Proxama

Proxama PIN Manager

Bringing PIN handling into the 21st Century

"I am not a number – I am a free man…"

So said the 'The Prisoner' in that 1960s cult TV show, but Personal Identification Number, or PIN, was adopted by the banking industry as the only reliable method of verifying customer identify at the new Automatic Teller Machines when these started to appear in the late 1960s. Use of PIN is a form of *two-factor authentication* – using something you have (the card) and something you know (the PIN). The spread of PIN to point-of-sale purchases, especially for debit cards that were also used in ATMs, was the next logical step, with the PIN being checked during an online transaction between the ATM or POS and the bank host. The use of PIN received an another endorsement from the payments industry when it was written into EMV, the global chip payment card standard, in the form of an *offline* PIN that could be checked within the chip on the card itself.

The effectiveness of PIN as an identification method (or a CVM – a Cardholder Verification Methodology, to be more accurate) relies on it being a secret kept between the card issuer or bank and the cardholder or customer. Systems of enormous cost and complexity have been developed to ensure that the PIN keyed in by a cardholder when making a purchase or withdrawal can be conveyed in secrecy from the device to the bank for checking, and that the handling of PINs within the bank or issuer and their delivery to cardholders takes place in conditions of the utmost security. Yet things still go wrong – PINs can be corrupted, revealed or stolen during generation, distribution or use; banks and card issuers have to wrestle with synchronising PINs across different systems, and where EMV offline PIN is used, keep the PIN(s) known to their system for each cardholder aligned with the PINs stored in their EMV chip cards.

In response to these operationally demanding and costly problems that banks, card issuers and their processors or service providers face, Proxama has developed the **Proxama PIN Manager**, a unified solution for the end-to-end management of PINs that is secure, innovative and cost-effective.

PIN management

PIN management is a complex business. PINs must be generated and shared securely with the authorised parties – the cardholder and authorisation system and, for EMV, the card itself via the card production process. In addition, PIN handling systems may have to support cardholder choice of PIN before card issuance, changing and synchronising the PIN (in back office systems and in EMV cards) after issuance and, depending on issuer policy, potentially re-advising the PIN to the cardholder if forgotten. But the PIN management programs commonly in use are often legacy systems, maybe from the early days of PIN adoption, and often batch processes which may or may not be integrated with other parts of the card management system(s).

There are further issues with the ways in which PINs are currently used. The prevalent method of distributing PINs to cardholders is still the PIN mailer – a printed document with some security features designed to prevent exposure of the PIN before it reaches the cardholder. Where a determined fraudster is involved, this provides little protection – a substantial level of fraud results from *mail non-receipt* cases where card and/or PIN are stolen in transit. In the UK, this category of fraud had been falling from a peak in 2004, but has now been rising by 20–30% year-on-year since 2009. When coupled with Card ID fraud in which PIN compromise plays a significant role, the total *reported* loss to UK issuers in 2011 amounted to £34m – the true figure is unknown. While the UK's adoption of EMV Chip and PIN has mitigated the losses from these types of fraud, in countries where Chip and PIN has not been adopted the equivalent losses will be higher.

A recent report from the Smart Payment Association has revealed that the PIN mailer is also a source of substantial losses from delays in card activation. Andreas Strobel, SPA President, said: *"It's incredible to think that we're still using the same distribution method today that we did 50 years ago. Today it can take up to 3 days to send PINs out to customers – we could be doing it in seconds via SMS. Sending PINs by post is costing the industry millions. Every PIN in transit means a card not activated or not being used. That means lost transaction fees, and very frustrated customers."*

We would add that every PIN in transit is a potential Card ID fraud waiting to happen.

Yet another issue with PINs that affects processors and service providers results from the operation of multiple issuing platforms. This situation often comes about from merger or acquisition of processors, where an unintended consequence is that PIN processing is spread across several incompatible systems. The result is multiplication of the effort needed for operation, maintenance and security administration, an increased risk of failures and customer dissatisfaction from having to interact with differing PIN select, change and unlock procedures.

To address all of these issues and to provide a single unified solution to all requirements for PIN management within issuers and processors in payments and other fields, **Proxama PIN Manager** has been developed.

Proxama PIN Manager

Proxama PIN Manager (PPM) provides issuers and processors with a modern, fully-featured stand-alone PIN management solution to replace out-dated legacy PIN handling systems, to unify PIN management across two or more issuing platforms or to provide PIN management capability where none presently exists.

PPM meets the business and functional requirements both for traditional PIN processes and for new and innovative methods of PIN handling, managing all PIN lifecycle events from generation and distribution to self-selection, update and re-synchronisation. PPM supports a many-to-many relationship between PINs and card/token functions, such that multiple applications on a card may share a common PIN or multiple PINs may exist for a single application.

PIN Import and Generation

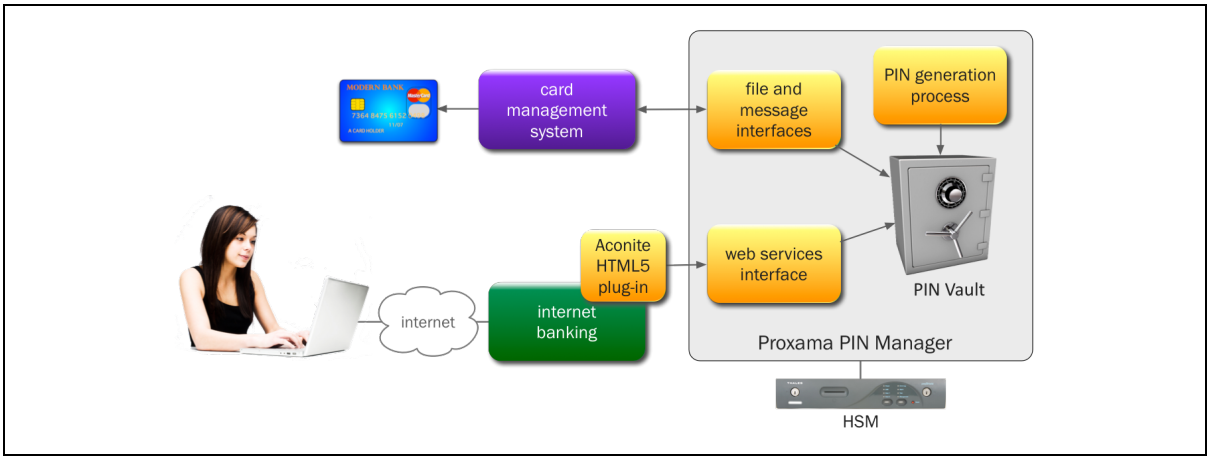
PPM can can act as a client and/or a server to collect PINs or generate internally:

- PINs generated by existing systems during the card production process or by a separate process can be imported into PPM and taken under management
- PINs input through an Internet banking service as part of the card ordering process can be captured directly in PPM through the use of a supplied website plug-in
- PPM can act as the PIN generation server and supply PINs to card production and other card and token provisioning systems, generating PINs on demand or in batches in advance.

An optional feature of PPM is the PIN Vault, where PINs can be stored securely prior to use and during their lifecycles. PINs can be associated with a physical (or virtual) card directly or can be held anonymously through the use of tokenisation. PPM can store either the encrypted PIN, PIN Verification Value (PVV) or, for backwards compatibility, PIN Offset. Security of information held in the PIN Vault is guaranteed through the use of hardware encryption.

PPM operates in both real time and batch modes, so imported PINs can be available to other processes immediately after loading.

The diagram below illustrates the sources of PIN data available to PPM:



PIN Verification

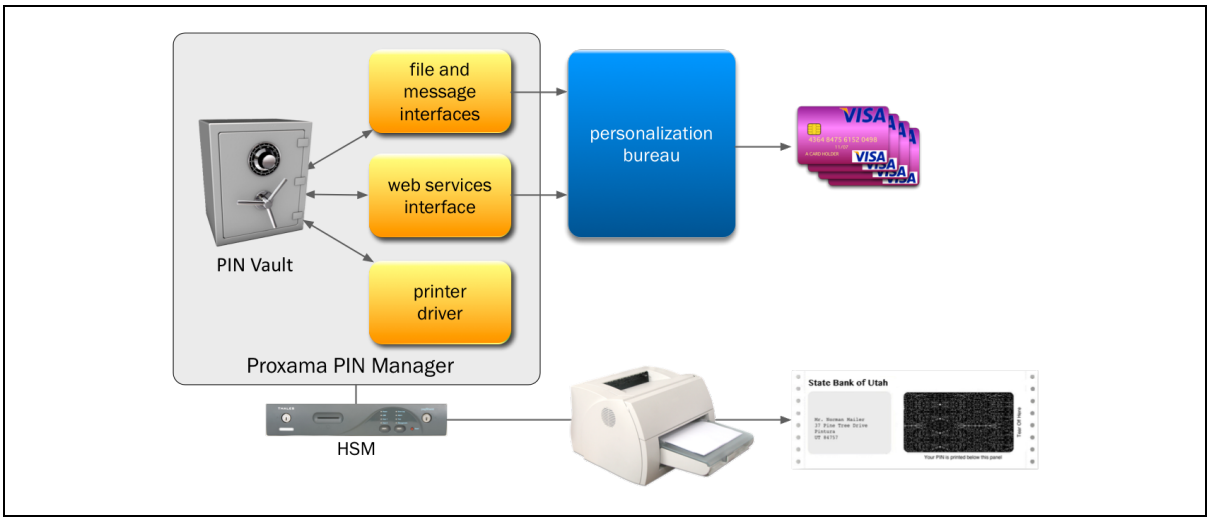
PPM provides messaging and web services interfaces for authorisation systems to call for verification of a PIN Block (in a wide range of supported formats) or the PVV.

PIN Delivery

PPM supports both traditional (in the form of PIN Mailer) PIN delivery and innovative methods based on SMS and internet banking. These are described below.

PIN Mailers

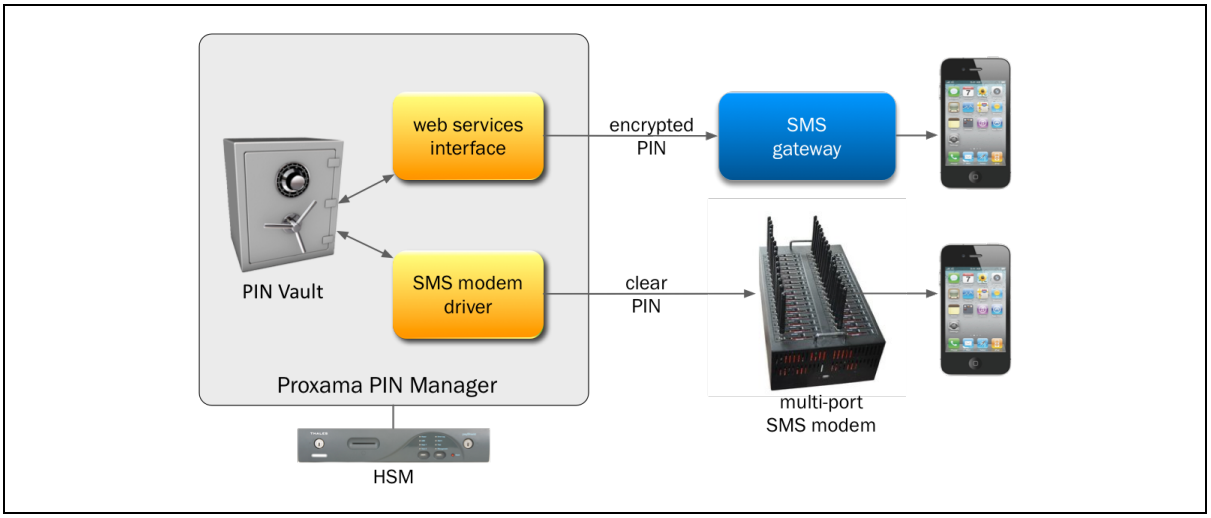
PPM can drive a PIN Mailer printer directly via an HSM connected to PPM or can produce encrypted PIN Mailer files for transmission to a third party bureau. Mailer format is configurable and multiple languages are supported. PIN data can be sent simultaneously to the card personalization bureau for merging with perso data from the CMS. This diagram illustrates the flows:



SMS PIN Delivery

PPM supports SMS text advice of a PIN to a cardholder. In addition to saving the *cost* of PIN Mailers, this approach has the additional benefit of avoiding PIN Mailer interception. SMS PIN delivery meets the highest standards of PIN data protection, with decryption taking place only at the latest stage of the end-to-end process, and conforms to all current card scheme requirements. PPM can deliver SMS messages containing the PIN either via an external SMS gateway, in which case the PIN is encrypted when transmitted and decrypted at the gateway prior to delivery, or by driving an SMS modem array within PPM's secure environment directly.

The following diagram shows these options:



PPM additionally supports out-of-band PIN delivery with use of a one-time cardholder verification password. On receipt of a PIN notification request from the issuer's internet banking server, a password is generated by PPM and sent by SMS to the cardholder's registered mobile. The cardholder is prompted to enter the password via the internet banking website and it is verified in a call from the internet banking server to PPM. Once the cardholder is authenticated, PPM sends an SMS text containing the PIN to the same registered mobile.

Web PIN Delivery

Web PIN delivery is a cost effective method of advising PINs to cardholders and operated within the secure environment that is established to support internet banking. In common with SMS PIN delivery, this method eliminates both the cost of PIN mailers and the possibility of PIN mailer interception. PPM comes bundled with an HTML5-compatible plug-in that implements advanced security features for the protection of PIN data, and is designed to be easily integrated into the issuer's internet banking system.

Included in the plug-in is Proxama's Virtual PIN Pad. This can be used for capture of a new PIN, entry of an existing PIN for authentication purposes or display of an newly assigned PIN. The PIN Pad is a secure, browser-based solution that uses advanced encryption to protect PIN data. The PIN Pad avoids use of the computer keyboard for entering the PIN and instead uses the mouse pointer and random positioning on the computer display, and is therefore safe from key logging and screen capture attacks. Virtual PIN Pad does not store the PIN data but maintains an on-line connection to PPM while in use. All transmitted PIN data is protected by encryption under unique session keys generated dynamically by PPM's HSM.

The PIN Pad display for a four-digit PIN is shown below, but PIN lengths up to twelve digits can be accommodated:

The cardholder is advised on receipt of their card that they should visit their internet banking site to be advised of their PIN. On navigating to the relevant page and potentially re-authenticating themselves, Proxama Virtual PIN Pad is used to display the PIN – one digit at a time, each digit only being revealed when the mouse pointer hovers over the digit's position.

PIN Self-Select, Change and Unblock

The ability for cardholders to self-select their PIN either in advance of card issuance or to change the assigned PIN at a later time is often seen as a positive customer service gesture. The security requirements for capturing a cardholder-input PIN have to date restricted self-select PIN entry to ATMs and devices in secure environments such as bank branch terminals. PPM uses advanced encryption techniques and a unique design to permit secure PIN capture using internet banking – the Proxama Virtual PIN Pad described above is used to achieve this.

On navigating to the relevant page on the internet banking website, the cardholder nominates the pending or existing card for which the PIN is to be captured or changed. The Proxama browser plug-in establishes a secure session with PPM and the Virtual PIN Pad is displayed. The cardholder uses the mouse pointer to select the new PIN by clicking on the numeric keypad. The PIN can be checked by hovering the mouse pointer over the PIN display. The PIN is then sent securely to PPM, for storage in the PIN Vault and/or advice to the card personalization and authorisation systems.

Similar techniques can be used for other PIN management operations where secure capture of the PIN is required, including PIN change and unblock for EMV Offline PIN cards, where the Proxama EMV scripting engine can be used to send a PIN Change script back to the EMV card inserted in a card reader attached to or integrated with the PC.

Technical

In common with other Proxama software products, Proxama PIN Manager is a Java application that runs in an Application Server such as WebLogic. It is therefore hardware, operating system and database independent, although Proxama recommends Unix and Oracle, but any JDBC-compliant database can be used. PPM is optimised for Thales payShield 9000 HSMs but other HSMs can be supported.

Next step…

Contact Proxama. Find out more about **Proxama PIN Manager** and other smart product solutions. Put yourself on the path to innovative smart products based on chip that can help your business to grow through increased customer numbers, market share and profitability.

Visit our website: www.proxama.com Call: +44 (0)203 688 2888

email: hello@proxama.com