Secure ePIN

BLUE FORTRESS

Where Are We **TODAY?**

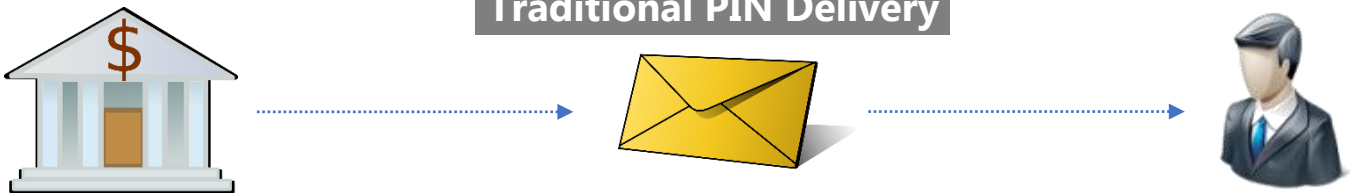
In the recent years, many banks have moved from traditional cards to EMV cards which requires PIN verification upon transactions. However, PIN delivery methods used by many banks today have its own challenges including delivery time and maintaining anonymity of delivered PINs.

Blue Fortress offers a solution to securely and efficiently deliver customers' PINs with no idle time. Secure ePIN is an immaterial PIN delivery which complies to industry security standard in a split-channel delivery regardless of customers' locations at any time. Customers will receive their PINs that are embedded inside an encrypted PDF document via their emails along with a SMS notification which contains a password to the PDF document, utilizing a multi-factor security design in real-time.

Benefits of Secure ePIN Electronic PIN Delivery

- Provides a secure split-channel PIN delivery
- Manages risks of physical PIN mailer that is vulnerable to machine-based attacks
- Helps banks and credit card companies to save costs on physical PIN mailer
- Reduce consumers' idle time as PIN delivery is instant regardless of customers' locations
- All PIN process and business operations is performed inside a secure tamper-proof hardware security module

Traditional PIN Delivery



Over the years

Over the years, evolution in technology has resulted in countless changes in credit card history. With the replacement of magnetic strips to EMV chip technology, revenue from online shopping has surged beyond the roof, with items being delivered in no time.

Ever since the domination of smartphones, people live in a real-time environment. Customers expect nothing less than "fast". Hence, immediate services and deliveries are no longer an expectation, but a norm to many businesses today.

The common methods

The common methods banks use to deliver credit card PINs, when a card is first issued or when customers request to change PINs, is by printing it behind a scratch-off panel inside an envelope that invites tampering attempts.

The risks, cost and time

The risks, cost and time needed for delivery is coupled tightly with such method of delivery. Customers are expected to wait for their PINs to reach them while they wait idly, resulting in banks to lose out on the idle time that is caused by an ineffective yet costly PIN delivery method. Consumers should not have to go through such lengthy procedure to splurge or enjoy the privilege of their credit cards.

Banks today

Banks today have been reaching out for alternatives to effectively, yet securely deliver customers' PINs, to rid off the PIN mailer process that has been taken for granted for the past 30 years, where a PIN postal delivery would take about a week's operating hours, causing banks to lose out on a compelling amount of revenue each year.

It is important to understand

It is important to understand that PIN is an information, not a document. Therefore, there is no significantly good reasons to send a document when only an information needs to be delivered – the PIN. While traditional PIN mailer encourages tampering, attempts to utilize technology that is readily available – email, SMS, web browsers could also lead to sniffing or information thieves in the internet world. Delivering consumers' PINs securely with minimum security threats has now became a new challenge to most banks who are evaluating different alternatives.

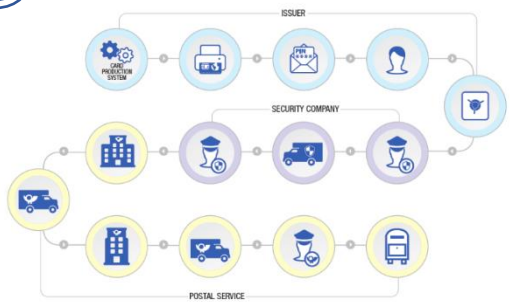
This is where Secure ePIN

This is where Secure ePIN comes into the picture. Secure ePIN offers a more efficient and effective approach in PIN distribution whilst enforcing out of band requirement in conventional PIN mailer.

Secure ePIN - PIN Distribution

BLUE FORTRESS

1 Risks



Traditionally, a "specially" designed envelope was able to protect a PIN from being exposed, provided the envelope was not opened by anyone. However, an envelope that had to go through numerous parties before it reaches to the consumers' doorsteps does not insure that. A machine-based attack without opening the envelope is also possible as the PINs are only hidden behind a scratch-off tape. Therefore, the security risk is undeniably high.

Why Secure ePIN with Blue Fortress?

Secure ePIN is a software that runs on Gemalto's SafeNet Java HSM (Hardware Security Module). Every business operation from PIN Generation/Process to PIN Distribution is performed inside the HSM. Hence, while security is guaranteed with the tamper-proof device, the PIN Distribution performance of Secure is solely dependent on the OS inside the HSM and therefore, will not be affected by any applications outside of its parameter.

Gemalto's SafeNet Java HSM

Gemalto's SafeNet Java HSM is a standard FIPS 140-2 Level 3-validated Hardware Security Module that comes with its individual hardened Operating System and allows an application (Secure ePIN) to be hosted in its server. SafeNet Java HSM increases application security by providing a trusted execution environment that protects an application's sensitive software components and cryptographic keys from physical, logical and operational threats.

Cryptographic Algorithms

- AES 256 and RSA 2048
- PDF ISO Standard ISO 32000-1

Type of Application

- Web Application hosted in SafeNet Java Hardware Security Module

Database

- Database stored inside the HSM
- Supports High Availability Setup

Performance

- 5000 PDF Generation per hour (with embedded PIN)

Operating System Supported

- Any OS with a browser to access web application

End-to-End Encryption

- Every sensitive data involved will be fully encrypted from the browser to application level, all the way to the database

HSM/PIN Keys

- End-to-End Encryption technology
- Encrypted in the database with keys generated by the Hardware Security Module solely for Secure ePIN which is unexportable from the appliance

2 Delivery

Password to the PDF

SMS Gateway

Secure ePIN utilizes multi-factor authentication to deliver consumers' PINs. As a solution to machine-based attacks, clear PINs will be transformed into CAPTCHA format, which will then be embedded inside an encrypted PDF file. A pure random number will be generated inside the Java HSM, which Secure ePIN is running on, to encrypt the PDF file containing the CAPTCHA PIN.

The encrypted PDF file will be sent to consumer's emails where they will also receive an SMS notification for the password to the PDF file.

On top of reducing the waiting time as customers could receive their PINs within seconds, it provides maximum security at a lower price because even if one channel of delivery is compromised, consumers' PINs will not be exposed in any way.

Email Gateway

PDF containing the PIN

Customer

enquiry@blue-fortress.com

+60 16-333 1366 (Luke Shu)