How does Zimperium help drive Reserve Bank of India (RBI) Compliance for Digital Payments

MAPS™

ZIMPERIUM®

Who is Zimperium?

Zimperium is an industry-leading Mobile Security company. We secure mobile devices and mobile applications to access sensitive data and systems to deliver value safely. Our Mobile Application Protection Suite (MAPS) enables organizations to build secure and compliant applications for mobile and connected devices.

What is the objective of this document?

The objective of this document is to help private enterprises and government agencies in India understand how MAPS helps achieve compliance for the Master Direction on Digital Payment Security Control regulation issue by the Reserve Bank of India.

What is the overall objective of the RBI regulation?

To help Regulated Entities(RE) set up a robust governance structure for such systems and implement common minimum standards of security controls for channels like the internet, mobile banking, card payments, among others. While the guidelines will be technology and platform agnostic, it will create an enhanced and enabling environment for customers to use digital payment products more safely and securely.

Who is the Regulatory Agency?

Reserve Bank of India (RBI)

When did the regulation go into effect?

August 18, 2021

Who does the policy apply to?

The provisions of these directions shall apply to the following Regulated Entities (REs):

a) Scheduled Commercial Banks (excluding Regional Rural Banks);
b) Small Finance Banks;
c) Payments Banks; and
d) Credit card issuing BFCs.

Which policy requirements does Zimperium help you comply with?

Policy Requirement	zSCAN™	zKEYBOX™	zSHIELD™	zDEFEND™
5. REs shall incorporate appropriate processes into their governance and risk management programs for identifying, analyzing, monitoring and managing the specific risks, including compliance risk and fraud risk, associated with the portfolio of digital payment products and services on a continual basis and in a holistic manner.	✓			✓
9. REs shall evaluate the risks associated with the chosen technology platforms, application architecture, both on the server and client side. Further, REs should undertake a review of the risk scenarios and existing security measures based on incidents affecting their services, before any major change to the infrastructure or procedures is made or, when, any new threats are identified through risk monitoring activities. Further, unused or unwanted features of the platform should be closely controlled to minimize risk.	✓			✓
10. REs shall develop sound internal control systems and take into account the operational risk before offering digital payment products and related services. This would include ensuring that adequate safeguards are in place to protect integrity of data, customer confidentiality and security of data.	✓			
16. The key length (for symmetric/ asymmetric encryption, hashing), algorithms (for encryption, signing, exchange of keys, creation of message digest, random number generators), cipher suites, digital certificates and applicable protocols used in transmission channels, processing of data, authentication purpose, shall be strong, adopting internationally accepted and published standards that are not deprecated/ demonstrated to be insecure/ vulnerable and the contigurations involved in implementing such controls are in general, compliant with extant instructions and the law of the land.		✓	✓	
18. The mobile application and internet banking application should have effective logging and monitoring capabilities to track user activity, security changes and identify anomalous behavior and transactions.				✓
20. REs shall follow a 'secure by design' approach in the development of digital payment products and services. REs shall ensure that digital payment applications are inherently more secure by embedding security within their development cycle.	✓	✓	✓	✓

Policy Requirement	zSCAN™	zKEYBOX™	zSHIELD™	zDEFEND™
22. REs (including those partnering with other entities to co-brand/ co-develop applications) shall adopt and incorporate a threat modelling approach during application lifecycle management into their policies, processes, guidelines and procedures.	✓			✓
24. REs shall conduct security testing including review of source code, Vulnerability Assessment (VA) and Penetration Testing (PT) of their digital payment applications to assure that the application is secure for putting through transactions while preserving confidentiality and integrity of the data that is stored and transmitted.	✓			
31. Testing has to necessarily verify for vulnerabilities including, but not limited to OWASP/ OWASP Mobile Top 10, application security guidelines/ requirements.	✓			
34.REs may also adopt adaptive authentication to select the right authentication factors depending on risk assessment, user risk profile and behavior.				✓
38. Fraud analysis shall be conducted to identify the reason for fraud occurrence and determine mechanism to prevent such frauds.				✓
48. REs may continuously create public awareness on the types of threats and attacks used against the consumers while using digital payment products and precautionary measures to safeguard against the same.				✓
55. On detection of any anomalies or exceptions for which the mobile application was not programmed, the customer shall be directed to remove the current copy/ instance of the application and proceed with installation of a new copy/ instance of the application. REs shall be able to verity the version or the mobile application before the transactions are enabled.			✓	✓
56. Specific Controls for mobile applications include: a. Device policy enforcement (allowing app installation/ execution after baseline requirements are met b. Application secure download/ install; d. Storage of customer data; e. Device or application encryption; g. Application sandbox/ containerization; h. Ability to identify remote access applications (to the extent possible) and prohibit loginaccess to the mobile application as a matter of precaution; and code obfuscation.	✓	✓	✓	✓

Policy Requirement	zSCAN™	zKEYBOX™	zSHIELD™	zDEFEND™
57. REs may consider to perform validation on the security and compatibility condition of the device/ operating system and the mobile application to ensure that activities relating to the account are put through the mobile application in a safe and secure manner.				✓
58. REs may explore the feasibility of implementing a code that checks if the device is rooted/ jailbroken prior to the installation of the mobile application and disallow the mobile application to install/ function if the phone is rooted/ jailbroken.				✓
59. Applications must be able to identify new network connections or connections from unsecured networks like unsecured Wi-Fi connections and must implement appropriate authentication/ checks/ measures to perform transactions under those circumstances.				✓
62. Applications must be able to identify new network connections or connections from unsecured networks like unsecured Wi-Fi connections and must implement appropriate authentication/ checks/ measures to perform transactions under those circumstances.				✓
64. REs shall ensure that their mobile application limit the writing of sensitive information into 'temp' files. The sensitive information written in such files must be suitably encrypted/ masked/ hashed and stored securely.	✓	✓	✓	✓
65. REs may consider designing anti-malware capabilities into their mobile applications.				✓
66. REs shall ensure that the usage of raw (visible) SQL queries in mobile applications to fetch or update data from databases is avoided. Mobile applications should be secured from SQL injection type of vulnerabilities. Sensitive information should be written to the database in an encrypted form. Web content, as part of the mobile application's layout, should not be loaded if errors are detected during SSL/TLS negotiation. Certificate errors on account of the certificate not being signed by a recognized certificate authority; expiry/ revocation of the certificate must be displayed to the user.	✓			✓