White Paper

Card Issuance at the Speed of Life: Part 2 – Securing the Software Stack

Second in a Series on Instant Issuance Security

ENTRUST

SECURING A WORLD IN MOTION

This whitepaper is second 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 cloud.

Delivering Secure Instant Card Issuance: Protecting the Software

Banks and credit unions want to deliver an improved cardholder experience by providing new and differentiated services that create preference for their products and services. In most cases, this involves using technology in new and innovative ways. However, ensuring that the digital systems at the heart of these services are secure is critically important. In addition, compliance and legal demands must be met as a part of any solution.

To provide the best level of defense for sensitive data, it is crucial that effective security be in place to protect the software components of any digital service. Most cyber-attacks are focused on corrupting existing software or adding unauthorized software. In many cases, these types of attacks are hard to identify and remediate. Therefore, any new digital solution needs a fully integrated software security stack to protect it. Integrating software security at the outset is essential, since it provides a much higher level of protection than simply bolting on a few individual security or issuance products and hoping that there are no gaps or missing protection for new types of attacks.

As more banks and credit unions look to add new digital solutions for instant card issuance, the need for a secure-from-the-start product must top the list of decision criteria. A fully-secured solution will include not only issuance software, including key management and secure third-party integrations, but hardware-based protections and supply services as well. For example, it is a best practice for issuance hardware systems to utilize a trusted platform

> **Integrating software security at the outset is essential, since it provides a much higher level of protection than simply bolting on a few individual security or issuance products . . .**

module (TPM) for handling sensitive key information, to run Secure Boot processes at startup, and feature dual-access locks with physical and software controls. The integration of hardware and software security functionality to provide more cohesive protection is the hallmark of a best-in-class solution. To learn more about the specific hardware security features necessary to protect instant issuance devices, check out this **companion document** focused on that subject.

The ability to pay securely and easily is top priority for cardholders today. A dual interface contactless card enables the most secure way for customers to acquire a card.

> *Tools that empower the financial services institution to work more effectively with the vendor help ensure better security in the long run and ease of operations is more than just a nice-to-have.*

Protecting Instant Card Issuance Services with Comprehensive Software Security

Instant issuance vendors can take specific actions and approaches that provide more than just basic security. As noted previously, evaluating the total solution is important to picking the right instant issuance provider. Providers that deliberately design and build to an integrated solution are inherently more secure and easier to maintain. Trying to protect this type of solution after the fact with anti-malware or antivirus software isn't nearly enough. Banks and credit unions must demand this approach to security.

Another important element of deploying a more secure instant card issuance solution is a vendor that works directly with the financial institution to ensure the solution is built to work with their existing IT stack. Having to conform to the requirements of the provider often leaves institutions with an experience that is harder on the branch operators and end users. Tools that empower the financial services institution to work more effectively with the vendor help ensure better security in the long run and ease of operations is more than just a nice-to-have. Good examples of this are tools that quickly inform the bank or credit union when there is a security issue or when a specific device needs resupply or firmware updates. This makes operating a secure fleet of systems across a branch network simple, safe, and intuitive.

The next step is ensuring that the most important individual technologies or components of a secure solution are in place. Securing the software components demands multiple layers of protection. It requires integration with hardware and cloud and/or on-premises processing. Perhaps the most important element is the use of a hardware security module (HSM). An HSM is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, enables trusted authentication, and serves as the cryptographic engine to all communication to and from the issuance device. Ensuring that keys are protected is elemental to any card issuance operation.

> **TEP ensures that the cloud services to support card issuance are communicating with a device that is verified to be secure and is not propagating malware either upstream or downstream.**

The second component to focus on is the use of Trusted Endpoint (TEP) technology. TEP ensures that the cloud services to support card issuance are communicating with a device that is verified to be secure and is not propagating malware either upstream or downstream. Other approaches for increasing security can enhance what TEP delivers. For example, the Entrust cloud is PCI-CP-compliant, meeting the same stringent security requirements that bureaus and central issuers must achieve. TEP also makes it possible for a bank or credit union to be confident that the card issuance device can be trusted for secure interaction with the financial institution's own card management or other internal systems. With TEP, it is possible to have secure links between the Entrust cloud, the bank or credit union, and other third party providers that the bank has integrated into the instant card issuance solution such as card management systems, switch, and core providers.

Adding to this layered approach to security is the use of Trusted Identity Access tools. This is one of the primary integration points of software-based protection and the HSM. There are many complementary activities at work here. Using keys protected with the HSM means that credentials are well protected and dramatically reduces the likelihood of unauthorized access. Trusted Identity Access tools also work synergistically to provide more complete access protection. One of the most important ways they protect the system is by preventing rogue or ex-employees from gaining access. This is important because card issuance devices need stricter controls than some other pieces of technology.

The ability to securely manage keys is a recurring theme for securing instant card issuance solutions. Key management systems (KMSs) must be designed to provide comrphensive protection. A KMS should secure every step in the key delivery and use process, not just the front end or during changes. It is also important to choose a solution that simplifies managing multiple keys. Some instant issuance providers offer customized packages based on your existing key management processes, if you have them, or provide a full solution from end-to-end. This tailored approach means a simpler more secure solution for the institution and end user.

One of the most overlooked parts of securing the issuance platform is the ability to holistically manage all aspects of the deployment, ensuring that the necessary security tools are in place and working effectively. Managing the entire fleet of card issuance devices from a single management console that provides details on each device is the starting point. This device management capability also identifies devices that are experiencing issues or need particular attention.

Entrust Is a Leader in Secure Card Issuance Solutions

Entrust Datacard pioneered the instant card issuance solution. The company's experience, institutional knowledge, and expertise in providing optimized solutions allows banks and credit unions to deliver this exciting new capability that enhances cardholder experiences. This solution delivers the features and benefits that dramatically improve card portfolio performance including:

- Cards that have the same look and feel to centrally issued cards
- Instant activation
- Support for personalized designs
- Touchless issuance options
- A full portfolio of cards and card types

The Entrust solution meets the demands that financial institutions have for instant card issuance platforms. Security is a major focus, and this solution has a comprehensive and holistic approach to security, as noted in this installment of the security whitepaper series. The company provides comprehensive and integrated software security to protect not only the application, but the keys and credentials necessary to access the system as well. This offering is also designed to be highly reliable and available to ensure customers can get cards when they want them, whether you're running to solution on-premises or as a Service through our PCI-CP certified cloud. And Entrust supports all of this with a full range of secure in branch and remote services that provide a seamless experience for your branch staff and cardholders.

Key Takeaways

Across the world the proven preferred way to pay is the physical credit or debit card, accelerated by recent contactless innovations, and providing that most-favored product in an instant is invaluable to your customers or members. As banks and credit unions consider deploying technology to deliver this capability, ensuring that the entire environment is highly secure is the starting point. Entrust a proven provider of this solution, delivers a completely secure solution, including meeting all the requirements noted in previous sections of this document to ensure security of the software component of the offering.

Entrust starts by using an HSM to provide the highest level of cryptographic protection for keys, ensuring that they are delivered to the individual device without any breaches or compromises. This is followed up by using TEP security to ensure the device has not been compromised or infected with malware. Bank employees are verified using Trusted Identity Access tools that prevent unauthorized use, an important protection as changes in employee status or turnover must be accounted for. Finally, there is a secure KMS to protect the keys during every phase of the card issuance process. All of these activities are coordinated through a single management platform that monitors and provides the ability to interact with every issuance device in all banking locations as needed.

For those wishing to get more information about the Entrust solution, please go to: **https://www.entrust.com/solutions/instant-card-issuance** or **get in touch**.

To find out more about Entrust Instant Issuance Solution

https://www.entrust.com/issuance-systems/instant/financial-card

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