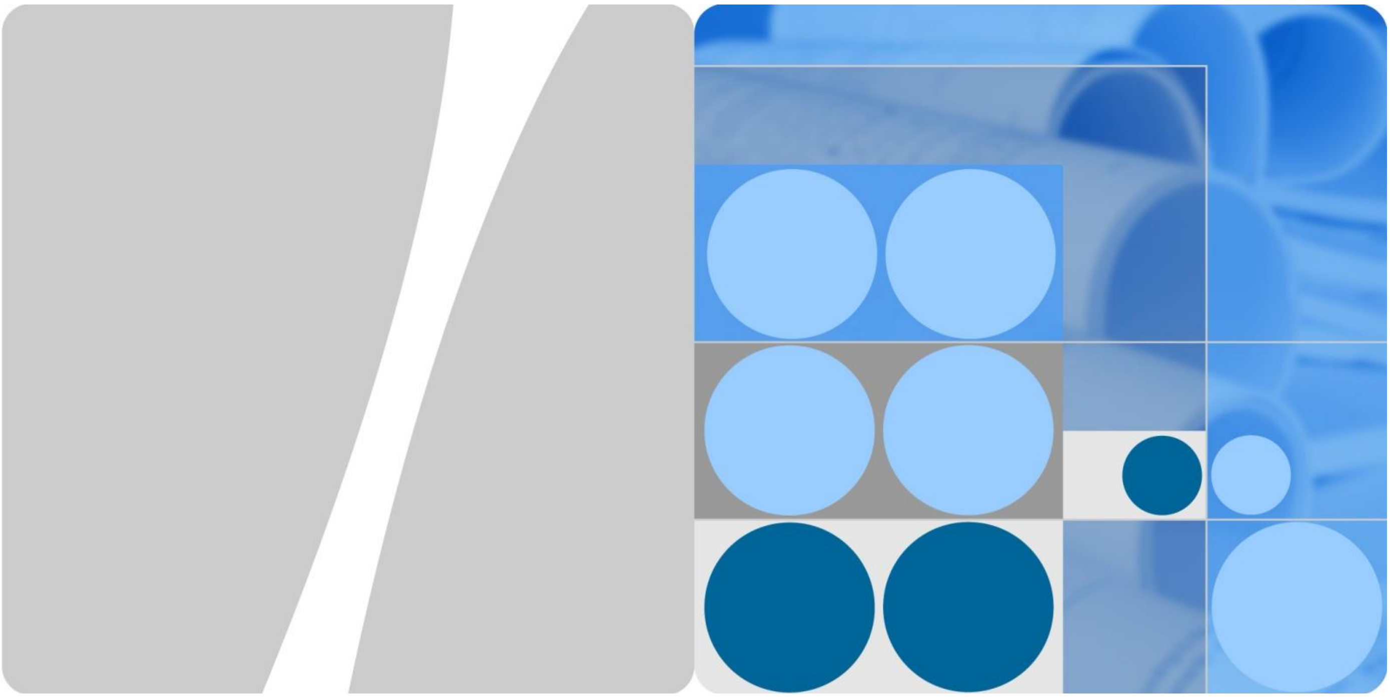


HUAWEI Mobile Services (HMS)

Security Technical White Paper

Issue	**V1.0**
Date	**2020-05-19**

Huawei Device Co., Ltd.

Secure and Trustworthy HUAWEI Mobile Services (HMS)

Huawei Device Co., Ltd.

Address:	No.2 of Xincheng Road, Songshan Lake Zone, Dongguan, Guangdong, P.R. China
Website:	https://consumer.huawei.com/en/
PSIRT Email:	PSIRT@huawei.com
Fax:	+86-0769-23839866

Contents

Note: Supported capabilities vary depending on device models or market characteristics in different countries. For more information, refer to specific product descriptions.

1 Introduction

HUAWEI Mobile Services (HMS) incorporates Huawei's chip, device, and cloud capabilities. It includes easy to use, smart, and secure HMS apps, a full portfolio of HMS Core, HMS Capability, and HMS Connect that are exposed to developers, and corresponding IDE tools for development and testing. The focus of this document is the security of HMS. (For more information about chip and OS security, see the EMUI Security Technical White Paper at https://consumer.huawei.com/en/privacy/whitepaper/.)

HMS has been developed to build industry-leading privacy and security experiences, positioning security as a key capability in product build. It not only ensures the security experience of HMS apps, but also exposes HMS Core to give developers access to innovative security technologies and security experiences.

HMS builds industry-leading security capabilities through chip-device-cloud synergy. It stores key data in protected security chips to prevent malicious use and theft, protects system integrity based on enhanced OS security capabilities, prevents unauthorized access through address space layout randomization (ASLR) and other means, and prevents information leak through data protection techniques, such as end-to-end (E2E) encryption.

This white paper describes how HMS, throughout its lifecycle, protects users' privacy and data, as well as how developers build secure and trustworthy apps by integrating HMS Core. For more information on HMS Core development, visit https://developer.huawei.com/consumer/en/.

This document consists of the following:

- Chip-based Hardware and OS Security: security protection by integrating security chips into the Kirin processor, processing sensitive personal data in secure encrypted zones, and other means
- Secure Service Access: techniques for secure access to services, including HUAWEI ID, multi-factor authentication, heuristic security authentication, and risky operation notification
- Encryption and Data Protection: file partition, encryption key management and distribution, certification and digital signature, trusted identity authentication and integrity protection, and TCIS
- Network Security: methods used to protect network security, including secure transmission channel, network border protection, network partition, host protection, in-depth defense, and vulnerability management

- Service Security: security of services including HUAWEI Mobile Cloud, HUAWEI SkyTone, Find My Phone, HUAWEI Browser, HUAWEI Wallet/Huawei Pay, and Service Anti-Fraud
- AppGallery and App Security: methods used to protect HUAWEI AppGallery and its apps, including malicious behavior detection, security vulnerability scanning, privacy breach detection, download and installation assurance, runtime security detection, and isolation of quick apps
- HMS Core (Developer Kits): security of developer kits; integrated security technologies and capabilities; security capability exposure: Safety Detect and FIDO
- Privacy Control: privacy control principles and technologies, including local deployment, transparency, data minimization, data subjects' rights, obligations of a data processor, data isolation, differential privacy, federated learning, and protection of minors' personal information
- Security and Privacy Certification and Conformance: international security and privacy certifications
- Oriented Future: a vision into the future

Security & Privacy Protection Are Huawei's Top Priorities

Huawei is committed to delivering innovative, high-quality, and secure telecommunications equipment and services to customers throughout the world. Cyber security, in particular, is of paramount importance to Huawei, and this can be seen in Huawei's engagement with security researchers and the hardware researcher community. In particular, Huawei has rolled out a bug bounty program covering all Huawei and Honor mobile phones, as well as HMS. The program rewards security researchers up to €200,000 for finding a single vulnerability, depending on severity. You can send identified security issues to PSIRT@huawei.com for participating in the Huawei Bug Bounty Program.

We are committed to building a trusted privacy protection brand. We believe that privacy is a basic right of yours, you should have complete control over your privacy, and that privacy protection is a cornerstone of product design which is just as important as the actual service that the product provides.

Transparency: The way we process personal data is transparent to you. You can make decisions according to your wishes, and have full control over your privacy.

Benefits to users: The collection of personal data should benefit you and provide you with a better user experience.

Security: We use enhanced security technology to protect your personal data. For example, we use techniques such as differential privacy and federated learning to improve user experiences while protecting your privacy.

Legal compliance: We strictly abide by the laws and regulations of each region and country that we operate in, and incorporate legitimate compliance into product design and business processes.

These four principles are integrated into Huawei's products from product design, and continue being integrated throughout the whole product development process.

We have established independent privacy and security teams worldwide to continuously research innovative privacy and security technologies, integrate the latest achievements with HMS, and supervise and ensure strict compliance of products. We start to build privacy and security capabilities from product design, and continue to apply them throughout the product development and go-to-market processes. We also maintain effective interaction with customers, actively listening to their suggestions on privacy and security improvement during the use of products.

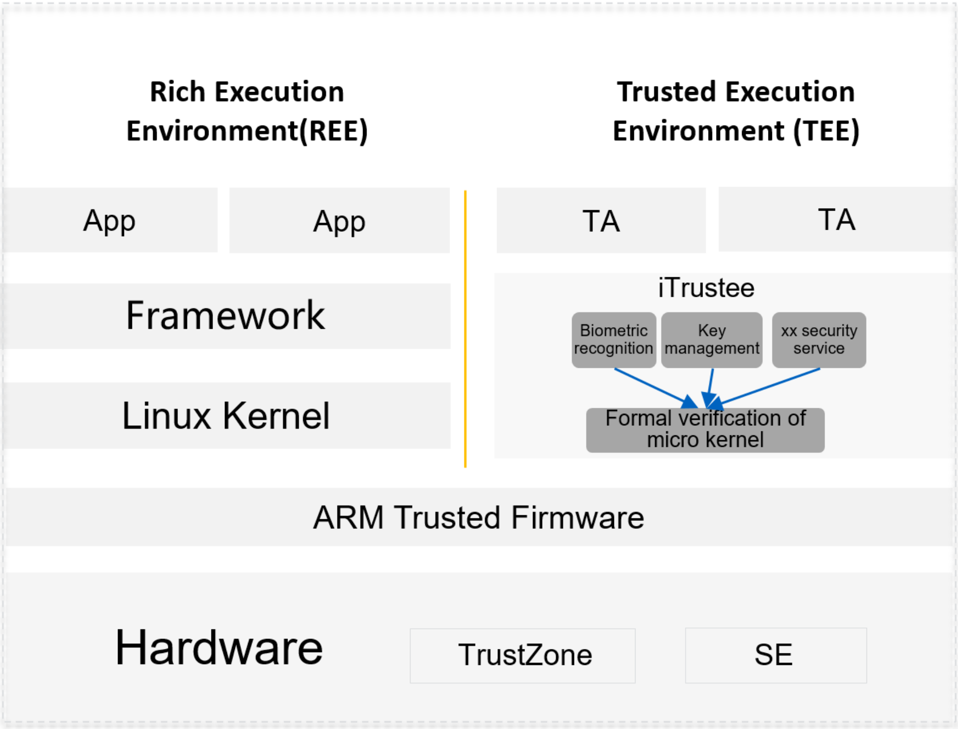
For more information on privacy and security, visit https://consumer.huawei.com/en/privacy/whitepaper/.

2 Chip-based Hardware and OS Security

Chip-based hardware and operating system (OS) security can effectively defend against software attacks initiated by attackers, preventing attackers from accessing the system and obtaining user data without authorization. HMS uses enhanced chip security as the foundation of its security capabilities. In this way, it protects users' sensitive personal information while providing services.

For more information about chip-based hardware and OS security, see the EMUI Security Technical White Paper at https://consumer.huawei.com/en/privacy/whitepaper/.

Security Chip Integrated into the Kirin Processor



- Secure element

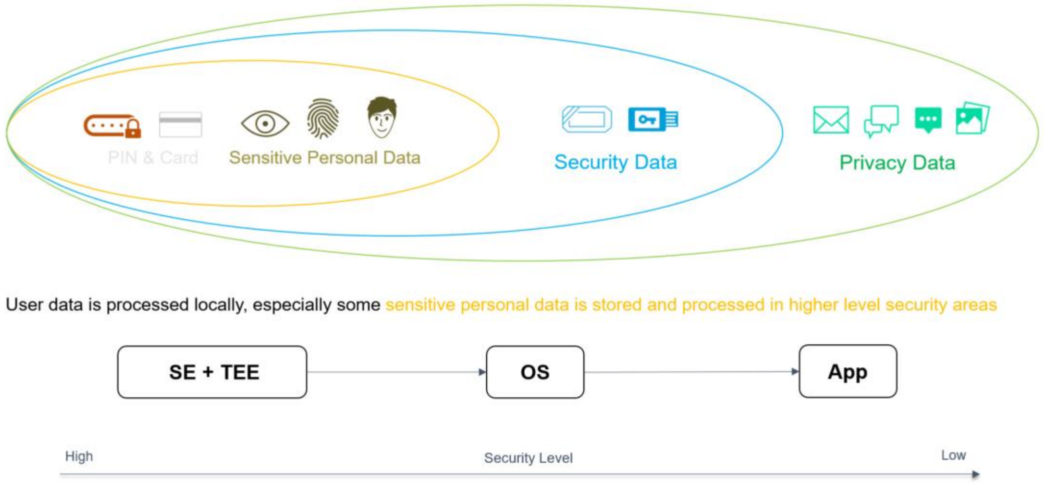
  A secure element (SE) is a subsystem that provides a secure execution and storage environment. Since Emotion UI (EMUI) 5.0, SEs have been used to enhance mobile payment security in order to meet industry certification requirements.

  The SE security solution provides protection at both the software and hardware levels through System-on-a-Chip (SoC) level security isolation and encryption. This solution not only provides software security protection capabilities, but also defends against physical attacks. It provides higher security, fundamentally ensuring the security of Huawei devices. In addition, the solution conforms to the Payment Card Industry Data Security Standards (PCI DSS), making it applicable to international mobile payment and mobile financial services.

- TEE OS

  EMUI supports the TEE OSs of various chip platforms. The iTrustee is a TEE OS developed by Huawei based on ARM® TrustZone®. It is a customized real-time OS that creates a TEE to provide a protected, isolated environment for users' confidential data and apps. The iTrustee is independently developed by Huawei in compliance with GlobalPlatform TEE specifications based on the Huawei-developed microkernel, and its independent intellectual property rights belong to Huawei. It features high security, performance, scalability, and stability, and provides software development kit (SDK) and device development kit (DDK) frameworks for security service development.

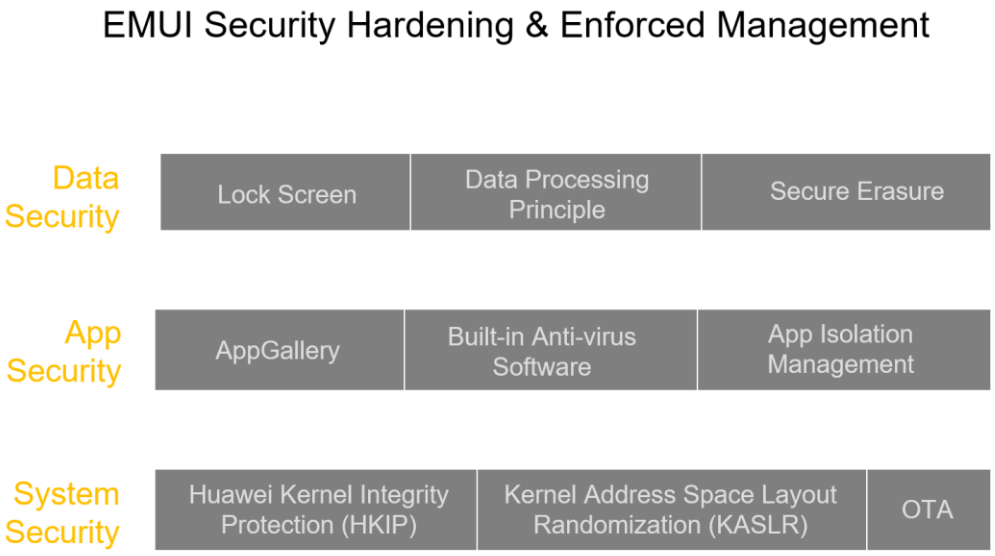
Sensitive Personal Data Processed in Secure Encrypted Zones


PIN & Card
Sensitive Personal Data
Security Data
Privacy Data
User data is processed locally, especially some sensitive personal data is stored and processed in higher level security areas
SE + TEE
OS
App
High
Security Level
Low

EMUI provides a hierarchical protection mechanism for data of different security levels and in different application scenarios. For example, data that is highly sensitive and has low requirements on system resources (such as lock screen passwords and core keys) is stored in SEs and can defend against physical attacks, whereas large-volume sensitive data that requires a low processing latency (such as biometric features) is encrypted and stored in a TEE. In addition, common sensitive data (such as user data) is encrypted using AES256 and stored in common storage areas; the encryption key is also protected by the TEE.

For example, in the Huawei Pay service, the bank card information of a user is converted into a specific device code by the card issuer, and is encrypted and separately stored in a security chip. During login and payment, the security chip provides a fully isolated space for storing and using users' biometric information (such as fingerprints and faces), avoiding malicious behavior that may occur in a non-isolated space.

EMUI Security Hardening & Enforced Management



EMUI Security Hardening & Enforced Management

Data Security: Lock Screen | Data Processing Principle | Secure Erasure

App Security: AppGallery | Built-in Anti-virus Software | App Isolation Management

System Security: Huawei Kernel Integrity Protection (HKIP) | Kernel Address Space Layout Randomization (KASLR) | OTA

To safeguard users, EMUI provides enhanced security capabilities through system security, app security, and data security:

- System security: EMUI provides Huawei Kernel Integrity Protection (HKIP) to prevent the tampering of kernel code snippets, key kernel data, and important system registers, in addition to protecting key locations against malicious code injection in privileged mode. Kernel address space layout randomization (KASLR) is also implemented, making it difficult for attackers to launch attacks by exploiting the vulnerability of out-of-bound memory access. In addition, the over-the-air upgrade based on security encryption and verification prevents malicious tampering or exploitation of upgrade packages.
- App security: EMUI verifies the installation of apps, embeds virus detection software, and implements sandbox-based strong isolation of apps.
- Data security: Lock screen passwords can be securely stored or erased.

3 Secure Service Access

HUAWEI ID enables users to securely log in to HUAWEI Mobile Services, such as HUAWEI Mobile Cloud, HUAWEI Wallet, HUAWEI Video, HUAWEI Music, and HUAWEI Reader. HUAWEI ID provides security detection that covers devices, login and runtime environments, and user login credentials. Such security detection also prevents unauthorized users from stealing account information for login based on multi-factor verification of user login environments and devices, thereby preventing users' personal information from being obtained or illegal payments being made using their account.

HUAWEI ID ensures account security by providing identity authentication measures and technical measures based on Huawei devices' software and hardware advantages. Identity authentication measures include complex login password, fingerprint login, trusted device verification, verification code for new device login, and security phone number/security email address; technical measures include prevention of screen capture/recording. In addition, real-time fraud detection is used to prevent attacks on HUAWEI IDs. That is, the security operation team periodically analyzes new cyber attacks in the industry and reviews existing security policies to quickly respond to security threats that may affect HUAWEI IDs.

Password Complexity

HUAWEI ID requires a password of at least eight characters including uppercase letters, lowercase letters, and digits. This is the minimum complexity, but users are encouraged to use more complex passwords to further improve security. Brute force cracking is also prevented by limiting the number of password attempts.

Image Verification Code

When a HUAWEI ID detects a potential automated attack, it will display an image verification code to block brute force cracking. The system provides complex images to ensure that image verification codes cannot be automatically bypassed by a machine. Brute force cracking is further prevented by limiting the number of verification code attempts.

Account Protection and Multi-factor Authentication

With account protection, a user can only log in to a HUAWEI ID from its trusted devices. When you log in to your HUAWEI ID on a device for the first time, you must log in through two-factor authentication. The second authentication factor can be a verification code sent via SMS, a trusted device, or something similar. Account protection significantly enhances the security of HUAWEI IDs and HUAWEI Mobile Services.

If a verification code is used as the second authentication factor, it will be automatically displayed on your trusted device. You can enter the password and verification code on your new device, which will then become your trusted device. For example, if you are currently using a HUAWEI Mate 20 and want to log in to your HUAWEI ID on a newly-purchased HUAWEI Mate 30, the HUAWEI Mate 30 will prompt you to enter your password and the verification code displayed on your HUAWEI Mate 20.

Risky Operation Notification

When a user attempts to log in to a HUAWEI ID in an unknown environment, reset the password, modify account information, or perform any other risky operations, the user will be notified through an SMS message, system message, IM message, or email. The user can then confirm the operation as prompted to prevent unauthorized users from accessing the account.

Heuristic Security Authentication

HUAWEI ID provides security question authentication in password retrieval or changing of personal details (for example, the user has stopped using a phone number or email address bound to the account).

Accounts for Children

HUAWEI ID allows users to create an account for their child to provide a more secure and reliable service environment. Such accounts shall be created and managed under the authorization of parent accounts. Parents can use accounts for children to provide a safe online environment for their child. HMS provides additional protection for children in products and services, including filtering out apps that are not suitable for children in HUAWEI AppGallery, restricting the payment capacity of accounts for children, and filtering out content that is not suitable for children in Video and Reader services.

Account Anti-Fraud

Huawei devices provide a proactive risk monitoring mechanism for account login, password reset, account change, and appeal to proactively identify risks and prevent unauthorized users from logging to accounts.

Login: To prevent account theft caused by phishing, Trojan horses, and credential stuffing, Huawei Device has established a multi-dimensional identification policy and model based on risky networks, device environments, and operation exceptions. This ensures quick and accurate identification of risks and prevention of unauthorized account access, thereby preventing user information leakage or financial loss and ensuring account security.

Password reset: Attackers may maliciously reset the passwords of users' HUAWEI IDs through fake mobile towers or SMS Trojan horses, and exploit HUAWEI IDs for personal gain. Also, when users forget their password, it is important that they can conveniently reset the password. In these two scenarios, the risk control platform distinguishes normal user operations from attack behavior based on multiple factors such as operation information, device environment, and network environment, thereby allowing users to quickly retrieve their passwords and preventing attackers from exploiting HUAWEI IDs.

Appeal: Similar to the password reset process, the appeal process can also determine the ownership of a HUAWEI ID. Attackers may exploit the appeal process to seize control over users' HUAWEI IDs for personal gain. Users may also need to restore access to their HUAWEI IDs through appeal. The risk control platform distinguishes normal user operations from attack behavior based on multiple factors such as operation information, device environment, and network environment, accelerates the appeal process of normal users, and blocks attack behavior to improve user experience while ensuring security.

In business scenarios such as flash sales, coupons, gift packages, and lottery drawing, attackers attempt to register a large number of fake user accounts in one go through various channels to participate in, and profit from, such campaigns. During HUAWEI ID registration, the system identifies fake accounts based on expert rules, machine learning, and various means such as operation exceptions, mobile phone number exceptions, email exceptions, and risky networks, to prevent fake registrations and protect users' legitimate rights and interests.

Account Privacy Protection

The passwords of HUAWEI IDs are not stored on devices; user names are anonymized for storage and display, and cannot be restored. When storing user accounts' personal information, the server isolates and encrypts the information by user ID and protects user passwords using the PBKDF2 algorithm. User passwords are not stored in plaintext. HUAWEI IDs use HTTPS to transmit data, safeguarding data transmission.

4 Encryption and Data Protection

HMS positions user data protection as a key security design objective. It provides secure login through HUAWEI IDs and takes advantage of the following capabilities and technologies: (a) data protection capabilities provided by EMUI; (b) security encryption capabilities provided by the SE and TEE; (c) industry-leading data protection technologies during service processing and data exchange; (d) other technologies used during transmission, service processing, and storage, such as E2E encryption, trust relationship authentication for the certificate chain, signature to prevent data tampering, and mutual trust between devices in a trust circle. HMS safeguards user data, regardless of whether it is stored on the cloud or transmitted over the network, preventing malicious or unauthorized access to and tampering with information and services.

Data Security Empowered by EMUI

To protect the file system, EMUI divides it into the system partition and user partition. The system partition can only be read and is isolated from the user partition. Common apps have no permission to access the system partition, ensuring that its data cannot be modified by malicious programs.

For data stored in the user partition, the system provides file-based data encryption and directory permission management mechanisms to restrict data access between apps. EMUI provides various mechanisms for critical data in the user partition to ensure the secure storage, use, and destruction of highly sensitive user data. Such mechanisms include lock screen password protection, secure storage of short data, password vault, and secure erasure.

For more information about these mechanisms, visit https://consumer.huawei.com/en/privacy/whitepaper/.

Encryption Key Management and Distribution

To fully protect service data, HMS uses E2E encryption during service data processing and exchange. HMS uses the Key Management Service (KMS) to manage the application, distribution, use, resetting, and recycling of keys in a unified manner for better protection.

KMS uses a hardware security module (HSM) with industry-leading security to serve the root key, which generates other keys. The HSM is a FIPS certified (Level 3) dedicated cryptographic device that is capable of physical anti-tampering and provides encryption, digital signature, and key security management services for apps. In addition, the root key of the HSM is safeguarded using physical access and multiple physical keys.

KMS uses multi-level key management and distributed deployment to ensure key security and high performance of services. It uses international standards or security algorithms (such as AES, RSA, and SHA256) common throughout the industry. Insecure algorithms (such as MD5, SHA1, and DES) are prohibited. In addition, the key of a security algorithm must meet a certain security strength (for example, the key must contain more than 128 bits for AES and at least 2048 bits for RSA). Such algorithms include symmetric encryption algorithms (AES128 and AES256), asymmetric encryption algorithms (RSA2048, RSA3072, RSA4096, ECC-p256, ECC-p384, and ECC-p521), and hash algorithms (SHA256, SHA384, and SHA512). KMS also provides a strict process for managing keys, certificates, authorization, and authentication.

- In HMS, each service applies for a key from KMS for user information (for example, user account registration information) to be encrypted for storage. After KMS distributes an encryption key to the HMS service, the service uses the key to encrypt the information to be stored in order to prevent unauthorized access.
- E2E encryption is used for processing and transferring hosted user data, such as files in HUAWEI Mobile Cloud (supported only in certain regions). Each user is provided with a unique encryption key based on that provided by KMS and the encryption factor of the user device, preventing information leakage caused by unauthorized access. When copyright-based services such as Music, Themes, and Reader are used, the key is used to protect content during transmission. When a service starts, a pair of device-related public and private keys is generated on the device. The specific key pairs vary depending on the device. When using the Music service, for example, the public key is transferred to and stored on the music server. When a user plays a song, the server uses the public key to deliver the symmetric key used for encrypting the song content and uses the symmetric key to encrypt the content to be transmitted to the device. After receiving data, the device uses its unique key to decrypt the song. Different devices use different keys to ensure that the copyrighted data is not accessed without authorization.
- Certain products without independent authentication UIs, such as kids watches, also use protected authentication keys for trusted communication with a server.
- Service configurations to be protected, such as authentication credentials between services, are also encrypted using the encryption key.

Certification and Digital Signature

To prevent data from being tampered with by malicious attackers and provide trusted interactive services, HMS uses trust relationship authentication for the certificate chain and digital signature verification. This prevents the data from being hijacked by malicious attackers or tampered with during transmission.

HMS uses the cloud certificate service (CCS) to issue certificates and verifies the identities of certificate holders on the service server. Using root certificate-dedicated HSMs with industry-leading security, the CCS can issue, update, and revoke digital certificates such as user-level certificates, microservice identity certificates, and app signature certificates. The private key of the root CA certificate is stored in an HSM, and the certificate is issued in the HSM to ensure that the signature information cannot be forged.

- To ensure app security, EMUI installer verifies apps during installation. EMUI can verify the signature of a "green app" that has been reviewed by HUAWEI AppGallery using a certificate, thereby preventing apps from being tampered with without authorization.
- After a developer uploads a quick app package to HUAWEI AppGallery, HUAWEI AppGallery signs the package. After a user downloads a quick app to his/her device, the quick app engine verifies the signature when loading the quick app package. If the signature does not meet specified requirements, the quick app is rejected, preventing it from being tampered with during installation and deployment.
- When a user subscribes to the payment service, the mobile phone submits the private key signature corresponding to the device certificate to the cloud for verification, and then obtains a payment certificate. The CCS issues a unique payment certificate for each device and stores it in the TEE of the mobile phone for confidentiality. To ensure the security and integrity of user payments, the hardware-protected private key of the digital payment certificate is used to sign key payment data (for example, payment amount), and the payment signature is computed in the TEE. After receiving the key exchanged information, the server verifies the signature of the key payment data to ensure that payment data sent from mobile phones is not tampered with throughout the service process, thereby safeguarding user data and payments.
- A third-party pass supplier applies for a pass certificate from Huawei Device and uses the pass certificate to sign pass data. When a user adds a pass (such as a supermarket membership card, airline membership card, or fitness card) to HUAWEI Wallet, the signed pass data is transmitted to the wallet server for verification to ensure that the pass is not tampered with during transmission and ensure the security and integrity of the pass. Verified pass information is written into HUAWEI Wallet and can be used by users.
- During the initialization of the digital rights management (DRM) client, the device certificate of the mobile phone is submitted to the cloud for verification to obtain the DRM client certificate. The CCS issues a unique DRM client certificate to each device. When DRM is used on mobile phones to safeguard digital content such as audio and video content, DRM uses certificates to encrypt content keys. This ensures that only authorized devices and apps can obtain the content keys, preventing digital content from being leaked.

Trusted Identity Authentication and Integrity Protection

When a user uses Huawei Pay for fingerprint payment, the user's enrolled fingerprint is first verified in the TEE of the mobile phone. After the fingerprint verification is successful, the digital certificate signature algorithm RSA2048 is used in the TEE to protect payment message signatures for payment integrity.

When a user deletes a transportation card and is returned the outstanding balance, the outstanding balance is signed using the RSA2048 algorithm in the TEE and then transmitted to the server. The server verifies the signature to confirm that the outstanding balance and status are not tampered with during transmission to the server, and then delivers a balance return instruction.

TCIS

When a user logs in to a HUAWEI ID on a Huawei device for the first time, a key pair (consisting of a public key and a private key) is automatically generated for establishing a trust circle. The public key is uploaded to the trust circle index service (TCIS) server. When a user logs in to multiple devices through the same HUAWEI ID, a list of public keys is generated for this HUAWEI ID on the TCIS server. This list is a trust circle, and the server protects its integrity. The trust circle is sent to each device for integrity check.

When users subscribe to the HUAWEI Mobile Cloud service, the server randomly generates a user-level key for each user. The keys are encrypted using public keys in the trust circle and then sent to the corresponding device. When files are uploaded to HUAWEI Mobile Cloud, the device generates a file encryption key for each file to encrypt the file content, preventing such content from being stolen during transmission and storage. A file encryption key is encrypted using the user-level key and then uploaded to and stored on the server.

When a user uses Huawei Share to transfer files, the key pair in the trust circle is used to authenticate the device identity and establish a secure transmission channel between devices. After a device passes identity authentication, a temporary key is generated through negotiation to implement encrypted data transmission and integrity protection.

5 Network Security

In addition to data protection on devices and in services, user data security protection on networks is also critical. Protection methods include the use of secure and reliable encrypted channels to transmit data, trusted security management and access protection on the cloud, isolation through network partitions, border attack defense, proactive detection of unauthorized access, encrypted data storage, and comprehensive access audits.

Secure Transmission Channel

All data transmitted on networks, including data between a mobile device and server, is transmitted through a secure transmission channel to ensure data security. In addition, integrity check is performed on app downloads to ensure that information on the network connection between a mobile device and server is not stolen or tampered with.

Mobile apps use international standards or industry-recognized security protocols, such as TLS v1.2 and TLS v1.3. In addition, commercial CA root certificates are preconfigured on clients, and commercial SSL certificates are deployed on cloud devices. To ensure the security of the network request channel, clients connect to a cloud server only after the cloud SSL certificates pass strong verification.

Cloud Network Border Protection

Multiple border protection measures work in cohesion to safeguard cloud data at the ingress. Specifically, all hosts with a port exposed to the Internet connect to a firewall between the hosts and Internet, ports that must be used for service exposure are configured to provide access for Internet users, and data packets that enter and exit the system are filtered to defend against network-layer attacks.

In addition to the security zones implemented by traditional network technologies and firewalls, the following enhanced border protection capabilities are provided on the service plane:

- Cleaning of abnormal and excess DDoS traffic: To detect and clean DDoS traffic, professional anti-DDoS devices are deployed at the border of each cloud data center.

- Intrusion detection system/Intrusion prevention system (IDS/IPS): To defend against attacks from the Internet and between security zones, IDSs/IPSs are deployed at network borders, including security zone borders. They provide real-time network traffic analysis and blocking capabilities to defend against various intrusions, such as abnormal protocol attacks, brute-force attacks, port/vulnerability scanning, viruses/Trojan horses, and attacks exploiting vulnerabilities.
- On the management plane, access control based on secure VPN and HTTPS channels is implemented throughout the process, including login authentication, permission management, and access control.
- Access management: Systems are centrally managed on the network using identity accounts and two-factor authentication, such as dynamic SMS verification codes and USB keys. To comprehensively audit user logins and operations, accounts are used to log in to the virtual private network (VPN), bastion host, and jump server.
- Permission management: Role-based access control (RBAC) is implemented based on various services, as well as different responsibilities of the same service. In accordance with the minimum authorization principle, only necessary permissions are assigned to users. The scope of the login permissions includes the core network, access network, security device, service system, database system, hardware maintenance, detection and maintenance, and more. Personnel can only access devices within their authority.

VPN-based Fine-grained Security Protection

To minimize the impact of attacks on the cloud, security zones and service isolation are implemented based on the security zone division principles and proven practices within the industry. Physical and logical isolation is achieved by dividing a data center into multiple security zones based on service functions and network security risks, improving the network's self-protection and fault tolerance capabilities against intrusions.

- External border protection zone: This zone is deployed with front-end components (including load balancers and web container servers) for external networks and tenants, as well as with services connected to the external public network.
- Service security zone: This zone is deployed with service servers that are not directly connected to the public network. An independent service host subnet is assigned for each service, and service hosts are isolated from database hosts.
- Database hosting security zone: This zone is deployed with the database system and object-based storage system to store both user and service data. The data is isolated through partitions, and each service is assigned an independent database cluster subnet. To implement point-to-point trusted access between service and database hosts, the database controls the trust relationship for application layer access.
- O&M network security zone: This zone is connected with O&M components, which access nodes by using a jump server, through a VPN.

In addition to horizontal network divisions based on attack surfaces, security groups are vertically divided based on apps. Each security group uses an independent VLAN for control.

Trust relationships are established between service planes for trusted planes and host group domains divided by service. Only authorized objects can access services, and untrusted connections are prohibited. For example, connections to service hosts can only originate from the O&M network security domain, and the connection to a database must originate from a trusted zone of the same service.

Host and Virtualization Container Protection

The host OS is minimized and services are security-hardened to safeguard the system. In addition, an IDS is deployed to detect possible intrusions.

Web applications and underlying systems utilize the distributed data sampling and centralized analysis & protection model to match intrusion rules for warning and protection. The provided functions include host protection, Trojan horse detection, account security detection, tracing & query, intrusion forensics tracing, software fingerprint collection, policy management, user-defined policy, whitelist, script delivery, upgrade service, and policy library.

Standard images, which are created by professional teams and released after strict tests, are deployed for services, including the OS and installed software. These images consist of the basic OS and hardened initialization components. In addition, the kernel can be upgraded to the latest stable version to ensure system integrity without tampering.

The host-based intrusion prevention system (HIPS) is deployed on hosts to detect attacks, including abnormal shell, rootkit, web shell, and account privilege escalation, in real time.

Multi-layer Intrusion Prevention

In addition to ingress defense, a data-centric and multi-layer in-depth security defense system is established based on the IDS.

- App protection: Web application firewalls (WAFs) are deployed to defend the web application services, which are deployed in the demilitarized zone (DMZ) towards the external network and background core logical systems and services, against attacks such as web application layer CC attacks, SQL injection, cross-site scripting (XSS) attacks, cross-site request forgery (CSRF), component vulnerability attacks, and identity forgery.
- Host protection: The HIPS is deployed on hosts to detect abnormal shell, rootkit, web shell, and account privilege escalation among other attacks.
- Runtime application self-protection (RASP): The web application layer intrusion detection system can detect mainstream high-risk web security threats and certain zero-day attacks.
- Vulnerability scanning: Regular vulnerability scans and risk mitigations are performed for hosts and apps.
- Database firewall (DBF): Abnormal database traffic can be detected and audited.

The risk-based big data security analysis system associates the alarm logs of security devices to support real-time and orderly analysis and quickly identify possible attack threats. To promptly detect and respond to intrusions, a dedicated security team analyzes alarm data generated by security devices.

Based on threat intelligence and security information, the big data security analysis system supports various threat analysis models and algorithms, as well as accurately identifies attacks, including common brute force cracking, port scanning, zombies, web attacks, unauthorized web access, and APT attacks. In addition, the system analyzes potential risks and provides warnings based on threat intelligence.

Zero Trust Architecture

In a zero trust network environment, apps can access the system only after being authenticated. The system continuously authenticates apps and performs dynamic access control. The zero trust architecture senses the runtime environment in real time and promptly makes decisions and handles issues when detecting any exception.

Vulnerability Management

With technical support from the Huawei Product Security Incident Response Team (PSIRT), HMS has built a comprehensive vulnerability management system that provides vulnerability collection, vulnerability handling, and vulnerability information collaboration. Comprehensive research on system vulnerabilities, virtualization-layer vulnerabilities, and application-layer vulnerabilities is conducted to generate rapid vulnerability handling capabilities, providing users with more secure products and services.

Huawei continues to closely collaborate with mainstream OS vendors in the industry. Dedicated departments and staff track the vulnerabilities and patch releases of mainstream OSs and middleware to promptly update patches. In addition, we prioritize the OS security policy configuration to ensure proper allocation of system permissions, disable unnecessary services and protocol ports, and properly manage system accounts. Furthermore, check tools are used to periodically scan system vulnerabilities, and OS security risks are promptly assessed and rectified.

To maintain high security, comprehensive vulnerability awareness and collection channels are essential. Huawei PSIRT proactively and legitimately synchronizes information from popular vulnerability databases, security forums, security conferences, and other public channels across the industry to promptly detect security threats if possible. To help security researchers and tenants submit security threats more conveniently, respond to vulnerabilities more directly and efficiently, and mitigate security threats, HMS provides an online method of submitting vulnerabilities. You can contact us via PSIRT@huawei.com.

We adhere to the principle of responsible disclosure to safeguard users' data. With regard to vulnerabilities, we will promptly push workarounds and fixes to end users under the condition that greater attack risks will not be caused by proactive disclosure.

Operation Audit

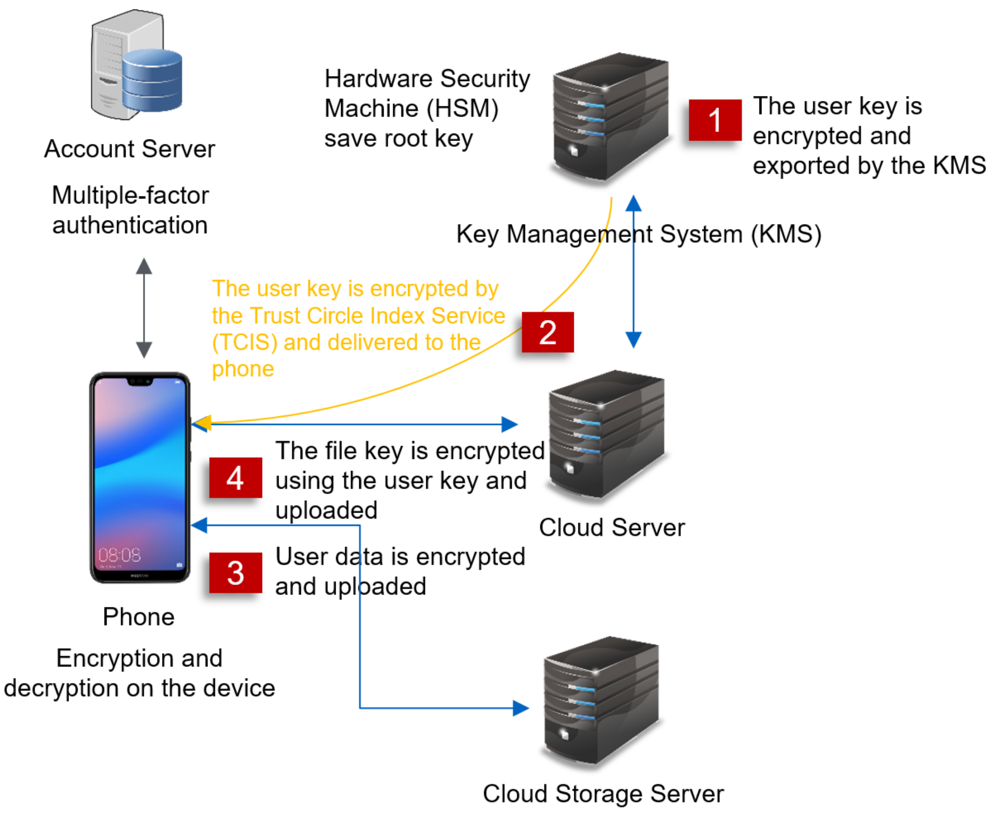
To audit suspicious operations, a centralized and comprehensive log audit system is implemented. The system aggregates the operation logs of physical devices, networks, platforms, apps, databases, and security systems to ensure that risky operations are recorded and can be queried in real time to enable post-event audits.

6 Service Security

HMS apps include HUAWEI Mobile Cloud, HUAWEI Assistant, HUAWEI AppGallery, HUAWEI Wallet, HUAWEI SkyTone, HUAWEI Video, HUAWEI Music, HUAWEI Reader, HUAWEI Themes, HUAWEI HiLives, and more. These apps provide high-quality experience in terms of digital life in all scenarios, such as payment, travel, and entertainment. Huawei protects the privacy and security of all these services through various means, such as authentication, authorization, encryption, signature, synchronization, and backup.

HUAWEI Mobile Cloud

HUAWEI Mobile Cloud is an HMS app for storing user data, including photos, videos, contacts, in a secure manner. It also automatically synchronizes the data on devices that are logged in with the same HUAWEI ID. All data synchronized and backed up in HUAWEI Mobile Cloud is encrypted during transmission and before being stored on a cloud server, enabling users to manage data more securely and conveniently.


Account Server
Multiple-factor authentication
Hardware Security Machine (HSM) save root key
1
The user key is encrypted and exported by the KMS
Key Management System (KMS)
The user key is encrypted by the Trust Circle Index Service (TCIS) and delivered to the phone
2
4
The file key is encrypted using the user key and uploaded
Cloud Server
3
User data is encrypted and uploaded
Phone
Encryption and decryption on the device
Cloud Storage Server

1. The key management system (KMS) generates user keys, and exports the keys based on user key seeds and other related key materials.
2. The KMS encrypts user keys using the trust circle and then delivers them to mobile phones, thereby preventing key leakage during delivery.
3. User data is encrypted using file keys through the block cipher on mobile phones and then uploaded to the server. Plaintext data will not be transferred out of mobile phones.
4. The key used for encrypting data is encrypted using the user key and then uploaded to the cloud server to ensure secure transmission and storage.

HUAWEI SkyTone

HUAWEI SkyTone provides mobile access services for users across multiple countries and regions. Without the need to change SIM cards, users can access the Internet anytime and anywhere by simply purchasing and enabling a destination package. With underlying chip technologies developed for years, SkyTone can automatically authenticate device identities and download soft SIM card data securely, delivering high-speed Internet access to users.

SkyTone encrypts and stores personal data to be cached on mobile phones, and stores sensitive service data (such as SkyTone package traffic information) in the TEE to provide chip-level data security protection.

Certain SkyTone services involve collaboration with third-party platforms. To redirect to a third-party HTML page, the system performs whitelist-based control on third-party platforms' domain names as well as the interfaces that can be accessed by the HTML page, and performs blacklist-based control over sensitive interfaces.

Find My Phone

If users' mobile phone is lost or stolen, they can utilize Find My Phone to locate, call, or lock the phone, or remotely erase its data. When Find My Phone is utilized, Huawei will not collect information regarding the mobile phone's location before the user logs in to HUAWEI ID and gives consent.

When Find My Phone is enabled, users can locate their devices and play ringtones at maximum volume levels. Users can also remotely lock their device and enter screen lock information. After screen lock information is set, it is displayed on the device. The lock function enables the device to enter the lock screen state and automatically report location data to the server. All location data is encrypted, and only records from within a 24-hour period are stored. Furthermore, users can erase data from their devices and permanently delete all data (including in the SD card) after entering the HUAWEI ID and password.

Find My Phone also provides the activation lock function. After data is remotely erased from a device or the device is illegally reset, a user must enter the HUAWEI ID and password linked to their device to reactivate it. To a large extent, this prevents unauthorized device use.

HUAWEI Browser

HUAWEI Browser offers services such as web browsing, information recommendation, website navigation, download, and search. It enables users to surf the Internet with maximum security and privacy.

HUAWEI Browser is equipped with powerful capabilities for detecting and blocking malicious websites. It can promptly identify phishing, Trojan horses on websites, malware, and black-market websites (such as those for gambling and pornography), as well as display different alerts or block websites based on hazard levels, safeguarding users' information and devices.

Users can enable the private browsing mode. In this mode, HUAWEI Browser does not record users' browsing information.

When a user browses a web page, the browser controls app startup, restricts JavaScript running, and blocks automatic app startup by JavaScript. Users need to authorize app startup when they tap to start an app. This prevents web pages from automatically starting or deceiving users to start malicious apps.

HUAWEI Browser also provides the password vault function. The user name, password, and bank card number automatically saved by websites are encrypted and stored in the TEE of the mobile phone, as is the key used for encryption. In addition, sensitive data (such as user names and passwords) that is automatically saved by websites is securely stored in HUAWEI Browser.

HUAWEI Browser encrypts and stores web page credentials that are marked as auto-fill and stores the encryption key in the TEE for multi-layer encryption.

HUAWEI Wallet/Huawei Pay

HUAWEI Wallet provides Huawei Pay and Pass functions.

Huawei Pay is a secure, convenient, and smart electronic wallet that integrates various transportation cards, bank cards, passes, and eIDs into a Huawei mobile phone. With just a tap, you can use your phone to shop, take a bus, open a door, and authenticate your identity.

The bank card information you add to Huawei Pay will be converted into a unique device code by the card issuer, encrypted, and then stored independently on your device's security chip. These security chips provide a fully isolated operating space for sensitive data, protecting it from potentially malicious acts in non-isolated environments.

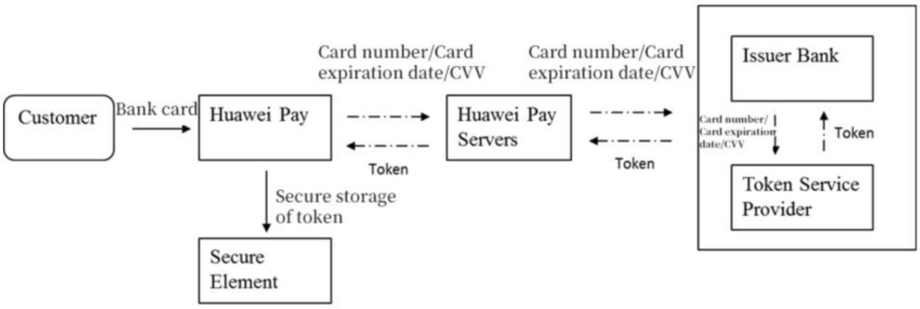
You can also use your enrolled fingerprints or face to conduct payments. Your biometric information including fingerprints is not uploaded to Huawei servers; instead, it is stored as a unique code in your device's security chip. Huawei devices cannot restore your fingerprints or facial data based on this code.

HUAWEI Wallet is a user-oriented channel for collecting and launching cards, certificates, coupons, tickets, and passes, providing convenience to merchants and users. Users can add their card, certificate, coupon, ticket, and pass information to HUAWEI Wallet for unified management. Furthermore, they can view their bank payment cards, information about card issuers, privacy policies of card issuers, and recent transactions in HUAWEI Wallet. They can also view information about the electronic cards bound to HUAWEI Wallet, such as passes, transportation cards, and membership cards.

Huawei Pay server: The server communicates with devices and payment servers through a secure TLS channel. During payments, devices, the app, and users are all authenticated.

Near Field Communication (NFC) controller: It processes near field communication protocols and sends communication packets between the app processor and SE, as well as between the SE and POS terminal. A mobile phone can be placed within close proximity to a POS terminal that supports Quick Pass for payment, without the need to connect to the Internet or unlock the phone.

Secure storage: HUAWEI Wallet does not store sensitive information such as your bank card's CVV (the last three digits on a bank card's magnetic stripe) and validity period. Only the token information of a bank card number is stored in the chip. To ensure data security when a bank card is added to Huawei Pay, the card information is transmitted to the card issuer through the security control it provides. The issuer will then send an authorized token to Huawei Pay. This means that users' actual card numbers are never stored in the mobile phone. Identity verification by Huawei Device and the card issuer is also required during the binding process to ensure that the HUAWEI ID and bank card both belong to the same user.

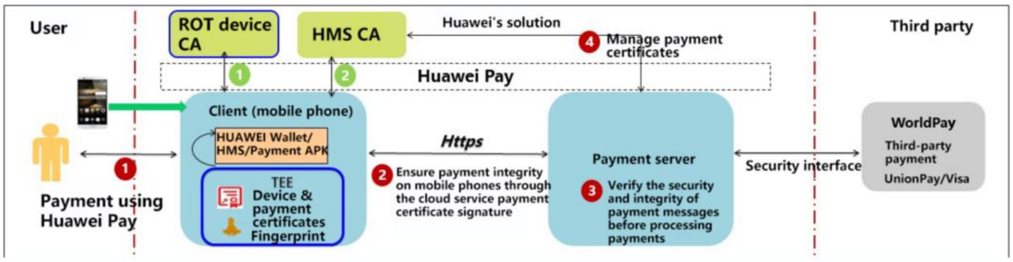


Secure payment and verification: Huawei Kirin chips have obtained the EMVCo certification (unified technical standards for debit and credit applications of international financial IC cards). These chips integrate SEs to store users' original fingerprints and other biometric information. When a user utilizes Huawei Pay, the data comparison process for fingerprint recognition is also performed in the hardware module. Therefore, users' original biometric information cannot be obtained by any app including HUAWEI Wallet. Biometric information including fingerprints will not be uploaded to a server. Even if a mobile phone is lost or under brute force cracking, the biometric information in SEs cannot be restored or copied. Huawei Pay uses digital certificate signatures to ensure the integrity of payment messages; therefore, user payments are not maliciously deducted or tampered with. In addition, Huawei Pay uses the risk control system to intelligently identify risky payments, such as those involving large sums, and triggers the manual confirmation process or rejects payments deemed high risk.

In-App Purchases (IAP) is provided to global developers, and it delivers a unified and simple offering definition, offering ordering and purchase, as well as service delivery capabilities for apps. IAP builds a comprehensive payment system by aggregating third-party mobile payment platforms and gateways. It also connects to downstream payment systems as well as calculates and settles app revenues through a settlement system.

With IAP, users can use Huawei mobile phones or devices integrated with the IAP SDK to conveniently, securely, and confidentially make payments (using bank cards or HUAWEI Points).

Fingerprint/Facial payment security


User
ROT device CA
HMS CA
Huawei's solution
4 Manage payment certificates
Third party
1
2
Huawei Pay
Client (mobile phone)
HUAWEI Wallet/ HMS/Payment APK
TEE
Device & payment certificates
Fingerprint
1
Payment using Huawei Pay
Https
2 Ensure payment integrity on mobile phones through the cloud service payment certificate signature
Payment server
3 Verify the security and integrity of payment messages before processing payments
Security interface
WorldPay
Third-party payment
UnionPay/Visa

Users need to authorize IAP to enable the fingerprint payment function, which is based on the CCS. After a mobile phone's device certificate (key attestation) passes verification, the PKI system server issues an app payment certificate for the app integrated with IAP. During payments, the certificate signs specified sensitive data, thereby enabling three-layer security verification — device, app, and user — and ensuring message integrity.

When a user makes a payment on Huawei Pay through fingerprint/face verification, the system verifies whether the fingerprint/facial data is consistent with the corresponding data stored in the TEE of the mobile phone, and then requires the user to enter the bank card's payment password. After successful verification, transaction data must be signed by the PKI digital certificate in the TEE before being uploaded to the server, ensuring payment security. During the entire payment process, fingerprint and facial information is stored only in the TEE, as opposed to the cloud, safeguarding users' privacy data.

The IAP server abides by the encrypted storage mode of the financial industry. Only the first six and last four digits of a bank card are displayed on a mobile phone. When the HUAWEI Points balance records of a user are stored, the current balance digest is stored to prevent data tampering. The PBKDF2 algorithm is used to export digests for storing users' payment passwords without storing original passwords.

IAP and Huawei Pay have obtained the PCI-DSS certification of international finance, ADSS certification of China UnionPay, and TSM certification for hardware.

Service Anti-Fraud

Service anti-fraud is dedicated to service security. To protect users' virtual assets and ensure a fair and convenient service experience, it utilizes big data and machine learning technologies to address various issues, such as credential stuffing, account theft, fraudulent acts, click farm, and service fraud.

Anti-cheat in marketing activities: accurately and promptly identifies fraudulent acts that maliciously take advantage of coupons, flash sales, and other promotional campaigns. This provides users with fair and convenient service experience.

Payment transaction protection: identifies theft and fraudulent acts in HUAWEI Wallet/Huawei Pay as well as scalping, ranking manipulation, and click farm in transactions.

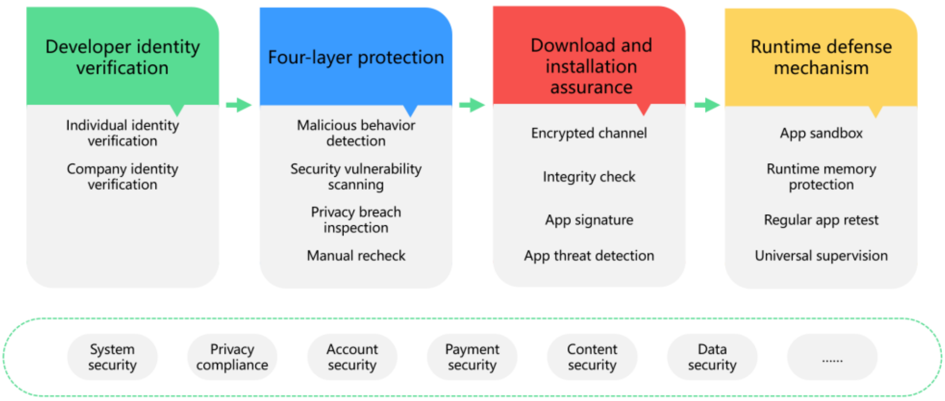
7 AppGallery and App Security

Huawei selects as well as strictly tests and reviews mobile apps to be launched in HUAWEI AppGallery to identify and remove apps that may infringe upon users' privacy or steal users' information. HUAWEI AppGallery provides strong protection for the privacy and security of apps in the developer ecosystem throughout their lifecycle, including their release, download, installation, use, and removal, without affecting consumers' experience.

Overview of AppGallery and App Security

Huawei Device strictly manages the apps distributed through the AppGallery, and provides security assurance throughout the apps' lifecycle, including reviews of developers' qualifications, security checks before the apps' release, as well as periodic checks and user feedback tracking after their release.

Comprehensive Security System

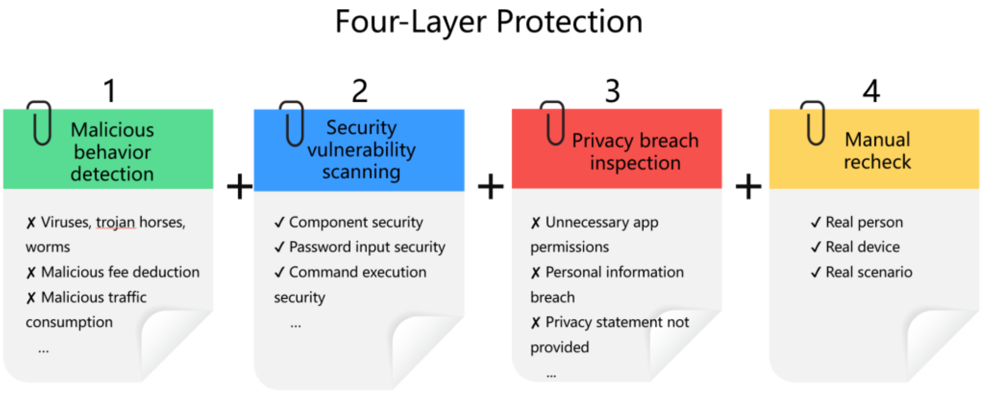

Developer identity verification
Individual identity verification
Company identity verification
Four-layer protection
Malicious behavior detection
Security vulnerability scanning
Privacy breach inspection
Manual recheck
Download and installation assurance
Encrypted channel
Integrity check
App signature
App threat detection
Runtime defense mechanism
App sandbox
Runtime memory protection
Regular app retest
Universal supervision
System security
Privacy compliance
Account security
Payment security
Content security
Data security
......

Developer Identity Verification

To safeguard users' information and rights, we strictly review the qualifications of developers. Individual developers must provide valid identity information; enterprise developers must provide their Data Universal Numbering System (DUNS) number or business registration license to prove their identities from a legal standpoint. This ensures that developers of apps that perform malicious behavior can be effectively traced.

Four-Layer Malicious App Detection System

Huawei uses SecDroid, a security detection platform of Huawei antivirus cloud, to strictly test the security of each app to be released. Using the dynamic execution and static feature analysis technologies, SecDroid detects and analyzes sensitive behavior performed by apps, scans apps for security vulnerabilities, and identifies privacy breaches to ensure the security of apps released by developers, and provide convenient security detection services for developers.


Four-Layer Protection
1
Malicious behavior detection
✗ Viruses, trojan horses, worms
✗ Malicious fee deduction
✗ Malicious traffic consumption
...
+
2
Security vulnerability scanning
✓ Component security
✓ Password input security
✓ Command execution security
...
+
3
Privacy breach inspection
✗ Unnecessary app permissions
✗ Personal information breach
✗ Privacy statement not provided
...
+
4
Manual recheck
✓ Real person
✓ Real device
✓ Real scenario

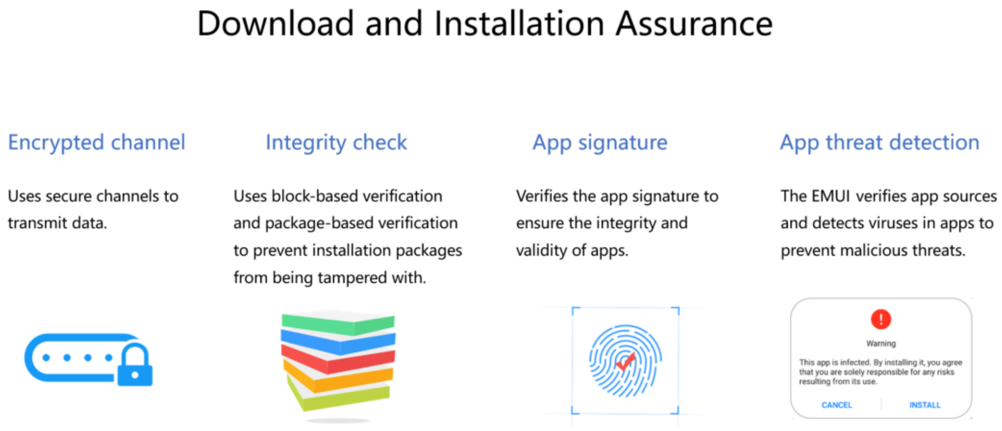
Malicious behavior detection: To handle large numbers of app release requests, HUAWEI AppGallery launches SecDroid, a cloud-based automatic scanning platform in Android mobile apps. SecDroid works with multiple well-known antivirus engines in the industry to detect viruses for Android packages (APKs). In addition, SecDroid uses the sandbox-based dynamic execution technology and static feature analysis technology to detect and analyze sensitive behavior, such as malicious billing, excessive traffic consumption, and malicious tampering of personal information.

Security vulnerability scanning: HUAWEI AppGallery scans security vulnerabilities in static and dynamic modes. Static vulnerability analysis enables static scanning and analysis of APKs for potential vulnerabilities. It detects the security of components and data, excessive traffic consumption, insecure command execution, password autocompletion, service enabling, WebView security, and sensitive behavior, and covers tens of analysis and detection aspects. Dynamic vulnerability analysis detects APKs running in the sandbox and analyzes security vulnerabilities in the APKs based on recorded dynamic run logs.

Privacy breach inspection: includes static and dynamic privacy analysis. Static privacy analysis uses data flow tracking technology, analyzes the static data flows of APKs, and detects sources of corruption and breach points to identify the complete path along which private data (such as phone numbers, SMS messages, and location history) is breached. Dynamic privacy analysis scans keys, functions, algorithms, and more to identify common issues such as key leakage, dangerous functions, and insecure algorithms. Filter criteria (such as suffix and type) are then set for refined control over scanned objects to determine the exact match locations and contexts as well as highlight the matched contents.

Manual recheck: All apps to be launched in HUAWEI AppGallery are tested by the dedicated security test team for HUAWEI AppGallery on actual devices in real-world scenarios. The team is regularly trained and study state-of-the-art security test methodologies to improve their testing capabilities. The security tests cover all Huawei and Honor device types as well as OS versions to ensure compatibility of the apps with all the devices. In addition, the apps are tested in various real-world scenarios.

Download and Installation Assurance



Download and Installation Assurance

Encrypted channel

Uses secure channels to transmit data.

Integrity check

Uses block-based verification and package-based verification to prevent installation packages from being tampered with.

App signature

Verifies the app signature to ensure the integrity and validity of apps.

App threat detection

The EMUI verifies app sources and detects viruses in apps to prevent malicious threats.

Warning
This app is infected. By installing it, you agree that you are solely responsible for any risks resulting from its use.
CANCEL
INSTALL

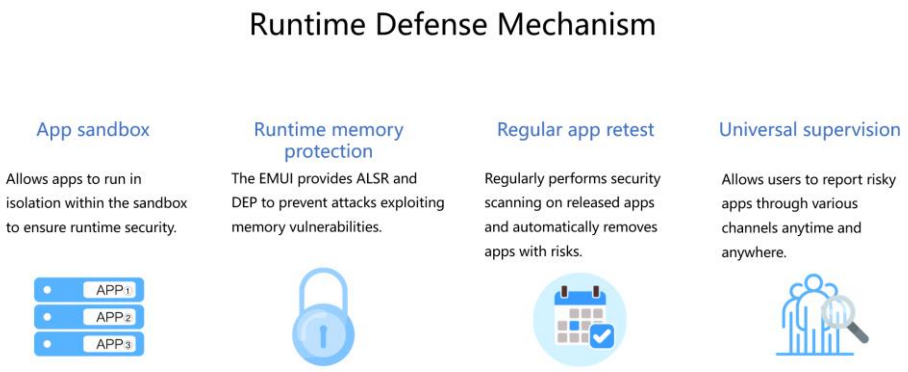
Integrity check: The SHA256 information digest algorithm is used to verify the integrity of an app installation package by checking the consistency between the digest value of the uploaded installation package and of the downloaded installation package. App installation packages that are uploaded in blocks are verified in real time during download. An app installation package that is uploaded as a whole is verified after download.

Signature verification: Only apps with complete developer signatures can be installed in EMUI. App signatures can be used to verify the integrity and legitimacy of the source of apps. The system verifies the signature of an app to check whether it has been tampered with before installing the app. Apps that fail this verification cannot be installed. The system also verifies app signatures before updating pre-installed or user-installed apps. Such an app can only be updated when the signature of the updated version is the same as the existing signature. This prevents malicious apps from replacing existing verified ones through updates.

Threat detection: Security risks may exist in apps due to unknown third parties, and downloading apps from unverified sources may bring with them malicious security threats. It is recommended that default security settings be retained to prevent unnecessary risks. EMUI has an industry-leading built-in antivirus engine, which is used to detect viruses in user-installed apps. The system supports local and online virus scanning and removal, to ensure that app risks are identified regardless of whether user devices are connected to the Internet. The antivirus engine can scan viruses during app installation and in the backend. Once a virus is detected, a risk warning is displayed, prompting users to handle the virus.

AI security defense: EMUI provides a hardware-based AI computing platform for device security protection. It has a built-in industry-leading AI antivirus engine encompassing a security defense-oriented AI model that is built upon deep learning and training. EMUI observes the behavior of unknown app software in real time to identify new viruses, new variants of existing viruses, and dynamic loading of malicious programs, and runs the AI model on devices to analyze the activity sequence of unknown software. This quickly and effectively detects threats and improves app threat detection capabilities. Once a malicious app is detected using AI security defense, the system will immediately generate a warning to prompt the user to handle the app. (This function is available only for certain chip models.)

Runtime Defense Mechanism



Runtime Defense Mechanism

App sandbox

Allows apps to run in isolation within the sandbox to ensure runtime security.

Runtime memory protection

The EMUI provides ALSR and DEP to prevent attacks exploiting memory vulnerabilities.

Regular app retest

Regularly performs security scanning on released apps and automatically removes apps with risks.

Universal supervision

Allows users to report risky apps through various channels anytime and anywhere.

App sandbox: EMUI provides an app sandbox mechanism, which enables all apps to run in isolation within the sandbox to ensure runtime security. When an app is installed, the system allocates a private storage directory to the app, which cannot be accessed by other apps, ensuring static data security. The sandbox isolation technology protects the system and apps against attacks from malicious apps. The system allocates a unique user identity (UID) to each app and builds an app sandbox based on UIDs. The sandbox provides multiple kernel access control mechanisms, such as discretionary access control (DAC) and mandatory access control (MAC), to restrict apps from accessing files and resources outside the sandbox. By default, all apps are sandboxed. To access information outside the sandbox, an app needs to use services provided by the system or exposed interfaces of other apps and obtain the required permissions, without which the system will deny access to apps. Apps with the same signature can share a UID, and share code and data in the same sandbox.

Runtime memory protection: Malicious apps usually obtain memory addresses by viewing the memory if the allocated memory addresses are relatively fixed during app operation. EMUI provides ASLR and data execution prevention (DEP) to prevent attackers from exploiting memory vulnerabilities.

Regular app retest: Security scans and retests are performed on released apps every month to identify and remove apps with security issues. The security operation team periodically updates the sensitive word library, with focus on hot events, and handles apps that control malicious behavior through developers' cloud environment.

Universal supervision: Users can report apps with security issues through HUAWEI AppGallery, contacting customer service, or other channels. HUAWEI AppGallery staff will handle such apps promptly after verification.

Age Rating of Apps

Different countries or regions have different requirements on the age rating of apps. HUAWEI AppGallery provides age rating solutions in compliance with local requirements.

Apps in HUAWEI AppGallery are categorized into five levels based on age: 3 years old, 7 years old, 12 years old, 16 years old, and 18 years old. HUAWEI AppGallery automatically hides apps that are not age-appropriate based on users' age settings.

In addition, HUAWEI AppGallery provides the download reminder function specifically for children if their parents create an account for them in the account center. This function displays a pop-up reminder to parents when a child attempts to install an app that is not appropriate for his/her age.

Security of Quick Apps

Huawei Device's quick app engine provides a series of security mechanisms on the client to ensure quick apps are stable, reliable, and secure.

In EMUI10.0 and later versions, quick apps do not provide device identifiers for developers. Different IDs are generated for different quick apps to isolate user data, reduce data association, and protect user privacy.

Huawei Device verifies the integrity of quick app packages to ensure that they have not been tampered with. Each quick app needs to be signed using the app developer's private key. Signature verification is performed during the installation and upgrade of a quick app to ensure that the quick app package has not been tampered with.

In scenarios where quick apps need to use personal data when providing services, Huawei provides standard security algorithms such as RSA and AES to encrypt and decrypt data, ensuring that developers can enhance security protection for user data.

Huawei Device provides permission management for quick apps. Quick apps' interfaces involving users' personal data need to obtain independent authorization from users. A permission management UI is also in place for users to manage authorization.

Software Green Alliance

The Software Green Alliance is China's first joint organization dedicated to improving the experience of Android apps. This alliance has released the Software Green Alliance App Experience Standards 2.0. Version 2.0 provides stricter regulations over apps' compatibility, stability, security, power consumption, and performance compared with version 1.0, as well as supplements and updates the code of behavior, privacy, security, and more of apps, improving the experience of apps.

Open Security Cloud Test

HUAWEI AppGallery works with Huawei 2012 Labs to set up open labs for Huawei devices in Beijing, China and Dusseldorf, Germany, to build the DevEco system (for app detection) and expose HMS capabilities.

1. Compatibility test: An app test report can be generated within a minimum of 8 minutes. The following types of issues are tested: installation failures, boot failures, crash, no response, black and white borders, rollback failures, UI exceptions, runtime errors, account exceptions, and uninstallation failures.
2. Stability test: Random traversal tests are performed based on control identification technology.
3. Performance test: The memory of apps and CPU usage of mobile phones are observed in real time.
4. Power consumption test: The frequency and duration of background app operation are recorded and analyzed to comprehensively measure apps' power consumption.
5. SecDroid security test: Huawei antivirus cloud's SecDroid scanning system can detect viruses, vulnerabilities, ads, malicious behavior, malicious billing, and privacy issues. The AI-based unknown threat defense technology with device-cloud synergy can defend against unknown malware in real time.

The DigiX Innovation Studio provides a platform for Huawei to further strengthen in-depth cooperation with developers and improve user experience. It focuses on various popular fields, such as gaming, education, children's activities, finance, quick apps, augmented reality/virtual reality (AR/VR), and AI. The DigiX Innovation Studio leverages its strong technical advantages to provide global developers with innovation and testing for all categories of app content, including basic services, development services, and growth services.

8 HMS Core (Developer Kits)

HMS Core provides open, on-cloud core services and capabilities, such as account, payment, push, and map services. These services and capabilities will help apps acquire more users, improve user activity, and achieve business success. HMS Core capabilities are exposed to global developers, helping them create high-quality apps and services.

HMS Core Framework

HMS Core complies with privacy laws and regulations such as GDPR, and provides unified privacy protection specifications for exposed capabilities to strictly protect user privacy. The signing entity and data storage location are determined based on the region a consumer is located (app distribution location). The 3+X deployment policy for physically isolated data storage of different regions enables strict control over the risks of cross-border data transfer. The data isolation mechanism is used to prevent abuse of data. Data isolation refers to the isolation between data for which Huawei acts as a data controller and data for which Huawei acts as a data processor and isolation of data among different developers.

In services in which Huawei acts as a data controller, such as in account and payment services, Huawei notifies users of personal data processing information in the out-of-box experience (OOBE) phase or in apps, and gives users full control over their personal data, including downloading personal data copies, controlling statistic reporting, and disabling automatic updates.

In services in which Huawei acts as a data processor (such as in Analytics Kit), Huawei responds to developers' requests, discloses sub-processor information, records the data processing process, supports the fulfillment of developers' data subject rights and obligations, and strictly implements obligations for data processing.

When deciding to build apps based on HMS, a developer should first register as a Huawei developer and apply for the required exposed capabilities. The HMS Core framework provides developers with the registration, exposed capability application, exposed capability access credential setting, and cloud-based exposed capability token generation and verification capabilities. This framework uses the AES algorithm to encrypt and store developers' registered personal data, such as their identity and bank account information.

HMS Core Kit can be released with HMS Core, or be independently released and dynamically loaded by HMS Core. HMS Core integrated with HMS Core Kit is launched in HUAWEI AppGallery. Users can decide whether to update HMS Core, and HMS Core can be updated only with users' prior authorization. If HMS Core is updated, its signature will be verified. Overwrite installation is allowed only after signature verification is successful. If HMS Core Kit is independently released in HUAWEI AppGallery, the HMS Core framework downloads and updates the kit. HMS Core verifies whether the signature certificate fingerprint of the kit is whitelisted prior to an update. If not, the kit cannot be loaded. If the fingerprint is whitelisted, the APK signature is verified. Overwrite update is allowed only after both signature verifications are successful.

Authentication Credentials

Before accessing HMS Core's exposed capabilities, developers need to create authentication credentials on the HUAWEI Developer website. Developer apps can access the exposed capabilities with authentication credentials. Currently, supported credentials are API Key, OAuth2.0 ClientID, and Service Account Key.

API Key, OAuth2.0 ClientID, and ClientSecret are generated using secure random numbers, encrypted using AES-GCM, and stored on the server to prevent leakage of authentication credentials. The public key of Service Account Key is stored by HMS Core, and the private key is stored by developers. Authentication credentials are used in the following scenarios:

1. API Key: This is a simple encrypted string that can be used to utilize HMS's exposed capabilities to access public resources. For example, a developer can use API Key to access Site Kit and Map Kit.

   Developers can set usage restrictions on API Key, including app and API restrictions. App restrictions allow only specified websites or Android apps to use API Key, and specify exposed HMS services that can be accessed by API Key.
2. OAuth2.0 ClientID: When a developer app needs to access an HMS exposed capability that requires login with a HUAWEI ID, the app can use Account Kit to obtain the user's authorized access token based on OAuth2.0. The app can then access HMS exposed capabilities related to the user through the access token. For example, a developer app uses OAuth2.0 ClientID and ClientSecret to access Drive Kit and Health Kit.

   Developer apps can access exposed HMS services through a mobile device or on the web. After obtaining an authorization code for user login, a developer app sends the authorization code and ClientID/ClientSecret to the Account Kit server through the developer server to obtain the access token. When an Android mobile app accesses exposed capabilities through HMS Core, HMS Core can authenticate the app based on the developer-configured APK certificate fingerprint and ClientID to prevent APK identity spoofing.
3. Service Account Key: This key is used for authentication between the developer and HMS Core servers. The developer server generates a JSON Web Token (JWT) and uses the private key of Service Account Key to sign the JWT. After the HMS Core server authenticates the JWT and returns an access token, the developer server can access the exposed capabilities of the HMS Core server through the access token. For example, a developer uses Service Account Key to access Nearby Service.

Service DR

HMS Core servers are deployed in multi-site disaster recovery (DR) mode. Data is periodically synchronized to DR sites, and backed up between master and backup databases. Dedicated lines are used to safeguard data transmission between the production and DR environments. During a DR failover, domain name service (DNS) is used to switch service traffic to a DR site. DR drills are regularly conducted to ensure availability of the DR environment.

Account Kit

Authorized Developer Login

Account Kit enables developers to log in to developer apps using a HUAWEI ID. After obtaining an ID token or temporary authorization code of a HUAWEI ID from Account Kit, a developer can log in to apps using the HUAWEI ID.

Account Kit complies with international standards and protocols such as OAuth2.0 and OpenID Connect. By leveraging HUAWEI ID's security capabilities, it also supports password authentication and SMS verification code to ensure high security. When the security status of a HUAWEI ID changes, Account Kit quickly notifies developers, helping developers improve service security.

Account Kit also complies with privacy laws and regulations such as GDPR, strictly protects user privacy, and supports users' data subject rights. During login to a third-party app, only user-authorized account information is shared with the user's prior consent. The user can withdraw login authorization at any time in the account center. Authorization is on a per-OpenID basis for isolation among apps.

Anti-fraud

In business scenarios such as flash sales, coupons, gift packages, and lottery drawing, attackers may attempt to register a large number of fake user accounts in batches through various channels to participate in such campaigns and receive benefits. During registration, Account Kit detects fake accounts based on specialized rules, machine learning, and various factors such as operation exceptions, suspicious mobile phone numbers and email addresses, and risky networks, to prevent registrations of fake user accounts and mitigate risks to back-end services.

After a developer app is connected to Account Kit, the developer app can subscribe to the HUAWEI ID risk status synchronization API on the server. After identifying a fake user account, the system immediately notifies the developer app, which is logged in to with a HUAWEI ID, through the risk status synchronization API to enable the developer app to promptly respond to the issue.

Push Kit

Push Kit is a messaging service provided by Huawei Device for developers that establishes a messaging channel from the cloud to mobile phones to enable developers to quickly notify users of the latest information. If the developer server implements the Extensible Messaging and Presence Protocol (XMPP), it can receive messages sent from apps to the push server. Push Kit allows messages to be pushed and received between the cloud and mobile phones, helping developers get closer to users and increase user awareness and engagement.

Push Kit provides precise messaging for developers. Each app is assigned a different AAID for data isolation among apps. After messages are successfully sent from developers to users, Huawei immediately deletes the messages and does not store them.

Identity Authentication

When a developer app applies for a push token during runtime, the HMS Core framework verifies the AppID and APK signature certificate fingerprint. After the verification is successful and the server certificate is verified, a persistent connection is established between the Push Kit client and server using TLS. The Push Kit server allocates a unique push token to the developer app. A push token contains the AppID and secure random number of the developer app, which is encrypted and stored on the server.

When a developer sends a Push message to the client through the push server, the ClientID and ClientSecret are required to obtain the access token. The push server authenticates the Push message using the access token and checks whether the ClientID in the push token matches the ClientID in the access token. If they do not match, the Push message is discarded. The Push message is sent only after matching is successful.

Push Message Protection

An app can obtain Push messages from Push Kit through directed broadcast or the Android interface definition language (AIDL) API. The security of directed broadcast is protected by Android. The AIDL API uses the app identity verification mechanism provided by the HMS Core framework for authentication. Only an app that has passed verification can read Push messages. If the app does not obtain Push messages in a timely manner, Push Kit encrypts the messages and stores them in a private directory.

When an app sends a subscription message to the Push Kit server through the Push Kit client, HMS Core verifies whether the app is able to send the message. The Push Kit client uses the key negotiated with the server to generate a message verification code for the subscription message through HMAC-SHA256. The server verifies the message verification code to ensure that the subscription message has not been tampered with.

The Push Kit server verifies whether a message complies with applicable laws and regulations and sends the message only after it passes verification.

Secure Transmission of Push Messages

The Push Kit client and server use TLS to safeguard the content transmitted between them, and when connected, they negotiate a session key and use it to encrypt messages to be sent. When the connection is set up again after interruption, a new session key is negotiated.

In-App Purchases (IAP)

IAP is exposed to global developers and provides unified and simple offering definition, offering ordering and purchase, and service delivery capabilities for developers.

Merchant and Transaction Service Authentication

To safeguard users' payments, when a merchant initiates a payment request, the merchant server uses the RSA private key to sign the payment message. The signed payment order is sent to the IAP server to verify message integrity.

Screen Capture and Recording Prevention

IAP provides screen capture and screen recording prevention functions on UIs with confidential information (such as a UI to enter a payment password). In this case, if a user attempts to capture a screenshot, the system will remind the user not to do so. Furthermore, if screen recording of confidential information is attempted on such a UI, a black screen will be displayed to prevent such data from being leaked.

Prevention of Floating-Window-based Interception

Apps with the floating window permission can float on all screens. If a user uses a keyboard or other means to enter information, such apps may crack the user-entered password according to the means by which the user entered the password (for example, which keys they pressed or where the screen was tapped).

IAP can prevent floating-window-based interception. If the system detects a floating window (for example, a video call floating window) on top of a payment page when a user enters the page, the system hides the floating window to prevent it from intercepting user operations, thereby protecting the security of the user's input and payment.

Copy-Out Not Allowed in Password Input Controls

Certain apps provide copy-out from input controls. This function reads the last copied information and uploads it for identification and analysis, which can easily leak users' privacy data. However, IAP safeguards certain UIs used for critical sensitive data input (such as the UI for entering a HUAWEI Gift Card password) by prohibiting copy-out from such UIs, thereby preventing a possible financial loss from leaked information.

Ads Kit

Ads Kit provides an ad display service for developers and ecosystem partners, helping partners establish connections with users and deliver valuable information and quality services to users.

Huawei Device provides users with various free, high-quality services. To protect user privacy, ad services do not collect users' sensitive information such as health or payment information, contacts, and call records or disclose any user information to advertisers. When personalized ads are placed based on user information, each user group contains no fewer than 5000 users. If a user enables the **Disable personalized ads** setting, all vendors including Huawei Device cannot obtain the advertisement ID of the user's device and therefore cannot push personalized ads to the user. In addition, ad placement is disabled for minors.

High-Quality Ad Choices

Ads Kit aims to provide users with high-quality ad choices and continuously enhance machine screening capability and coverage, such as portrait rights detection, contraband detection, and child protection.

Ads Kit provides developers with anti-tampering capabilities for ad content. The Ads Kit server obtains the SHA256 digest of ad images and videos to be displayed. The digest and ad images are transmitted through two different service flows and HTTPS channels, and the digest is verified in the Ads Kit SDK, which ensures that ad content is not tampered with during transmission.

Anti-cheat System

Ads Kit provides an anti-cheat system for developers. When the system identifies a cheating device, cheating IP address, or similar, it invalidates such traffic. The anti-cheat system provides anti-cheat rules such as data integrity, blacklist and whitelist, data association and rationality, user behavior rationality, and masking policies.

Data Security

The Ads Kit SDK provides developers with user data storage protection. All user data on mobile phones is stored in a private directory of HMS Core, among which important data is encrypted. This provides developers with an OS-based private data isolation mechanism and ensures that data on the developer apps integrated with Ads Kit cannot be accessed by other apps.

The Ads Kit server provides developers with hierarchical and classified protection of user data; both high-impact personal data and important system data (such as IMEIs and third-party observing service addresses) are encrypted. Other data, such as device identifiers (OAIDs), is pseudonymized using an encryption algorithm to ensure that users cannot be directly identified using the data.

When a developer app needs to share data (such as ad click, download, and installation) with third-party ad placement platform, third-party observing service, or media app servers, Ads Kit uses the pre-shared key mechanism and HTTPS encryption channel to ensure identity validity and data transmission security.

Drive Kit

Drive Kit allows developers to create apps that use HUAWEI Mobile Cloud. HUAWEI Mobile Cloud provides cloud storage for developer apps, enabling users to store files that are created when using the apps, including photos, videos, and documents in HUAWEI Drive, as well as download, synchronize, share, and search for these files on demand. Drive Kit also safeguards various types of data, enabling users to manage data in a secure and convenient way.

A user-level access token is obtained after a HUAWEI ID is used to log in to Drive Kit. This token ensures that a user's private files stored in HUAWEI Mobile Cloud can be accessed only by the user, and shared files can be accessed only by authorized users. In addition, file-level keys are used to encrypt the stored files to prevent data leakage.

Authentication and Authorization

A developer app can access Drive Kit only after the user logs in using a HUAWEI ID and gives authorization. The developer app first obtains the access token through Account Kit. When invoking the Drive Kit API, the developer app must obtain user authorization to access HUAWEI Mobile Cloud space, where the Drive Kit server authenticates the access token. Developer apps can access user data in HUAWEI Mobile Cloud as authorized only if authentication is successful.

Data Integrity

If an app provides a file's hash value during file uploading, Drive Kit verifies the integrity of the uploaded file. When an app downloads a file, Drive Kit provides the file's hash value so that the app can verify file integrity.

Data Security

Each file uploaded to Drive Kit is encrypted using a unique key for storage. The encryption keys are also encrypted by KMS under the protection of an HSM.

Active-Active Services and Data DR

Drive Kit is deployed in active-active mode and provides physical DR for data to improve service continuity. Data is periodically backed up between master and backup databases for synchronization to the DR site. Furthermore, dedicated lines are used to safeguard data transmission between the master site and DR site. When services at the active site are unavailable, the service environment at the DR site is used to provide services.

Game Service

Game Service allows game apps to provide elaborative scenes, configurations, and network information for the system and enables it to provide its status information to game apps, for closer and in-depth collaboration between both parties, as well as better gameplay experience even with limited system resources.

To safeguard user data, Game Service encrypts personal data regardless of whether the data is stored on user devices, transmitted, or stored on the cloud. Users' personal data can be shared to third-party games only with users' prior authorization, which users can withdraw at any time. Game Service provides an independent game user ID system, which is isolated from personal data in other services of HUAWEI ID.

Data Protection

When processing personal data on devices, Game Service uses standard security algorithms, such as AES and RSA, to encrypt, decrypt, and sign user data, thereby safeguarding user data on devices.

Leaderboard, achievement, event, and player statistics are sent to the HMS server for storage, and data stored is isolated by AppID. Different apps can use their unique AppID to access their game service data only, and not the game service data of other apps.

After game records are uploaded to the HMS server using HTTPS, the records are stored in isolation by user and app, and are encrypted using AES in two-layer encryption mode. The key of the first layer (file encryption key) is derived from the attribute value of a file and is used to encrypt the file; the key of the second layer (user encryption key) is derived from a user attribute value and is used to encrypt the key of the first layer. This ensures that users can use only their own encryption keys to encrypt their game data for storage.

User Authorization

If third parties need to use users' personal information, independent explicit user authorization is required.

When Game Service attempts to use sensitive functions of a mobile OS, the OS prompts the user and only allows access with user authorization.

Identity Kit

Identity Kit provides unified address management services for developers and allows third-party apps to access users' addresses upon user authorization. It also provides address management and address selection capabilities.

Identity Kit uses the ClientID and APK certificate fingerprint to authenticate access from developer apps, preventing access from fake apps. It also uses HTTPS for the encrypted transmission of address data, and verifies the developer server certificate to prevent address data from being sent to a spoofing server.

The Identity Kit SDK does not store users' address information, which is encrypted using AES128-CBC and stored on the Identity Kit server. Address data of different users is logically isolated using user-level access control, and if a user attempts to access such data, the user-level access token must be verified.

Identity Kit provides easy to use and convenient address management capabilities for users. Users' personal data can be shared to third-party apps only with the users' prior authorization. Users' address information is encrypted and stored on the cloud; a user's identity must be authenticated before access.

Wallet Kit

HUAWEI Wallet provides Huawei Pay and Pass functions. It is a user-oriented channel for collecting and launching cards, certificates, coupons, tickets, and passes, providing convenience for merchants and users.

Wallet Kit provides payment functions based on the SE, NFC, fingerprint recognition, and TEE. Through this, users can use mobile phones in replacement of bank cards or transportation cards for payments on a card reader (bank POS terminal or bus gate) that supports NFC.

In addition, users can add card, certificate, coupon, ticket, and pass information generated by apps integrated with the Wallet Kit Pass SDK to HUAWEI Wallet for unified management through HUAWEI Wallet's Card Store, AI Tips, and HUAWEI Push service.

System Environment Security Identification

Wallet Kit provides developers with system-level root security detection capabilities to detect in real time whether the OS of a mobile phone is rooted. If the OS has been rooted, a message is displayed to notify users of the security risks in HUAWEI Wallet. After this, users can decide if they wish to continue payment.

Health Kit

Health Kit provides a fitness and health data platform and service exposure capabilities for developers. Developers can integrate the Health Kit SDK to provide users with health care, workout guidance, and other services.

Health Kit uses hardware-level file encryption to protect users' fitness and health data and provides fine-grained data read and write access control, which safeguards users' data and makes the data visible, controllable, and manageable.

Access Control over User Data

A developer app or service cannot access users' fitness and health data in Health Kit without explicit user authorization. Health Kit's access authorization allows users' fitness and health data to be classified into 23 types, and the read and write permissions for each type of data can be controlled separately. A specific category of data cannot be accessed if users have not ticked the read and write permissions of this category. To ensure the accuracy of important data, additional approval is required when a developer applies for the write permission on healthcare data on Huawei Developer Alliance. When a mobile phone's screen is locked, the user's personal data can be written but cannot be read, preventing user data leakage in the background.

Data Encrypted for Storage

On mobile phones running EMUI8.1 or later versions, fitness and health data is encrypted using a file encryption mechanism based on system hardware. After the screen is locked for 10 seconds, encrypted fitness and health data cannot be read or written, preventing abuse of the data. In this case, the fitness and health data to be written can only be stored in a temporary database, and the data will be stored in the formal fitness and health database only after the mobile phone is unlocked.

Fitness and health data stored on the Health Kit cloud is encrypted using the advanced encryption algorithm AES. Each user is assigned an independent data encryption key, which is encrypted by the KMS system under the protection of an HSM.

FIDO

Fast Identity Online (FIDO) is an exposed service for quick online identity authentication. It provides BioAuthn (local biometric authentication) and FIDO2 (online user identity authentication) capabilities, which provide secure and easy to use password-free authentication service for developers.

FIDO has mature specifications and a comprehensive ecosystem in place to support a wide range of applications. It uses either biometric features or external devices for identity authentication, reducing password leakage risks. Users' personal privacy, such as biometric features, is verified on mobile phones, and data is not transmitted out of devices, further safeguarding user privacy.

Local Authentication (BioAuthn)

BioAuthn includes both fingerprint and 3D facial authentication. It provides secure, easy to use password-free authentication for developers and ensures secure, trustworthy authentication results. Before invoking BioAuthn, developers need to invoke the SysIntegrity API of Safety Detect to verify runtime environment security.

1. The FIDO BioAuthn SDK is integrated into apps.
2. The SDK invokes the SysIntegrity API of Safety Detect to verify whether a runtime environment is secure.
3. If the environment is secure, the FIDO BioAuthn SDK performs local biometric authentication. If not, however, the SDK returns that the operating system fails the integrity check.

FIDO provides secure fingerprint authentication. If the system has security issues, an error code is returned; however, if the runtime environment is secure, fingerprint authentication is performed.

FIDO also provides secure 3D facial authentication. If the system has security issues, an error code is returned; however, if the runtime environment is secure, 3D facial authentication is performed.

EMUI5 (API level 24) and later versions support fingerprint authentication; EMUI10 (API level 29) and later versions support facial authentication. Ensure that a device supports these functions prior to use.

External Device Authentication

Clients that comply with external device authentication specifications shall:

1. Provide Android Java APIs in compliance with FIDO2 specifications for browser and app developers.
2. Allow mobile phones to connect to a roaming authenticator.
3. Allow mobile phones to use a local platform authenticator.

FIDO2-compliant authenticators provide the FIDO2 roaming authenticator function so that Huawei mobile phones can be used as external authenticators when FIDO is used on other devices.

1. When a PC uses a browser, a mobile phone can be used as a roaming authenticator.
2. When a mobile phone uses a browser or app, it can be used as a platform authenticator.

WisePlay DRM Kit

WisePlay DRM Kit provides developers with digital copyright protection capabilities at hardware and software levels, including applying for a client certificate online, encrypting content in multiple formats and using various encryption algorithms, as well as playing content online and offline. Third-party apps use keys to encrypt content, which must be decrypted using the keys before playing.

WisePlay DRM Kit applies for a DRM certificate based on the user device ID (UDID or DIEID) and delivers the certificate to the device chip.

Hardware-Level Secure Runtime Environment

The core module of the DRM client runs in the TEE of Huawei mobile phones. The TEE provides a hardware-level secure runtime environment for the DRM client and protects the storage and use of confidential data in the DRM client.

1. The DRM certificate and private key are stored in the TEE's secure storage area.
2. The content key is decrypted into plaintext in the TEE only when the content is played, and is not cached.
3. The video content is decrypted in the TEE, and the plaintext video content will not be transmitted out of the TEE.

Secure Video Path

A secure video path safeguards encrypted videos throughout the transmission process covering content decryption, video decoding, local rendering and playback, and projection output, preventing decrypted video content from being breached.

Encrypted videos are decrypted by the DRM client in the TEE. The decrypted video content is then transferred to a secure decoder and is decoded, rendered, and played back. The content is also protected by the TEE security mechanism and HiSilicon security chip. The Android OS has no access to the content, and users cannot record the videos using screen recording software.

After users connect their mobile phone to a large-screen device (such as a TV) using a high definition multimedia interface (HDMI) cable and set DRM video content to be displayed on the large screen, the video content is encrypted using HiSilicon's High-bandwidth Digital Content Protection (HDCP) chip before being transmitted to the large-screen device for protection, such as validity authentication and video content encryption.

Secure Clock

The DRM client uses the TEE's secure clock (which cannot be modified by users) to verify and control the playback validity period in the content license.

DRM Certificate Authentication

When the DRM client applies for a DRM certificate, the DRM server provides authentication using the Huawei device certificate and private key signature. Huawei device certificates and private keys are pre-configured in the secure storage area of devices before delivery. Each device has both a unique certificate and private key, which can be accessed by authorized apps only.

When the DRM client applies for a content license from the DRM server, two-way identity authentication is required using the DRM client certificate and DRM server certificate.

Secure Transmission

The DRM server uses the public key of the DRM client certificate to encrypt the content key and sends the encrypted content key to the DRM client. DRM requests and responses are signed using a DRM certificate so that the messages will not be tampered with by man-in-the-middle attacks during transmission.

ML Kit

ML Kit provides vision and language services for developers based on machine learning technology. Vision services include AI such as text recognition, face detection, image classification, object detection and tracking, landmark recognition, and image segmentation. Language services include speech recognition, natural language detection, and translation. ML Kit covers ML capabilities on both devices and the cloud, as listed in the following table.

Scenario & Function		Device	Cloud
Face detection		√	
Text recognition	Text recognition	√	√
	Document recognition		√
	Card recognition	√	√
Object detection and tracking		√	
Image classification		√	√
Landmark recognition			√
Text translation			√

Language detection		√
Product visual search		√
Image segmentation	√	

ML Algorithm Package Security

ML algorithm packages can be downloaded to apps in either of the following ways:

Maven repository: ML algorithm packages are exposed in the Maven repository to apps for code integration and are installed and updated with apps. In this case, whether ML algorithm packages are updated in a timely manner depends on the installation and update frequency of apps.

HUAWEI AppGallery: ML algorithm packages are packed into an APK, which is downloaded to users' mobile phones through HUAWEI AppGallery. HMS Core verifies the integrity of an ML algorithm package based on the certificate signature to ensure that the package is not tampered with.

Data Processing

ML Kit uses only the minimum amount of personal data. It processes personal data on devices if possible, including face detection and card recognition. If devices are incapable of certain processing, ML Kit uploads relevant personal data to the cloud without associating the data with personal identifiers, and deletes the data after processing is complete.

Nearby Service

Nearby Service enables apps to easily discover nearby devices and communicate with them using technologies such as Bluetooth and Wi-Fi. The service also provides Nearby Connection and Nearby Message functions.

Nearby Connection discovers devices and sets up direct communication channels with them without connecting to the Internet. User confirmation is required for connection setup, and all data transmitted over the connection is encrypted using a negotiated key to ensure data confidentiality and integrity. Throughout the process, data will not be transferred to any servers.

Nearby Message enables a subscriber (app) to receive the sharing code broadcasted by a publisher (beacon or another app) over the Internet, and based on the sharing code, obtain message content from the cloud server. The client communicates with the cloud server using HTTPS and uses the API key for identity authentication to safeguard message confidentiality and integrity. When a user publishes a nearby message through an app, the message is stored on the HMS server. Huawei will not associate the message with any personal identity or device identifier; therefore, the message is anonymous. When a user uses a beacon to publish a message, the message is also stored on the HMS server, and the message is associated with the beacon's sharing code (BeaconID), so that other users can subscribe to the message by using the sharing code.

We advocate that developers obtain users' consent prior to publishing messages or subscribing to services in the background. After this, the message service can be enabled, and a convenient subscription switch can be provided for users.

Location Kit

Location Kit enables developer apps to quickly obtain users' precise locations using GPS, Wi-Fi, and base stations. It provides developers with various capabilities including fused location, location-based notification, user activity status identification, and geocode querying.

Location Kit uses HTTPS for encrypted transmission of location request data and verifies the location server certificate to prevent the data from being sent to a spoofing server. It requires developer apps to obtain authorization to collect data on users' locations before providing services.

Location Kit does not store users' location information and will delete the information after processing is complete. In addition, location information is not associated with any user or device identifiers and therefore cannot be used to track user locations, protecting users' privacy. Location Kit also provides the geofence function. Fence data set by users is stored only on user devices and will not be uploaded to servers. Furthermore, Location Kit does not disclose any data to third parties.

User Authorization

Location Kit uses the Android permission control mechanism to determine whether a developer app is authorized to obtain location information. It also verifies whether the developer app has obtained the user's authorization for high-precision, low-precision, and background location permissions.

Data Storage

Location Kit isolates and protects geofence information (including fence IDs, longitudes, and latitudes) submitted by developer apps. Geofence information:

1. Is not uploaded to the Location Kit server.
2. Is isolated by developer app package name. A developer app can access only its own geofence information.

Site Kit

Site Kit provides the map search function for developers and allows search results to be displayed on a map.

It uses the ClientID, APK certificate fingerprint, and API key to authenticate developers, and limits invocations to prevent the invocation of fake apps. Site Kit uses HTTPS for encrypted transmission of site request data and verifies the site server certificate to prevent the data from being sent to a spoofing server.

Site Kit stores anonymized search data only with users' consent to improve site service. In other scenarios, Site Kit does not collect or process personal data. Huawei Device cannot obtain users' site search and access records, and cannot track or identify user locations. Huawei Device will not disclose personal data to third parties.

Map Kit

Map Kit provides a set of SDKs for development of map services. It covers map data of more than 200 countries and regions, and supports tens of languages. With this SDK, developers can easily integrate map-based functions into their apps to improve user experience.

Map Kit uses the ClientID, APK certificate fingerprint, and API key to authenticate developers, and limits invocations to prevent the invocation of fake apps. It uses HTTPS for encrypted transmission of map request data and verifies the map server certificate to prevent the data from being sent to a spoofing server.

Map Kit does not collect or store users' personal data and therefore cannot track users' activities. When a user requests map data, Map Kit converts the longitude and latitude location of the user into map coordinates on the device, and then initiates a service request, without reporting information on the user's location. In addition, third-party map service suppliers shall follow the same requirements for processing data as Huawei Device to ensure that users' personal data is fully protected.

Awareness Kit

Awareness Kit enables developers to obtain contextual information including users' current time, location, activity, levels of ambient light, and weather, enabling a smarter, more user-oriented experience.

Awareness Kit may need to obtain location, Bluetooth, and network permissions, as well as data including ambient light levels, headset status, user activity, geofence, and the like. All data is processed on user devices and will not be sent to a server. Awareness Kit needs to send approximate location information (km-level) to servers to obtain information on the weather and local national holidays. HTTPS is used for encrypted transmission, and the approximate location information is not associated with devices or users, nor is it stored on the cloud.

Analytics Kit

Analytics Kit is a one-stop data analytics platform for app developers. It provides product optimization and operational decision references for developers based on user activity and user attribute data reported by apps under user authorization as well as a large number of analytics models preset on the platform.

Analytics Kit leverages multi-layer encrypted transmission between devices and the cloud as well as logically isolated storage on the cloud to ensure the security of operational indicators among developers' analytics data and the security of business analytics of app services.

Analytics Kit assigns a unique AAID to each device as an identifier. It does not collect persistent identifiers such as IMEIs and SNs. Developers' data will not be used for any other purposes or shared with third parties without their consent. An automation interface is used to uphold data subjects' rights and obligations, including the right of access, right to object, and right to erasure.

Server Spoofing Prevention

Analytics Kit verifies server certificates to ensure that data is transmitted to a trusted server. The certificate issuer, validity period, and domain name are verified to prevent developer app data from being reported to a malicious spoofing server, preventing breach of data.

Secure Data Transmission

Analytics Kit uses HTTPS for secure transmission of data to a server. This prevents app data from being intercepted by attackers through a local or network man-in-the-middle agent and, therefore, prevents the disclosure of apps' business secrets.

It also uses a randomly generated key to encrypt the transmitted data. In addition, it uses an RSA public key to encrypt the randomly generated key, and uploads the data and key ciphertext to the server, preventing malicious attackers from obtaining the data of developer apps.

Server Data Isolation

Analytics Kit isolates data on a server by developer app to ensure that data of different developers and apps cannot be accessed by each other.

Dynamic Tag Manager

Dynamic Tag Manager (DTM) is a system that helps developers quickly configure and update measurement code and related code snippets, as well as dynamically update tracing code through web pages to track specific incidents and transfer data to third-party analytics platforms, allowing marketing data to be observed on demand.

DTM verifies the source of tag code. The DTM server also controls access of different developer roles. The code of different developer teams and apps is isolated. In addition, the DTM server verifies the customized template configurations submitted by developers. DTM also provides mechanisms such as tag code preview/debugging and version management to ensure that developers can detect abnormal tag code in a timely manner and resolve the issue through version overwrite.

DTM developers must comply with all applicable laws and regulations as well as agreements with Huawei Device when using HUAWEI DTM and processing users' personal data in relation to HUAWEI DTM. Developers must accurately identify platforms that may collect, receive, or use end users' personal data through the use of HUAWEI DTM. Developers must notify end users of these platforms, personal data to be collected, and purposes for data collection. In addition, developers must obtain and store end users' legal consent to the use of cookies or similar technologies, and provide end users with the ability to withdraw consent. If a developer does not comply with applicable laws and regulations or the agreement with Huawei Device, Huawei Device may restrict or suspend the use of HUAWEI DTM by the developer. Developers must not upload information that can identify users (such as name, email address, device identifier, or invoice) to the DTM server. In addition, we may collect and process information about how HUAWEI DTM is used for the purpose of improving and maintaining HUAWEI DTM. We will not share the information with third parties without the developer's consent, unless those third parties are operating under contract and acting on our behalf.

Anti-spoofing

DTM verifies DTM server certificates to ensure that the dynamic tag code to be updated or downloaded is from a trusted DTM server. DTM verifies a certificate's issuer, validity period, domain name, and other information to prevent the server from being spoofed.

Limited API-based Code Execution Permissions

DTM provides limited API-based code execution permissions. APIs can only be used to execute measurement code and track specific incidents. DTM strictly reviews the APIs and will not obtain sensitive permissions or information of devices.

Security Management for Dynamic Tag Code

DTM performs input verification on the configuration parameters of dynamic tag code templates submitted by developers to prevent malicious or abnormal tag code templates from being imported to the database. If DTM detects any app with non-compliant or malicious dynamic tag code, it can quickly suspend the app's capability to invoke DTM.

Safety Detect

Safety Detect is a multi-dimensional open security detection service launched by Huawei Device. It detects system integrity, app security, malicious URLs, and fake user accounts, helping developers quickly build app security by leveraging the unique advantages offered by Huawei mobile phones.

Integrity and app security are detected only on devices, and data will not be reported to servers. The URLs used for detection are reported after query parameters are removed on devices and are not associated with personal data. Detection of fake user accounts requires the collection of users' HUAWEI IDs, device IDs, and IP addresses. The information is encrypted and stored only for a necessary period of time and will not be shared to any third party.

- SysIntegrity API: checks whether the device running a developer app is secure (for example, whether it is rooted).
- AppsCheck API: obtains a list of malicious apps.
- URLCheck API: determines the threat type of a specific URL.
- UserDetect API: checks whether your app is interacting with a fake user account.

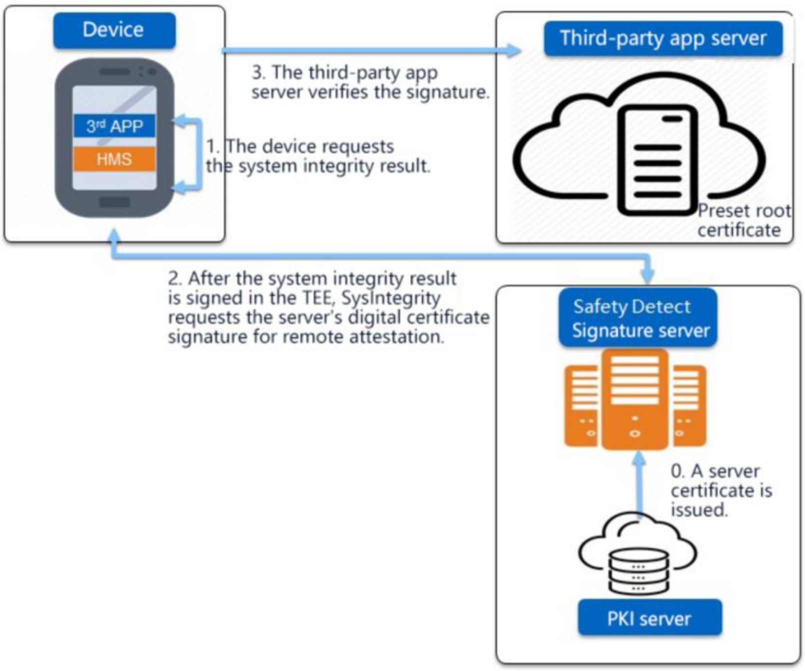
SysIntegrity

Before using Safety Detect's SysIntegrity API, ensure that HMS Core of the required version has been installed on the device. If your app detects that the installed HMS Core is not the required version, it should prompt the user to update HMS Core.

When invoking the SysIntegrity API, a nonce value should be transferred, which is contained in the detection result. Developers can verify the nonce value to determine whether the returned result matches the request, preventing replay attacks. The SysIntegrity API contains the nonce value and AppID. The AppID is available in the configuration of the signature certificate fingerprint.

SysIntegrity provides developers with secure and trustworthy detection of system integrity in the TEE of a mobile phone. It then signs the detection result in the TEE, uploads the signed result to the SysIntegrity server to request a signature, and returns the signed system detection result to the developer app.

SysIntegrity provides developers with the capability to verify the system detection result. Developers can verify the system detection result on their own app servers or upload the signed system detection result to the Safety Detect server for verification.


Device
3rd APP
HMS
1. The device requests the system integrity result.
3. The third-party app server verifies the signature.
Third-party app server
Preset root certificate
2. After the system integrity result is signed in the TEE, SysIntegrity requests the server's digital certificate signature for remote attestation.
Safety Detect Signature server
0. A server certificate is issued.
PKI server

AppsCheck

Before using Safety Detect's AppsCheck API, ensure that HMS Core of the required version has been installed on the device. If your app detects that the installed HMS Core is not the required version, it should prompt the user to update HMS Core. An app can invoke the getMaliciousAppsList() API of SafetyDetectClient to obtain the list of malicious apps.

AppsCheck provides the list of malicious apps for developers to assess whether to restrict app activity based on risks (risky apps or virus apps). It provides 14 types of capabilities to detect malicious apps and unknown threats.

URLCheck

URLCheck enables developers to identify malicious URLs such as those with phishing or Trojan horses, with performance and efficiency taken into consideration. It provides developers with simple, operation-free, and trustworthy security services and reduces the cost for implementing secure browsing services.

Developers can specify the types of concerned threats as the input parameters of the URLCheck API. Constants in the UrlCheckerThreat class contain the supported threat types.

Developers can invoke getUrlCheckResponse() of URLCheckResponse to obtain the URL detection response. The returned List<UrlCheckThreat> contains the detected URL threat types. If the list is empty, no threat has been detected. If the list is not empty, invoke getUrlCheckResult () of UrlCheckThreat to obtain the specific threat code.

UserDetect

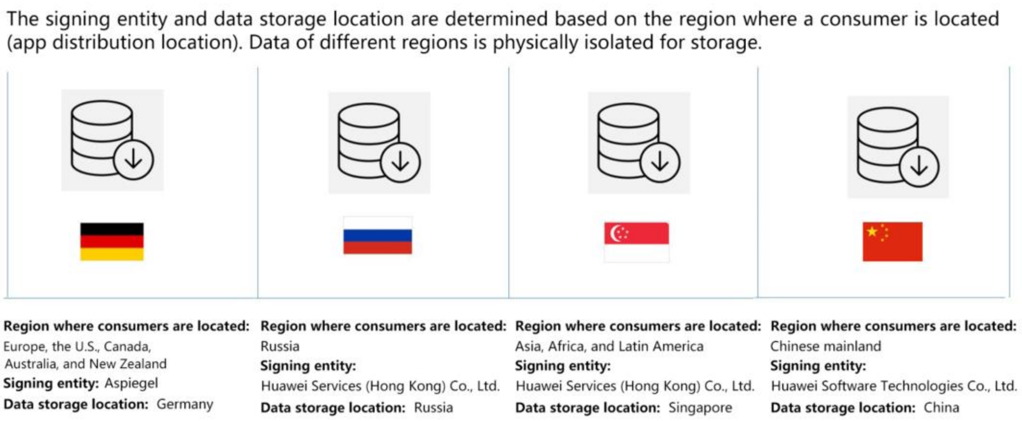
UserDetect enables developers to detect fake user accounts. It identifies fake devices based on the device signature, identifies risks such as root, simulator, VM, changer, and anonymous IP addresses, identifies fake user accounts based on analysis of touchscreen and sensor behavior, and uses image- and semantic-based verification codes to prevent batch registrations, credential stuffing attacks, fraudulent activities, and content crawlers.

9 Privacy Control

Personal information stored on HMS will be properly protected, including photos, contacts, call records, emails, chat information, and frequently visited websites. In addition, all processing of personal information is in compliance with local applicable laws and regulations, and users' privacy is fully considered. For example, users are explicitly informed of data collection in advance, and have full control over the collection, processing, and sharing of their personal information. We will never provide any third party with a user's personal information without the user's authorization.

Local Deployment

HMS provides products and services through global resources and servers, and ensures that user data is fully protected by applicable laws and regulations. If local servers must be deployed and cross-border data transfer is not permitted by local law, user data will be stored on local servers and under the operation as well as O&M of locally registered subsidiaries subject to local laws, unless users are informed of or give consent to otherwise. For example, the photos and personal files of European Union (EU) users are stored on servers in the EU.



The signing entity and data storage location are determined based on the region where a consumer is located (app distribution location). Data of different regions is physically isolated for storage.

Region where consumers are located: Europe, the U.S., Canada, Australia, and New Zealand	**Region where consumers are located:** Russia	**Region where consumers are located:** Asia, Africa, and Latin America	**Region where consumers are located:** Chinese mainland
Signing entity: Aspiegel	**Signing entity:** Huawei Services (Hong Kong) Co., Ltd.	**Signing entity:** Huawei Services (Hong Kong) Co., Ltd.	**Signing entity:** Huawei Software Technologies Co., Ltd.
Data storage location: Germany	**Data storage location:** Russia	**Data storage location:** Singapore	**Data storage location:** China

Clear and Transparent Data Processing

No matter whether an app is used for the first time or a new function is used, we will remind users to check the privacy statement before collecting personal data. Users can decide how their data will be used and have full control over their own privacy.

In certain HMS Core capabilities, Huawei acts as a data processor and explicitly notifies developers of the scope, purposes, and storage location of data to be collected as well as the measures to be taken to ensure privacy protection, helping developers fulfill their notification obligations.

For details about the privacy statement, visit:

https://consumer.huawei.com/minisite/cloudservice/privacy/

Data Minimization

Huawei takes reasonable and practical measures to ensure that the personal information collected or shared is minimal and relevant to what is necessary in relation to the purposes for which it is processed.

HMS assigns random IDs when sharing data to developers, and each developer or app obtains different device IDs and user IDs, even for the same user, so that personal data is isolated and not associated with specific users, thereby preventing data abuse and reducing breach risks.

HMS uses the unique device ID as the primary identifier for collecting device data, and this device ID cannot be identified by non-Huawei developers. This prevents data from being associated across developers, improving data security and privacy protection.

HMS does not collect data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, and data concerning sex life or sexual orientation.

HMS Core always adheres to data minimization principles in privacy design for capability exposure to developers. Such principles include but are not limited to the following:

1. Account Kit is used for authorizing third-party app login based on an OpenID rather than a HUAWEI ID, which enables isolation among apps.
2. Analytics Kit assigns a different AAID to each installation, which acts as the unique device identifier. It does not collect persistent identifiers such as IMEIs and SNs.
3. Location Kit does not store users' location information and will delete the information after processing is complete.
4. Map Kit does not collect or store users' personal data and therefore cannot track users' activities.
5. ML Kit and Awareness Kit perform local computing on devices, where possible.

Data Subjects' Rights and Privacy Control

Users can submit personal information access requests through Huawei Consumer's official website, through the account center, or by contacting Huawei (by phone, email, and online customer service) or visiting a store. We recommend that users submit requests through the official Huawei Consumer website or account center, to facilitate communication and feedback of the request handling progress and results. This prevents the right to request personal information from being embezzled or abused by others. Huawei releases a dedicated privacy notice or supplementary statement for each product or service, describing how users can access, rectify, or delete personal information collected by the product or service.

Users can request to disable or deregister their HUAWEI IDs from their Huawei products. After a HUAWEI ID is deregistered, HMS will not provide further services for the HUAWEI ID, and will delete the user's personal information unless otherwise specified by laws and regulations. A deregistered HUAWEI ID cannot be restored. The user must register a new HUAWEI ID if he/she wants to use the services again.

Users can view or revoke HUAWEI ID access permissions granted to third-party apps or websites in **Account center** > **Privacy center** > **Control account access**.

HUAWEI Browser provides Private Browsing. If a user enables this function, HUAWEI Browser will not record any visited websites or search content, or store any form of information filled in online, thereby protecting user privacy.

To protect user privacy, HUAWEI Ads Kit sends targeted ads to users in apps by using an ad identifier. Advertisers use ad identifiers to control the display frequency of specific ads to users and measure their effect. Similarly, ad identifiers can also provide users with ads that they may be more interested in. Apps will not send targeted ads only if users enable the **Disable personalized ads** setting.

Location service determines a user's location based on GPS, Wi-Fi hotspot, and base station data, thereby providing better, local services for users. If users enable location service, navigation apps are more accurate, and weather apps can provide local weather information. Any apps that attempt to access a user's location data must obtain the user's consent, and users reserve the right to disable location service whenever they want.

HMS collects service invoking information for service improvement with users' prior consent. Users can withdraw consent at any time in **Settings** > **Privacy** > **Permissions** on a mobile phone. HMS will then stop collecting such information.

Obligations of a Data Processor

HMS Core provides analytics, push, and other services for developers. In these services, developers determine the purposes of data processing and how the data will be used and are therefore data controllers. Huawei acts as the data processor that collects and processes personal data on behalf of developers.

Huawei signs data processing agreements (DPAs) with developers to specify the rights and obligations of the data controller and processor. HMS Core processes personal data only in accordance with a DPA and the controller's instructions, and does not process personal data for Huawei's purposes. For example, in analytics services, HMS will not use developers' data for the purpose of HMS ad or service improvement.

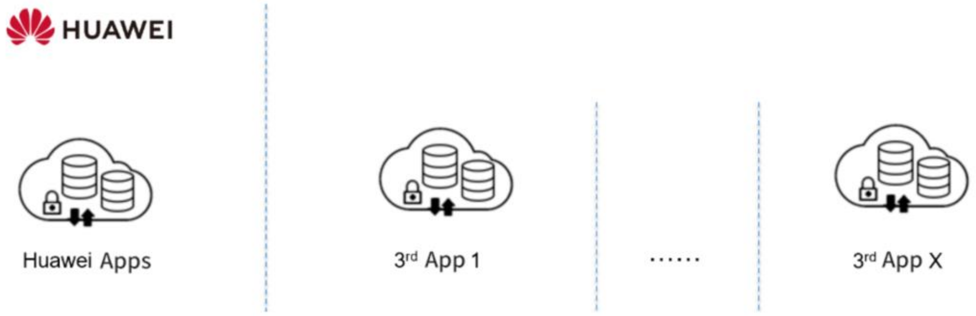
For data processing activities that need to be subcontracted, only suppliers (sub-processors) that provide sufficient technical and organizational measures are used. Subcontracting suppliers requires written authorization from developers.

As the data processor, Huawei assists the controller in responding to requests for the exercise of data subjects' (end users') rights and complies with the requirements of personal data processing, data breach notification, data protection impact assessment, and prior consultation. Huawei will delete or return personal data once cooperation with the developers has been completed. Huawei will also provide the controller with information to demonstrate compliance with the processor's obligations and provide audit/inspection channels.

Data Isolation

The data of Huawei apps and developer apps is stored separately. Developer data will not be used for Huawei's data processing purposes.

The personal data of different developers is also isolated to prevent data sharing and misoperations.



Differential Privacy

Differential privacy technology is used in certain scenarios of HUAWEI Music and will be continuously used in more scenarios to improve user experience and reduce the information you share with Huawei.

This technology prevents original information about the app from being uploaded, by generating a digest of the app information and adding random noise information to it so that the uploaded information cannot be associated with your device. Relevant differential privacy patterns appear only when your data is combined with the data of a large number of other users and the randomly added noise information averages out. These patterns help Huawei understand how users use their devices (for Huawei to improve relevant services and products) without collecting personal information.

Federated Learning

Federated learning technology is used in certain scenarios of HUAWEI Video and will be continuously used in more scenarios. In AI training, we do not directly upload video viewing records, but rather we use the basic model delivered by the server for training, optimize the learning model on devices, and build a privacy protection AI solution in compliance with GDPR through the device-cloud distributed machine learning system. This consequently reduces the risk of personal data breaches while video content recommendation is personalized to users. Furthermore, user data is stored on devices, and only the trained model updates are anonymized and reported to the server, preventing user privacy breaches. In addition, model updates from a large number of devices are aggregated to continuously optimize app-level learning models. This improves user experience and reduces the amount of information you share with Huawei.

Protection of Minors' Personal Information

For minors who use HMS, additional preventive measures shall be taken to protect their privacy and security.

When a minor's personal information is collected with the prior consent of the holders of parental responsibility, Huawei will only use or disclose the information as permitted by law, explicitly consented to by the holders of parental responsibility, or necessary for protecting the minors. If the holders of parental responsibility need to access, rectify, or delete the personal information related to minors under their guardianship at any time, see the privacy notice or supplementary statement of the specific product or service.

10 Security and Privacy Certification and Conformance

HMS has been certified by multiple international security authorities and complies with global applicable security, privacy laws and regulations. We are committed to actively and continuously participating in the formulation of industry security standards in addition to making our own contributions to the sound development of the industry.

ISO/IEC 27001/27018 Certification

The ISO/IEC 27001 information security management system is an internationally accepted and widely used certification standard system for information security. This certification indicates an enterprise has established a scientific and effective information security management system to unify the enterprise's development strategy and information security management and ensure information security risks are properly controlled and correctly handled. HMS first obtained this certification in January 2016 and renewed the certificate in January 2019.

https://www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=licence%3d637452%26company%3d&page=1&licencenumber=IS 637452

ISO/IEC 27018 is an international code of conduct that focuses on personal data protection on the cloud. It is based on ISO 27002 and provides guidelines for implementing the ISO 27002 control system applicable to personally identifiable information (PII) on the public cloud. This ensures that PII is properly protected when being processed by the cloud-based personal identity information processor and therefore provides a common compliance framework for cloud service providers operating in multiple countries. HMS obtained this certification in October 2019.

https://www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=licence%3dPII%2b714315%26company%3d&licencenumber=PII%20714315

ISO/IEC 27701 Certification

The ISO/IEC 27701 privacy information management system provides a comprehensive set of personal data processing methods and a privacy information management framework from multiple dimensions, such as organizational governance, legal compliance, process specifications, information technology, as well as supervision and audit. This certification indicates that an enterprise has a comprehensive personal information protection management system in place in design, R&D, operations, and O&M phases and is in a global leading position regarding personal information security management, transparency, and privacy compliance. HMS obtained this certification in November 2019.

https://www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=licence%3d719801%26company%3d&licencenumber=PM%20719801

CSA STAR Certification

CSA STAR certification adds the cloud control matrix (CCM) and other security requirements based on ISO/IEC 27001. It covers 16 control domains, including risk governance, data security, app security, infrastructure security, development and design, identity and access management, data center security, change management, configuration management, business continuity management, operations recovery, human resources, and supply chain management. HMS first obtained this certification in January 2016 and renewed the certificate in January 2019.

https://www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=licence%3d637452%26company%3d&page=1&licencenumber=STAR%20637452

CC Certification

Common Criteria (CC) certification is a highly recognized product information security certification in 31 countries, and is segregated into seven levels (EAL1 to EAL7). A higher level indicates a stricter review process and, consequently, more comprehensive product security.

Huawei HarmonyOS kernel obtained CC EAL5+ in September 2019. EAL5+ is a commercial OS kernel security certification, indicating that sensitive data, such as fingerprints, facial data, and lock screen passwords, of Huawei/Honor mobile phone users during app use is properly protected.

https://www.commoncriteriaportal.org/files/epfiles/Signed%20certificate%20CC-19-217235.pdf

PCI DSS Certification

Payment Card Industry Data Security Standards (PCI DSS) certification is one of the world's highest-level financial data security standards and one of the most authoritative data security standards for the payment card industry. It aims to strictly control data storage to ensure the security of online transactions of payment card users. PCI DSS is widely supported and promoted by global card organizations and financial institutions and has become a standard that must be followed by merchants and service providers. IAP in HUAWEI Wallet obtained this certification in January 2018.

https://www.atsec.cn/cn/pci-attestation/ASPIEGEL-PCIAttestation-atsec-PCI-DSS-C-01100-33.pdf

https://www.atsec.cn/cn/pci-attestation/HuaweiServicesHK-PCIAttestation-atsec-PCI-DSS-C-01100-51.pdf

EuroPriSe for HUAWEI ID

In January 2020, the European Privacy Seal (EuroPriSe) granted the EuroPriSe Seal to Aspiegel Limited, a wholly owned subsidiary of Huawei Technologies Cooperatief U.A (Netherlands), for its HUAWEI ID service in the European Union (EU) and European Economic Area (EEA). The EuroPriSe offers a trans-European privacy trust mark issued by an independent third party certifying compliance of IT products and IT-based services with European regulations on privacy and data security. The EuroPriSe provides transparent procedures and reliable criteria. More information about the EuroPriSe for HUAWEI ID (EU/EEA) can be found here (https://www.european-privacy-seal.eu/EPS-en/news/n/12172/europrise-seal-for-huawei-id-as-provided-by-aspiegel-ltd-to-users-in-the-eueea).

FIDO Certification

The Fast Identity Online (FIDO) Alliance was founded in 2012, aiming to address interoperability issues between strong identity authentication technologies and preventing users from having to create and manage multiple groups of user accounts and passwords. FIDO certification proves that an enterprise's products comply with FIDO specifications and can interoperate with any other FIDO-certified products.

HMS FIDO obtained UAF 1.1 certification in March 2019, helping developers build FIDO security capabilities and bringing a fast and secure identity authentication experience to app users.

11 Oriented Future

HMS will continuously enhance its security by leveraging Huawei's unique security advantages in chipset-device-cloud synergy to provide E2E security protection capabilities for chips, systems, apps, and data, as well as safeguard against intrusions and the black market. In addition, it uses self-updating security capabilities as well as open cooperation as the foundation for a secure mobile service future.

As the demands for stronger security are growing, systems are becoming more complex and intertwined with each other. This, along with evolving threats and adversarial attack vectors, puts a greater strain on future cloud security. It is challenging for users to understand and keep up with the various security and privacy risks that they are exposed to when they use various smart apps and devices in their daily routines.

Therefore, to overcome this problem, we strive to create a sustainable, secure and safe ecosystem that comprises an enormous collection of smart apps and 1+8+N devices in our ecosystem for the long term. We seek to continuously address these challenges from the perspective of users, developers, and legislation in collaboration with our academic and industry partners, while adhering to the following objectives:

- Protect and empower users
- Fortify foundation against emerging threats
- Prepare for disruptive technology

Protect and Empower Users

Users' data security and privacy protection have always been the focus of HMS. To improve user experience, Huawei HMS will become atomized and smart to bring users direct and convenient service results and build a smart service distribution platform. Technologies, such as big data, machine learning, and AI, are widely used to proactively address privacy protection and data security challenges.

We are passionate in helping our users to be productive while keeping their information secure and protecting their privacy. It is important to innovate new solutions that are secure and privacy-friendly while ensuring usability. The implementation of security and privacy solutions often relies on the use and research of several fundamental technologies. This requires continuous research on data protection technologies that are used for securing data including client-side encryption and E2E encryption, as well as enabling privacy protected use of data with multi-party computation, homomorphic encryption, differential privacy, functional encryption, and privacy-preserving AI-based technologies such as federated learning.

Additionally, support for secure collaboration is needed. This will ensure that user data is protected at the client side prior to transmission to the cloud so that the user has full control over who has access to their data in every circumstance. Approaches where data can be managed in zero trust environment are also needed. To build a robust AI system where users rely on with the increasing use of AI, it is important to protect against adversarial AI, prevent privacy breaches due to membership inference, and make AI explainable.

Another important aspect is to explore ways and methods of enhancing users' understanding of an app and assisting them before, during, and after using an app. There is a clear need for usable solutions that will help users understand what data is collected and generated about them by service and how widely that data is used and exposed within and between different organizations, and enable users to control their data.

Developers shall prove the security and privacy protection capabilities of their solutions through measures, such as privacy seals, which can be used to build trust between developer apps/services and users.

Fortify Foundation Against Emerging Threats

Security is a constant race that requires a high level of anticipation of new security and privacy threats resulted from emerging attack vectors, rapid technology changes, and changes on business operation models or legislation. We continuously invest in state-of-art detection technologies to protect infrastructure, systems, devices, apps, and data, and we work with various security partners to enhance anomaly detection at system, web, app, and device levels.

We envision a trustworthy, ethical, and safe ecosystem by ensuring that it is free from illegal, harmful, inappropriate, and copyright-infringed content.

By building and exposing HMS Core security capabilities, HMS continuously enhances services such as system integrity detection, app security detection, malicious URL detection, and fake user detection in Safety Detect, helping developers provide more secure apps.

Huawei has set up a computer emergency response team (CERT) that is dedicated to improving product security. Any organization or individual that finds security vulnerabilities in Huawei products can contact Huawei at PSIRT@huawei.com. Huawei PSIRT will respond as soon as possible, organize internal vulnerability fixing, release security advisories (SAs), and push patch updates.

Prepare for Disruptive Technology

We prepare for disruptive technology that may either present unforeseeable threats or result in new opportunities to innovate solutions. For example, a breakthrough in quantum computing will result in public key cryptography being broken in post-quantum era and affect current technologies that are based on public key cryptography, such as HTTPS, key management, and signature.

Deepfake technology leverages machine learning and AI to create images or videos that are deceptive and difficult for an average user to identify as being fake or real. This may potentially lead to misinformation or abuse that affects an individual's online safety.

We believe it is essential to work with our academic partners to address these future challenges in our mission to create a safe ecosystem for our users.

A Acronyms and Abbreviations

Acronym or Abbreviation	Full Name	Description
ADSS	Account Data Security Standard	A standard approved by the China UnionPay Risk Management Committee to reinforce account information security management on a UnionPay card acquiring network. This standard further specifies and refines the account information security management requirements for the participants of the acquiring service to prevent account information leakage risks.
AES	Advanced Encryption Standard	A block encryption standard, also known as Rijndael.
AI	Artificial intelligence	A new technical science that studies and develops theories, methods, techniques, and application systems for simulating and extending human intelligence.
AIDL	Android Interface Definition Language	A service that enables cross-process access.
API	Application programming interface	A collection of predefined functions or a set of conventions that specifies how different components of a software system are connected. It enables apps and developers to access a set of routines through software or hardware, without having to access source code or understand the details of internal working mechanisms.
App	Application	Software installed on smartphones.
APT	Advanced persistent threat	Uses sophisticated malware and techniques to exploit vulnerabilities in systems.

Acronym or Abbreviation	Full Name	Description
ARM	Advanced RISC machine	A 32-bit reduced instruction set computer (RISC) processor architecture.
ASLR	Address space layout randomization	A computer security technology designed to defend against memory corruption exploits.
CA	Certificate authority	A trusted third party in e-commerce transactions, which is responsible for verifying the validity of public keys in the public key system.
CBC	Cipher block chaining	A mode in which each plaintext block is exclusively ORed (XORed) with the previous ciphertext block and then encrypted.
CC	Challenge collapsar	Using an agent server, an attacker generates a valid request pointed to an aggrieved host in order to implement distributed denial of service (DDoS) or masquerade attacks.
CCM	Counter with CBC-MAC	A traditional method of MAC construction.
CCS	Cloud Certificate Service	Certificate management services including online (offline) issuance, deregistration, freezing, and status query of service certificates.
CERT	Computer emergency response team	An expert group that analyzes and responds in real time to computer security incidents happening both at home and abroad, and provides solutions and emergency countermeasures to protect the computer information system and network against damage.
CPU	Central processing unit	Computing and control core of a computer system, which processes information and runs programs.
CSRF	Cross-site request forgery	An attack method that coerces a user who has logged in to a web application to execute undesired operations on the application.
CVV	Card verification value	A code on the back of a credit card.
DBF	Database firewall	A database security protection system based on database protocol analysis and control technology.

Acronym or Abbreviation	Full Name	Description
DDoS	Distributed denial of service attack	An attack launched by multiple attackers in different locations against one or more targets, or launched by an attacker who has seized control over and exploits multiple machines in different locations against victims.
DES	Data Encryption Standard	A block algorithm used to encrypt keys.
DEP	Data Execution Prevention	Prevents code from being run from a specific part of memory in order to protect computers.
DMZ	Demilitarized zone	A buffer area between an insecure system and a secure system.
DPA	Data processing agreement	A security and privacy agreement signed between a data controller and a data processor, or between a data processor and a data sub-processor, which specifies the responsibilities and obligations of both parties in the processing of personal data.
DRM	Digital rights management	A technology that offers enhanced protection of the copyright of digital audio and video programs, documents, and ebooks.
DTM	Dynamic tag manager	A dynamic tag manager system that helps developers quickly configure and update measurement code and related code snippets. It can also dynamically update tracing code through web pages to trace specific events and transfer data to third-party analytics platforms, so that marketing data can be observed on demand.
ECC	Elliptic curves cryptography	An approach to public-key cryptography based on the algebraic structure of elliptic curves.
EMUI	Emotion UI	An Android-based OS developed by Huawei.
EMVCo	Ease of Movement Value	An international financial standard for smart payment cards, POS terminals that can use chip cards, and automatic teller machines (ATMs).
FIPS	Federal Information Processing Standards	A set of standards used by government agencies for automated data processing and remote communications.
GCM	Galois/Counter Mode	A mode of operation for symmetric-key cryptographic block ciphers.

Acronym or Abbreviation	Full Name	Description
GDPR	General Data Protection Regulation	Any organization that collects, transfers, retains, or processes personal information in any EU member state is subject to this Regulation.
HDCP	High bandwidth digital content protection	Protects uncompressed digital audio and video content.
HDMI	High definition multimedia interface	A fully digital audio/video interface for transmitting uncompressed audio and video signals.
HIPS	Host intrusion prevention system	A host security system that adopts the client/server (C/S) structure, and which is capable of rapidly detecting and addressing server system security issues to ensure secure operation of the system.
HKIP	Huawei Kernel Integrity Protection	A real-time kernel integrity protection module, which observes the integrity of core data such as kernel code and page tables in the runtime state, and detects and blocks unauthorized behaviors such as tampering and malicious access.
HMS	HUAWEI Mobile Services	A collection of exposed device and cloud capabilities, helping developers achieve efficient app development, rapid growth, and flexible monetization.
HMAC	Hashed message authentication code	A message authentication method based on a combination of hash functions and keys.
HTML	Hypertext Markup Language	A markup language that includes a series of tags used to provide one simple format for documents on the Internet, and which connects scattered Internet resources as a logical whole.
IAP	In-App Purchases	A service that provides convenient purchases within apps.

Acronym or Abbreviation	Full Name	Description
IDS/IPS	Intrusion detection system/Intrusion prevention system	IDS: a network security device that observes network transmissions in real time and generates alerts or takes proactive measures when detecting suspicious transmissions. IPS: a computer network security device that observes the network information transmission behavior of a network or network devices. It can efficiently interrupt, adjust, or isolate abnormal or harmful network information transmission behavior.
IM	Instant messaging	A service that offers real-time communication over the Internet.
IMEI	International mobile equipment identity	Identifies a mobile communications device, such as a mobile phone, on a mobile phone network.
KASLR	Kernel address space layout randomization	Loads kernel images to different addresses at each startup for enhanced security.
KMS	Key Management Service	KMS provides key management capabilities for users and services. KMS assigns a pair of master keys encrypted using an HSM to each service, and extracts the final user and service keys using the HKDF algorithm.
NFC	Near Field Communication	A short-range, high-frequency radio technology that enables data exchange when devices are close to each other.
OOBE	Out-of-box experience	A step taken to configure basic Windows settings after the Windows OS is installed.
OTA	Over the air	A technology used for the remote management of mobile device and SIM card data through an air interface for mobile communications.
PCI-DSS	Payment Card Industry Data Security Standard	Security requirements for agencies using credit card information, including requirements for security management, policies, processes, network architecture, and software design, in order to ensure secure transactions.
PBKDF2	Password-Based Key Derivation Function 2	Uses a pseudo-random function to derive keys.

Acronym or Abbreviation	Full Name	Description
PIA	Privacy impact assessment	Before processing data, the data controller or processor conducts PIA on the processing operations to be performed.
PKI	Public key infrastructure	A collection of hardware, software, personnel, policies, and regulations used to generate, manage, store, distribute, and revoke keys and certificates based on the public-key cryptography.
POS	Point of sale	A multifunctional terminal installed in a commercial business or other sites involved with credit card use, which is connected to a computer network for automatic electronic fund transfer.
PSIRT	Product Security Incident Response Team	Receives, handles, and discloses security vulnerabilities related to Huawei products and solutions.
RASP	Runtime application self-protection	RSAP injects and integrates itself into an app to identify and block attacks in real time, providing the app with self-protection capabilities.
RBAC	Role-based access control	An effective access control method designed for enterprise security policies.
REE	Rich execution environment	An OS and related apps that run in common mode, which is different from a TEE running in a secure world.
ROM	Read-only memory	A type of storage that stores read-only data and can retain data even in the case of power failure. Specific conditions must be met if data needs to be stored or modified in ROM.
RSA	Rivest-Shamir-Adleman	A cryptographic system that uses various encryption and decryption keys to ensure that it is computationally impossible to deduce decryption keys from known encryption keys.
SD	Secure digital memory card	A new generation of storage device based on semiconductor flash memory.
SDK	Software development kit	A collection of development tools used by software engineers to develop app software for specific software packages, software frameworks, hardware platforms, and OSs.

Acronym or Abbreviation	Full Name	Description
SE	Secure element	Containing encryption/decryption logic circuits in a chip, it is used to prevent external malicious parsing attacks and protect data security.
SHA	Secure Hash Algorithm	A FIPS-certified secure hash algorithm, and part of a family of cryptographic hash functions. It can calculate the fixed-length string (also called message digest) corresponding to a digital message.
SIM	Subscriber identity module	IC card held by a mobile user in the GSM system.
SoC	System-on-a-chip	An integrated circuit with dedicated objectives, which contains a complete system and all of the embedded software's content.
SSL	Security Socket Layer	Widely used for identity authentication and encrypted data transmission between the web browser and server. The data encryption technology is used to prevent data from being intercepted or eavesdropped during transmission.
TCIS	Trust circle index service	A TCIS server is a server component used to manage public key information in a trusted service. All services are provided in web mode based on the applicability of the Internet.
TEE	Trusted execution environment	An OS and trusted apps running in a secure world (such as TrustZone).
TLS	Transport Layer Security	Enables confidentiality and data integrity between two apps.
TSM	Tivoli storage manager	Provides enterprise-level management software, such as system management, security management, and storage management.
VLAN	Virtual local area network	A group of logical devices and users, which are organized based on functions, departments, and applications, regardless of their physical locations. Such devices and users communicate with each other as if they are on the same network segment.
VPN	Virtual private network	A private network established on a public network, and used for encrypted communications.

Acronym or Abbreviation	Full Name	Description
WAF	Web application firewall	A product that protects web applications by implementing a series of HTTP/HTTPS security policies.
XMPP	Extensible Messaging and Presence Protocol	A subset XML protocol based on standard generalized markup language.
XSS	Cross-site scripting	An attack that steals information from users by exploiting website vulnerabilities.