FUTUREX

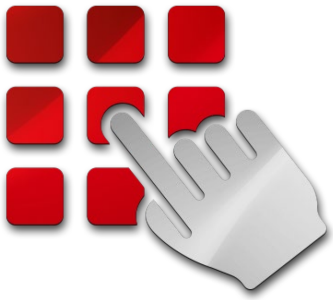
WHITEPAPER

Online and Mobile PIN Issuance

TABLE OF CONTENTS

OVERVIEW: ONLINE AND MOBILE PIN ISSUANCE

Personal Identification Numbers, or PINs, represent a cornerstone of security for banks, credit unions, merchants, and other issuers of payment cards. These numbers, typically 4 to 6 digits in length, are used to verify an accountholder's identity for withdrawing or depositing money, updating account details, making purchases, and more.



PINs are traditionally used as part of a multi-factor method of authentication. With multi-factor authentication, customers present something they physically have, such as a card, and something they know, such as their PIN. Historically, this required dedicated PIN Entry Devices (PED), limiting their use to ATMs, bank branches, retail Point of Sale terminals, or through automated Interactive Voice Response (IVR) based phone systems.

With the rise in mobile and web-based technology over the past decade, demand for additional methods of accountholder authentication and PIN management has increased. Just as solutions have been introduced into the market for software-based PIN entry for purchases, so too have techniques emerged for software-based PIN issuance and management.

This whitepaper outlines the cryptographic techniques involved in deploying a secure solution for online and mobile PIN issuance, along with the associated high-level features and benefits.

BUSINESS DRIVERS FOR ONLINE AND MOBILE PIN ISSUANCE

SECURITY

Above all else, ensuring the security of PIN distribution is paramount. Legacy methods of issuance, including IVR and paper-based PIN mailers, are fraught with risk, much of which is mitigated by online and mobile PIN issuance.

IVR phone systems are often used by card issuers to validate identities and perform PIN and account management tasks. These systems rely on automation and compensating backend controls to provide security, but still have vulnerabilities that must be considered, especially since the phone calls themselves are not encrypted.

Despite the near-universal use of tamper-evident packaging, PINs sent on paper-based mailers through the postal system can present a security risk. Since this distribution method often leaves the mailers in an uncontrolled environment, they are at risk for theft or unauthorized viewing.

When using online and mobile PIN issuance, the PIN is always distributed in a controlled environment where the end customer specifically requests it. Additionally, when changing PINs, the new PIN is encrypted using TLS from the mobile device or web browser all the way to the hardware security module (HSM), providing end-to-end security.

SPEED

Simply put, legacy methods of PIN distribution are not designed with speed in mind. The fastest methods of PIN distribution require the customer to physically visit a brick-and-mortar branch of their financial institution or an ATM. For many customers in rural or underserved areas, this can introduce additional delays. Mail-based PIN distribution, which is often used when accounts are created, is even slower and has additional risk of mailers being lost.

For online-only banks, speed issues have an even greater impact. With no brick-and-mortar locations, they must rely almost exclusively on PIN mailers. This means replacing a forgotten PIN often takes days, and even over a week in some cases.

When online and mobile PIN solutions are used, both for issuance and PIN changes, issues of speed are eliminated. Accountholders can change PINs on demand, reducing the service time to minutes.

COST

Distributing PINs through the postal service or through in-branch assistance is expensive. Manual labor is required for both service types, and postal distribution has the added expense of postage and mailing supplies.

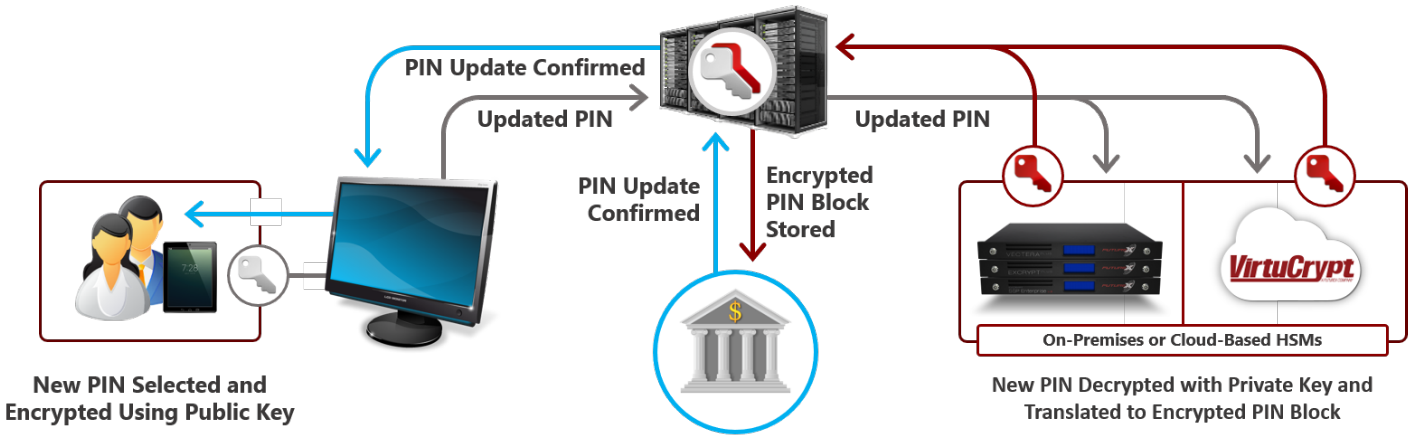
In many cases, organizations processing large volumes of PIN mailers can cover the cost of an online and mobile PIN solution completely from the operational budget savings that result from the associated reduction in PIN mailers.

CUSTOMER EXPERIENCE

Modern consumers seeking immediate gratification and self-service have led to the rise of mobile and web applications and along with that, entirely new types of financial institutions like online-only banks. Financial institutions around the world have taken advantage of this trend to launch smartphone apps enabling tasks like balance transfers, bill payments, account status updates, and remote deposit capture.

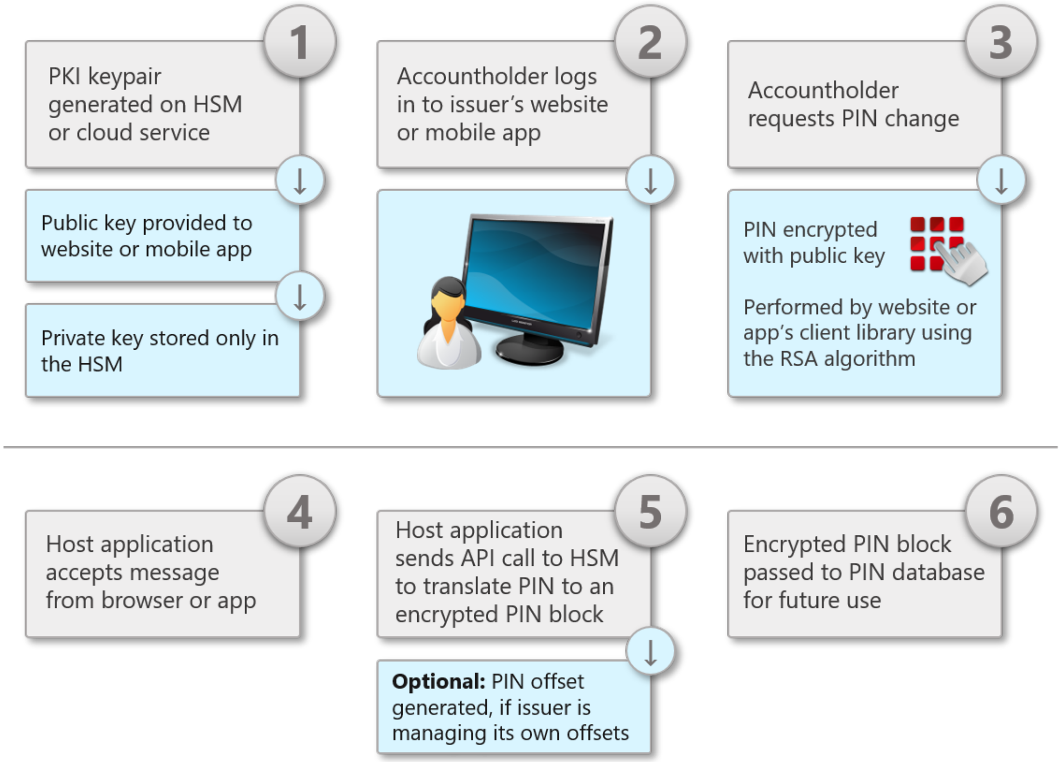
By adding PIN management functionality to their web portal or apps, financial institutions give customers an additional reason to use them. This creates opportunities for further cross-promotion of products and, ultimately, a better customer experience.

HOW DOES MOBILE AND WEB PIN ISSUANCE WORK?


PIN Update Confirmed
Updated PIN
Updated PIN
PIN Update Confirmed
Encrypted PIN Block Stored
VirtuCrypt
On-Premises or Cloud-Based HSMs
New PIN Selected and Encrypted Using Public Key
New PIN Decrypted with Private Key and Translated to Encrypted PIN Block

Conceptual Overview: Online and Mobile PIN Issuance

When performing a PIN change through an issuer's website or mobile app, the new PIN, encrypted using the web browser or app's RSA public key, is sent to the HSM or VirtuCrypt service instance. Within its secure, FIPS 140-2 Level 3 and PCI HSM compliant boundary, the HSM translates that PIN into an encrypted symmetric PIN block and provides it in a response which can then be stored in the issuer's PIN database for future use.



1. PKI keypair generated on HSM or cloud service
   - Public key provided to website or mobile app
   - Private key stored only in the HSM
2. Accountholder logs in to issuer's website or mobile app
3. Accountholder requests PIN change
   - PIN encrypted with public key
   - Performed by website or app's client library using the RSA algorithm
4. Host application accepts message from browser or app
5. Host application sends API call to HSM to translate PIN to an encrypted PIN block
   - **Optional:** PIN offset generated, if issuer is managing its own offsets
6. Encrypted PIN block passed to PIN database for future use

SECURITY CONSIDERATIONS

Successful mobile and web PIN issuance environments require collaboration and standardized communication protocols between the end user's web browser or app, the financial institution's host application, and the HSM. The backbone of the solution is a foundation of trust established by an RSA algorithm-based Public Key Infrastructure (PKI). The web browser or app is provided with a public key to encrypt PINs with, and the corresponding private key is stored on the HSM for use in decrypting the message and generating an encrypted PIN block.

Using this technology, PINs entered by the user are encrypted immediately and are only decrypted within the secure, FIPS 140-2 Level 3 compliant boundary of the HSM. This goes beyond the traditional TLS-based security of web applications where private keys are stored in the web server or host application itself. Storing the private keys solely in an HSM provides end-to-end security and assurance that even if the traffic were to be intercepted, malicious actors would not be able to decrypt it to learn the PIN.

Unlike symmetric cryptography where a single encryption key can be used to encrypt and decrypt a message, asymmetric cryptography requires two keys to communicate. A public key is used to encrypt and send the message by the sender, and a private key is used to decrypt the message by the recipient. This adds another layer of security in that not only is the message encrypted, but the recipient's identity is verified and authenticated by possessing the appropriate private key.

PREREQUISITES FOR DEPLOYING ONLINE AND MOBILE PIN ISSUANCE

- A client library, housed in the device used by the accountholder to access the issuer's website or mobile app, that is capable of encrypting data using the RSA algorithm
- A public key, bundled in the issuer's website or mobile app, that will be used to encrypt the PIN selected by the accountholder
- An application that receives communication from the issuer's website or mobile app and formats it into the proper API call to the HSM for PIN block generation
- A FIPS 140-2 Level 3 and/or PCI HSM compliant HSM or Crypto-as-a-Service environment

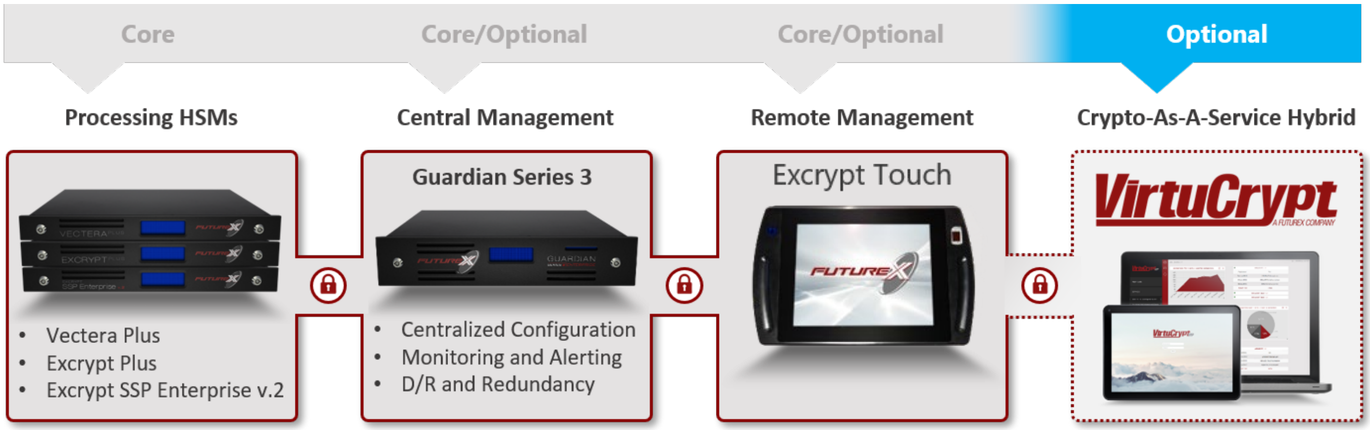
FUTUREX AND VIRTUCRYPT'S SOLUTIONS FOR ONLINE AND MOBILE PIN ISSUANCE

Futurex and VirtuCrypt are the industry's only single-vendor providers of complete cryptographic infrastructures for payment security. Many of Futurex's most important services, like PIN encryption and validation, P2PE, and tokenization, rely on similar encryption and key management techniques as those used for online and mobile PIN issuance.

In response to the growing demand for online and mobile PIN issuance with the financial services industry, Futurex and VirtuCrypt have developed the most robust solutions in the industry. Whether choosing cloud functionality through VirtuCrypt, on-premises hardware through Futurex, or a combination of both, each solution has the functionality needed to build a comprehensive, single-vendor solution for all cryptographic processes related to financial services and payment processing.

ON-PREMISES HARDWARE SOLUTION: FUTUREX HARDENED ENTERPRISE SECURITY PLATFORM

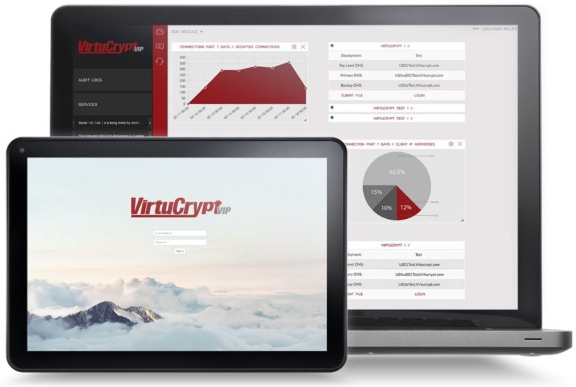
Futurex's Hardened Enterprise Encryption Platform is an advanced product line of HSMs, key management servers, and payment data security solutions. Within the Hardened Enterprise Security Platform, the primary PIN management devices include the Excrypt Plus, Excrypt SSP Enterprise v.2, and Vectera Plus HSMs.



The Futurex Hardened Enterprise Security Platform

CLOUD SOLUTION: VIRTUCRYPT CLOUD PAYMENT PLATFORM

For clients who prefer "as-a-service" cryptographic functionality, Futurex's online and mobile PIN issuance functionality is available through the VirtuCrypt Hardened Enterprise Security Cloud. VirtuCrypt is best-suited for organizations who prefer hosted cryptographic services as opposed to maintaining their own on-premises hardware.



With the VirtuCrypt Elements Debit Processing service, VirtuCrypt securely stores private keys and generates encrypted PIN blocks on-demand, with virtually limitless scalability in throughput and enterprise-grade high availability. VirtuCrypt is powered by Futurex hardware, which means that VirtuCrypt clients receive the same security and compliance benefits that come from owning Futurex hardware, in particular FIPS 140-2 Level 3 and PCI HSM compliance

Security concerns about the cloud usually revolve around the idea that sensitive data being transferred or stored within the cloud may be viewed by unauthorized people. However, VirtuCrypt's innovative approach to the cloud alleviates these concerns, with all sensitive data being encrypted, decrypted, and authenticated in FIPS 140-2 Level 3 compliant Secure Cryptographic Devices located within SSAE 16 (SOC 1, 2, and 3), PCI, TIA-942 Tier 4, and HIPAA-compliant data centers.

The VirtuCrypt Intelligence Portal (VIP) Dashboard gives customers this centralized management platform for all their VirtuCrypt hosted services. With the VIP Dashboard, users can securely communicate directly with the Futurex device performing the service at the VirtuCrypt data centers. Additionally, users can view and export audit logs detailing past operations and various other individual user actions.

VirtuCrypt A FUTUREX COMPANY	
Crypto-as-a-Service powered by Futurex hardware	✓
Virtually limitless scalability with enterprise-grade high availability	✓
Customized whitelabeling of the VIP Dashboard web interface	✓
Solutions for fully-hosted or hybrid on-premises deployments	✓

COMMUNICATING WITH THE EXCRYPT PIN ISSUANCE API

Whether using an on-premises HSM or VirtuCrypt Elements' Debit Processing services, clients use Futurex's own application programming interface (API) to send cryptographic processing requests. This is a full-featured API and command set for integration with host application software.

Communication with the Excrypt API must be made via TCP/IP using a socket connection wrapped in a Transport Layer Security (TLS) tunnel. In most cases, applications communicate directly with the API by sending commands and receiving responses. The Excrypt API format uses a four-character alphabetic command. There are 2 primary commands used in the Excrypt API for PIN issuance:

- Command TRPN: Translate PIN from RSA to Symmetric Key Block
- Command GOFF: Generate a PIN Offset

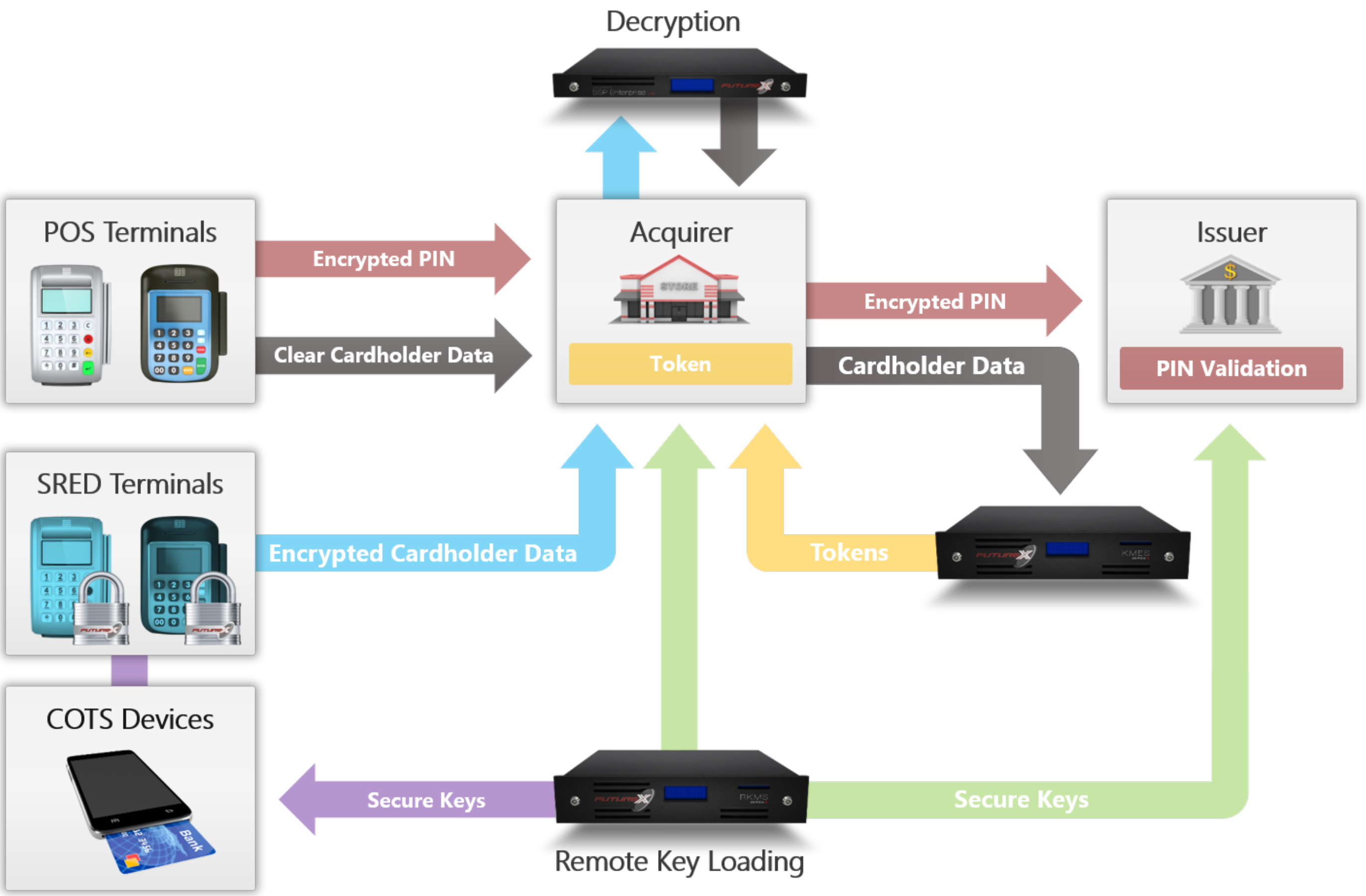
The TRPN command is used to perform the PIN translation and will always be part of an online and mobile PIN issuance deployment. The other command, which is not used in all deployments, is the GOFF command. This command generates an offset used to reference the customer-selected PIN with the natural PIN generated by the issuer's PIN generation key. If the issuer is generating their own offsets, using the GOFF command will be required. In other environments, a third-party organization such as a card brand may generate the offsets.

For additional security, the TRPN command supports padding the input with random data according to either the OAEP or PKCS #1.5 specifications. In order to take advantage of this security feature, the PIN encrypted at the accountholder's web browser or app must be padded using one of these methods at the time of creation.

END-TO-END PAYMENT SECURITY

While this whitepaper is focused on online and mobile PIN issuance, it is important to understand that debit processing is just one of many elements of a secure payment processing infrastructure. Complementary solutions addressing other elements of data security include Point-to-Point Encryption for PAN protection, tokenization for secure storage of data at rest, remote key management to securely transmit encryption keys to endpoint devices, and several other encryption-based security solutions. While each one is important on an individual basis, a holistic approach to transaction security would requires utilization of all these measures for a complete umbrella of payment security.

There are multiple security providers on the market that provide individual elements of this functionality. However, Futurex and VirtuCrypt represent the industry's only single-source provider of an entire suite of payment processing cryptographic functionality.



Enterprise Payment Environment with P2PE, Tokenization, Debit Processing, Online and Mobile PIN Issuance, Software-Based PIN on COTS Management, and RKL

FUTUREX ENGINEERING CAMPUS
OFFICE: +1 830 - 980 - 9782 TOLL FREE: 800 - 251 - 5112
864 OLD BOERNE ROAD, BULVERDE, TEXAS, USA 78163