Manipal Technologies Limited

MIRITOKEN

# End User Scenarios & Use cases document


## Abstract

MTL's disruptive technology of Virtualization is Secure & Dynamic and works even when there is no connectivity. This document describes end user scenarios in which the solution is applied.


**Confidential Document**


**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.

## Table of Contents

## About the Solution

MTL's, **"MIRI Token"- Offline OTP** solution is a US patented software solution developed by Miri Systems. It was developed by members including 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 Token is based on a unique patented process that creates a single use dynamic number that looks and functions like an OTP number. The complete solution can provide 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 frauds like Phishing sites, MITM (Man in the Middle), MITB (Man in the Browser) attacks etc.

It is ideal MFA (Multi Factor Authentication) solution for e-commerce transactions, Internet/Mobile Banking and even ATM/POS transactions. The Miri Token number is generated on the click of a button and subsequently submitted for payment processing.

The Miri Token reduces the risk of payment fraud by avoiding SMS/Email/IVR channels to send OTP to consumers. In today's drive for digital payments, innocent consumer and business information has become accessible by hackers and computer malware to steal credentials and information.

It is an efficient solution for the distribution, activation and reuse of tokens that is critical to strong and reliable authentication allowing an institution to establish an enterprise-wide authentication policy that protects its most valuable applications, resources and information.

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

## MIRI Token (OTP) use cases for different industries

*Finance:* The banking industry is a perfect application of OTP. All the transactions are money related. Such operations must process using verified details. The Multi factory authentication solution "MIRI TOKEN" application covers multiple banking authentication requirements. Some of them listed below

- Financial
  - Ecommerce transactions
  - Internet Banking
  - Mobile Banking
  - ATM transactions
  - PoS/Mobile mPoS transactions
- Non-Financial transactions
  - Profile Changes authentication
  - Beneficiary Addition/Removal
  - Password changes
  - Services Requests etc. to name a few

*Business Ecosystem:* OTP serves as a unique tool to maintain the validity of accounts for business. They allow authorizing the accounts to access any vital information with ease. Such methods can prevent data leak and result in maintaining the integrity of an ecosystem.

*Insurance sector:* OTP is useful for fraud prevention. Fraud operations are prevalent in the insurance sector. The insureds and legatees are notified if any fake transaction occurs. Even little modifications in the accounts can be treated as suspicious activity. So, OTP alerts should always be prioritized.

*Healthcare:* Healthcare industry has become a private affair over a period. The patients have turned sensitive with respect to sharing the medical reports and details. As all the details are available on portals, they are at the risky end of leakage. Whenever someone who is not authorized to login tries to get in the account he is asked for the OTP.

*Government Services:* The government uses the One-time password for validation procedures. For example- to check Aadhaar card with the registered mobile verification. Even the PAN card confirmations, and in some cases, it is a perfect way to protect the identity from getting leaked. The illegal actions such as- accessing the passport information without permission can be safe with this.

*Retail:* Effective use of eCommerce is only possible when the information remains secure. E-commerce groups like- Amazon and Flipkart maintain security by using One Time Password techniques.

## Use Case – Offline OTP for Banking

Let us consider a specific scenario of internet banking transaction flow as shown below

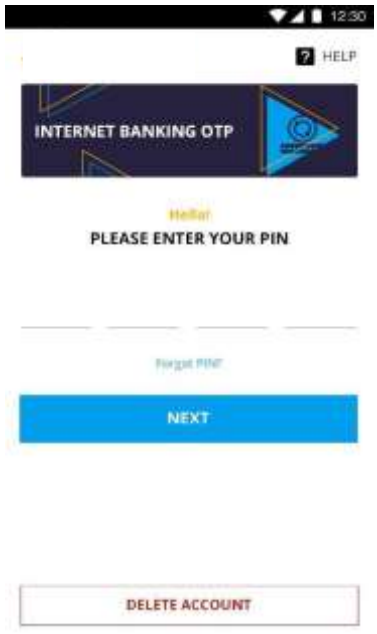
- Account activation
- OTP Generation
- Transaction

### Account Activation

1. Activation request/account creation is triggered by the user
2. Bank Offline OTP application user receives a 16 characters alphanumeric activation code along with a QR code representation of the same via email/SMS/screen display.


*Activation Step- 1*


*Activation Step 2*




*PIN Entry Screen Post successful activation*

3. During first time application run, user will be guided using app trainer through the interface, activation process and first-time key generation process. The system calls the web service method using an SSL encrypted connection.

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 an end user to restart the process. To complete registration to Offline OTP server, steps one and two must be completed within the timeout period. All activation attempts are logged along with the activation account, source IP address, date, time and a status indicating success or failure.

## OTP Generation

The OTP is passed with the to the Host, which will respond to the Bank System with the authentication status message. Based on the response received, the authorization/access will be granted to the user logging in.

In this scenario, the OCRA OATH Challenge Response Algorithm protocol is followed.