Manipal Technologies Limited

*MIRI*CARD

Product Note

Abstract

MTL indroduces disruptive technology of Virtualisation which is Secure & Dynamic and works even when there is no connectivity

Confidential Document

INNOVATION. TRUST.

Mumbai Office :
101/123, 1st Floor, The Summit Business Bay
Off Andheri Kurla Road, Opp PVR Cinema
Next to WEH Metro Station, Andheri East
Mumbai 400093
LandLine: 022-49368700

Registered Office:
Manipal Technologies Limited
Udayavani Building, Press Corner,
Manipal, India-576 104.
Tel: +91 820 2205000, +91 820 4275000 Fax: +91 820 2574827
www.manipaltechnologies.com

Confidentiality Clause

This proposal contains confidential information of Manipal Technologies Limited which is provided for the sole purpose to evaluate the proposal submitted. In consideration of receipt of this document, 'Bank' agrees to maintain such information in confidence and to not reproduce or otherwise disclose this information to any person outside the group directly responsible for the evaluation of its contents, except that there is no obligation to maintain the confidentiality of any information which was known to the 'bank' prior to the receipt of such information from Manipal Technologies Limited or becomes publicly known through no fault of the 'bank', or is received without obligation of confidentiality from a third party owing no obligation of confidentiality to Manipal Technologies Limited.

This proposal has been prepared in accordance with accepted techniques for services offering and MTL understanding of your requirements based on the information provided to us; all timings, flow charts, processes and related information contained in this proposal reflect Manipal Technologies Limited best estimates based on this information.

All registered and trademarked names are owned by their respective owners.

Table of Contents

1. About the Solution

MTL's, **"Miri Card"** solution is a US patented software solution developed by Miri Systems. Miri Systems are Partners with Manipal Technologies, Ltd. for customizing, implementing and deploying its platform to the Asia market. The solution was developed by a team of software developers and banking experts with decades of experience in software development and credit card solutions as well as experts in quantitative analysis of complex systems and intellectual property development.

Miri Card is based on a unique patented process that creates a single use dynamic number that looks and functions like a credit/debit card number. It provides an exact virtual representation of various electronic identity cards (access, transit and banking) cards using software. It protects a transaction from a host of attacks and card frauds like skimming, CNP (Card Not Present), counterfeits due to theft or loss or card, BIN Attacks, Phishing sites, MITM (Man In the Middle) attacks etc.

It is ideal for internet-based e-commerce transactions, the rapidly growing QR based or contactless POS (Point of Sale) transactions as well as ATM transactions. The Miri Card number is generated on the click of a button and subsequently submitted for payment processing. Rest of the processing of the transaction is like any other debit or credit card transaction.

Miri Card reduces the risk of payment fraud by removing confidential consumer credit/debit card data from the payment ecosystem. Original (physical card) sensitive card numbers are replaced by a onetime use dynamic number. Miri Card numbers appear like a valid credit card number but are based on a patented algorithm that cannot be traced back to the real card number. The original or physical card numbers stays in control of the bank and customer.

By introducing this disruptive technology, MTL offers a unique opportunity for issuers to mitigate risk and at the same time gain market share and increase transaction volume and revenue. Consumers are eager for a secure, simple and easy-to-use payment method and will quickly embrace the Miri Card solution.

2. Standout features of "Miri Card"

2.1 Patented high security single-use dynamic number

Miri Card Numbers produced by the Miri algorithm have no statistical patterns. Hence, it is impossible to guess the next number in the sequence even if hundreds or thousands of numbers are captured by hackers.

Single use cards keep sensitive information secure and at the same time makes it problematic to run brute force repeat transactions. Single-use cards are useful for protecting businesses that do not have repeat customers. Database breach of such stores in tourist-heavy areas are often origin points of fraud.

A Report on Security of Miri Encoding Algorithm conducted at a prominent US University analyzes the Miri Encoding Algorithm security against attacks based on acquiring encoded credit card numbers. Based on the experiments, the study concludes that an attacker can collect hundreds or thousands of Miri Card numbers for a user at different times, but he/she can not produce a valid new credit number for the same user at any future time.

2.2 Can be generated offline

The special feature of this product is that the numbers can also be generated offline i.e it works in the absence of the internet connectivity. The Miri Card application utilizes the local encrypted encoding keys to generate the numbers, making the process fast and available anywhere.

2.3 Recurring payment card

Generate time/spend-limit/usage limit based Dedicated card number for merchant payments and avoid storing original card information at payment gateways and 3rd party sites

Cardholders can set thresholds and set the card to expire when

- amount exceeds transaction threshold limit
- usage exceeds time threshold limit

These repeatable and simplified transactions stay associated with a credit card for life and help speed up the checkout process and reduce shopping cart abandonment.

2.4 One time activation - Strong seed data encryption method

The device running the application utilizes the local encrypted encoding keys delivered to the device during the activation process as seed data

2.5 Built-in 2FA (two-factor authentication)

Miri Card takes advantage of an individualized, user chosen password to generate one-time user dynamic card numbers, and local encryption which helps to combat application misuse by hackers

2.6 Multi-channel scalability

Miri Cards are an enterprise wide solution that can perform authentication across any channel through a single installation. Some scenarios include, Credit/Debit Card/ Closed Loop etc.

2.7 Available as a local app for mobile platforms

Institution can utilize the solution as their branded iOS and Android smartphone application to facilitate the end user experience. Ready SDK/APIs for server-side integration, and app integration.

2.8 IT friendly

Appliance utilizes current stable technologies for ease of deployment. Storage requirements are minimalized as Miri Card numbers are time limited and generated. No need to store unlimited card number possibilities that may never be used. Decoder interface is stateless, scalable and fast.

2.9 Additional features

- Card On/Off
- Forensic/Security tools to identify last legal user

- Spend Limits
- Instant receipt generation
- Alert Management
- User Groups

3. The compelling case

3.1 Addressing risks

Technological: Miri Card is an emerging, competitive and disruptive service. It's an innovative digital payments process technology that can offset IT risks of cyber-security breaches which could adversely impact the Bank/ company's ability to compete and further reducing reputation risk.

Operational: Risks related to malfunction or disruption in the operation of the systems, especially supporting services leading to loss of business. These risks are addressed as Miri Card eliminates the risk of a single point of failure by decentralizing the card number generation mechanism. Breaches are expensive, and many retailers and banks have experienced huge losses because of data theft.

Ponemon Institute's 2018 "Cost of a Data Breach" study pegged the average cost of a data breach at $3.86 million. Ponemon's cost estimate for each lost or stolen record containing confidential information now stands at $148.

The risks are further mitigated as Miri Card can be traced to a single merchant, thus the onus/liability of the fraud can be transferred from the bank. The risk can be further capped through limits set by the bank/customer on the card generated.

Compliance: An increasing stringency of regulatory standards (EMV 2.0, 3D secure 2.0, PSD2 Directive), regulations and requirements, puts banks at a risk due to non-compliance. The new standards suggest a shift from channel-based authentication toward tokenization. Miri Card solution is right in that alley and positions the institution in compliance with the regulations.

3.2 Security benefits

Institution

Each online transaction comes with the risk of fraud, so it's crucial to reduce the risk and provide secure payments. The payment process is done without sensitive cardholder data.

Miri Card reduces the risk of a data breach. Even if someone steals a token number, it will be meaningless random numbers, so it's impossible to use them to steal money.

Miri Card also eliminates the possibility of frauds through skimming at ATM/PoS and cloning of cards at merchants and vendors

The authentication is stateless. No information about the user is stored either on the server or in a session.

Miri Card makes it easier for merchants to become PCI compliant. Because retailers don't store any data, they don't have to invest as many resources protecting sensitive customer information. It also makes PCI audits much easier (and cheaper).

An Ideal Défense Against Malicious Insiders

An employee or contractor of the merchant who has access to front-end retail application but is unauthorized to access the back-end payment system. These insiders may be in system admin, developer, DBA, or similar roles. The ideal defensive position is to implement Miri Card solution such that the malicious insider's ability to attack is futile.

Customer

Miri Card solutions works across multiple channels, this lay the foundations for new channel use by a customer with multiple vendors.

Customer's data isn't stored on merchant's servers minimizing the risk of exposing sensitive data and increasing customer confidence. In a 2018 Frost & Sullivan study, 59% of consumers said a data breach had a negative impact on their trust in the impacted company.

Beyond avoiding the worst-case scenario of a data breach, using advanced security such as Miri Card fosters customer trust. Consumers don't want their payments data falling into the wrong hands.

A further benefit for customers is that they no longer must deal with the hassle of a lost or stolen credit card. Currently, when a physical card is lost or stolen, a customer must call their bank, cancel the card and then alert all the businesses who use the card to process recurring transactions.

However, if a phone or device containing the token is stolen or lost, the customer need only request the Miri Card be cancelled. A new card can be issued without requiring the creation of a brand-new credit card number.

3.3 Instant issuance

A true sign of digitization for any financial institution issuing cards. Instead of taking days, it takes a matter of seconds to generate the card information and the card being ready to use with the end customer.

3.4 The green initiative

The Miri Card eliminates the use of plastic and other materials involved in the manufacture of physical cards and its reissue. This directly results in the increase of your carbon footprint by eliminating the use of plastic to the volume of the physical cards being issued.

3.5 Easy integration

A technology that is compatible with all communication channels: IS0 8583, Web Service Calls (Soap, Restful, WSDL. JSON, W3C) etc. Platform Compatibility across Operating systems (Linux, Windows), (Oracle/SQL)

OATH Compliant Standalone Setup and Cloud Support compatible for 2 tier and 3 tier architecture.

3.6 Improve transaction efficiency

The current transaction cycle of a card transaction can be sped up significantly by using the QR and in-built 2FA features that eliminate any dependency on the network for the end customer streamlining the transaction processing cycle

Simplifies repeat purchases using recurring card payments and increases customer payment conversion

3.7 Smooth user experience

Miri Card is more than just a security technology—it helps create seamless payment experiences and satisfied customers. It reduces risk from data breaches, helps foster trust with customers, and drives digital payments as a popular service.

3.8 Cost savings/offsets

Over the service period of the solution, Miri Card will significantly reduce costs related to

- Card printing
- Logistic and Delivery
- Re-Carding/ Reissuance
- Network/Service Provider
- Customer management

4. Process requirements for the solution

Account activation/seeding

"Seeding" is a one-time activation process for applications. It is a quick, reliable 2-step process that locates and registers the application to the server.

Activation codes are product specific and created by the Appliance/Server for the respective Issuer/Client. Every application has an account attached to it.

The activation codes which are sent to individual users to activate their accounts. When the web service is called, a time lock activation record is created in the database using the activation timeout period set in the management tool. While activation is in process, no other activation is permitted for the same activation code.

If the activation does not complete within the activation timeout period, the activation time lock record is removed allowing a end user to restart the process.

Account management and use

Card issuance Cycle:

1. Post KYC by the bank, an account for the customer is opened
2. Bank sends the data MTL to create a Miri Card through backend appliance
3. Appliance creates a card for the customer
4. Account created in CBS

5. Card data generated in CBS
6. Activation code sent to the customer
7. Customer downloads and installs the Miri Card application
8. Uses activation code to activate the app and is then ready to use the app for making e-commerce and contactless POS transactions

Card transaction cycle:

Customer having a Miri Card can make transactions either on e-commerce, contactless POS using NFC or QR Code and even ATM channels;

Transaction flow:

1. E-commerce:
a) Customer purchase item online and initiate payment against the same
b) Chooses Miri Card as a payment option
c) Generates a Miri Card by entering a static password
d) App generates a dynamic Miri Card number (holds good for one transaction), expiry date, CVV and name on card(encoded)
e) This data once filled in goes to payment aggregator who sends the transaction to association
f) Basis the first six digits of Miri Card number (constant for an issuer), association will identify the issuer and sends the transaction to issuer host system
g) Issuer host system will then identify based on an unusual and unique identifier that it's a Miri Card and then send the transaction to decoder
h) Decoder will then decode the Miri Card details and send the response. If it's a negative response, then the decoder sends a negative response back to the host and the reverse flow is followed & transaction doesn't go CBS. If it's a positive response, then the decoder sends a mapped value Account Number through which host system will identify which real account number it belongs to and then send the same to CBS for debiting the actual account.

2. For contactless PoS transaction using QR code:
Only process change from e-commerce is instead of generating Card information the app generates a QR Code which consists of Miri Card information and the merchant would scan it and send the transaction to acquiring host. Rest of the process remains the same as e-commerce transaction.

3. Cash withdrawal using ATM or micro ATM/cash @POS transactions
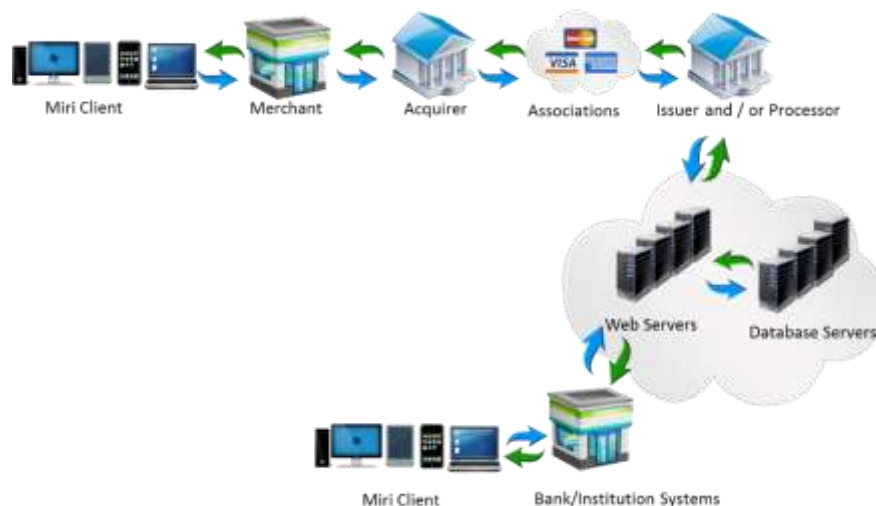In lines with card less withdrawal MiriCard information from the app can be keyed in directly at the terminal of use the QR Code/NFC medium. The device would transmit the transaction to acquiring host. Rest of the process remains the same as any transaction.

Account deactivation and use

In case of deactivation of services, the seed data is deleted from the device (in offline mode), thus, rendering the solution unable to generate any new numbers. When the device comes online, the Account check request will update the same on the server end

5. Summary of the application flow

The below image shows the high-level message flow. Client device receives card number input from user and communicates it with Server/Switch system. The authorization request is validated by the decoder and authorization recommendation, and post-authorization messages are completed between the decoder and host systems

It offers an encoder to generate the Miri Card number and a decoder to retrieve and validate the information hidden in the number. The encoder is installed on a payment device such as a smart phone, computer, tablet and other PDAs (personal digital assistants) and is unique to each device. This is downloaded when a user downloads the 'app' on his device. The decoder is hosted on the issuing bank's payment authorization system or in MTL's (here MTL acts as a Service Provider) secure environment.

5.1 Systems connectivity

Both the systems are housed in OATH compliant architecture, MTL's Offline OTP Solution (Host) and the Bank's Server (Client) would be interfaced through an SSL layer encapsulated over HTTPS.

The Solution would play the role of the server in the HTTPS connection while the Bank's system would play the role of the client. Client will be responsible for establishing the connection with the server.

There would be only one HTTPS socket connection between the client and the server. This connection would be kept alive always thus ensuring high and continuous availability of the interface. This single connection would be used to pass multiple messages from the Bank's system to the host and vice-versa.

The performance of the system is dependent on the pooled connection to the database and the ability of the database to respond to the web server requests. A general rule of thumb is that a decode transaction completes in few milliseconds.

Scaling up can be achieved by adding additional decoder instances that share the pooled connection to the database and as needed distributing the load across database servers. The faster the database server can process connection the faster the decoder will respond to requests