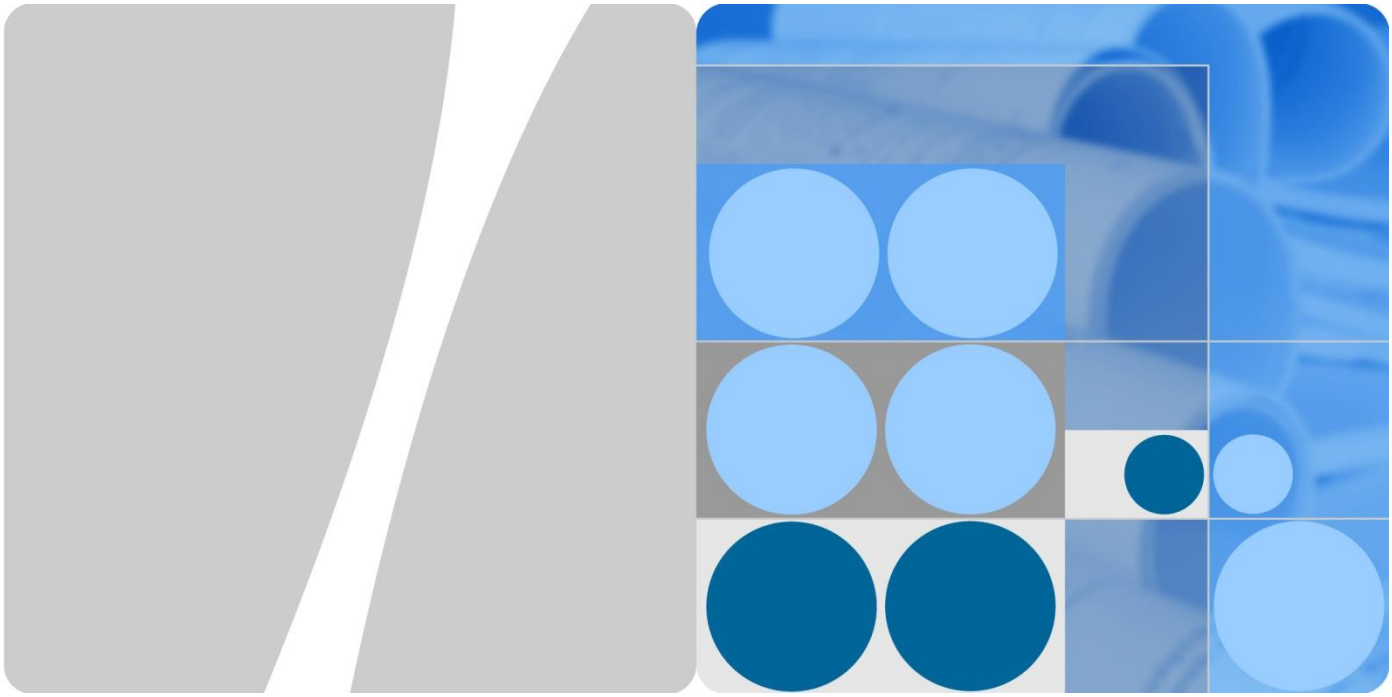
HUAWEI Mobile Services (HMS) Security Technical White Paper V2.0

Issue	**V2.0**
Date	**2021-12-31**



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

 Copyright © Huawei Device Co., Ltd.

 Copyright © Huawei Device Co., Ltd.

 Copyright © Huawei Device Co., Ltd.

1 Introduction

1.1 Security & Privacy Protection Are Huawei's Top Priorities

Cyber security and privacy protection are Huawei's top priorities. We place network and service security assurance over our commercial interests. To that end we have devised four proposals and three commitments regarding the security and privacy protection of our consumer services.

From an organizational perspective, we have established a top-down organization governance architecture, and implanted security and privacy protection activities throughout all of our service processes. From the very start of product design, we adhere to strict security and privacy protection principles and processes, and services that violate them are prohibited from being released. We work with industry authorities to build an independent security verification system for verifying the security and privacy protection capabilities of our products and services. We also open up our security and privacy protection capabilities to our ecosystem partners, in order to build a secure and trustworthy ecosystem for all 1+8+N scenarios together with our partners.

We and our ecosystem partners spare no effort when it comes to protecting the privacy and security of consumers and make three major commitments to ensure consumer privacy protection. Firstly, protecting consumer privacy is our top priority, and we do so through the use of innovative technologies. Secondly, only consumers themselves can view their data, and no one else has access to such data without the consumer's authorization. Thirdly, from device startup to service usage, consumers' prior consent is a must for using their data and permissions in each step.

Because privacy protection is our primary concern, we implement privacy protection measures throughout the entire product lifecycle – from product design and development to operations and maintenance. We always adhere to the following privacy protection principles, and utilize multiple innovative privacy protection technologies to safeguard consumer data security from multiple dimensions:

- Data minimization: We only use the least amount of personal information required to provide services for consumers.
- On-device data processing: We try as much as possible to process and analyze consumers' personal data on their own devices.

 Copyright © Huawei Device Co., Ltd.

- Transparency and controllability: We clearly and explicitly notify consumers before using and analyzing their personal data, and ensure that they know how the data is used and how to cancel their authorization for the use of their data.
- Identity protection: We anonymize consumers' identities with the aid of privacy enhancing technologies (PET) when transferring their data out of their devices.
- Data security assurance: We constantly improve and add security capabilities for our hardware, operating systems, apps, and services because we firmly believe that data security is the basis of privacy protection.

We have established independent privacy and security teams worldwide to continuously research innovative privacy and security technologies, integrate the latest technologies into HMS, and monitor and ensure strict compliance of our products. We build privacy and security capabilities into our products from the very beginning of product design, and continue to apply them throughout the product development and go-to-market processes. We also actively communicate with consumers, and listen to their feedback and suggestions on privacy and security improvement.

For more information about Huawei's commitment to privacy and security, visit https://consumer.huawei.com/en/privacy/.

 Copyright © Huawei Device Co., Ltd.

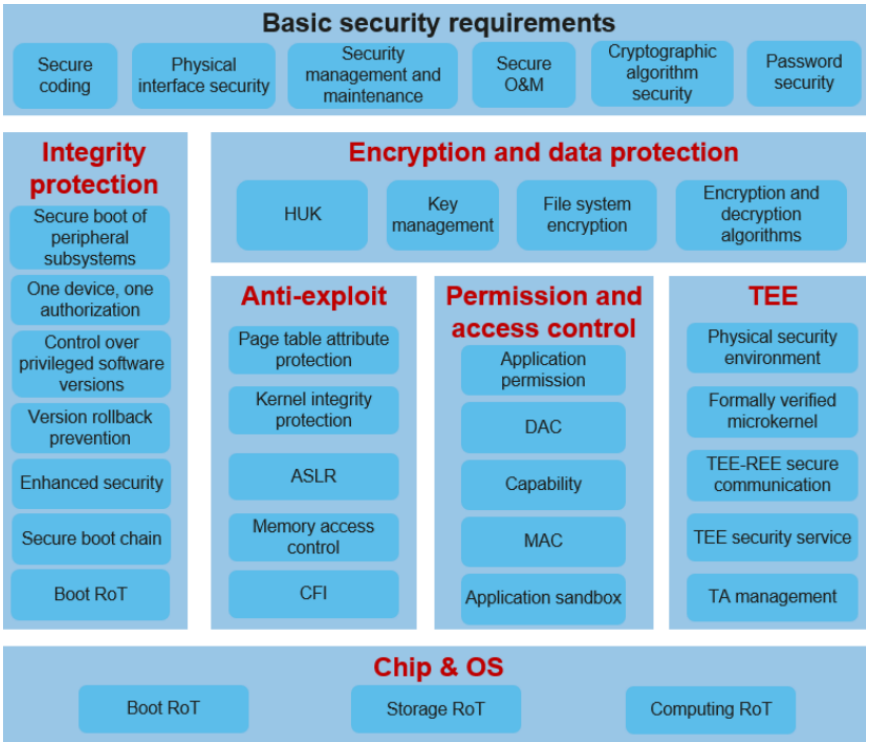
2 HarmonyOS-based Security

HarmonyOS is a next-generation operating system designed by Huawei for smart devices, with the goal of providing a unified language for intelligence, interconnection, and inter-device synergy. It provides users with a smooth, seamless, secure, and reliable all-scenario interactive experience.

The backbone of HarmonyOS's security capabilities is its three hardware-based roots of trust (RoTs): startup, storage, and computing. HarmonyOS leverages these to ensure device integrity, data confidentiality, and vulnerability exploit protection.

The figure below shows the security architecture of HarmonyOS.

Figure 2-1 HarmonyOS security architecture



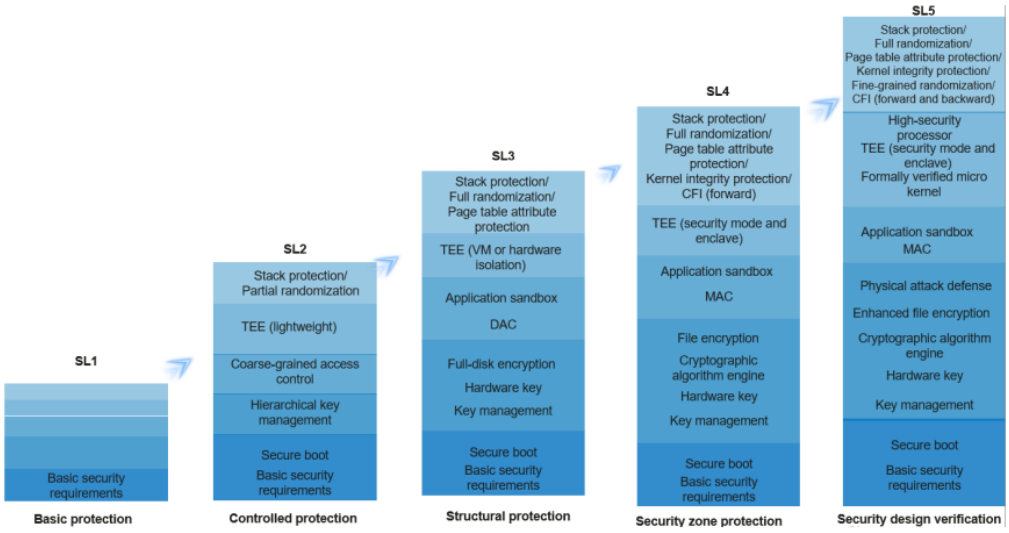
 Copyright © Huawei Device Co., Ltd.

The above figure shows a typical security architecture of a single HarmonyOS device. The architecture may vary depending on the risk level and the software and hardware resources of the device.

HarmonyOS classifies security capabilities of HarmonyOS devices into five levels from SL1 to SL5, based on an industry-standard security classification model, and taking into account actual HarmonyOS service scenarios and device types. Higher security levels include the capabilities of lower security levels by default.

The figure below shows the security levels of HarmonyOS devices.

Figure 2-2 HarmonyOS device security levels



HarmonyOS provides security measures for protecting consumer and developer data throughout the data lifecycle, and takes into account personal data sensitivity level, system data importance, and app data asset value. With the device security level system, all data is assigned an appropriate security level when it is generated, and appropriate access control permissions and policies are adopted for the data based on its security level throughout the data lifecycle. During data storage, appropriate encryption measures are adopted for different data security levels, and during data transmission, the system prohibits the transfer of highly sensitive data to devices with low security capabilities. In addition, devices with low security capabilities are not allowed to deliver instructions for controlling highly sensitive resources and peripherals.

For more information about HarmonyOS-based security, please refer to the HarmonyOS security technology whitepaper at https://consumer.huawei.com/en/privacy/whitepaper/.

 Copyright © Huawei Device Co., Ltd.

3 Secure Service Access

HUAWEI ID enables users to securely sign 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, sign-in and runtime environments, and user sign-in credentials. Such security detection also prevents unauthorized users from stealing account information for sign-in based on multi-factor verification of user sign-in environments and devices, thereby preventing users' personal information from being obtained or illegal payments being made using their accounts.

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 sign-in password, fingerprint sign-in, trusted device verification, verification code for new device sign-in, 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.

3.1 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.

3.2 Image Verification Code

When HUAWEI ID detects an automated attack attempt through Safety Detect's UserDetect feature, it will display an image verification code to help prevent the attack. The system provides complex verification images, which cannot be spoofed by a bot. Brute force cracking is further prevented by limiting the number of verification code entry attempts.

 Copyright © Huawei Device Co., Ltd.

3.3 Account Protection and Multi-factor Authentication

With account protection, a user can only sign in to a HUAWEI ID from its trusted devices. When a user signs in to their HUAWEI ID on a device for the first time or enables forcible two-factor authentication, they must sign in through two-factor authentication, which further ensures sign-in security. 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 the user's trusted device. The user can enter the password and verification code on their new device, which will then become their trusted device. For example, if the user is currently using a HUAWEI Mate 20 and want to sign in to their HUAWEI ID on a newly-purchased HUAWEI Mate 30, the HUAWEI Mate 30 will prompt the user to enter their password and the verification code displayed on their HUAWEI Mate 20.

3.4 Risky Operation Notification

When a user attempts to sign 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.

3.5 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). If the user has completed identity verification, they can also retrieve their account and password through liveness detection and facial authentication.

3.6 Child Accounts

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 child accounts to provide a safe online environment for their children. HMS provides additional protection for children in products and services, including filtering out apps that are not suitable for children on HUAWEI AppGallery, restricting the payment capacity of child accounts, and filtering out content that is not suitable for children in Video and Reader services.

 Copyright © Huawei Device Co., Ltd.

3.7 Account Anti-Fraud

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

Sign-in: 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 passwords, it is important that they can conveniently reset the passwords. 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 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 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.

3.8 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.

 Copyright © Huawei Device Co., Ltd.

4 Encryption and Data Protection

4.1 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.
- On-device 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

 Copyright © Huawei Device Co., Ltd.

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.

4.2 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, HarmonyOS installer verifies apps during installation. HarmonyOS can verify the signature of an 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 their 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 Trusted Execution Environment (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

 Copyright © Huawei Device Co., Ltd.

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.

4.3 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.

4.4 TCIS

When a user signs 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 signs 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. 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.

 Copyright © Huawei Device Co., Ltd.

5 Network Security

5.1 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.

5.2 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.

 Copyright © Huawei Device Co., Ltd.

- On the management plane, access control based on secure VPN and HTTPS channels is implemented throughout the process, including sign-in 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 sign-ins and operations, accounts are used to sign 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 sign-in 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.

5.3 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.

 Copyright © Huawei Device Co., Ltd.

5.4 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 apps 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, trustlist, 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.

5.5 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 app firewalls (WAFs) are deployed to defend the web app 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 unknown vulnerability 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.

 Copyright © Huawei Device Co., Ltd.

5.6 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.

5.7 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.

5.8 Operation Audit

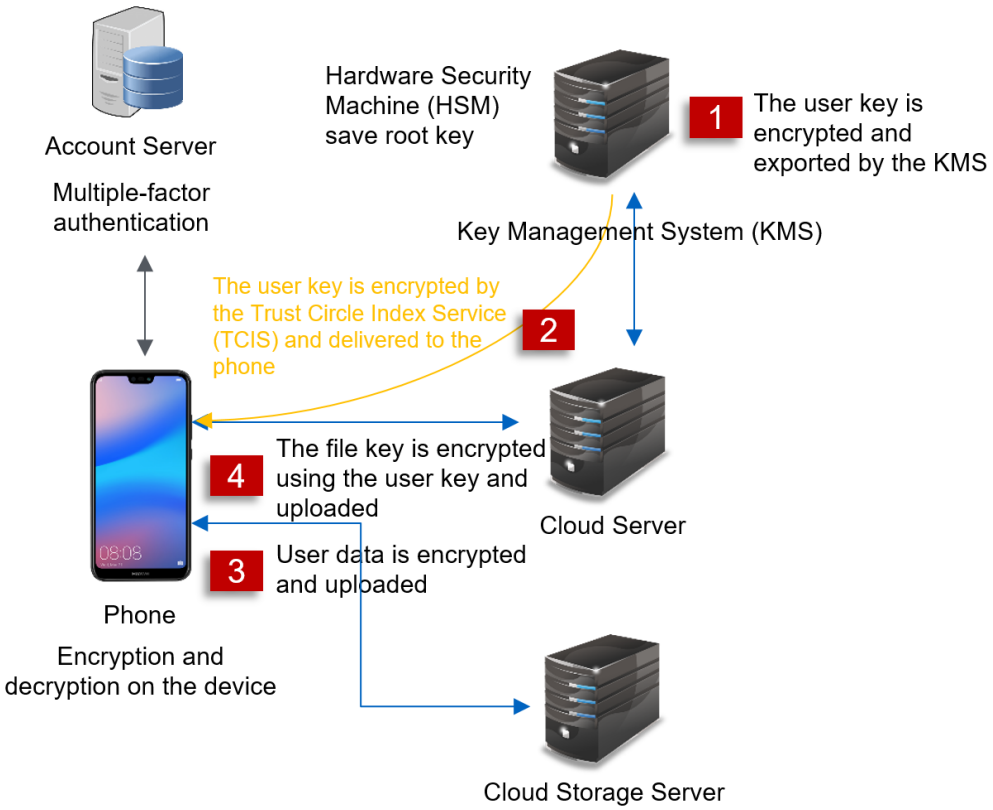
To audit suspicious operations, a centralized and comprehensive log audit system is implemented. The system aggregates the operation logs of physical devices, networks, platforms, apps, databases, and security systems to ensure that risky operations are recorded and can be queried in real time to enable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

 Copyright © Huawei Device Co., Ltd.

6 Service Security

6.1 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 signed 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.



1. The key management system (KMS) generates user keys, and exports the keys based on user key seeds and other related key materials.

 Copyright © Huawei Device Co., Ltd.

2. The KMS generates a key for each user, and the app can only obtain the key of a user using the user's valid identity, preventing key leakage.
3. User data is encrypted using file keys through the block cipher on mobile phones before being uploaded to the cloud storage server. This means that plaintext data will not be transferred out of mobile phones.
4. The key used for encrypting data is encrypted using the user key before being uploaded to the cloud server to ensure secure transmission and storage.

6.2 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 information 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 trustlist-based control on third-party platforms' domain names as well as the interfaces that can be accessed by the HTML page, and performs blocklist-based control over sensitive interfaces.

6.3 Find Device

If users' Huawei devices such as mobile phones, tablets, earphones are lost or stolen, they can utilize Find Device to locate, call, or lock the device, or remotely erase its data. When Find Device is utilized, Huawei will not collect information regarding the device's location before the user signs in to HUAWEI ID and gives consent.

When Find Device is enabled, users can locate their devices and play ringtones at maximum volume levels. Users can also remotely lock their devices 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 Device 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.

Find Device's position sharing feature allows users to authorize specific friends to view their shared positions. Users can stop sharing their position at any time, after which the invited users will be unable to view the shared positions anymore. The invited users can also reject sharings at their own discretion.

 Copyright © Huawei Device Co., Ltd.

6.4 HUAWEI Browser

HUAWEI Browser offers various mobile services, including 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 attempts, Trojan horses, malware, and websites that contain illegal content (such as gambling and pornography), as well as display different alerts and block websites that have a certain level of risk, safeguarding users' information and devices. In addition, HUAWEI Browser allows users to report malicious websites using a button in **Toolbox**, and view a list of malicious websites that they reported.

HUAWEI Browser's ad blocking feature can identify whether a website URL contains junk, nuisance, or other malicious ads. It can also identify and block malicious ads and popups on visited web pages, ensuring a safe and enjoyable browsing experience for users. HUAWEI Browser also allows users to manually mark ads on web pages, enhancing ad blocking capability and further ensuring nuisance-free Internet browsing.

HUAWEI Browser can proactively detect trackers during web page browsing and block tracking cookies by default, preventing them from storing users' personal information or tracking users' Internet browsing behavior.

During Internet browsing, HUAWEI Browser prevents web pages from opening apps without the user's permission. This prevents web pages from opening malicious apps when the user visits the web pages.

HUAWEI Browser provides users with a visualized report regarding privacy and security protection. Users can view the report to check event details such as blocked ads and tracking cookies.

Users can also choose to browse websites in a private browsing mode. In this mode, HUAWEI Browser does not record users' browsing information.

HUAWEI Browser also provides users with the ability to surf the Internet in basic mode, in which only basic functions are available. By default, this mode restricts personalized content and provides a blank home page, offering users a streamlined and uncluttered browsing experience.

HUAWEI Browser provides a password vault function, which encrypts and stores user names, passwords, and bank card numbers automatically saved by websites in the TEE of the user's mobile phone, alongside the encryption key. 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 auto-fill web page credentials for storage and stores the encryption key in the TEE for multi-layer encryption protection. When users need to view or modify their auto-fill web page credentials, they must verify their identity by providing their lock screen passwords or fingerprints. This serves to prevent such credentials from being leaked or maliciously tampered with.

HUAWEI Browser provides a kids mode, which is specially designed for children. When child mode is activated, in-feed recommendations on the home page are disabled and websites with content unsuitable for children are automatically blocked. Parents can also select specific websites to block. With child mode, HUAWEI Browser leverages its technical capabilities to build a healthier Internet environment for children, and protect children from being exposed to age-inappropriate content.

 Copyright © Huawei Device Co., Ltd.

6.5 HUAWEI Wallet/Huawei Pay

Huawei Pay is a secure, convenient, and smart electronic wallet that allows users to access their public transport passes, bank cards, door keys, and eIDs on their Huawei mobile devices. With just a single tap, users can use their phones to shop, take a bus, open a door, authenticate their identities, and more.

HUAWEI Wallet does not store sensitive information such as a 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 security chip. To ensure data security when a bank card is added to Huawei Pay, the binding information is transmitted to the card issuer through the security control it provides. The issuer will then send an authorized token to the security chip for storage. This means that the actual card number is never stored on the mobile phone. The security chip provides an isolated space for storing sensitive information, avoiding malicious behavior that may occur in a non-isolated space.

Users can pay using Huawei Pay only after they complete identity verification using their payment passwords or biometric data. Biometric data analysis is performed in the TEE. No apps, including HUAWEI Wallet, can access the user's raw biometric data, and biometric data will not be uploaded to any server.

The Huawei Pay server communicates with devices and payment servers through a secure TLS channel.

Huawei Pay signs payment messages using a digital certificate to ensure their integrity, preventing user payments from being maliciously deducted or tampered with.

In-App Purchases (IAP) provides in-app payment capabilities for global developers, and delivers unified capabilities such as product definition, product ordering and purchase, and service delivery for apps.

With IAP, users can make in-app payments (using bank cards or HUAWEI Points) conveniently, securely, and confidentially.

Users can authorize IAP to use their fingerprints or faces for payment, which is based on the CCS. After a mobile phone's device certificate (key attestation) passes verification, the PKI system server issues a payment certificate for the app with IAP integrated. During payments, the certificate will be used to sign specified sensitive data, thereby enabling security verification from the device, app, and user perspectives, as well as ensuring message integrity.

When a user makes a payment on Huawei Pay using their fingerprint or face, the system verifies whether the fingerprint or face data is consistent with that stored in the TEE of the user's mobile phone. If the fingerprint or face data is consistent, transaction data will be signed using the PKI digital certificate in the TEE before being uploaded to the server, ensuring payment security. Throughout the payment process, fingerprint and face data is stored only in the TEE, as opposed to the cloud, safeguarding users' private information.

The IAP server adheres to the storage encryption requirements 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, only a digest of the current balance is stored to prevent data tampering. The PBKDF2 algorithm exports digests of users' payment passwords, and does not store the actual passwords.

 Copyright © Huawei Device Co., Ltd.

Huawei Pay and IAP have obtained PCI-DSS certification, ADSS certification of China UnionPay, and BCTC certification.

6.6 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.

HMS provides the capability for anti-cheat in marketing activities, which can 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.

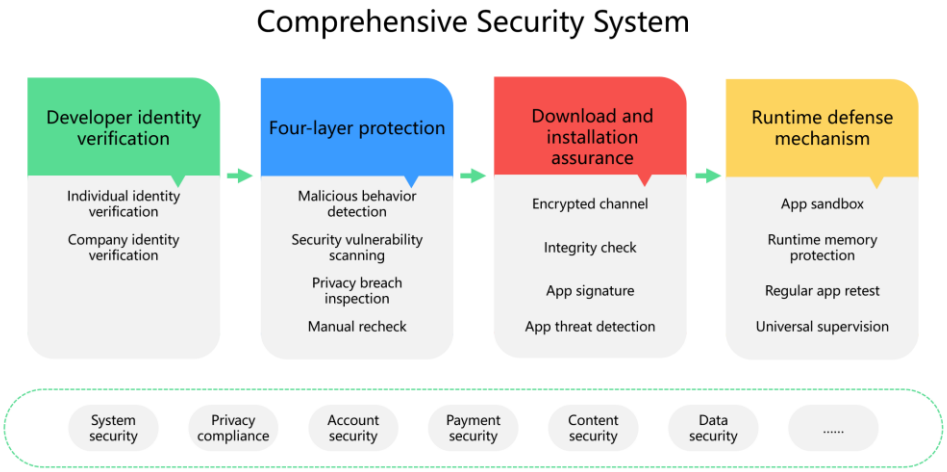
In addition, HMS identifies theft and fraudulent acts in HUAWEI Wallet/Huawei Pay as well as scalping, ranking manipulation, and click farm in transactions.

 Copyright © Huawei Device Co., Ltd.

7 AppGallery and App Security

7.1 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.



7.2 Developer Identity Verification

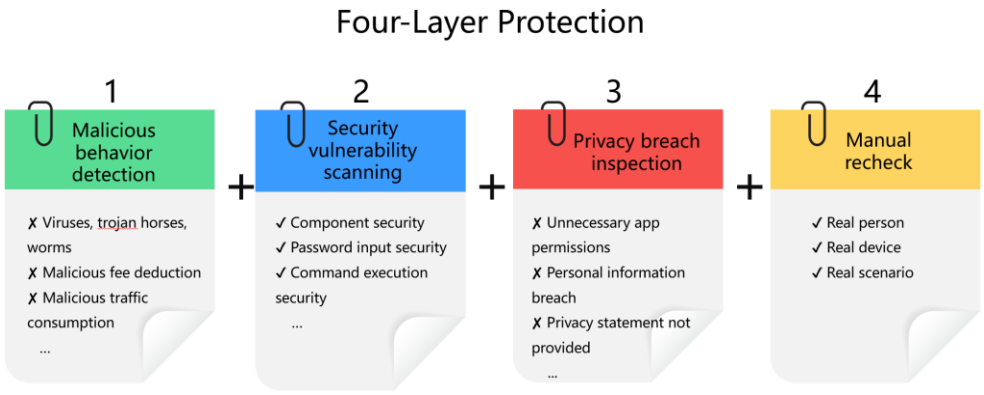
To safeguard users' information and rights, we strictly review the qualifications of developers. Individual developers must provide valid identity information; enterprise developers must provide their original business licenses, scanned copies of their business licenses, and photos of their legal representatives' ID cards to prove their identities from a legal standpoint. This ensures that developers of apps that perform malicious behavior can be effectively traced.

 Copyright © Huawei Device Co., Ltd.

7.3 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.

AppGallery periodically performs tests to ensure that the personal data generated by listed apps has not been exposed to potential threats (such as Trojan horses) that may cause user data leakage. In addition, all apps listed on AppGallery must ensure that users' sensitive data will not be processed outside of their devices, and that they comply with all relevant laws and regulations.



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.

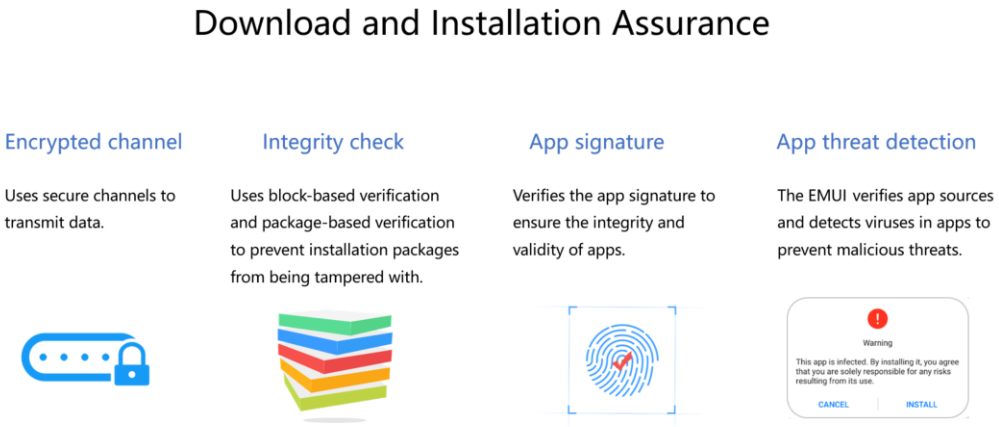
Security vulnerability scanning: HUAWEI AppGallery scans security vulnerabilities in static and dynamic modes. Static vulnerability analysis enables static scanning and analysis of APKs for potential vulnerabilities. It detects the security of components and data, excessive traffic consumption, insecure 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: The inspection includes static and dynamic privacy analysis. Static privacy analysis uses data flow tracking technologies, 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.

 Copyright © Huawei Device Co., Ltd.

Manual recheck: All apps to be launched on 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 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.

7.4 Download and Installation Assurance



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 HarmonyOS. 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.

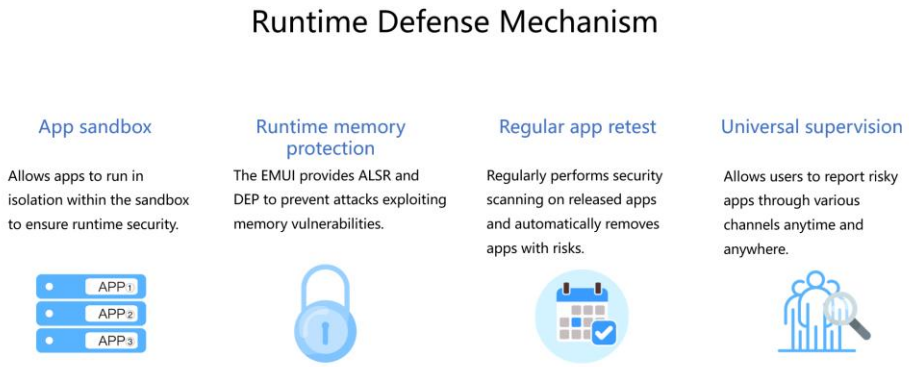
Threat detection: Security risks may exist in apps due to unknown third parties, and downloading apps from unverified sources may bring with them malicious security threats. It is recommended that default security settings be retained to prevent unnecessary risks. HarmonyOS has an industry-leading built-in 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: HarmonyOS provides an AI computing platform for device security protection. It has a built-in industry-leading AI antivirus engine encompassing

 Copyright © Huawei Device Co., Ltd.

a security defense-oriented AI model that is built upon deep learning and training. HarmonyOS 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.)

7.5 Runtime Defense Mechanism



App sandbox: HarmonyOS 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. HarmonyOS 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.

 Copyright © Huawei Device Co., Ltd.

7.6 Age Rating of Apps

Requirements on the age rating of apps vary depending on the country or region. HUAWEI AppGallery provides age rating solutions in compliance with local requirements.

Apps on 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 their age.

7.7 Security of Quick Apps

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

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 update 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 information 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.

7.8 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.

 Copyright © Huawei Device Co., Ltd.

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.

 Copyright © Huawei Device Co., Ltd.

8 HMS Core (Developer Kits)

8.1 HMS Core Framework

HMS Core complies with privacy laws and regulations such as the General Data Protection Regulation (GDPR), and provides unified privacy protection specifications for open 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, as well as isolation of data among different developers.

In services in which Huawei acts as a data controller, such as in Account Kit and IAP, 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 information, including downloading personal information 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 flow, 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 Core, a developer should first register as a Huawei developer and apply for the required open capabilities. The HMS Core framework provides developers with the registration, open capability application, open capability access credential setting, and cloud-based open capability token generation and verification capabilities. This framework uses the Advanced Encryption Standard (AES) algorithm to encrypt and store developers' registered personal information, such as their identity and bank account information.

HMS Core kits can be released with HMS Core (APK), or be independently released and dynamically loaded by HMS Core (APK). HMS Core (APK) that contains HMS Core kits of a new version is launched on HUAWEI AppGallery. Users can decide whether to update HMS Core (APK), and HMS Core (APK) can be updated only with users' prior authorization. If HMS Core (APK) is updated, its signature will be verified. An overwrite installation is allowed only after the signature verification is successful. If an HMS Core kit is independently released on HUAWEI AppGallery, the HMS Core framework downloads and updates the kit. The HMS Core framework verifies

 Copyright © Huawei Device Co., Ltd.

whether the signing certificate fingerprint of the kit is added to the trustlist prior to an update. If not, the kit cannot be loaded. If the fingerprint is in the trustlist, the APK signature is verified. An overwrite update is allowed only after the signature verification is successful.

8.1.1 Authentication Credentials

Before accessing HMS Core's open capabilities, developers need to create authentication credentials on the HUAWEI Developers website. Developer apps can access the open capabilities with authentication credentials. Currently, supported credentials are API key, OAuth 2.0 client ID, and service account key.

The API key, OAuth 2.0 client ID, and OAuth 2.0 client secret are generated using secure random numbers, encrypted using AES-GCM, and stored on the server to prevent from leakage. The public key of a 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 Core's open capabilities to access public resources. For example, a developer can use an API key to access Site Kit and Map Kit.

   Developers can set usage restrictions on an API key, including app and API restrictions. App restrictions allow only specified websites or apps to use this API key, and API restrictions specify the enabled APIs that this key can call.

2. OAuth 2.0 client ID: When a developer app needs to access an HMS Core capability that requires sign-in with a HUAWEI ID, the app can use Account Kit to obtain an access token via OAuth 2.0 after user authorization. The app can then access HMS Core capabilities involving HUAWEI ID through the access token. For example, a developer app uses an OAuth 2.0 client ID and secret to access Drive Kit and Health Kit.

   Developer apps, mobile or web, can access HMS Core services. After obtaining an authorization code for user sign-in, a developer app sends the authorization code and client ID/client secret to the Account Kit server through the developer server to obtain the access token. When an Android mobile app accesses HMS Core capabilities, HMS Core can authenticate the app based on the developer-configured APK certificate fingerprint and client ID 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 a 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 open capabilities of the HMS Core server through the access token. For example, a developer app uses a service account key to access Nearby Service.

8.1.2 Security Sandbox

The security sandbox for HMS Core kits is built on various technologies for security isolation at the system level and the virtual container technologies. A kit running in the sandbox has a completely isolated file namespace, and any request from the kit for the system resources (including the network, external storage, location, contact, and recording) is forcibly authenticated. Thanks to the security sandbox mechanism, impacts brought by faults or vulnerability exploitations on a kit are isolated and mitigated, strengthening the security of HMS Core.

 Copyright © Huawei Device Co., Ltd.

8.1.3 Service DR

HMS Core servers are deployed in multi-site disaster recovery (DR) mode. The database is deployed in active-standby mode, and data is periodically synchronized from the active database to the standby database. Dedicated lines are used to safeguard the data transmission between the production site and DR site. During a DR failover of the HMS Core server, domain name service (DNS) is used to switch service traffic to the DR site. DR drills are regularly conducted to ensure availability of the DR site.

8.2 Account Kit

8.2.1 Authorized Sign-In

Account Kit enables users to sign 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 user can sign in to apps using the HUAWEI ID.

Account Kit complies with international standards and protocols such as OAuth 2.0 and OpenID Connect. By leveraging HUAWEI ID's security capabilities, it also supports identity verification by password or SMS 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 sign-in to a third-party app, only user-authorized account information is shared with the user's prior consent. The user can cancel sign-in authorization at any time in the account center. Authorization is on a per-OpenID basis for isolation among apps.

8.2.2 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 integrated with 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 has a HUAWEI ID signed in, through the risk status synchronization API to enable the developer app to promptly respond to the issue.

8.3 Push Kit

Push Kit is a messaging service provided for developers to establish a cloud-to-device messaging channel and quickly notify their users of the latest information. This helps the developers maintain closer ties with users and increases user awareness of and engagement with developers' apps.

 Copyright © Huawei Device Co., Ltd.

Push Kit provides precise messaging for developers. Each app is assigned a different AAID for data isolation among apps. Once messages are successfully sent, Huawei will immediately delete the messages.

8.3.1 Identity Authentication

When a developer app applies for a push token during runtime, the HMS Core framework verifies the app ID and APK signing certificate fingerprint. After the verification is successful, and the certificate of the Push Kit server 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 developer app ID and secure random number, which are encrypted and stored on the Push Kit server.

To send a message to the app through the Push Kit server API, the developer needs to use the client ID and secret (that is, app ID and secret) to obtain an access token. The Push Kit server will authenticate the messaging request via the access token, and check whether the app ID in the push token matches that in the access token. If so, the message will be sent; otherwise, the message will be discarded.

8.3.2 Message Protection

An app can obtain messages sent by 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. The app can read the messages only after it passes the identity verification. If the app does not obtain the messages in a timely manner, Push Kit will encrypt the messages and store them in a private directory.

When an app sends a subscription message to the Push Kit server through the Push Kit client, HMS Core will check whether the app is able to send such a message. If so, the Push Kit client will use the key negotiated with the server to generate a message verification code for the subscription message through HMAC-SHA256, and the server will verify the message verification code to ensure that the subscription message has not been tampered with.

The Push Kit server will send the message after confirming that the message complies with applicable laws and regulations.

8.3.3 Secure Message Transmission

The Push Kit client and server use TLS to safeguard messages 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.

8.4 IAP

IAP is available for global developers and provides unified and simple offering management, offering ordering and purchase, and service delivery capabilities for developers.

 Copyright © Huawei Device Co., Ltd.

8.4.1 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.

8.4.2 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.

8.4.3 Prevention Against 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.

8.4.4 Fingerprint/Facial Recognition-based Payment

IAP delivers a secure and convenient payment experience via fingerprint/facial recognition. IAP does not collect or process the data of users' fingerprints/faces. A user completes fingerprint or face authentication on their mobile phone locally, and authorizes IAP to use the user-level private payment key to sign the payment data. Then, the IAP server verifies the signature via its server-side APIs, to ensure the payment has been authorized by the user, and finally completes the payment.

8.4.5 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.

8.5 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.

To protect user privacy, Ads Kit does 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

 Copyright © Huawei Device Co., Ltd.

information, each user group contains no fewer than 5000 users. If a user enables the **Disable personalized ads** setting, all vendors including Huawei 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.

8.5.1 High-Quality Ad Choices

Ads Kit aims to provide users with high-quality ad choices and to continuously enhance the machine-based 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 SHA-256 digest of ad images and videos to be displayed. The digest and ad images and videos are transmitted through two different service flows using HTTPS encrypted connections, and the digest is verified in the Ads SDK, which ensures that ad content will not be tampered with during transmission.

8.5.2 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-cheating system uses AI technologies to analyze data integrity, blocklist and trustlist, data association and reasonableness, user behavior reasonableness, and blocking policies to identify cheating behavior.

8.5.3 Data Security

The Ads SDK provides developers with user data storage protection. All user data on users' devices is stored in a private directory of HMS Core, among which the important data is encrypted. This provides developers with an OS-based private data isolation mechanism and ensures that data of 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 information and important system data (such as IMEIs and third-party tracking URLs) 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 the server of a third-party ad platform, third-party tracking service, or media app, Ads Kit uses the pre-shared key mechanism and HTTPS encrypted channel to ensure identity validity and data transmission security.

8.6 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 they use the apps, including photos, videos, and documents in HUAWEI Drive, as well as to 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 sign in to an app integrated with Drive Kit. This token ensures that a user's private files stored in

 Copyright © Huawei Device Co., Ltd.

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.

8.6.1 Authentication and Authorization

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

8.6.2 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.

8.6.3 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 a hardware security module (HSM).

8.6.4 Active-Active Services and Data DR

Drive Kit is deployed in active-active mode and provides physical DR for data to improve service continuity. The database is deployed in active-standby mode, and data is periodically synchronized from the active database to the standby database. Dedicated lines are used to safeguard the data transmission between the active site and DR site. When services at the active site are unavailable, the service environment of the DR site will be used to provide services.

8.7 Game Service

Game Service allows game apps to provide elaborative scenes, configurations, and network information for the system and enables the system to provide its status information for 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 information regardless of whether the information is stored on user devices, transmitted, or stored on the cloud. Users' personal information can be shared to 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 information in other services dependent on HUAWEI ID.

8.7.1 Data Protection

When processing personal information 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.

 Copyright © Huawei Device Co., Ltd.

Leaderboard, achievement, event, and player statistics are sent to the HMS Core server for storage, and data stored is isolated by app ID. That is, an app can access its own data only by ID.

After game records are uploaded to the HMS Core 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.

8.7.2 User Authorization

If third parties need to use users' personal information, independent explicit user authorization is required. When Game Service attempts to use sensitive permissions of a mobile OS, user authorization is also required.

8.8 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 client ID 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 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.

8.9 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 offers open capabilities using the secure element (SE). Users of an app integrated with this kit can use their mobile phones in place of bank cards or transportation cards for payments on a card reader (bank POS terminal or bus pass reader) that supports NFC. The kit also supports in-app payments, enabling apps to use bank cards added to HUAWEI Wallet for payments.

In addition, users can add card, certificate, coupon, ticket, and pass information generated by apps integrated with the SDK to HUAWEI Wallet for unified

 Copyright © Huawei Device Co., Ltd.

management through HUAWEI Wallet's Card Store, AI Tips, and HUAWEI Push Service.

8.9.1 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.

8.10 Health Kit

Health Kit provides a fitness and health data platform and open capabilities for developers. Developers can integrate the Health 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.

8.10.1 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 type of data cannot be accessed if users have not ticked the required read and write permissions. To ensure the accuracy of important data, additional approval is required when a developer applies for the write permission on healthcare data on the HUAWEI Developers website. When a mobile phone's screen is locked, the user's personal information can be written but cannot be read, preventing user data leakage in the background.

8.10.2 Data Encrypted for Storage

On Huawei mobile phones running EMUI 8.1 or later versions, fitness and health data is encrypted using hardware-level file encryption. 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 can only be written into 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 AES. Each user is assigned an independent data encryption key, which is stored after being encrypted by the KMS system under the protection of an HSM.

8.11 FIDO

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

 Copyright © Huawei Device Co., Ltd.

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.

8.11.1 Local Authentication (BioAuthn)

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

If the system has security issues, an error code will be returned; if the runtime environment is secure, fingerprint authentication or 3D facial authentication will be performed.

EMUI 5 (API level 24) and later versions support fingerprint authentication; EMUI 10 (API level 29) and later versions support facial authentication. Ensure that a device supports these functions prior to use.

8.11.2 FIDO2

FIDO2 provides the following features:

1. Implements Android-based password-free user authentication via a FIDO2-compliant client as well as a platform authenticator for local biometric authentication. The FIDO2 specification includes Client to Authenticator Protocols (CTAP) and W3C WebAuthn.
2. Completes user authentication via communication modes like USB, NFC, and Bluetooth Low Energy (BLE) to communicate with FIDO security key devices.
3. Provides an SDK for Android app developers.
4. Provides web app developers with the WebAuthn JavaScript APIs which are offered via the integration with HUAWEI Browser.
5. Allows use of a mobile phone with the biometric authentication capability to act as the FIDO security key, for seamless user authentication on other devices.
6. Before processing a request, the FIDO2 client calls the **SysIntegrity** API of Safety Detect to check whether the device where the app runs is secure. If the device is secure, the FIDO2 client continues to process the request. Otherwise, the client returns an error indicating that the device has failed the system integrity check.

8.12 WisePlay DRM

WisePlay DRM provides developers with digital copyright protection capabilities at enhanced hardware, 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. Apps use keys to encrypt content, which must be decrypted using the keys before playing.

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

 Copyright © Huawei Device Co., Ltd.

8.12.1 Hardware-Level Secure Runtime Environment

The core module of the WisePlay DRM client runs in the trusted execution environment (TEE) of Huawei mobile phones. The TEE provides a hardware-level secure runtime environment for the WisePlay DRM client and protects the storage and use of confidential data in the WisePlay 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.
4. WisePlay DRM offers the enhanced hardware-level DRM for some chipsets to defend against side-channel attacks.

8.12.2 Secure Video Path

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

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

When users connect their mobile phone to a large-screen device (such as a TV) using a high definition multimedia interface (HDMI) cable and play a video on the large screen, the video is encrypted using the High-bandwidth Digital Content Protection (HDCP) chip, before being transmitted to the large-screen device. In addition, the large-screen device needs to pass the validity authentication.

8.12.3 Secure Clock

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

8.12.4 DRM Certificate Authentication

When the WisePlay DRM client applies for a DRM certificate, the WisePlay DRM server authenticates the client 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 a unique certificate and private key, which can be accessed by authorized apps only.

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

8.12.5 Secure Transmission

The WisePlay DRM server uses the public key of the WisePlay DRM client certificate to encrypt the content key and sends the encrypted content key to the WisePlay DRM client. DRM requests and responses are signed using the certificates of the

 Copyright © Huawei Device Co., Ltd.

WisePlay DRM server and WisePlay DRM client, to ensure that the messages will not be tampered with by man-in-the-middle attacks during transmission.

8.13 ML Kit

ML Kit provides vision and language services for developers based on machine learning technology. Vision services include AI-empowered ones such as text recognition, face detection, image classification, object detection and tracking, landmark recognition, and image segmentation. Language services include speech recognition, language detection, and translation.

8.13.1 Data Processing

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

8.14 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 provides Nearby Connection, Nearby Message, and Contact Shield 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, to 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 server of Nearby Service. 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 server of Nearby Service, 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.

Contact Shield is a basic contact tracing service developed based on the Bluetooth Low Energy (BLE) technology. To use Contact Shield APIs for checking whether a user has been in contact with a person who tested positive for COVID-19, the developer must have obtained authorization from the public health institutions of the countries or regions involved and passed the strict review of Huawei. After a user enables Contact Shield, a dynamic shared code is generated. This code is updated

 Copyright © Huawei Device Co., Ltd.

every 10 minutes and shared via Bluetooth among mobile phones where Contact Shield is enabled. After the public health institution announces a person has tested positive for COVID-19, Contact Shield will notify the user of whether they have been exposed to the confirmed case. Contact Shield will not use users' location information, nor collect or share users' identity information. Users can switch Contact Shield on or off, and manually delete all data records.

8.15 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 notifications, user behavior 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, to protect 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.

8.15.1 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.

8.15.2 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.

8.16 Site Kit

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

It uses the client ID, APK certificate fingerprint, and API key to authenticate developers, and limits calls to prevent the call 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.

 Copyright © Huawei Device Co., Ltd.

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

8.17 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. Using these SDKs, developers can easily integrate map-based functions into their apps to improve user experience.

Map Kit uses the client ID, APK certificate fingerprint, and API key to authenticate developers, and limits calls to prevent the call 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 information 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 the user's location information. In addition, third-party map service suppliers shall follow the same requirements for processing data as Huawei does, to ensure that users' personal information is fully protected.

8.18 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 behavior, 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 about local weather and holidays. HTTPS is used for encrypted transmission, and the approximate location information is neither associated with devices or users, nor is it stored on the cloud.

8.19 Analytics Kit

Analytics Kit is a one-stop data analytics platform for app developers. It provides reference for product optimization and operations for developers based on user behavior 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.

 Copyright © Huawei Device Co., Ltd.

Analytics Kit assigns a unique AAID to each device. 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.

8.19.1 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.

8.19.2 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 both the data and key in ciphertext to the server, preventing malicious attackers from obtaining the data of developer apps.

8.19.3 Server Data Isolation

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

8.20 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.

Developers must comply with all applicable laws and regulations as well as agreements with Huawei when using DTM and processing users' personal information in relation to DTM. Developers must accurately identify platforms that may collect, receive, or use end users' personal information through the use of DTM. Developers must notify end users of these platforms, personal information 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, Huawei may restrict or suspend the use of DTM of the developer. Developers must not upload information that can identify users (such as name, email address, device

 Copyright © Huawei Device Co., Ltd.

identifier, or invoice) to the DTM server. In addition, we may collect and process information about how DTM is used for the purpose of improving and maintaining 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.

8.20.1 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.

8.20.2 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.

8.20.3 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 call DTM.

8.21 Safety Detect

Safety Detect is a multi-dimensional open security detection service from Huawei. It detects system integrity, app security, malicious URLs, fake user accounts, and malicious Wi-Fi networks, helping developers quickly build app security by leveraging the strengths offered by Huawei mobile phones.

System integrity check is only performed on the user device, and raw data on the user device will not be reported to the server. Only the check result is reported to the server for verification and digital signing.

App security check is also only performed locally on the user device, and the list of apps installed on the user device and related apps are not reported to the server.

During URL check, URLs will be reported to the server for security check.

During fake user account detection, users' HUAWEI IDs, device IDs, and IP addresses will be collected. Such information is encrypted and stored only for a necessary period of time and will not be shared to any third party.

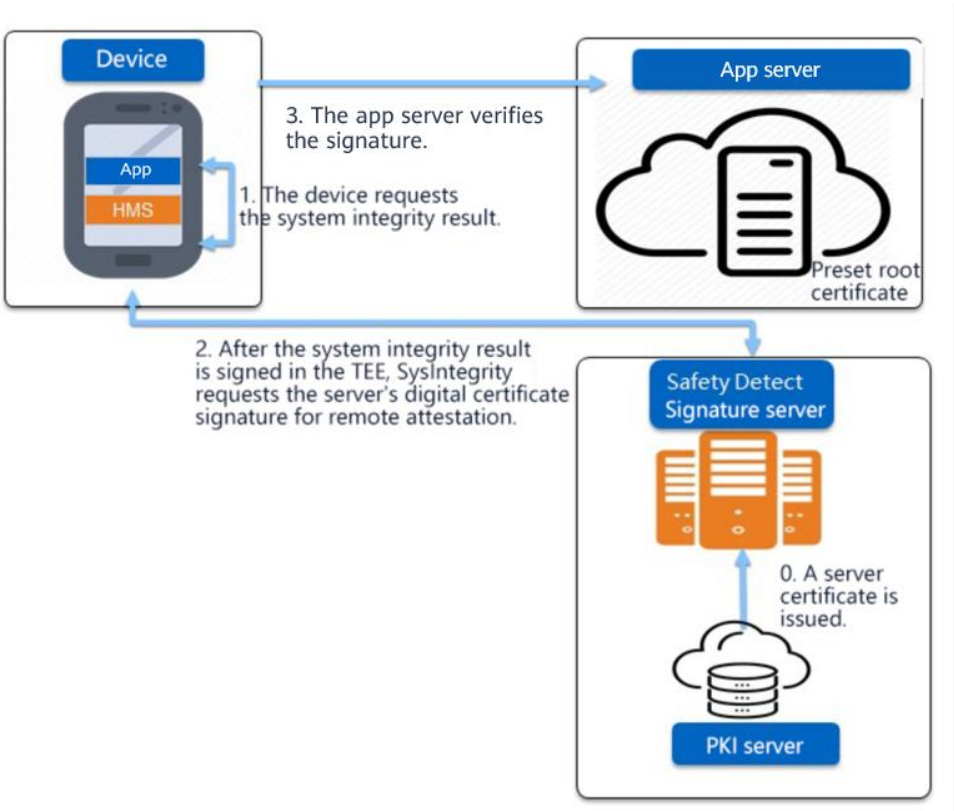
- **SysIntegrity** API: checks whether the device running a developer app is secure (for example, whether it is rooted).
- **AppsCheck** API: obtains a list of malicious apps.
- **URLCheck** API: determines the threat type of a specific URL.
- **UserDetect** API: checks whether an app is interacting with a fake user.
- **WifiDetect** API: checks whether the Wi-Fi to be connected is secure.

 Copyright © Huawei Device Co., Ltd.

8.21.1 SysIntegrity API

The **SysIntegrity** API 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. Developers can preconfigure the Huawei root certificate on their own app servers to verify the digital signatures in the detection results.

When calling the **SysIntegrity** API, developers pass a nonce value, which will be also 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 of Safety Detect contains the nonce value and app ID. The app ID can be obtained during the configuration of the signing certificate fingerprint.



8.21.2 AppsCheck API

This API 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.

8.21.3 URLCheck API

This API 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.

 Copyright © Huawei Device Co., Ltd.

8.21.4 UserDetect API

This API 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.

8.21.5 WifiDetect API

This API checks the characteristics of the Wi-Fi network and router to be connected, analyzes the Wi-Fi network information, and returns the Wi-Fi detection results after classification, safeguarding developers' apps from malicious Wi-Fi networks.

8.22 Search Kit

Search Kit opens up Petal Search capabilities through the device-side SDK and cloud-side APIs, enabling ecosystem partners to quickly provide the best possible mobile app search experience.

This kit authenticates accesses via the app-level client ID. Developers can set API restrictions on client IDs and set a validity period of each access token, to avoid accesses from fake apps.

The Search SDK is loaded to an app during app packaging. It starts when the app is launched and is stopped as soon as the app is closed, without performing any operations in the background.

Search Kit stores only anonymized data — which cannot be used to identify a user — and automatically deletes the data in a maximum of six months.

The collected data is encrypted locally. During reporting, the data is encrypted using HTTPS.

8.23 Keyring

Keyring offers the Credentials Management API for storing user credentials on user devices and sharing them across different apps and platforms, helping developers create a seamless sign-in experience.

8.23.1 Secure Credential Storage

After a user successfully signs in to an app with Keyring integrated, the app calls the Credentials Management API to store the authentication credential of the user in Keyring. Keyring encrypts the credential and stores it on the user's device. When storing credentials, the app developer can set whether to verify the user's biometric features or lock screen password when the app tries to access the stored credentials.

When the user reopens the app, the app can find the available user credential to automatically sign the user in.

 Copyright © Huawei Device Co., Ltd.

8.23.2 Credential Sharing

If multiple apps from a developer share the same account system, the developer can share credentials stored by one app to other apps. In this case, when a user signs in to one app, other apps can sign the user in seamlessly without requesting the user to enter their account details. A developer can also share credentials across their Android app, quick app, and web app.

The developer has complete control over how credentials are shared. When setting the credential sharing relationship, the developer must specify the app identifiers where the credential is shared. More specifically, when configuring the settings for sharing credentials with an Android app or a quick app, the developer should specify the app package name and certificate fingerprint; when configuring the settings for sharing credentials with a web app, the developer should specify the full domain name of the app.

 Copyright © Huawei Device Co., Ltd.

9 Privacy Control

9.1 Privacy Compliance Framework

We take privacy protection as the cornerstone of product design and hold this principle during the entire process of product design, development, operations, and maintenance to continuously optimize product and service experience. In addition, to better meet international privacy compliance requirements, we have built a global privacy compliance framework based on Generally Accepted Privacy Principles (GAPP), (GDPR), and the local laws and regulations of the relevant countries and regions to protect data security for users worldwide.

9.2 Local Deployment

We provide products and services through global resources and servers, and ensure that user data is fully protected in accordance with applicable laws and regulations. If local servers must be deployed and cross-border data transfers are not permitted by local laws, user data will be stored on local servers and under the operations as well as maintenance of locally registered subsidiaries subject to local laws. For example, the personal information of European Union (EU) users are stored on servers in the EU.

9.3 Data Minimization

We only collect the minimum amount of personal information necessary for providing users with products and services. Irrelevant personal information will not be collected. In addition, we have taken reasonable and practical measures to minimize personal information sharing, preventing the abuse of information and reducing the risk of information leakage.

 Copyright © Huawei Device Co., Ltd.

9.4 On-device Data Processing

Owing to the powerful processing capabilities of Huawei devices, data can be retained and preferentially processed on these devices. Users' personal information will not be transferred from their devices unless some functions or services require the processing of data on the cloud.

9.5 Transparency and Controllability

Privacy is a fundamental right of users. We always believe that allowing users to be completely aware of how their personal information will be used and make decisions at their own discretion is the most basic requirement for privacy protection.

Whenever a user uses an app or a new feature of an app for the first time, we explicitly inform them of how the app will collect, use, store, share, and transfer data, and that their data will be processed only after they give explicit consent. In addition, to help users better understand how we process personal information, we have launched privacy tags on HUAWEI AppGallery to present in a clear manner how an app from AppGallery uses personal information.

We provide a one-stop privacy management platform, helping users better manage their personal information and privacy settings. By using the platform, users can obtain copies of their personal information online, rectify/delete their account information, decide whether to grant account access to third-party apps, and set preferences for receiving marketing messages, so as to enjoy a better user experience from Huawei products and services.

9.6 Identity Protection

Our products and services use multiple innovative privacy protection technologies to minimize our or any third party's access to users' personal information, helping users hide their identities to evade network trackers.

For example, we use random identifiers instead of user IDs to associate personal information when cooperating with third parties. Even if such random identifiers are sent to a remote server, they will not be associated with the users. Some of our products and services use differential privacy technology, which generates a digest of users' raw data rather than directly uploading the raw data. This technology adds random noise to the digest so that the data cannot be associated with a specific user. By using the privacy protection technologies, we can optimize relevant services and products without collecting user-related data and protect user identities.

9.7 Data Security Assurance

Safeguarding the security of users' personal information is our key objective for product design.

Users can sign in securely through HUAWEI IDs and benefit from the following capabilities and technologies: (a) data protection capabilities provided by HarmonyOS; (b) security encryption capabilities provided by the SE and TEE; (c) industry-leading data protection technologies during service processing and data

 Copyright © Huawei Device Co., Ltd.

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.

We protect user data from unauthorized access and tampering regardless of whether the data is stored on the cloud or transmitted over the network.

9.8 Obligations of a Data Processor

HMS Core provides services like Analytics Kit and Push Kit for developers. In these services, developers determine the purposes of data processing and how the data will be used. We act as the data processor that collects and processes personal data on behalf of developers.

We sign data processing agreements (DPAs) with developers to specify the rights and obligations of the data processor, namely us, and developers. We process personal data only in accordance with the DPAs and developer's instructions, and do not process personal data for Huawei's purposes. For data processing activities that need to be subcontracted, only suppliers (sub-processors) that provide an adequate level of technical and organizational measures and guarantees are used. The subcontracting of suppliers requires prior written authorization from developers.

As the data processor, we assist developers in responding to the requests for exercising the rights of data subjects (end users) and comply with requirements regarding personal data processing, data breach notifications, data protection impact assessments, and prior consultation. We will delete or return personal data once the cooperation with the developers ends. We will also provide developers with information to demonstrate our compliance with the processor's obligations and provide audit/inspection channels.

9.9 Protection of Minors

For minors who use HMS, we take additional measures to protect their privacy and data security. We offer the child account that is specifically tailored for children. When a child account is created and signed in to, our products and services will automatically enable kids mode. This mode filters content based on the child's age and blocks content such as comments, web recommendations, and direct marketing, to intelligently prevent negative influences and guide them towards being a rational consumer.

We provide customized content classifications and ratings for minors based on their ages to ensure that content shown to minors is appropriate. For example, HUAWEI Video offers modes for children, teenagers, and adults respectively. Minors only have access to the content suitable for their ages.

We collect minors' personal information only after obtaining the consent of their guardians, and use or disclose the information only when permitted by law, explicitly consented by the guardians, or necessary for the protection of minors. Guardians have the right to access, rectify, or delete minors' personal information at any time. For details, please refer to the privacy notice or supplementary statement of the specific product and service.

 Copyright © Huawei Device Co., Ltd.

10 Security & Privacy Certifications and Compliance

10.1 ISO/IEC 27001 and 27018 Certifications

ISO/IEC 27001 is an internationally recognized and widely used standard for information security management systems. This certification indicates that 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 that information security risks are properly controlled and correctly handled. HMS first obtained this certification in January 2016, it was annually reviewed afterwards, and the certificate was renewed in 2019. This certificate has been recognized by ANAB and UKAS.

ISO/IEC 27018 is an international code of practice that focuses on personal data protection on the cloud. It is based on ISO 27002 and provides guidelines for implementing the ISO 27002 controls 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 and was annually reviewed afterwards.

10.2 ISO/IEC 27701 Certification

ISO/IEC 27701 provides a comprehensive set of personal data processing methods and a privacy information management framework from multiple aspects, such as organizational governance, legal compliance, process specifications, information technology, as well as supervision and auditing. This certification indicates that an enterprise has a comprehensive personal information protection management system in place in terms of design, R&D, operations, and maintenance phases and is in a leading position globally regarding personal information security management, transparency, and privacy compliance, among others. HMS is in the first batch of the industry products to have obtained this certification in November 2019 and was annually reviewed afterwards. The certificate has been recognized by ANAB.

Copyright © Huawei Device Co., Ltd.

10.3 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 it was annually reviewed afterwards. In 2019 when renewing the certificate, HMS was awarded with a Gold rating.

10.4 CC Certification

Common Criteria (CC) certification is a product information security certification recognized in 31 countries and regions, and encompasses seven levels (EAL1 to EAL7). A higher level indicates a stricter review process and, consequently, tighter product security.

Huawei's TEE OS 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 mobile phone users during app use is properly protected.

10.5 PCI DSS Certification

Payment Card Industry Data Security Standard (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 and it was annually reviewed afterwards.

10.6 EuroPriSe Certification for HUAWEI ID

In January 2020, the European Privacy Seal (EuroPriSe) granted the EuroPriSe seal to Aspiegel SE (formerly 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). 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 scheme provides transparent procedures and reliable criteria.

Copyright © Huawei Device Co., Ltd.

10.7 ePrivacyseal Certification

ePrivacyseal is an authoritative European privacy certification that covers the requirements of the GDPR for digital products. The catalog of criteria for certification has been constantly adapting to the interpretation of the GDPR and other data protection laws. ePrivacyseal assesses both legal and technical aspects of an object to ensure its secure and visible compliance with the GDPR, thereby protecting consumer privacy. Our products and services for the EEA area, such as HUAWEI Ads, Petal Search, AppGallery, HUAWEI ID, and AppGallery Connect, were all certified by ePrivacyseal GmbH in July 2020.

Copyright © Huawei Device Co., Ltd.

11 Oriented Future

11.1 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 scenario. 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 a 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.

 Copyright © Huawei Device Co., Ltd.

11.2 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 advanced 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 opening HMS Core security capabilities, HMS continuously enhances services such as SysIntegrity (system integrity check), AppsCheck (app security check), URLCheck (malicious URL check), and UserDetect (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.

11.3 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.

 Copyright © Huawei Device Co., Ltd.

12 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 specify 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.

 Copyright © Huawei Device Co., Ltd.

ARM	Advanced RISC Machines	A 32-bit reduced instruction set computer (RISC) processor architecture.
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 attack	Challenge Collapsar attack	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 around the world, 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 signed in to a web app to execute undesired operations on the app.
CVV	Card verification value	A code on the back of a credit card or debt card.
DBF	Database Firewall	A database security protection system based on database protocol analysis and control technology.
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	A block algorithm used to encrypt keys.

 Copyright © Huawei Device Co., Ltd.

	Standard	
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	Offers a dynamic tag management system that helps developers quickly configure and update tracking tags and related code snippets on a web-based UI. They can then track specific events and report data to third-party analytics platforms, monitoring their marketing data as needed.
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.
FIPS	Federal Information Processing Standards	A set of standards used by American government agencies for automated data processing and remote communications.
GCM	Galois/Counter Mode	A mode of operation for symmetric-key cryptographic block ciphers.
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.
HarmonyOS	HarmonyOS	A next-generation OS for smart devices.
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.

 Copyright © Huawei Device Co., Ltd.

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 operations of the system.
HMS	Huawei Mobile Services	A collection of open 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.
IDS/IPS	Intrusion detection system/Intrusion prevention system	IDS: a network security device that monitors network transmissions in real time and generates alerts or takes proactive measures when detecting suspicious transmissions. IPS: a computer network security device that monitors the network information transmission behavior of a network or network devices. It can interrupt, adjust, or isolate abnormal or harmful network information transmission behavior in a timely manner.
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.
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.

 Copyright © Huawei Device Co., Ltd.

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.
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 monitor 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.
RSA	Rivest-Shamir-Adleman	A cryptosystem that uses various encryption and decryption keys to ensure that it is computationally impossible to deduce decryption keys from the known encryption keys.
SD	Secure Digital 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.
SHA	Secure Hash Algorithm	An 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	IC card held by a mobile user in the GSM

	module	system.
SSL	Secure 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.
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.
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.

 Copyright © Huawei Device Co., Ltd.