and more robust security is integrated into some select solutions on the market today.

In the last several years the tools for securing hardware physically and logically have improved by leaps and bounds. Some instant issuance providers that develop the entire solution have had the advantage of integrating software, hardware, and hosting components seamlessly. One example of this is the use of proactive protection from the instant the system is turned on. Secure Boot processes ensure the system has not been subject to a malware intrusion by using BIOS firmware to perform a hardware initialization prior to the operating system loading. With Secure Boot, the sensitive information used to program and encode permanent, activated payment cards doesn't fall into the hands of hackers or other bad actors. Another important cyber-security tool is the Trusted Platform Module – essentially the engine that securely encrypts all sensitive data that the system handles. TPM is an international standard for a secure crypto-processor, which is a dedicated microcontroller designed to secure internet-connected hardware through the secure creation, storage, and management of a variety of keys that are essential to payment card issuance. Both Secure Boot and Trusted Platform Modules come standard with certain instant card issuance systems that are available today; however, a majority of card issuance systems do not offer either option.

« Both Secure Boot and Trusted Platform Modules come standard with certain instant card issuance systems that are available today; however, a majority of card issuance systems do not offer either option. »

The following items represent a good checklist to use when evaluating instant card issuance solutions.

- Better protection for the hardware level of the device. As more stealthy, low-level attacks such as rootkits are used, it is necessary to protect hardware more fully below the operating system level and protect the BIOS as well.
- The use of Trusted Platform Module (TPM), a computer chip or microcontroller that securely stores the artifacts used to authenticate the hardware platform, is necessary. These artifacts can include passwords, certificates, or encryption keys.
- Utilization of Secure Boot, a security capability provided by Microsoft and other hardware providers that checks the signature of each piece of boot software to ensure that it is valid and has not been compromised, is the next step. This prevents malware from being loaded at startup. When a device on the network is breached, attackers load rootkits that inject malware when the system starts.

- Improved physical security is essential since the theft of the card issuance device or the materials housed inside poses risk exposure. In addition, electromechanical locks mean a physical key isn't the only way in. There are software locks that a security or branch manager could remote unlock from HQ or their home.
- Secure management of supplies, including destruction, has also become an important part of securing the overall hardware component. Stolen supplies have active card numbers and personalization information on them. Visa and Mastercard require the shredding of all instant issuance supplies with personally identifiable information.

Entrust Is a Leader in Secure Instant Card Issuance

Entrust pioneered instant card issuance and has used its experience and expertise to provide a highly secure solution that meets the needs of both financial institutions and their cardholders. The company has the only instant issuance offering that is certified under the PCI Card Production and Provisioning Security Requirements, an important and rigorous set of standards that embodies Entrust's commitment to security.

Focusing on the hardware component of secure instant card issuance, the company provides the most secure offering on the market. This solution utilizes both TPM and Secure Boot to prevent attackers from taking over the device and remotely controlling it. These protections also eliminate the installation of software that bypasses many other existing cyber-security software solutions. Coupled with other third-party security solutions that banks and credit unions typically deploy, the result is a far more secure card issuance device.

The focus on security extends to other "hard" aspects of the Entrust solution. One important feature is the use of electro-mechanical locks to physically secure the device and eliminate thefts. This also allows the branch operations to ensure the device stays in a physical location with excellent access security. An additional security focus is put on supply cassettes and ensuring opening, closing, and changing supplies is faster and more secure.

Another important extension of security is Entrust's Supply Management service. Proactive visits to the branch by badged Entrust technicians to shred sensitive spent supplies and reload the machine ensures that blank cards and other supplies don't become a risk.

For more than a decade, issuing instantly activated payment cards from a branch has proven to be a boon to cardholder satisfaction, branch effectiveness, and card portfolio performance for thousands of financial institutions across the globe. As payment security technology has evolved so have the underlying systems that support the issuance of those cards. Recently, with the move to single interface and then dual interface cards the instant issuance ecosystem has had to grow to take on greater security responsibilities. Entrust has remained at the forefront of innovation, offering a variety of hosting, hardware, software, service, and supply options – at the core is the firm's commitment to securing the end-to-end solution.

Key Takeaways

As the financial services industry experiences increased levels of competition for cardholders, providing services that result in cardholder delight is essential. Instant card issuance is one of these services. And with new offerings, such as Entrust's, that incorporate the latest advancements in hardware security, such as Secure Boot and TPM, providing this service is much simpler and more secure. With security enhancements such as those Entrust provides, it is now possible to offer this service with far lower levels of risk. The instant card issuance solution must also be designed to work seamlessly within a branch environment. Services such as support/maintenance and secure supplies management must be part of the solution.

Entrust is a leader in this field. Its latest offerings for secure instant card issuance provide much more secure hardware solutions that cyber-security professionals are demanding.

This is the first of a series of three white papers focused on secure instant card issuance. The remaining two will focus on the ecosystem/software and security hosting/nShield HSM from Entrust.

For more information on Instant Card Issuance from Entrust, please visit: **entrust.com/issuance-systems/instant/financial-card** or **get in touch**.

To find out more about Entrust Instant Issuance Solutions

entrust.com/issuance-systems/instant/financial-card

ABOUT ENTRUST CORPORATION

Entrust secures a rapidly changing world 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

Contact us:
entrust.com/contact/sales