



MIUI 12

SECURITY WHITE PAPER

2021.05

Contents

1	Introduction	1
2	Hardware and System Security	4
	Hardware Trusted Environment	5
	Secure Boot	7
	Security Kernel	9
	Network Security	9
	Device Control	11
	System Software Update	14
3	Encryption and Data Security	15
	Data Protection Architecture	16
	Key Management	18
	Encryption Application	20
4	Application Security	23
	Application Security Protection	24
	Application Security Features	26
	Privacy protection	27
5	Internet Service Security	30
	Mi Account	31
	Xiaomi Cloud	34



	Image AI	38
	MiPush	39
6	Compliance and Privacy Practice	42
7	Conclusion	47
8	Glossary	49
9	Document Revision History	54



Statement

The content of this document may change, subject to the upgrades and adjustments to Xiaomi products or services or other reasons, Xiaomi has the right to add, modify, delete or nullify the content of this document. Please download the latest version from the official website in time.

This document only serves as a reference for users to understand the basic principles of MIUI and Xiaomi Cloud Service. Xiaomi has strived to provide an appropriate introduction to these topics in line with the current MIUI version and the main hardware architecture in service. However, in view of potential problems such as technology upgrades, product iterations, changes of applicable laws and regulations and consistency of wording, Xiaomi hereby expressly declares that we do not offer any guarantees, whether explicitly or implicitly, to the completeness, accuracy or applicability of the content of this document.

In accordance with relevant laws, Xiaomi and its affiliates (hereinafter collectively referred to as "Xiaomi") own the intellectual property rights for all original content by Xiaomi in this document, including but not limited to images, architecture designs, descriptive texts, etc. No organisation, company or individual may extract, translate or copy the content of this document, in part or in whole, without the prior written consent of Xiaomi.

If you find any errors in this document or have any questions about the content of this document, please contact Xiaomi directly at security@xiaomi.com.



01

Introduction



1. Introduction

As the world's leading smartphone manufacturer, Xiaomi's corporate mission is to relentlessly build amazing products at honest prices so that everyone throughout the world can enjoy a better life through innovative technology. In the era of intelligent interconnectivity, security and privacy are the primary needs of users of products. Thus, Xiaomi attaches great importance to issues involving user security and privacy.

The MIUI designed by Xiaomi focuses on security and usability at its core. Software, hardware and services are tightly integrated and work together on each Mi phone to provide users with end-to-end security protection. This includes basic security capabilities such as hardware chips, system kernels and data security, as well as information security and privacy protection for a series of key services, such as Mi Account, Mi Pay, Mi Cloud, Image AI and so forth.

By adhering to the principles of objectivity and transparency, this document provides a detailed introduction of MIUI's security architecture, technical principles, functional design and privacy protection measures. Xiaomi hopes that its users, developers, partners and the relevant regulatory authorities can gain a clearer understanding of the architecture and implementation of Xiaomi's information security and privacy protection measures for mobile phones and cloud services.

MIUI's security technology originates from the security root-of-trust built from hardware, with the chain of trust then transferred to the operating system through the secure boot process. By using and enhancing the Android security kernel, it monitors the runtime status of applications to ensure operating system and application security. File system and user data security is protected through encryption and data protection functions. The cloud services are comprehensively protected by the partitioning of service functions and Defense-in-Depth protection. The figure below shows the logical structure of the Xiaomi MIUI Security and Privacy White Paper. This paper will expand on such structure.

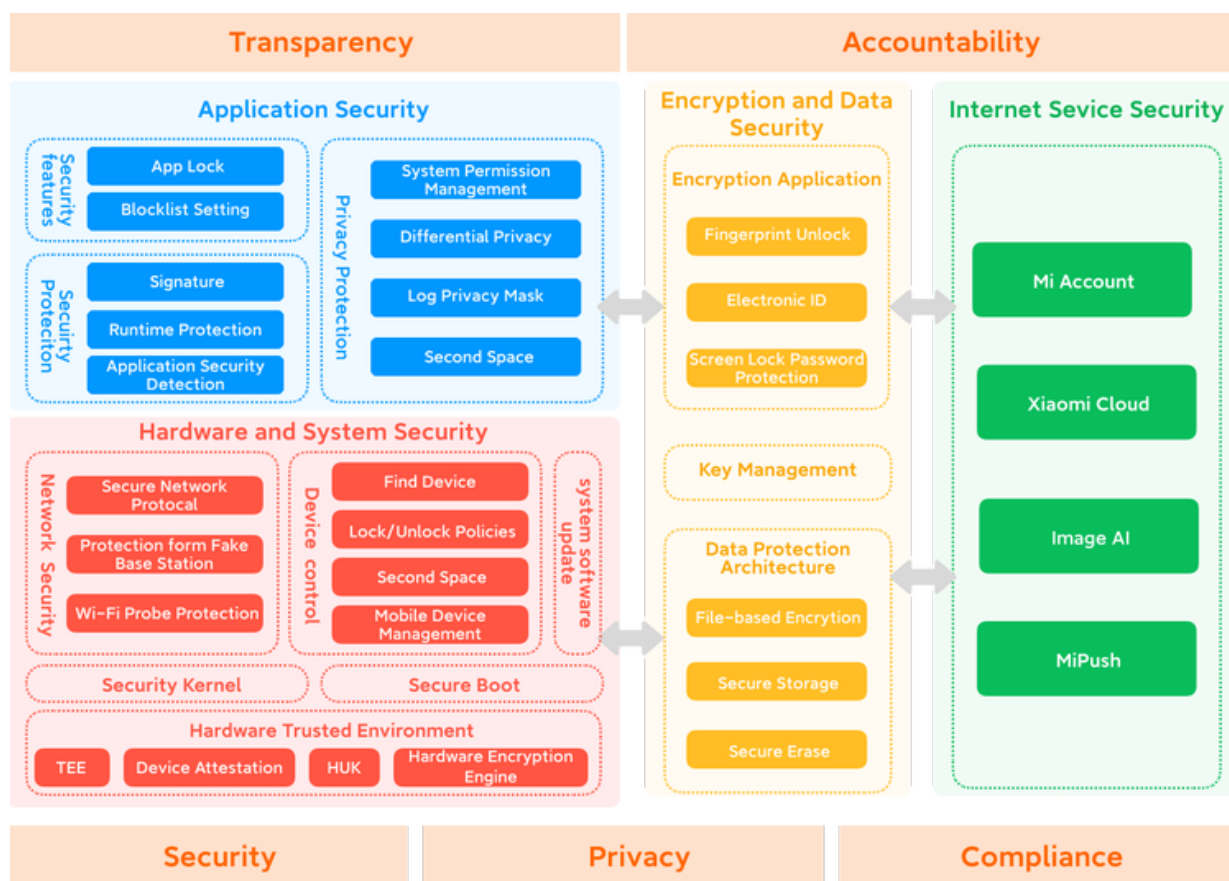


Figure 1-1 White Paper Logic Structure

Hardware and System Security: A Mi phone is a secure, integrated software and hardware platform that includes a hardware-built trusted environment, secure boot, security kernels, network and communication security, device control and system software updates.

Encryption and Data Security: The encryption application provided by the data protection architecture based on MIUI's design not only ensures the security of user data, but also improves MIUI usability and convenience as well.

Application Security: The basic protection mechanism and a series of application security features enables apps to run securely while protecting the security of user data.

Internet Service Security: For its primary Internet services running on MIUI, Xiaomi has taken the greatest degree of protection to protect users' privacy and data security.

Compliance and Privacy Practice: Xiaomi's overall principles, organizational architecture, security and privacy certification, privacy policies and continuous improvement mechanisms in terms of information security and privacy protection.



02

Hardware and System Security

2. Hardware and System Security

Hardware and system security is the foundation of application and data security, and provides the underlying framework for the overall security of MIUI, including hardware trusted environments, secure boot, security kernels, network and communication security, device control, system software updates and so forth.

By closely integrating hardware, systems and services, MIUI ensures that every component has a security authentication mechanism from initial startup to system software updates to the application itself, thereby maximizing the protection of user data to the greatest extent.

2.1 Hardware Trusted Environment

2.1.1 Trusted Execution Environment (TEE)

MIUI supports TEE (Trusted Execution Environment) secure operating systems. TEE is a small, independent operating environment isolated from the main operating system, allowing applications with higher security and privacy demands to run in isolation from the Android system.

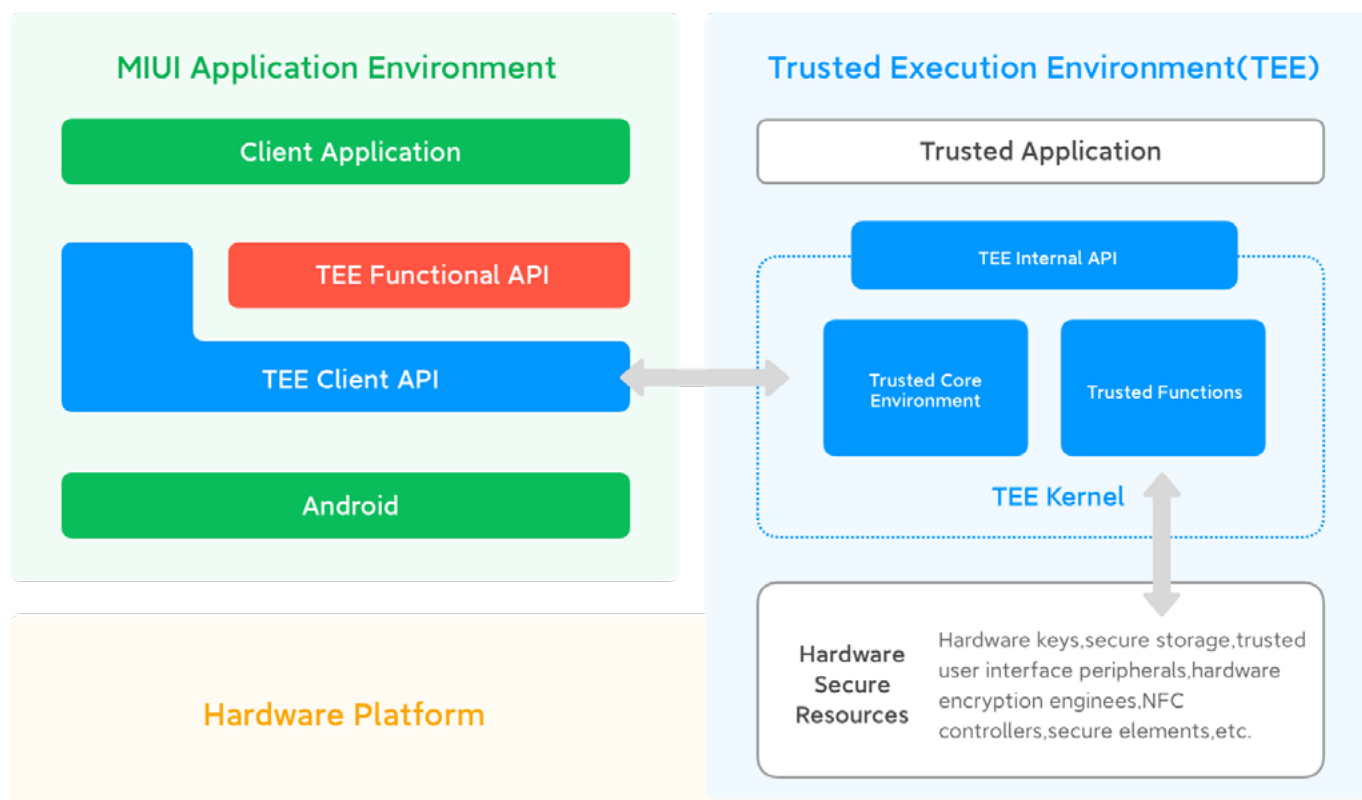


Figure 2-1 Logical Architecture of Trusted Execution Environment

The software and hardware resources that TEE can access are separated from the main operating system. TEE provides a secure execution environment for trusted applications, it also protects the confidentiality and integrity of, and access permissions to, the data and resources belonging to those trusted applications. To guarantee the root of trust of the TEE itself, the TEE needs to be verified and isolated from the main operating system during the secure boot process. Inside the TEE, each trusted application is independent from each other, and cannot access one another without authorization. TEE's internal API mainly includes key management, a cryptographic algorithm, secure storage, secure clock and other resources and services, as well as extended trusted UIs.

The trusted UI means that when displaying sensitive information and performing sensitive operations (e.g., entering a PIN or password), hardware resources, such as screen display and keyboard, are completely controlled by the TEE and thus cannot be accessed by software in the Android system.

2.1.2 Device Attestation

To ensure the trustworthiness of Mi phones, Xiaomi has pre-installed a device certificate in the TEE to uniquely identify each mobile phone. The public keys for such certificates are centrally stored in Xiaomi's servers. In scenarios where a higher level of security is required, the application can send authentication requests to Xiaomi servers to verify the authenticity of the device.

2.1.3 Hardware Unique Key (HUK)

The HUK (Hardware Unique Key), which is solidified to the motherboard before leaving the factory, varies from phone to phone and cannot be tampered with. It is accessible only by the hardware encryption engine and it guarantees device uniqueness with respect to the keys used for screen lock password protection and file system encryption.

2.1.4 Hardware Cryptographic Engine

Encryption and decryption are very complicated operations and require great computing power. For mobile devices, computing speed, energy conservation and security are of vital importance. Mi phone has taken these factors into consideration in its design, and the device is equipped with a high-performance hardware encryption engine* to ensure that the device achieves a balance in terms of running speed, battery life and data security. The main algorithms supported by the encryption engine are:

- 3DES



- AES-128、AES-256
- SHA-1、SHA-256
- HMAC-SHA1、HMAC-SHA256
- RSA-1024、RSA-2048
- ECDSA-256

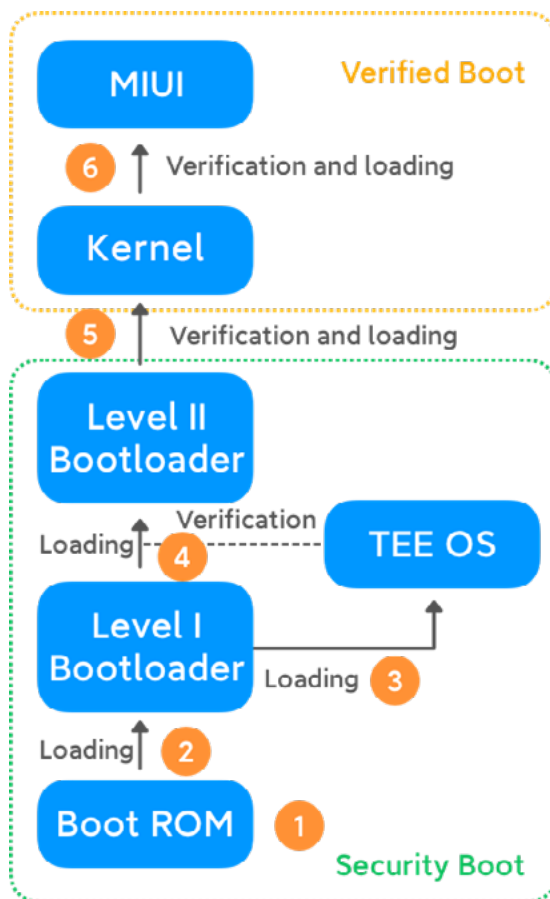
*Note: Some models are not equipped with hardware cryptographic engines.

2.2 Secure Boot

Secure boot is a program that verifies the digital signature of files and applications using the corresponding public keys to ensure the integrity and authenticity of the boot file or program, so as to prevent unauthorized programs from being loaded and running during the boot process.

Under the secure startup mechanism, all startup files (e.g., the bootloader, kernel image, baseband firmware) must pass signature verification before they are allowed to load and run. If signature verification fails at any stage during the boot process, the process will be terminated.

The ROM SoC Bootloader is a bootloader written into a chip's internal ROM when the chip is manufactured, and cannot be modified after leaving the factory. This piece of code is the first to be executed after the device is powered on.



1. When the device is powered on, the PC pointer points to the Boot ROM address inside the chip, and the process is executed.
2. The Boot ROM is loaded from an external storage device, and the level I Bootloader gets executed after verification.
3. The level I Bootloader loads the TEE OS image file.
4. The level I Bootloader loads the level II Bootloader, then the TEE OS verifies its integrity.
5. The level II Bootloader verifies and loads the kernel file.
6. The kernel program verifies and loads the MIUI system.

Figure 2-2 MIUI Secure Boot Process

After the device is powered on, the ROM SoC Bootloader will first perform the basic system initialization and load the level I bootloader from the Flash memory chip. It will then utilize the public key stored in the FUSE space inside the main chip to verify the digital signature of the level I bootloader image. The level I bootloader will run after successful verification. After completing the above steps, the level I bootloader will load, verify and execute the TEE OS image. Once the TEE OS is in operation, it will verify, load and execute the level II bootloader together with the level I bootloader. Such process will continue until the entire system startup is completed in order to ensure the chain of trust is transferred during the boot process and prevent unauthorized programs from being maliciously loaded and run.

MIUI system supports Android's Verified Boot 2.0 (AVB2.0) feature. Prior to entering any subsequent stage in a device's startup process, code reliability must be verified through an authenticated encryption process to ensure that all components—from the hardware-protected root of trust to the bootloader and boot partition or other verified partitions



(including system, vendor and optional OEM partitions)—are free from any known security defects. AVB helps prevent persistent rootkit from holding root privileges and ensures the security of the device during the startup process.

2.3 Security Kernel

MIUI supports Android's native SELinux features, and enforces mandatory access control for the operations of all resources in the system, such as processes, files, directories and the like. Any process that intends to perform operations in the SELinux system must first be granted permission in the security policy configuration file. The access control policy file will be protected during the boot process of the device and cannot be tampered with by third parties. With SELinux, MIUI can prevent system processes from reading and writing protected data, bypassing the security mechanisms of the kernel, or attacking other processes.

MIUI supports KASLR (Kernel Address Space Layout Randomization) and allocates the kernel address space layout randomly whenever the system is booted. KASLR results in an unpredictable kernel address space layout, and increases the difficulty in performing code-reuse attacks. It reduces the possibility of a number of complex attacks, and further strengthens the security of the system kernel.

2.4 Network Security

2.4.1 Secure Network Protocol

Using secure network protocols can reduce the risk of data leakage and tampering when the user's device connects to a network. MIUI users can establish their own virtual private network (VPN) over public network connections. MIUI supports multiple VPN modes including: PPTP, L2TP/IPSec PSK, L2TP/IPSec RSK, IPSec Xauth PSK, IPSec Xauth RSA and IPSec Hybrid RSA. Users can select VPN mode as needed to access and transmit sensitive data.

MIUI's WLAN connection supports WEP, WPA/WPA2 PSK, 802.1x/EAP, WAPI and many other authentication methods to facilitate users' various security level needs.

MIUI's WLAN hotspot function is disabled by default. When the user enables the function, the WPA2 PSK authentication method is used by default to ensure the security of the connection. At the same time, the WLAN hotspot function also supports the configuration



of terminal MAC address blacklisting.

2.4.2 Identifying SMS messages from Fake Base Stations

Even when the user has not enabled the protection from fake base stations function, MIUI still provides the user with features to identify SMS messages sent from fake base stations. Such features do not rely on chips and are available to MIUI users of all models and versions.

The AI machine learning model of the mobile terminal is engaged to identify fake base station SMS messages by determining the degree of suspicion of the fake base station based on the characteristics of the fake base station accessing the phone and the textual characteristics of the SMS messages sent by the fake base station.

MIUI's identification of fake base station messages is performed offline on the user's mobile terminal. MIUI will prompt users whenever an SMS message is identified as being sent from a fake base station.

2.4.3 Wi-Fi Probe Protection

The Wi-Fi probe box identifies each user by monitoring Wi-Fi signals in the air sent by other electronic devices to acquire the MAC address from the data packet. MIUI is capable of sending data packets with random MAC addresses to prevent Wi-Fi probes from obtaining the real MAC address of the mobile phone*.

*Note: Most devices using MIUI 12 already supports Wi-Fi probe protection in the unconnected state. In addition, mobile phones upgraded to Android Q or newer versions support Wi-Fi probe protection in connected state.

2.5 Device Control

2.5.1 Find Device

MIUI provides users with a find device feature that assists users in locating lost mobile phones, while protecting the data security of the phone. This feature is turned off by default and can be used only when the user turns it on manually. If, after enabling this feature, the user loses his or her phone, the user can log in to Mi Cloud (<https://i.mi.com>) to remotely perform the following operations for the lost device: Locate, Sound, Lost mode, Erase data.

Locate	Allows users to obtain the current location of their mobile phone through a network or by SMS commands. The location of the lost device is then visually displayed on a map.
Sound	Users can utilize a network or SMS command to make their mobile phone ring as a means of finding their phone if it is nearby.
Lost mode	Users can lock their mobile phone through a network or by SMS commands. After being locked, the phone will automatically report its location periodically, while any bank cards linked to Mi Pay will be automatically unlinked.
Erase data	Users can reset their mobile phone through a network or by SMS command, and can disable data synchronization and unlink any bank cards linked to Mi Pay.

2.5.2 Mobile Phone lock/Unlock Policies

After the Find Device feature is enabled, the mobile phone will be linked to the Mi account currently logged in. MIUI has designed a variety of security policies to protect users' rights under such circumstances.

Activation locking	If, after enabling the Find Device feature, it is necessary to restore the mobile phone to its factory settings, the user must enter the account password linked to the device at the time that the Find Device feature is enabled. The mobile phone will lock after it has been flashed, and can only be unlocked after the user enters the account password linked to the device at the time that the Find Device feature is enabled.
Password reset protection	In order to prevent the credentials from being reset on a lost phone through mobile phone verification, "Find device" function cannot be turned off within 3 days of Mi account password reset. It provides time for the user who has lost the mobile phone to reobtain the SIM card and regain the control of the account and mobile phone.
Customer service unlocking	In the event that the user forgets his or her Mi Account password and cannot retrieve it, MIUI provides an unlock code on the mobile phone's Lock interface so that the user can unlock the phone via customer service. Users requesting an unlock code must submit an application. The phone will only be unlocked after a detailed manual review by the customer service team.

In addition, if a mobile phone is lost, the existence of a screen lock password makes it highly likely that the user will be forced to flash the device. MIUI stores the association between the account and the device to its cloud server (some devices write the association status into a special partition that cannot be flashed) to make the association tamperproof. When booting, the device is required to connect to the network and obtain the true association from the server. If the current login account is different from the associated account on the server, MIUI will require the user to switch back to the associated account before continuing to use it.

Users of devices with an unlocked BL lock can bypass the phone lock by forcibly flashing a non-MIUI system or unofficial, tampered MIUI system. However, this kind of ROM cannot perform OTA (Over the Air) and cannot login to Mi Account normally. When the device flashes back to the official MIUI pack, it will once again be protected by the Find Device feature.



2.5.3 Second Space

MIUI users can create a separate space completely independent from the original system through MIUI's second space. This allows the complete isolation, and with separate encryption protection, of users' accounts, applications and data from the main space. Additionally, users can set different unlock passwords for accessing the main space and the second space, thereby achieving a virtual mobile phone experience that is much like having a second device. By setting passwords to access the independent space, users can save all kinds of private files, pictures and other information, and install private applications. Moreover, this independent space is similar to a "sandbox." Any operations performed in this "sandbox" will not affect the main space of the mobile phone.

*Note: Mobile phones with a RAM of 4 GB or less will no longer support this function.

2.5.4 Mobile Device Management (MDM)

MDM (Mobile Device Management) is a device protection function MIUI provides to device management applications and functions as an interface for managing and operating mobile phone devices. Through the MDM application and API interface provided by MIUI, corporate IT systems can easily control and manage MIUI devices. API calls require authorization to ensure permission control and security.

For applications that guide or provide permissions for the abnormal use of the device manager, the system control policy must be implemented according to the relevant criteria, which include, without limitation, strongly reminding the user to close the application, and prohibiting the application from accessing services or permission interfaces.

For applications that guide or provide permissions through the device manager that may harm user data and device security, the following operations will be rigorously performed: the application will be removed from Xiaomi's GetApps, the application will be prohibited from accessing the relevant service interfaces and the relevant applications will be prohibited from being displayed in the device manager's app list.

*Note: Mobile phones customized by telecom operators do not support this function.



2.6 System Software Update

MIUI supports Android's native OTA (Over the Air) mechanism and provides more secure and efficient Android-based management for system upgrades.

Before the system software is updated, the system update program verifies the integrity of the ROM downloaded via OTA or copied offline to the mobile phone's storage. It verifies the size and hash value of the file. After passing verification, the mobile phone restarts to invoke the underlying recovery mode, and once again verifies the correctness of the signing key. The recovery mode will write the updated contents in the ROM to the system storage only after verification has been passed.



03

Encryption and Data Security



3. Encryption and Data Security

This chapter describes MIUI data security protection mechanism. The MIUI file system is divided into the system partition and user partition. The system partition is read-only and isolated from the user partition. And common applications can only access some system partition directories. For the user partition, the system provides file-based data encryption and directory permission management mechanisms to restrict data access between different applications. At the same time, MIUI provides more security functions and applications based on encryption technology, and improves the convenience and usability of use for MIUI while protecting user data security.

3.1 Data Protection Architecture

3.1.1 File-Based Encryption

This section describes MIUI's data security protection mechanism. The MIUI file system is divided into a system partition and user partition. The system partition is read-only and isolated from the user partition. Common applications can only access some of the system partition's directories. In the case of the user partition, the system provides file-based data encryption and directory permission management mechanisms to restrict data access between different applications. In addition, MIUI provides more security functions and applications based on encryption technology, and improves the convenience and usability of MIUI while also protecting user data security.

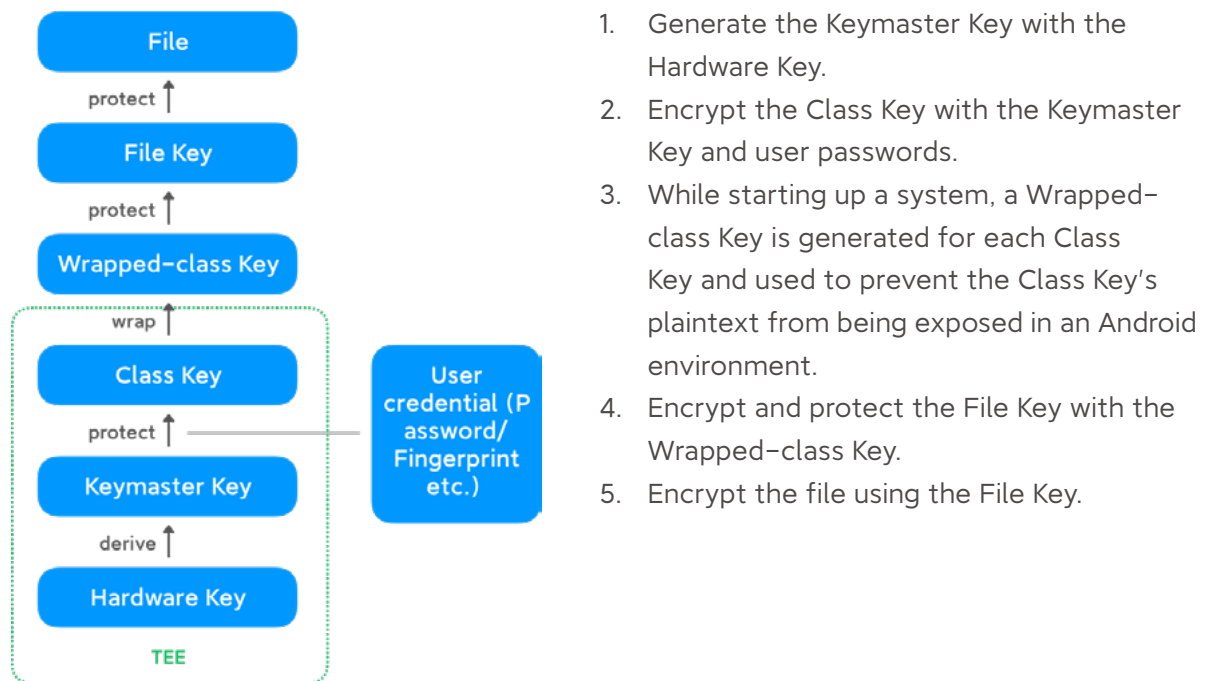


Figure 3-1 File-based Encryption Procedure*

*Note: This schematic diagram is suitable for Mi phones that use Qualcomm chips and support FBE.

Each Mi phone that supports FBE provides every user with two storage locations for applications:

- Credential encrypted (CE) storage area: The CE area is the default storage area and is only accessible after the user has unlocked the device.
- Device encrypted (DE) storage area: The DE area is accessible after the device has been powered on regardless of whether the screen is unlocked.

The CE storage area is the default storage area in MIUI for applications to store data to ensure the security of the application and application's data. Only applications such as wireless authentication, alarm clock, ringtone, Bluetooth and the like store certain data in the DE storage area. This ensures that certain essential services will run before users provide credentials while the system continues to protect user private information.

3.1.2 Secure Storage

The secure storage function of MIUI is achieved by a TEE-based Secure File System (SFS),

and is used to securely store sensitive information such as keys, certificates, fingerprint templates and so forth. The trusted application (TA) running in the TEE uses a secure storage API to encrypt and store data. Encrypted data are only accessible by the TA and therefore cannot be accessed by external applications. The secure storage in MIUI adopts AES-256 for encryption and decryption. The secure storage keys are derived from the hardware unique key (HUK) and invariably stored in the device's TEE. Data encrypted by the keys cannot be decrypted outside the TEE.

MIUI further provides the Flash-based RPMB (Replay Protected Memory Block) partitioning feature to protect certain system data from unauthorized deletions and access. RPMB is directly controlled by the TEE for security and linked to the keys derived from the hardware unique key (HUK). Only the TEE can access the RPMB-protected data, and the external Android side does not provide an interface to access the RPMB. RPMB prevents replay attacks through built-in counters, keys and an HMAC verification mechanism to ensure that data cannot be maliciously overwritten or tampered with.

3.1.3 Secure Erase

General "Factory reset" do not guarantee that data stored in physical storage will be thoroughly erased. In order to improve efficiency, this is usually achieved by deleting the logical address. However, physical address space is not actually wiped and the data can be recovered. MIUI provides users with the option to "format mock SD card" when they wish to restore factory settings. Once this option is chosen, the system will format the storage space and completely erase the data to protect user data security after the device is sold or scrapped.

3.2 Key Management

The MIUI's key management function is used primarily to manage the life cycles of the keys and certificates used by application developers, while also providing remote certification for device certificates in the TEE environment. Key management has the following functions:

1) Generation and storage

MIUI's key management provides a key storage mechanism protected by hardware. The key generated in the application is encrypted and can only be used by the corresponding device.

2) Encryption and decryption

When it is necessary for an application to use the key, the previously generated encrypted key and the data to be encrypted are sent back to the TEE of the corresponding device. The key can only be used to perform encryption and decryption operations in the TEE of the corresponding device.

3) Key Authentication

As every Mi phone is injected with a Google-issued certificate at the time of its manufacturing, any generated key can therefore be authenticated with Google's certificate. The key authentication function allows the network service to authenticate MIUI devices.

The technical basis of MIUI's key management is Android Keystore which prevents the unauthorized use of key material outside of and on the device through measures such as key extraction prevention and key use authorization:

1) Extraction prevention

Key material can be protected against unauthorized use outside of MIUI devices. When an application performs encryption operations using an Android Keystore key, the plaintext, ciphertext and messages to be signed or verified are fed to a system process to perform the encryption operations—as opposed to an application process. Therefore, even if an application process is compromised, the attacker cannot extract the key material.

At the same time, MIUI also links key material to the secure hardware (e.g., TEE) of the Mi device to ensure key material is never exposed outside of the secure hardware. Even if the MIUI OS is compromised or an attacker can read the device's storage area, key material linked to the secure hardware cannot be extracted from the device.

2) Key use authorization

In order to mitigate the unauthorized use of keys on MIUI devices, Android Keystore lets applications specify methods of authorized use for their keys when the keys are generated or imported. Once a key is generated or imported, its authorization cannot be changed. Authorizations are then enforced by the Android Keystore whenever the key is used. Supported key use authorizations in MIUI fall into the following categories:

- Encryption: authorized key algorithms, operations or purposes (encryption, decryption,

signatures, verification), padding schemes, block modes and digests with which the key can be used.

- Temporal validity interval: interval of time during which the key is authorized for use.
- User authentication: the key can only be used if the user has authenticated recently.

3.3 Encryption Application

3.3.1 Fingerprint Unlock

The fingerprint unlock function simply requires the user to place a finger on the device's fingerprint sensor while the device's local AI fingerprint recognition algorithm conducts a comparison against the one or more fingerprint minutiae input by the user beforehand, to authenticate the user's identity.

While in use, the user's fingerprint data will not leave the device, nor will it ever be backed up or uploaded to the server. When a fingerprint is input, the device only saves the minutiae information of the input fingerprint, while retaining none of the fingerprint's original biometric information.

Xiaomi's fingerprint unlock security framework extends Android's native fingerprint security architecture and uses it as a basis for expansion.

(1) The fingerprint minutiae template is encrypted by the AES-256 encryption algorithm and then stored in a secure file system (SFS) in the TEE environment. Encryption is achieved by invoking KeyStore. The fingerprint minutiae template is signed with the device's dedicated private key that makes the template unusable on other devices and unavailable to any other user registered on the same device. Encrypted fingerprint minutiae information can only be accessed by the TA itself. Even if the mobile device has been rooted, the attacker cannot read the fingerprint minutiae data through the hacked kernel and platform, thereby securing the user's fingerprint minutiae data stored on the device client.

(2) The entire fingerprint authentication process is performed in the TEE environment. During this process, applications outside the TEE environment that support fingerprint authentication can only initiate fingerprint authentication requests and receive authentication results through the external fingerprint framework. This makes the fingerprint authentication process secure since the fingerprint minutiae data itself cannot be accessed.

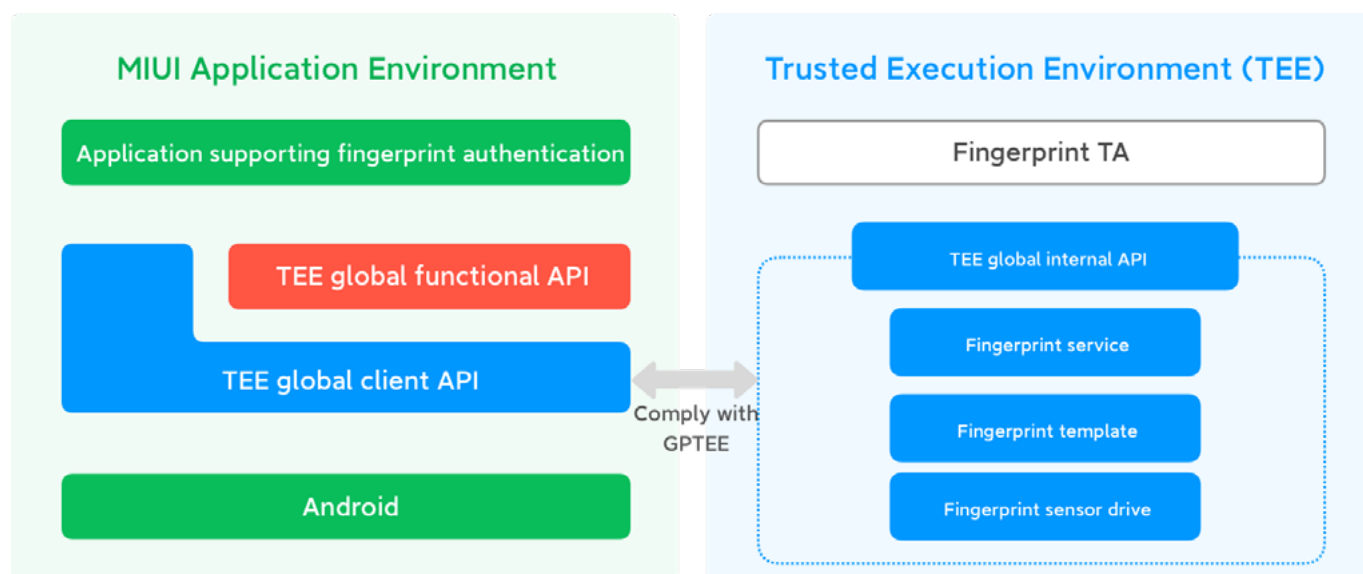


Figure 3-2 Fingerprint Unlock Security Framework

Xiaomi's AI fingerprint recognition algorithm is only used for device unlocking purposes, fingerprint payment features or other application service scenarios offered by Xiaomi's electronic products. In order to improve the accuracy and reliability of fingerprint recognition model, the algorithm will undergo repeated training on multiple occasions before going live. The datasets used to train the algorithm are procured through official channels. Xiaomi will not use user fingerprint data for algorithm model training purposes.

In order to enhance the security of a user when using the device, the fingerprint unlock service is restricted in the following scenarios:

- 1) When the user's device has just been turned on or restarted;
- 2) If the device has not been unlocked using a password for more than 72 hours;
- 3) If the fingerprint unlock function fails to unlock the user's device five times in a row.

3.3.2 Electronic Identification

The network electronic identification eID (hereinafter referred to as "eID") is an electronic ID application jointly developed by Xiaomi and the Third Research Institute of Ministry of Public Security of the People's Republic of China. The eID functions the same as the physical ID card in scenarios approved by the Ministry of Public Security.

Mi phones comply with eID-related standards and specifications, specifically including the following: employing the security chip as the carrier; the chip has an independent

processor, a secure storage unit and a cryptographic coprocessor; only the dedicated security chip operating system can be running. eID information is encrypted and stored in the security chip eSE and can only be accessed by specific programs. When eID is activated, the security chip uses asymmetric key algorithms to generate a pair of public and private key for signature, ensuring that eID cannot be authorized read, copied, tampered with and used, and users can be provided a more secure network digital identity service.

The MIUI's mobile wallet client supports the whole lifecycle management of eID, which allows users to open, download, use and deregistrate personal eID on the phone at any time.

*Note: Only some specific models are supported.

3.3.3 Screen Lock Password Protection

MIUI screen lock passwords support draw patterns, numeric passwords and hybrid passwords, each of which has a minimum password length requirement to ensure a more secure password.

- Draw pattern password: at least 4 dots need to be connected.
- Numeric password: these passwords support lengths of between 4–16 digits.
- Hybrid password: these passwords support any combination of uppercase and lowercase letters, numbers and symbols with lengths of between 4–16 characters.

MIUI screen lock passwords are protected by the hardware unique key (HUK) and encrypted in the TEE. When a user creates or modifies a lock screen password, or unlocks the screen using a screen lock password for verification, the screen lock password is processed in the TEE.

The MIUI limits the number of times an incorrect password can be entered. After attempting to use an incorrect password multiple times in a row, the phone will be locked to prevent the brute-forcing of the screen lock password.

04

Application Security

4. Application Security

On the basis of MIUI's underlying hardware security, system security framework and data security protection mechanism, the application runtime environment is protected through application layer security technologies, such as application signature, runtime protection and application security testing.

At the same time, MIUI further provides a series of security and privacy protection functions for users to choose from, such as: App lock, blocklist setting, differential privacy, log privacy masks and second space.

4.1 Application Security Protection

4.1.1 Signature

MIUI verifies the integrity of the application package (hereinafter referred to as "APK") and the officialness of its source, in order to:

- Ensure that the APK is tamper-proof

The developer generates the public key and the private key, signs the APK with the private key, and packages the public key into the APK. When the application is installed, the public key is used to verify that the APK has not been tampered with.

When updating the installed application, the application signature verification is also required. Only application with the same signature as the updated application are allowed to be updated, so as to prevent malicious applications from replacing existing ones.

- Ensure that the APK is forgery-proof

The APP ID of the APK and the certificate used to verify the signature are signed with the official private key. If developer A signs developer B's APK with its own certificate and packages this certificate file into the APK, the official signature verification will fail when developer A uploads it to the application store.

- Ensure that APK permissions cannot be changed at will

The authorization list, APP ID and certificate are all signed with the official private key. When installing and running the application, check the consistency of the authorization list and the system service it actually revokes, if these are not consistent, the MIUI service being invoked will fail.

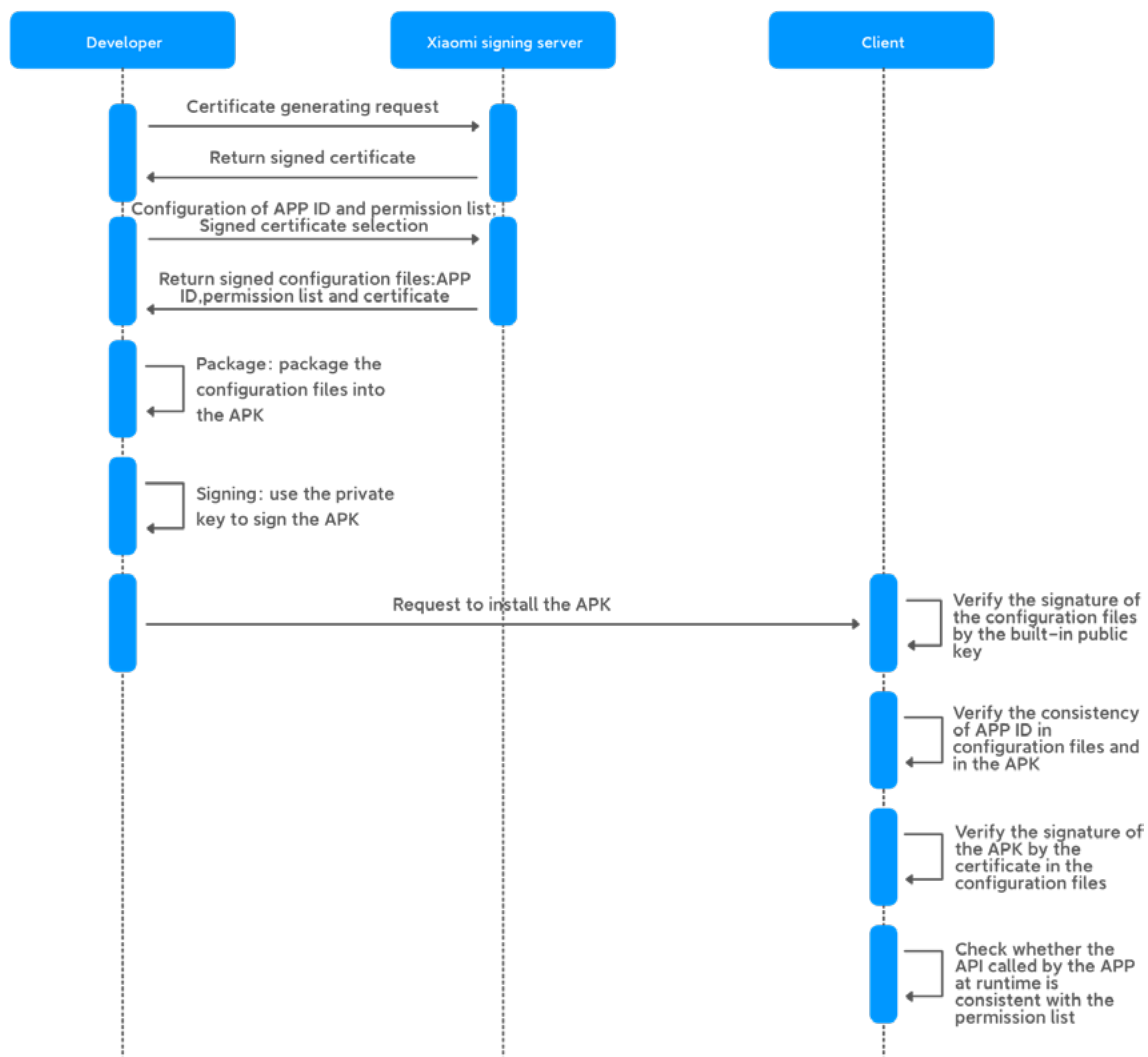


Figure 4-1 New Application Signature Process

4.1.2 Runtime Protection

MIUI supports Android's native Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP). ASLR is a security technique that protects against buffer overflow. It randomizes the layout of linear areas such as heaps, stacks and shared libraries, making it harder for attackers to predict target addresses and preventing them from locating attack codes, thereby preventing overflow attacks. ASLR makes it more difficult for attackers to take advantage of memory vulnerabilities. DEP marks specific memory areas as non-executable to prevent attacks exploiting memory vulnerabilities.

In addition, MIUI also uses the native Android application sandbox mechanism to ensure that each application runs in the sandbox and is isolated from each other, thus ensuring the security of the runtime application.

4.1.3 Application Security Detection

Xiaomi GetApps conducts automatic testing, security scanning and manual review for each application to ensure the security of the application's source.

For the device, MIUI provides system protection and detection mechanisms such as virus scanners and removers embedded with various antivirus engines, application installation monitor and so forth.

In addition, the "Security" – "Solve problems" features also provide ROOT security detection and anomaly detection in terms of mobile phone performance, operation, power consumption, and so forth to protect application security. The following functions are included:

Performance anomaly detection	This feature detects whether the app has enabled accessibility and device manager, and whether the device's remaining memory is insufficient.
Network & Setting anomaly detection	This feature detects whether the device has enabled flight mode, call blocking (for contacts and unknown callers), DND mode and eye protection mode.
Battery anomaly detection	This feature detects whether there are too many autostart applications (more than 5), and whether the hotspot feature has been enabled.
Other anomaly detection	This feature detects whether the system is rooted, and notifies the user that the application cannot be installed when the storage space is less than 5%.

4.2 Application Security Features

4.2.1 App Lock

The App lock not only protects the security of application data, but also prevents the private information in the application from being seen by others.



MIUI users can enter the "App lock" module through "Security" and choose from a wide range of options (Patterns, PIN and Password) for the application. Through this module, users can set the app to either lock after exiting the application or to lock one minute after exiting the application, and then verify the App lock when opening the application again after locking the screen. In order to increase the convenience and security of unlocking, MIUI adds fingerprint biometrics and facial recognition unlocking mechanisms.

4.2.2 Blocklist Setting

MIUI's blocklist settings can provide users with comprehensive blocklist setting functions, which are able to effectively intercept unwanted phone calls and text message spam such as advertisements, sales promotion and real estate agencies and the like. Users can quickly add phone numbers from their recent call history and contacts to the black/white list. Users can also add regions to the white/black list to intercept phone calls and allow known numbers. The updated real-time yellow pages database provides users with accurate yellow pages information for numbers and prevents users from being disturbed by calls from unknown numbers.

MIUI provides a variety of interception rules that users can manually configure as needed. These configurations can be backed up to the cloud to perform functions such as cross-terminal synchronization, among others:

- Black/white list: Allows whitelisted numbers while blocking blacklisted numbers.
- Unknown number: Intercepts calls from unknown numbers.
- Call forwarding: Intercept forwarded calls.
- Smart interception*: Filter unwanted calls and text messages spam via the yellow pages database and intercept engine.

*Note: The smart interception feature is available in India only.

4.3 Privacy protection

4.3.1 System permissions management*

MIUI provides applications with a dynamic permissions management mechanism, aiming to limit sensitive operations and protect personal user data. The application makes a request in the form of pop-up windows before obtaining the permission, prompting the user to

decide whether or not to grant authorization.

- Sensitive permission management and control: Permission for "Location", "Camera" and "Microphone" can be set to "Allow only while in use" or "Allow for current operations". When the user sets the permission to "Allow only while in use", the application cannot use the related permissions when the application is not in use or is running in the background. While when the user sets the permission to "Allow for current operations", the application can only use the permission during the current process, and when the application is started again, the application needs to ask the user for permission again.
- "Camera" is disabled in the background: No application is permitted to invoke the "Camera" permission from the background to take a picture or video.
- High-risk permission management and control: When the application requests high-risk permissions, such as the permission to send you push notifications, MIUI will notify the user of any possible risks associated with the granting of authorization through a full-screen reminder.

*Note: The above permission management mechanism is supported by versions newer than Android R.

4.3.2 Differential Privacy

MIUI uses differential privacy technology to protect the user's privacy. When the user agrees to share data with Xiaomi, MIUI will upload and analyze such data after adding random interference information. This technology ensures that Xiaomi can only use the data provided by the user to study the overall trend and cannot obtain accurate information of the user. For example, the MIUI User Experience Program uses differential privacy technology to collect the operating status and the user traffic statistics of the user's phone. MIUI will upload and analyze such data after adding interference information at random. While ensuring the availability of data, this technology ensures that no one can obtain the user's accurate information from the data, thereby protecting user privacy to the greatest extent.

4.3.3 Log Privacy Mask

MIUI uses "*" to partially mask private information involved in Android native logs (such as base station location, IP address and device identifier) in order to further protect the private information.



4.3.4 Second Space

MIUI provides users with a series of private space functions such as private text messages, private photo albums, private folders and private notes.

Users can set this through the "Settings"–"Password & security"–"Privacy protection password" menu, and get access to exclusive space for private items by way of privacy passwords or fingerprint passwords. In this space, users can manage their private contacts, album pictures, files and notes. In addition, text messages to or from private contacts, as well as private pictures, private files and private notes will only be displayed in the private space, thus enhancing the protection of user private information.

Users can also use settings to decide whether to display notifications for private text message on the conventional interface.

If users clone this feature to their mobile phones, the above functions will be linked to display private content in the cloned space and regular content in the primary space.



05

Internet Service Security



5. Internet Service Security

For Internet services running on MIUI and other Xiaomi applications, Xiaomi strictly follows the principles of Security by Design and Privacy by Design, fully protects the security of user data, and strictly abides by the legal requirements of privacy and compliance. While providing users with easy-to-use functions, users are also given corresponding privacy options to protect their rights of privacy.

5.1 Mi Account

Mi Account is an account used to identify Xiaomi users, and which allows users to access Xiaomi products and services like Xiaomi Cloud, Mi Pay, MiStore, Mi Home, Mi Community, Mi Music, and more. Users can also purchase Mi coins through their Mi account to use Xiaomi's various virtual products and value-added services (e.g. games, e-books, etc.).

Xiaomi takes the privacy of your personal information very seriously and employs the following industry-standard practices to safeguard your Mi account.

5.1.1 Account Security Setting

When creating an account or resetting passwords, users need to set strong passwords containing 8–16 characters, and which include numbers, letters and special characters. After successfully signing in, users can add a secure recovery phone number or email to their Mi account, and enable the cross-device authentication feature. These security authentication methods will be used to verify users' identity when they change their account information or reset passwords.

5.1.2 Login Protection

Mi Account uses intelligent risk control services to protect user login credentials and effectively reduce the risk of unauthorized logins and identity theft.

The risk is addressed by detecting the user's login environment and operating methods when signing in. If login attempts with a password, SMS or other authentication method fail on multiple tries, the Mi Account adopts a number of interactive verification methods to further identify malicious attacks. These include, among others, image verification codes, sliding codes or CAPTCHA codes. When an abnormal login is identified, the Mi Account will require users to perform further authentication via the secure phone number

or secure email associated with the account. If authentication still fails, the user be restricted in terms of the services it is allowed to access according to the risk level. When a serious login risk is identified, the account will be frozen and forced to log out all current logins, while the current password cannot be used or reused.

Abnormal logins defined by the intelligent risk control service include:

- Logins to Mi Account in untrusted environment.
- Viewing of private data (e.g., using web pages to view any photos, messages, contacts, etc. stored in Xiaomi Cloud).
- Modifications of the settings in "Account Security" (e.g., changing the secure recovery phone or email, etc.).

Authentication methods include but are not limited to cross-device authentication, text message authentication and email authentication.

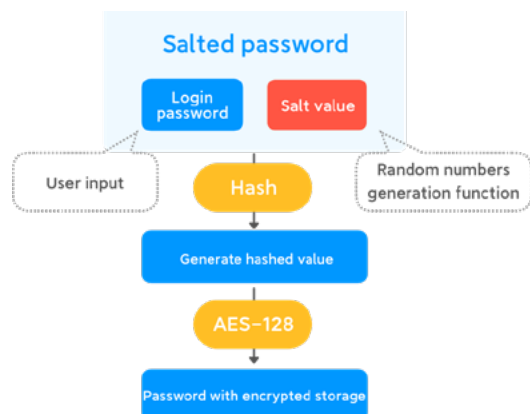
When the user's behavior of an account changes (e.g. change password, sign in on a new device, etc.), if it is determined as an abnormal risk, Xiaomi will send an e-mail and messages to notify the user, prompting the user to change the password immediately.

In addition, on a MIUI mobile phone, only the applications authorized by Xiaomi can log in with the Mi Account of the mobile phone system.

5.1.3 Data Security

Xiaomi encrypts the personal information that user entered during creating an account, including:

Personal information	Encryption method
Mobile phone numbers, e-mail addresses, account IDs	AES-128
Login password	Salted Hash, AES-128



A random number generator is used to generate a character string (random salt) and attach it to the login password. Once the cryptographic hash function (hash) generates a hash value, the AES-128 algorithm is used for encryption. The random salt of each user is different, even if two users use the same password, the final hash value is different.

Figure 5-1 Encryption Process for Login Passwords

When the user creates an account or signs in, the account-related information is transmitted to the server over an HTTPS encrypted channel. Users' personal information is encrypted and stored in a dedicated database with multiple backup copies. The security protection level of the backup data equals that of online data. Xiaomi performs role-based multi-level access control for user data and accepts the corresponding security audits.

User data encryption and decryption keys are uniformly managed by the Key Center. Key Center is the key management platform independently developed by Xiaomi and is operated and maintained by an independent team in order to separate business, data and key management responsibilities. Role-based access control ensures that no one obtains all of the permissions required to decrypt user data. In addition, the servers and databases that store user data have deployed real-time monitoring mechanisms to alert and block any abnormal access.

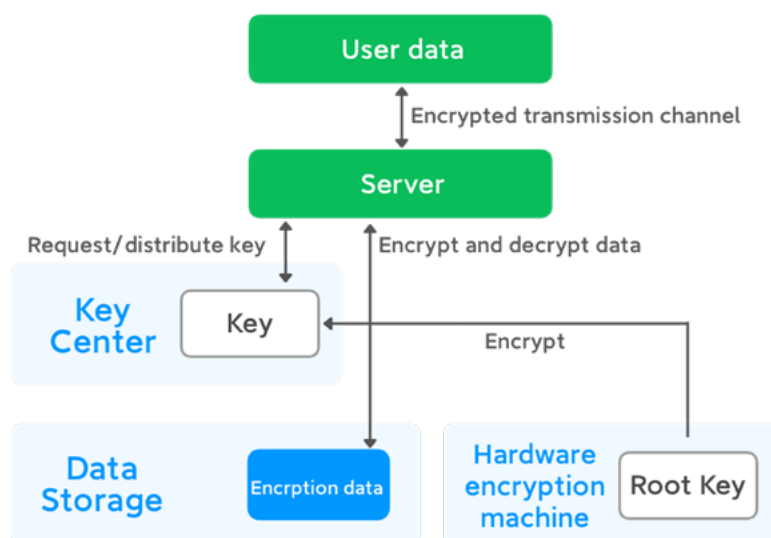


Figure 5-2 Key Management Logical Architecture of Key Center

In order to ensure the security of the key stored in the Key Center, keys are encrypted by a 4096-bit Root Key. The Root Key is generated by a hardware-based encryption device.

5.1.4 Other Account Login Methods

- QR code scanning login

Mi Account provides QR code scanning login functions. Users can scan the QR code on the web page to log in to their Mi account. The QR code will be automatically invalidated after a certain period of time, requiring the user to refresh the QR code web page.

- Third-party authorization login

Mi Account supports authorization for linking third-party accounts, which means users can log into their Mi account using a third-party account. Currently, users can log into their Facebook and Google accounts to connect to their Mi account. Mi Account uses OAuth2.0 (an open authorization protocol), which follows the standard OAuth2.0 protocol and process to authorize third-party account logins. The secure mechanism of OAuth2.0's ensures that Mi Account information will not be transmitted to such third parties.

5.2 Xiaomi Cloud

Xiaomi Cloud can store users' contacts, messages, photos, call history, notes and other information, and allow such information to be automatically synchronized between the user's devices. At the same time, users can recover data, to the extent possible, if the

device becomes damaged or lost. Users can browse and manage their own data anytime, anywhere on other devices or through the web (<https://i.mi.com>).



5.2.1 User data synchronization

After the user enables Xiami Cloud services, they can choose to synchronize the following data or set it to “Off” at any time.

Cloud service synchronization module	Synchronized data contents	Encrypted in transit	Encrypted on server	Notes
Messages	User's current phone number	yes	yes	A minimum of 128-bit AES encryption
	User's local text message data	yes	yes	
	The list of text message conversations and the list of private numbers the user pins to the top of screen.	yes	yes	

Cloud service synchronization module	Synchronized data contents	Encrypted in transit	Encrypted on server	Notes
Call history	User's current phone number	yes	yes	A minimum of 128-bit AES encryption
	User's local call records	yes	yes	
Contacts	User's contact and profile pictures	yes	yes	
Notes	User's local notes	yes	yes	
Mi Browser	The user's local browser bookmarks, history, labels, etc.	yes	yes	
Wi-Fi Settings	Settings and data for Wi-Fi networks to which the user is connected	yes	yes	
Recorder	User's local audio recordings and audio file information	yes	yes	
Home screen cloud backup	User's home screen layout, wallpapers	yes	yes	
	User's alarm, clock and time settings	yes	yes	
	User's notification settings	yes	yes	
	User's MIUI and system settings	yes	yes	
Calendar	User's Mi calendar data	yes	yes	
Gallery	The data in the local album and the data in the folders specified by the user to be synchronized	yes	yes	

5.2.2 Data security

In order to prevent user data from being stolen or tampered with, HTTPS encrypted channels are used for transmission among Web terminals, mobile phones and servers during the data synchronization process. In addition, the Cloud service website has a 15-minute session time-out and auto logoff mechanism.

During the data storage process, Xiaomi Cloud services divide each file into multiple blocks, with each block encrypted separately using AES algorithms with key lengths of at least 128 bits, i.e., in absence of the key, the data cannot be decrypted even when physical access to the disk is obtained.

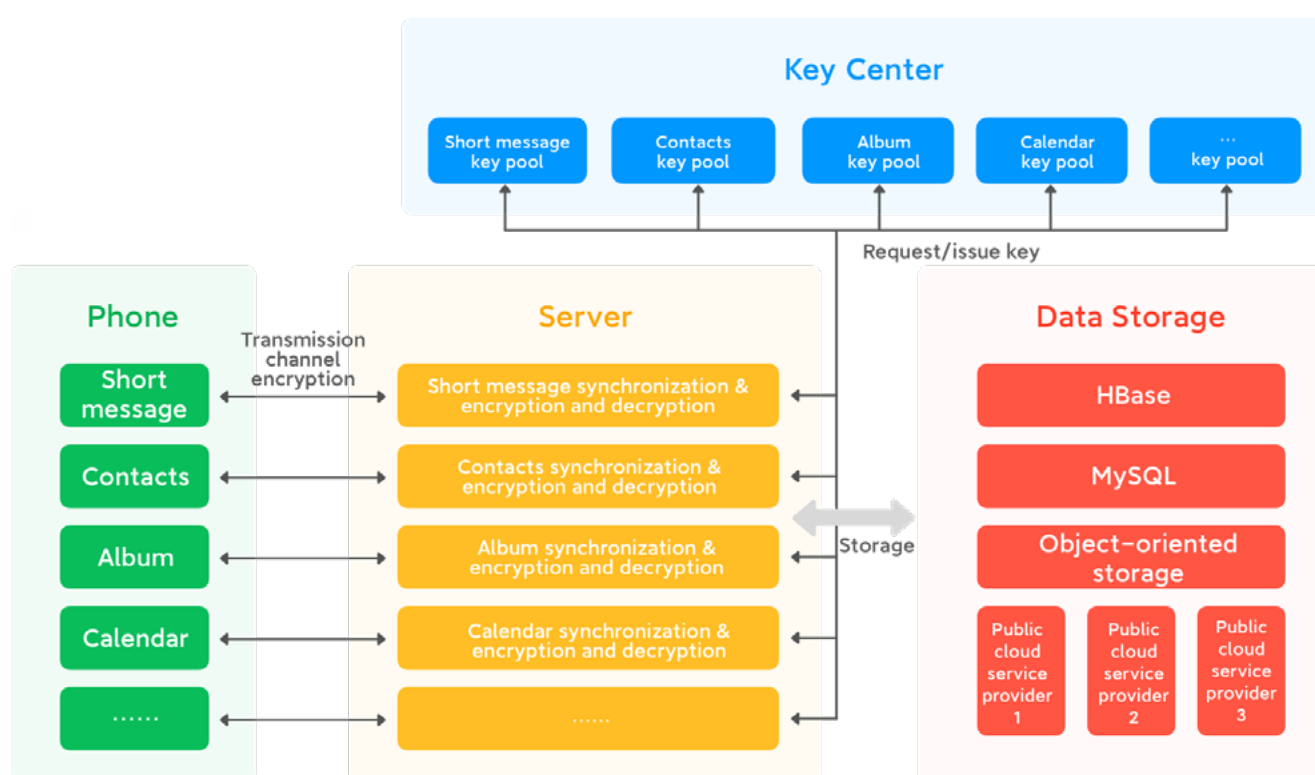


Figure 5-3 Cloud Service Data Security Architecture

In order to prevent the loss of users' cloud storage data due to force majeure factors, Xiaomi has chosen several public cloud service providers to provide data storage and backup services. For public cloud service providers that store user data, Xiaomi has formulated strict security requirements and evaluation standards, and has rigorously selected service providers that meet the relevant requirements. Xiaomi only stores encrypted data blocks on public third-party clouds and does not share encryption keys.

5.2.3 User Data Deletion



Users have the right to change or delete the data uploaded to cloud space. When the user deletes the data proactively, the corresponding data in the cloud space will be marked as deleted and temporarily stored in the recycle bin. The user can still recover the data sent to the recycle bin for a period to reduce any loss caused by accidental deletions. The data retention period in the recycle bin is subject to the user's membership plan and validity period, with a minimum retention of 30 days and a maximum retention of 180 days.

Data emptied manually or automatically from the recycle bin after the retention period will be permanently deleted from the server and cannot be recovered. If a user closes his/her Mi account, the user data in the cloud space will also be permanently deleted.

5.3 Image AI

The AI camera image optimisation AI algorithm makes the photo-taking process easier for MIUI users. It is mainly used for the following functions in camera: Supermoon, AI Camera, Document Mode, Front Portrait Mode With Background Blurring and Beautify Algorithm.

5.3.1 The training and using of AI algorithms

Training data sources for the AI algorithms are obtained through official channels (open source datasets, compliant procurement and so forth), Xiaomi will not use user's image data for the algorithm model training purposes. The AI camera image optimisation algorithm is integrated into the device's client and only runs locally on the device.

5.3.2 Data Security

The AI camera image optimisation algorithm is the underlying service being invoked. By using the deep integration mode of the independent and sealed SDK, it interacts with apps by invoking the interface, so as to prevent external attacks from directly accessing algorithm code or interfering with the algorithm's process. This feature effectively defends against external attacks while ensuring the security of the algorithms and user data.

In addition, the MIUI system cannot directly store images that were not captured by the camera. User data processed through the AI camera image optimisation algorithm is only stored locally on the device when authorised by the user and will not be backed up or uploaded to Xiaomi server.

5.4 MiPush

MiPush provides developers with message pushing services to client applications in real time by establishing a long, stable and reliable connection between the cloud server and the client.

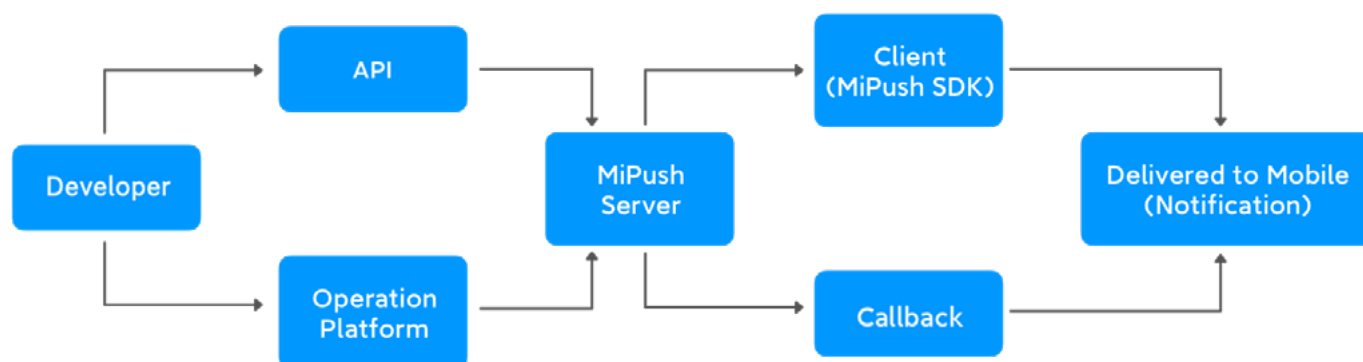


Figure 5-4 MiPush Service Architecture

MiPush supports notification bar messages and pass-through messages, and also provides two message delivery channels: API and the Push Operation Platform. MiPush SDK supports Android, iOS client and server mainstream languages, which can help the developers to better meet the complex business needs based on their own business logic.

5.4.1 Developer Privacy Compliance Requirements

Mi protects the personal information of end users by regulating developers through the developer agreement:

- Developers must agree to MiPush collecting, storing, using, disclosing and protecting personal information in accordance with Xiaomi Privacy Policy when using MiPush services.
- Developers must develop and publish their privacy policies and obtain the consent of end users. Moreover, the standards under such policies must be no lower than the privacy protection standards of MiPush.
- Xiaomi strongly recommends that developers include the key provisions from Xiaomi Privacy Policy in their product privacy policies for end users to ensure that end users agree to MiPush services collecting and using their data. Developers must not use MiPush services without end user consent.



- Xiaomi requires developers to comply with all laws, regulations, policies and industry standards applicable to MiPush services and which concern end user personal information.

5.4.2 Device Identification Method

MiPush does not use the device identifier (e.g., IMEI) directly to identify the device, but processes the user's personal information through technical methods such as de-identification. MiPush hashes the three device identification parameters (device identifier, serial number and Android ID) on the device and uploads the generated string to the server. The server maps the to a randomly generated ID which is returned to the client. MiPush uses this random ID as the unique identifier of the device.

MiPush also collects country codes in order to detect whether a device is located in a different area. The combination of the field and the device identifier is only used to determine the database cluster to which the device should be connected.

5.4.3 Data Minimization

MiPush is only used as a message channel and does not extract or use the contents of the message, user behavior or preferences. MiPush's original data, intermediate data and statistical results is not be provided to Xiaomi's partners, nor will such partners be allowed to access the data in any form. MiPush only provides developers with background statistics including time and message dimensions, excluding any personal user information.

5.4.4 Data Transmission Security

When the mobile APP initiates a registration request to the MiPush server for the first time, the device's information (the device identification field is irreversibly hashed) will be sent to the server, and the server will then return the random ID and message content key. HTTPS is used to encrypt the data in transit during this process.

MiPush services require developers to use the encrypted HTTPS channel to send the message content to the server. Communication between various server modules is encrypted using the AES-128 algorithm. After the message is encrypted by a symmetric encryption algorithm, the ciphertext is pushed to the device through AES-128 encrypted channel established between the server and the device, in order to achieve double encryption.



5.4.5 Data Deletion

Once the message is successfully delivered, the message content will be deleted from the server. If the message is not delivered due to abnormal circumstances, the server will keep the message content for seven days. MiPush services provide developers with a user data deletion interface that can be invoked to delete the MiPush registration information of the APP. If the device is not connected to the network within 90 days, the message content related to the device will also be deleted from the server. If the developer stops accessing MiPush services or requests to stop the push services, Xiaomi will delete all relevant APP information according to developer's instructions.



06

Compliance and Privacy Practice

6. Compliance and Privacy Practice

As the Xiaomi mission is to respect and protect user privacy and security, Xiaomi is committed to creating products that users can trust while enjoying the benefits of technology.

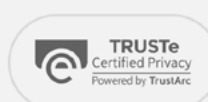
To ensure the implementation of the information security and privacy protection policies, Xiaomi formally established the Information Security and Privacy Committee in 2014, and set up a comprehensive security management system through technical protection measures, policies and processes, assessment and audit mechanisms and so forth. Furthermore, in order to comply with the legal requirements of the various countries we serve, Xiaomi has engaged experienced local lawyers to serve as the data protection officers for our activities in the European Union.

6.1 MIUI Certifications

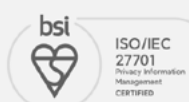
To provide the users with operating environments and services that comply with the requirements of laws, regulations and industry standards, Xiaomi has launched global compliance management projects and is audited by external regulatory authorities on a regular basis. Xiaomi's internet services comply with cybersecurity classified protection requirements and have passed level 3 under such requirements. The infrastructure, developments, operations, maintenance and internet services supporting MIUI products and services comply with the international authoritative certification system, and have passed the ISO27001, ISO27018 and ISO27701 certifications of the British Standards Institute (BSI). MIUI12 has passed the TÜV Rheinland Android system's test for enhanced privacy protection. The MIUI operating system, its built-in applications and cloud services have been evaluated and certified by TrustArc, the world's leading data privacy management company. Xiaomi's privacy policies and privacy practices conform to TrustArc's corporate privacy and data governance practices and evaluation standards, and have been awarded the TrustArc Privacy Certification Seal.



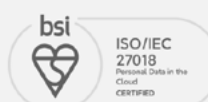
ISO 27001 is a widely accepted and applied international certification standard for information security management system. The standard takes risk management as the core, which effectively ensures the continuous operation of the organization's information security management system through regular risk regulation and corresponding control measures.



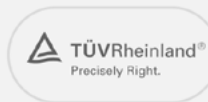
TrustArc is an international authoritative privacy compliance organization. Its TrustTe enterprise privacy certification standards have combined the privacy compliance requirements of countries. This certification shows that Xiaomi has established a complete privacy compliance system and obtained internationally recognized privacy data protection capabilities.



ISO 27701 is an authoritative guideline for the construction of a privacy management system. This certification indicates that Xiaomi has capabilities of information security guarantee and privacy data protection, and implements privacy by design in practice.



ISO 27018 is an international code of conduct that focus on personal data protection on cloud. This certification indicates that Xiaomi Cloud has a complete system for the protection of personal data.



TÜV Rheinland is a globally renowned product safety and quality certification agency. MIUI12, as the world's first mobile phone system that has passed the TÜV Rheinland Android system's test for enhanced privacy protection, has fully proved that it has in-depth and complete privacy data protection capabilities in the fields of application permission management, privacy information sharing, and malicious behavior detection and interception.

6.2 Privacy Practice

Xiaomi respects and protects the personal privacy right of all users. The five privacy principles are the key concepts in our product design.

Transparency	We strive to be transparent about our data processing practices so you can make informed choices.
Accountability	We hold ourselves accountable by reviewing our products according to privacy and data security concepts, and carefully considering feedback we receive from Xiaomi users and privacy experts.
Control	We seek to provide you with simple and easy-to-use methods to help you control your own information.
Security	We are dedicated to building systems and processes designed to secure and protect your personal information.
Compliance	We are committed to designing and developing our products to reflect data protection principles embodied in current privacy and data security laws and standards.

Xiaomi processes and backs up personal information through a global operating and control infrastructure. Your data is transmitted by the encrypted communication channels and stored in global top-tier cloud service providers.

Countries	Cloud Service Providers	Cloud storage locations for storing user data
European Union	Amazon Web Services	Germany, Unites States
	Alibaba Cloud	Singapore
India	Amazon Web Services	India
	Microsoft Azure	India
Russian Federation	Kingsoft Cloud	Russia
United Kingdom	Amazon Web Services	Germany, Unites States
	Alibaba Cloud	Singapore
United States	Amazon Web Services	Unites States
Mainland China	Alibaba Cloud	Mainland China
	Kingsoft Cloud	Mainland China
	21ViaNet	Mainland China
Others	Alibaba Cloud	Singapore
	Amazon Web Services	Unites States

Our privacy policies provides a detailed introduction on how Xiaomi collects, uses, discloses, processes and protects the information you provide to us or that we collect while you use Xiaomi products or services. Links to privacy policies in different languages: <https://privacy.mi.com/all> .

*Note: Some products have separate privacy policy links, which can be viewed on the corresponding product page.



6.3 Bug Bounty Program

Xiaomi owns a professional security and privacy team, which is responsible for providing technical support for the security and privacy of Xiaomi products, as well as review and test of security and privacy for developing and released products. Meanwhile, Xiaomi put forward “Bug Bounty Program” and actively invites security researchers around the world to carry out security tests on Xiaomi consumer products with high bonuses through a range of channels such as the self-built Xiaomi Security Center (SRC), Hackerone and mailbox, and rewards them according to the priority of the issue. Xiaomi will give the confirmed security issues a high priority and solve them as soon as possible.

Contact Xiaomi Security Center: <https://sec.xiaomi.com/> , <https://hackerone.com/xiaomi> , security@xiaomi.com.

07

Conclusion

7. Conclusion

Xiaomi is committed to providing fully functional, secure and easy to use digital software and hardware products to individuals, families and industry users around the world. MIUI, as the core component of MI phones, shoulders the responsibility of building a foundation of trust as well as providing security assurances. MIUI will give priority to enhancing security. This paper is a comprehensive presentation of MIUI's security design and implementation.

Xiaomi strives to ingrain awareness of security and privacy protection into the hearts of every business department, employee and partner. As mentioned earlier, Xiaomi has established a complete security and privacy management system that integrates security and privacy requirements into product design, development, testing, operation and other processes, and which subjects its partners to strict security and privacy audits while actively monitoring and resolving new security issues and threats, so as to ensure that user data are protected throughout the entire life cycle. In response to the evolving security situation, Xiaomi will continuously improve security technology capabilities, refine the security and privacy protection features of products and services, and optimize its security and privacy management system. This will be continually demonstrated through authoritative certificates, white papers, privacy policies and other means so that Xiaomi can build user confidence in Xiaomi's products and services, allowing users to choose and use Xiaomi products and services with an even greater peace of mind.

In an era driven by big data and artificial intelligence, there will always be certain contradictions between corporate development and user privacy. However, Xiaomi firmly believes that by respecting and protecting user information security and privacy, it can build users' long-term trust in Xiaomi's products. Therefore, Xiaomi insists on putting information security and privacy protection above all, and continually increasing its investment in security and privacy. Xiaomi is committed to sharing its standardized methods, best practices and technical capabilities relating to information security and privacy protection with its partners, in order to grow and protect user privacy together.

08

Glossary

8. Glossary

Abbreviations	Full name	Definition
3DES	Triple Data Encryption Algorithm	A symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block.
AES	Advanced Encryption Standard	A commonly used symmetric encryption algorithm. A variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.
AI	Artificial Intelligence	A wide-ranging branch of computer science concerned with building smart machines capable of performing tasks the typically require human intelligence.
API	Application Programming Interface	A set of functions and procedures that allow for the creation of applications that access data and features of other applications, services or operating system without accessing source code.
AVB	Android Verified Boot	A process of assuring the end user of the integrity of the software running on a device, which typically starts with a read-only portion of the device firmware which loads code and executes it only after cryptographically verifying that the code is authentic and doesn't have any known security flaws.
BL	Boot Loader	A vendor-proprietary image responsible for bringing up the kernel on a device.

Abbreviations	Full name	Definition
ECC	Elliptic Curve Cryptography	An approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.
ECDSA	Elliptic Curve Digital Signature Algorithm	A Digital Signature Algorithm (DSA) which uses keys derived from elliptic curve cryptography (ECC).
FBE	File-based Encryption	A form of disk encryption where individual files or directories are encrypted by the file system itself.
Flash	Flash Memory	An electronically non-volatile memory storage medium that can be electrically erased and reprogrammed.
Fuse	File System in User's space	A software interface for Unix and Unix-like operating systems that lets non-privileged users create their own file systems without editing kernel code.
HTTPS	Hypertext Transfer Protocol Secure	It is a secure communication channel for exchanging information between client and server through secure sockets layer.
HUK	Hardware Unique Key	A key solidified on the mainboard of the device when leaving the factory to identify and verify the uniqueness of the device.
KASLR	Kernel Address Space Layout Randomization	A technology that ensures the unpredictability of memory addresses and offsets of kernel image, which can greatly reduce the success rate of malicious software attacks and improve system security.

Abbreviations	Full name	Definition
MDM	Mobile Device Management	A product life-cycle management including all links of mobile device registration, activation, use and elimination.
OAuth	Open Authorization Standards	An open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords.
OEM	Original Equipment Manufacturer	A company that purchases parts and equipment that may be manufactured by another company.
OS	Operating System	System software that manages computer hardware, software resources, and provides common services for computer programs.
OTA	Over the Air	The technology of remote management of mobile terminal device and SIM card data through the air interface of mobile communication.
Pre-shared Key(PSK)	Pre-shared Key	A shared secret which was previously shared between the two parties using some secure channel before it needs to be used.
ROM	Read-only memory	A solid-state semiconductor memory that can only read data stored in advance.
Rootkit	/	A collection of computer software, typically malicious, designed to enable access to a computer or an area of its software that is not otherwise allowed and often masks its existence or the existence of other software.
RPMB	Replay protected Memory block	A partition with security characteristics in flash memory chips.

Abbreviations	Full name	Definition
RSA	Public-key Cryptosystems	A cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner.
SE	Secure Element	A microprocessor chip which can store sensitive data and run secure apps such as payment. Its internal components include: CPU, RAM, ROM, encryption engine, sensor, etc.
SELinux	Security-Enhanced Linux	A Linux kernel security module that provides a mechanism for supporting access control security policies.
SHA	Secure Hash Algorithms	A family of cryptographic hashing functions designed to keep data secured. The five algorithms of the SHA family are SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512.
SoC	System on Chip	An integrated circuit that integrates all components of a computer or other electronic system.
TA	Trusted Application	A highly secure application program that runs in a TEE environment.
TEE	Trusted Execution Environment (TEE)	A secure area on the main processor of a mobile device exists in parallel with the mobile OS, providing an isolated execution environment to ensure isolated execution, integrity of trusted applications, confidentiality of trusted data, secure storage, etc.
UI	User Interface	In the industrial design field of human - computer interaction, it is the space where interactions between humans and machines occur.



09

Document Revision History

9. Document Revision History

Version	MIUI Version	Date	Revisions
2.1	MIUI 12	May 2021	Features are not enabled for MIUI international version have been removed. Topics updated: - Fingerprint Unlock - Image AI - Compliance and Privacy Practice
2.0	MIUI 12	May 2020	Updated for MIUI 12 - Privacy Protection - Mi Account - Xiaomi Cloud - MiPush
1.0	MIUI 11	November 2019	First release

