aconite technology

Part of the CRYPTOMATHiC Group

PIN MANAGER

Product White Paper

OVERVIEW

Aconite PIN Manager is a secure enterprise solution that manages all PIN lifecycle events and enables on-demand customer access to PIN functions through digital channels. APM is built for single issuer or multi-client processor deployment and implements the highest standards of security, meeting all PCI, card brand and national requirements.

With paper PIN Mailers representing both a security risk and a substantial cost overhead, digital access for PIN notification, and for self-selection and change, delivers enhanced security, improved customer service and cost savings. Interchange revenue can even increase thanks to faster card activation.

APM can be the originator and the system of record for PINs across the enterprise, or can work alongside existing systems such as a Card Management System (CMS) that provide PIN storage. APM also supports PIN verification for customer authentication and for transaction processing, with performance and resilience to match any authorization system.

PIN MANAGEMENT

PIN Management is complex. PINs must be created and shared securely with the authorized parties – the cardholder, authorization system(s) and, for EMV® Offline PIN, with the card itself via the card production process. PIN management systems may also have to support cardholder choice of PINs before card issuance ('preselection'), changing PINs and synchronizing them with back-office systems and EMV cards, and possibly notifying cardholders of forgotten PINs. But the PIN management programs in use today are mostly legacy systems, maybe from the early days of PIN adoption, and are often batch processes which are incompatible with today's ondemand culture and unable to integrate with digital channels and other parts of the card payments landscape.

One more thing – the relationships between financial institutions and customers are no longer based on a single product such as a bank account or a card. Interactions are now multi-faceted with a portfolio of products available to each customer. Maintaining credentials for each of these products within their individual silos leads to duplication of effort, multiplication of costs and increased exposure to risk. Consolidation of credential management into a single system minimizes risk, reduces costs, and both standardizes and improves the customer experience.

RISK MITIGATION/ REVENUE MAXIMIZATION

The prevalent method of distributing PINs to cardholders is still the paper PIN mailer – a printed document with some rudimentary antitampering features designed to prevent exposure of the PIN before it reaches the cardholder. This provides little protection where a determined fraudster is involved – a substantial level of card fraud loss results from Card ID Theft in which PIN compromise plays a significant role. In the UK, as reported by industry body UK Finance, losses from this category of fraud had been falling but saw a massive 59% jump [UK Finance – Fraud The Facts 2019 June 2022]. When coupled with Card Non-Receipt, the total reported loss to UK issuers rose to over £53m in 2018 – the true figure is unknown and likely to be much higher. While adoption of EMV Chip and PIN in Europe and elsewhere has slashed the losses from counterfeit and lost and stolen fraud, in countries where Chip and PIN is not widely used, such as the USA, the ID fraud losses will also be corresponding.

In addition to the exposure to Identity Theft, a report from the Smart Payment Association has revealed that the PIN mailer is also a cause 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. 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 the mail is a potential ID fraud waiting to happen...

ACONITE PIN MANAGER

Aconite PIN Manager provides issuers and processors with a modern fully featured, enterprise-wide 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.

APM meets the business and functional requirements both for traditional PIN processes and for new and innovative methods of PIN handling. APM can manage all PIN lifecycle events from generation, secure storage and distribution to self-selection, update and resynchronization.

APM supports many-to-many relationships between PINs and card functions, such that multiple applications on a card (e.g. payment and ID) may share a common PIN, or multiple PINs may exist for a single card. APM is fully PCI compliant and meets the security guidelines of all relevant card payment schemes and national organizations.

EPIN CAPTURE & DELIVERY

APM supports innovative electronic capture and delivery through web and mobile banking, aligning with industry trends towards exclusively digital customer communications. APM also supports PIN operations via SMS and IVR. Major cost savings result from replacing paper PIN Mailers with ePIN delivery – not just printing and postage costs, but also the costs of the back-office and call center infrastructure needed to deal with non-delivery, lost and forgotten PINs, and the cardholder inconvenience, loss of business and potential fraud from having PINs in transit over an inherently insecure channel.

The ability for cardholders to select their PIN in advance of card issuance or to change PIN later, on demand, will be seen as providing enhanced customer service. Up to now the security requirements for capturing a cardholder-created PIN have restricted PIN entry to ATMs and devices in secure environments such as bank branch terminals, or to clunky paper-based solutions.

EPIN CAPTURE & DELIVERY CONTINUED...

Web & Mobile Banking

Web or mobile capture and delivery of PINs is cost-effective and operates within the secure environment that is established to support web or mobile banking. This eliminates the often-complex methods of PIN self-selection, the cost of PIN mailer production and the possibility of PIN mailer interception.

Two options are available for implementing ePIN capture and delivery. APM exposes an API that implements a secure, encrypted transport protocol and enables the development of a native PIN capture/display user interface within a web or mobile banking application. Similarly, a PIN capture/notification dialog can be developed within an IVR server. If PIN capture is not a requirement, The API can be used for PIN delivery only. Using the Aconite API, developers can implement any design of UI to maintain the website, app or IVR branding and user experience.

Alternatively, for desktop browser solutions, Aconite can supply **Virtual PIN Pad (VPP),** an HTML5-compatible JavaScript component that is easily integrated into the issuer's internet banking system or a dedicated web page and implements the same advanced security protocol as the API for the protection of PIN data.

APM uses advanced encryption techniques and a unique design to permit secure PIN capture and display. On the relevant page of the internet banking website or in the mobile app, the cardholder nominates the card for which the PIN is to be captured or changed. A secure session with APM is established and the PIN Entry/Display screen or the Virtual PIN Pad is displayed.

Aconite's API or the JavaScript VPP can be used to display a newly assigned PIN or a PIN reminder, to capture a new PIN for pre-selection or PIN Change, or to check an existing PIN for authentication purposes. The entire PIN is never shown, but individual masked digits must be clicked or touched to be revealed one at a time. VPP avoids use of the physical or virtual keyboard for capturing a PIN and instead uses mouse clicks or a touch interface, random positioning of the display and random arrangement of keys on the PIN Pad, and is therefore safe from key logging and screen capture attacks. VPP does not store the PIN data but maintains an end-to-end encrypted connection with APM while in use. Transmitted PIN data is protected under dynamically generated single-use session keys and is never associated with the card or account number.

The cardholder selects a new PIN by clicking the on-screen numeric keypad, and then re-enters the PIN for verification purposes. Only one digit of the PIN is visible at any time, and the PIN can be checked by clicking the individual PIN display digits. The PIN is then sent securely to APM for temporary or permanent storage in the PIN Vault and forwarding to card management, card personalization and authorization systems.

Similar techniques can be used for other PIN management operations where secure capture of the PIN is required, including PIN change for EMV Offline PIN cards, where the Aconite EMV scripting engine can be used to create a PIN Change script for delivery to the EMV card during its next online transaction.

In line with ISO, PIN lengths up to twelve digits can be accommodated.

EPIN CAPTURE & DELIVERY CONTINUED...

SMS PIN Delivery

Where mobile or web banking is not available, or smartphone penetration is not widespread, APM supports SMS text advice of a PIN to a cardholder. In common with web/mobile PIN delivery, this approach saves the cost of PIN Mailers and avoids PIN Mailer interception. SMS PIN delivery meets the highest standards of PIN data protection, with decryption taking place only at the final stage of the end-to-end process and conforms to all current card payment brand and network requirements. APM delivers SMS messages containing the PIN to an external SMS aggregator or gateway, with the PIN encrypted when transmitted and only decrypted at the gateway immediately prior to delivery.

APM additionally supports out-of-band authentication prior to SMS PIN delivery through use of a one-time passcode. On receipt of a PIN notification request from the issuer's internet, mobile banking or IVR server, a short-lived passcode is generated by APM and sent by SMS to the cardholder's pre-registered mobile phone. The cardholder is prompted to enter the passcode via that alternative channel, and it is verified in a call from the server to APM. Once the genuine cardholder's possession of the registered mobile phone is confirmed, APM sends an SMS message containing the PIN to that mobile.

PIN VERIFICATION

APM provides messaging and web services interfaces for authorization systems to call for verification of a PIN formatted in an encrypted PIN Block (in a range of supported formats) or a PVV. APM is highly performant and the impact on overall response time will be minimal.

PIN IMPORT, GENERATION & STORAGE

APM can act as a client and/or a server to capture PINs or to generate PINs internally:

- PINs generated by existing systems during the card production process can be imported into APM and taken under management
- PINs input as part of the card ordering process through web banking or a mobile app can be captured directly in APM using Aconite's API for PIN capture and display or Aconite's Virtual PIN Pad
- APM can act as a PIN generation server supplying PINs to card production and other card and token provisioning systems, generating PINs on demand or in batches in advance
- PINs can be captured during instant card issuance or while changing PIN through a secure PIN Entry device at a branch or other secure location.

Where secure storage is required, the PIN Vault stores encrypted PINs prior to use and during their lifecycles and can act as the system of record. PINs can be securely associated with a physical or virtual card or can be stored anonymously through the use of an alias. APM can store or generate either encrypted PIN block, PIN Verification Value (PVV) or, for backwards compatibility, PIN Offset. The security of information held in the PIN Vault is guaranteed through the use of multi-layered hardware encryption. APM operates in real time while also supporting batch file input and output, so PINs can be available to other systems immediately after creation or import.

COMMERCIAL

Aconite PIN Manager modules are licensed for a renewable five-year term based in the number of cards supported, or can be supplied for an initial implementation fee with per-event (e.g. PIN capture, PIN display) pricing. Aconite provides worldwide 24×7 support through a dedicated helpdesk and regular maintenance updates.

TECHNICAL

Aconite PIN Manager comprises a suite of Java applications for onpremise deployment that runs in a a servlet container, including Open Liberty, or a Java EE Application Server, inclusive of WebSphere or WebLogic. APM is hardware, operating system and database independent, although Aconite recommends Unix or Windows Server and Oracle or PostgreSQL. APM is optimised for Thales payShield 10K HSMs but other suitable HSMs can be supported.

APM uses web services APIs to support the functions described and can also implement messaging and file-based interfaces if required.

SUMMARY

We're the guys that enable you to receive a ready-to-use payment card from your bank, or to securely change your PIN in your mobile app. For over two decades we've helped stakeholders fulfil compliance obligations and preserve reputations for issuers, acquirers, card personalisation bureaus, payment service providers, processors and payment schemes.

Contact us to find out more about Aconite PIN Manager and our other smart product solutions.

www.cryptomathic.com

enquiry@cryptomathic.com

+45 8676 2288