Hikvision Access Control Product Security White Paper

www.hikvision.com

About this Document

Hikvision Access Control Product Security White Paper (hereinafter referred to as "the White Paper" or "the document") aims to give an overview on security strategies of Hikvision access control products with an open and transparent manner, allowing our users to have a deep insight on Hikvision's excellent abilities in terms of product security.

The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***).

Copyright

Trademarks Acknowledgment

海康威视, HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". OUR COMPANY MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION,

MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE.

NO WARRANTIES TO THE PRECISION OF THE DOCUMENT IS MADE. THE INFORMATION CONTAINED IN THE DOCUMENT IS SUBJECT TO RECTIFY OR EDIT WITHOUT NOTICE.

THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL OUR COMPANY BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF OUR COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Revision History

The first version was released in November 2024.

About Hikvision

Hikvision, founded in 2001, is a technology enterprise with a focus on technology innovation.

We stay committee to follow the business philosophy of "Professional, Honest, and Reliable", and live up to the core values of "meeting customers' needs, rooting in enterprise values, honest and pragmatic, and being excellence". For more than two decades, based on video technology, we have gradually built and developed the Artificial Internet of Things (AIoT) technology with IoT perception, artificial intelligence and big data technology as its core, providing products and services in terms of security and digital scenes for all industries and sectors.

By the end of 2023, there have been 58,544 employees in Hikvision, including 28,479 R&D staffs and technical service providers. The absolute amount invested in R&D in 2023 accounted for 12.75% of the annual income, ranking it forefront in the industry. Hikvision also serves as a postdoctoral program workstation. In addition to the R&D center in the headquarters in Hangzhou, multiple local centers have been established at home and abroad, forming a multi-level R&D system with the headquarters as the center and coordinate with regional branches.

By the end of 2023, 32 province-level service centers and over 300 branches and offices of Hikvision have been set up in Chinese mainland, and 80 branches, subsidiaries and offices have been set up in Hong Kong China, Macao China,

Taiwan China and abroad, all together providing products and services for customers from more than 150 countries and areas, and playing significant roles in major projects and events including the 19th Asian Games, the 11th G20 Summit, 2008 Beijing Olympics, Expo 2010 Shanghai China, the Annual APEC Economic Leaders' Meeting, Beijing Daxing International Airport, Hong Kong China-Zhuhai-Macao China Bridge, etc.

Hikvision listed in Shenzhen Stock Exchange in May 2010. Stock code: 002415. Thanks to the innovative management mode, together with excellent operating performance, Hikvision has been awarded with significant honors, including being selected in the 2024 China Quality Award nomination list, winning the Responsibility Model Award of 2023 Yicai the Corporate Social Responsibility Ranking in China, and ranked top 20 among 2023 Zhaopin Best Employers, etc.

Hikvision works to provide services of IoT perception, artificial intelligence and big data technologies for all industries and sectors, leading a new future of IoT; create better linkage between persons and things with comprehensive perception technologies, building the foundation of the intelligent world; observe and meet multiple demands of the market with diverse intelligent products, making them accessible to all people; build an intelligent world characterized by convenience, high-efficiency and security with advanced IoT applications, delivering a bright future to all persons.

Table of Contents

1 Access Control System Security Analysis

Through the advancement for several decades, access control system has developed from mechanical door locks to electronic door locks, then to today's intelligent access control system. The technology is increasingly mature and the function is constantly improving, all together facilitating people's daily life to a great extent. Despite providing safe and convenient services, however, access control system is threatening by potential risks at the same time, such as channel eavesdropping, biological information forgery, etc. The threats have post serious challenges for the security of access control system.

Access control system consists of the management terminal software, controller, recognition terminal, PIN and peripheral devices. Given the devices of the system are intricate and numerous, they might be invaded by security threats at all stages from construction to use. Based on the application architecture, these security threats can be divided into three types: perception-layer threats, transport-layer threats, and application-layer threats.

1.1 Perception-Layer Threats

- Physical Attack

The access control device deployed remotely without physical security control might be stolen or destroyed. The machine API might be illegally accessed for it is on the surface of the device without any protection.

The access control devices tend to be destroyed or cheated by fake identities as they are deployed outdoors in a widely scattered manner, making them easy to access and hard to manage, being accessible and without effective management.

- Data Leakage

The sensitive information leakage might occur When the access control device collects and processes data without encrypting the data or limiting the access permission.

- Illegally Access

The access control device that can be accessed without authentication, or is authenticated with a weak password, or the authentication mechanism is bypassed.

The debugging API is retained, with which the Internet attacker can obtain the running information of the device.

- Data Forgery

The core of access control system, identity authentication mechanism, confirms the user's identification based on the identity credential. With the rapid development of technology, however, numerous data forgery technologies such as IC card duplicating, fingerprint forgery and face picture simulation have emerged. Illegal invasion and mis-authentication might occur if relative protection and precaution measures are not taken on the access control system.

1.2 Transport-Layer Threats

- Network Attack

As the defects exist in network protocol, access-side leakage might occur if there is no valid authentication.

Man-in-the-middle attacks such as duress, replaying, tampering and eavesdropping might occur if the communication has not been encrypted.

- Data Leakage

Attacker can steal sensitive information by eavesdropping transmission channels if the control command and collected data have not been encrypted when communicating or transmitting via devices, cloud and mobile applications.

- Data Tampering

Attacker might tamper the control command and collected data if the integrity verification has not been performed on the network-transmitted data when devices communicate on network.

1.3 Application-Layer Threats

- Device Management

As the devices managed by application layer are scattered and varied, their upgrading and security status of are difficult to manage.

- Unauthorized Operation

Important data might be leaked due to unauthorized operation for the application layer permission management is not perfect.

- System Vulnerability

Logical defects or mistakes exist in application software or operating system software of access control devices, allowing attacker to implant Trojan virus, which causes the device to fail to run normally.

- Data Leakage

Data leakage might occur if the numerous data managed by application layer has not been encrypted, or the access permission to the data has not been limited.

- Configuration Vulnerability

Security vulnerabilities might occur if the application, framework, container, operating system, etc. have not been configured appropriately (such as using the version with security defects, giving too much permissions to some accounts, has not limited the access to sensitive resources etc.), allowing attacker to obtain important data illegally.

Considering potential security risks in IoT environment, combining with the complexity of access control devices in terms of software/hardware environment and the computing power, Hikvision works to create a fire-new security architecture and build a multidimensional security system to fully guarantee terminal security, data security, application security, network security, personal information, and safety compliance.

2 Access Control System Architecture

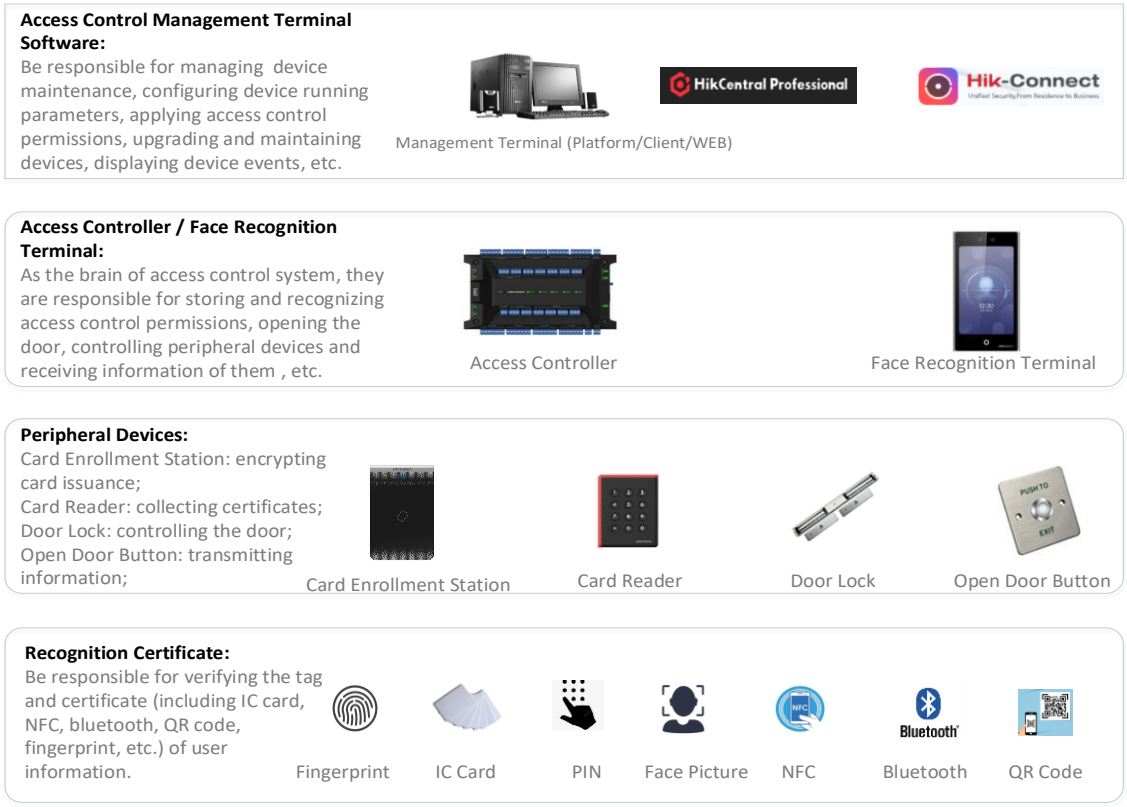


Fig 2-1 Hikvision Access Control System Framework Diagram

As shown in Fig 2-1, Hikvision access control system consists of four parts: terminal management software, access controller, peripheral devices, and recognition credential. The management software assumes key functions like visualization management of user information and device maintenance; the controller is the core of the system and is responsible for performing critical tasks such as identity authentication, permission control and door locks operation; peripheral devices, including card reader and door locks, are responsible for collecting information and opening the doors; PIN is the key to verify users' identifications.

Hikvision has adopted diverse security technology strategies to ensure the communication security among the four parts and the compliance.

3 Security Procedure

Combining our extensive R&D activities and referencing best security practices (such as OpenSAMM, BSIMM, CSDL, MSDL, and customers' feedback) of the industry, Hikvision has developed the Hikvision Security Development Maturity Model (HSDMM). This model quantifies security activities in product security development and ensures their effective implementation through a well-established organization structure, standardized security development management processes, and robust technical means. The HSDMM aims to enhance the confidentiality, integrity, and availability of products, strengthen personal information protection, and provide customers with more secure products and solutions.

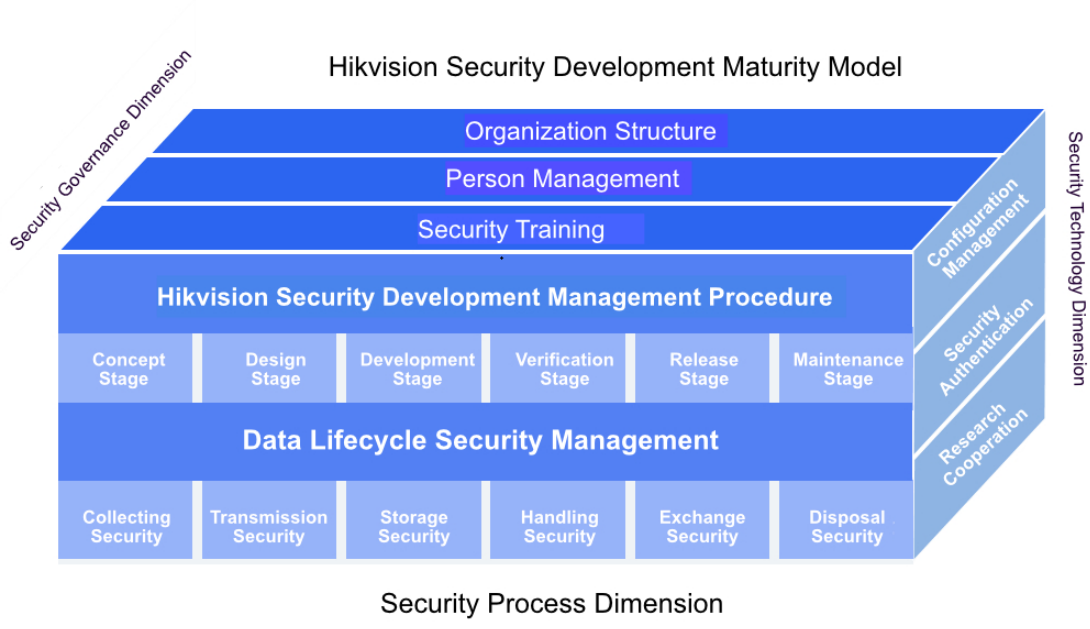


Fig 3-1 Hikvision Security Development Maturity Model

See details in Cybersecurity White Paper released by Hikvision: https://www.hikvision.com/cn/support/CybersecurityCenter/SecurityNotices/2023-07/

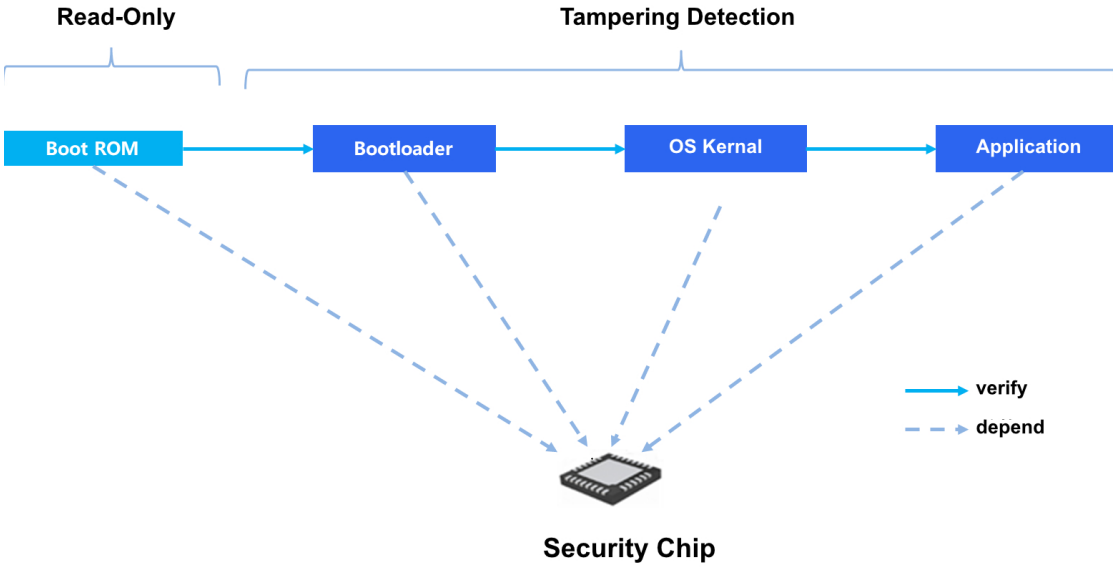
4 Security Process

4.1 Terminal Security

Secure Boot

Secure boot is the basis of terminal security. The code of secure boot is solidified in the chip so that the initial loading logic cannot be tampered. The device will execute the boot code in Boot ROM immediately upon startup. Boot ROM uses the public key of Hikvision firmware signature to check if the bottom-level Bootloader has been signed, then decides whether to allow it to load. The components involved in each step of the startup process have been digitally signed to ensure the integrity. Each step can be taken normally only after being verified, then the secure boot chain can be formed. Programs engaged in the startup process include Bootloader, kernel, application, etc. It can be ensured that the software cannot be tampered with the secure boot chain.

The startup process will be canceled if either step fails to be loaded or fails to be verified. Then the device cannot run normally.


Read-Only
Tampering Detection
Boot ROM
Bootloader
OS Kernal
Application
verify
depend
Security Chip

Application Upgrading and Protection

Guidance program, together with application program, is adopted in all mounting programs of Hikvision access control devices. Upgrading the application program is supported after the device leaving the factory.

- Invalid Upgrade Package Verification

The application upgrade package will be verified by the device before upgrading. Upgrading invalid upgrade package is not allowed.

- Upgrading Exception Protection

The upgrade of application will be canceled and the application will rollback to the previous version automatically if exception occurred (such as network outage, power off, etc.) during the process.

Data Backup

- Access Control Management Terminal Software Backup

Auto backup of data file is enabled in data server of resource management terminal. Users can restore the terminal data via restoring backup file if data exception occurred.

Hot backup is supported in resource management terminal. If main data server goes down, the system can still run normally with backup data server.

- Device Storage Backup

Device running profile and user information are stored in access control device. The file will be upgraded when managing access control users and configuring device running parameters on access control management terminal. Before editing the file, the device will create a backup in the memory. Device will read backup file by default and restore the storage if the source file is destroyed, and at the same time exception occurred (such as network outage, power off, etc.) during file upgrading.

Intrusion Detection

1、Security Network Service

All types of management protocols of various access control devices of Hikvision are disabled by default. Security protocol version is supported to reduce threats to devices.

- Telnet service is not supported.
- SFTP service is supported; FTP service is not supported.
- SSH service is disabled by default.
- SNMP service is disabled by default; secure SNMPv3 is supported.
- NTP service is disabled by default.
- UPNP service is disabled by default.

2、Interface Security

All products of Hikvision released to the public enable Interfaces directly related to customers' needs by default, and other interfaces are disabled. Information such as openable interfaces, service functions and authentication mode corresponding to interfaces, whether the interface is enabled by default, etc. are displayed in product communication matrix for customers to read and adjust accordingly.

3、 Lock Mechanism

Only permitted users can access to Hikvision access control devices, and all unauthorized access IP addresses will be recorded in the device. Given that the access times are limited, the IP address that has reached the limit is not allowed to access the device if the identification failed to be verified, thus preventing forced cracking.

4.2 Transmission Security

Network Transmission Security

Hikvision access control device and access control management terminal software have applied TLS1.2 of HTTPS communication protocol to provide secure transmission channel, AES 128/256 encryption algorithm, RSA 2048 secret key interactive algorithm in access controller products, and SHA 256 digest algorithm.

Read-Terminal Data Transmission Security

OSDP is an open access control communication standard applied by Security Industry Association (SIA) to enhance the interoperability between access control and secure products. OSDP protocol communication (version V2 or later) and communication data encryption (AES 128 encryption algorithm is applied) are supported in Hikvision access controller / all-in-one terminal and access control card reader.

Web Security

Comprehensive protective measures of web system have been taken by Hikvision to guarantee all-round security for users. Those measures include but not limited to:

- Verifying all data from untrusted data source on the server. Any data that fails to be verified will be rejected. If the data outputted to client is from untrusted data source, it will be encoded or escaped correspondingly.
- Performing strong verification on user access/operation permission to prevent landscape/vertical ultra vires.
- Check if the key information such as the type, format, content and size of uploaded file is valid so as to prevent malicious file from being uploaded.
- Encrypting sensitive information and controlling data permission to prevent unauthorized access and information leakage.

- Recognizing the source and detecting the content of requests accepted by the server to prevent all types of request forgery attack.

- Auditing web container configuration according to different application scenarios based on security configuration baseline to ensure configuration security.

- The session ID of web application is random and unique. It will be changed when authentication succeed so as to prevent session fixation.

- Auto disconnect timeout session: session timeout threshold can be set. It will be rolled back to login status and re-authentication of identity is required if there is no operation within the timeout threshold.

- Limit the session No.: the session No. can be set. The number of concurrent sessions can be limited to prevent illegal access.

- Lock the session: if the number of failed authentication attempts of a user exceeds the predetermined authentication number, his/her subsequent attempts will be auto locked so as to prevent forced cracking. Allowed failed attempts can be set.

- Session locked duration: the session locked duration can be set. The locked duration when authentication attempt exceeds the limit can be set by users themselves so as to provide better experience for them on a secure basis.

4.3 Storage Security

User data and logs of Hikvision access control devices are stored in non-volatile memory to ensure data persistence and security. Before stored in the memory, user data has been desensitized by the device so as to protect user privacy. Device data cannot be accessed in any way other than through the authorized API to prevent data leakage. To ensure data security, different secret keys have been applied to encrypt data according to different application scenarios. The encryption mode is AES 128/256.

- Secret Key Management

The secret key of device adopts a layered architecture and is stored in hardware secure zone. In general, there are three layers in secret key architecture: service key is protected by key-encrypting key, and key-encrypting key is protected by master key at the same time. Based on its purpose, service key can be divided into file key, data encryption key, etc. Secret key architecture can be trimmed or enriched in different application scenarios. At least two layers are required in secret architecture.

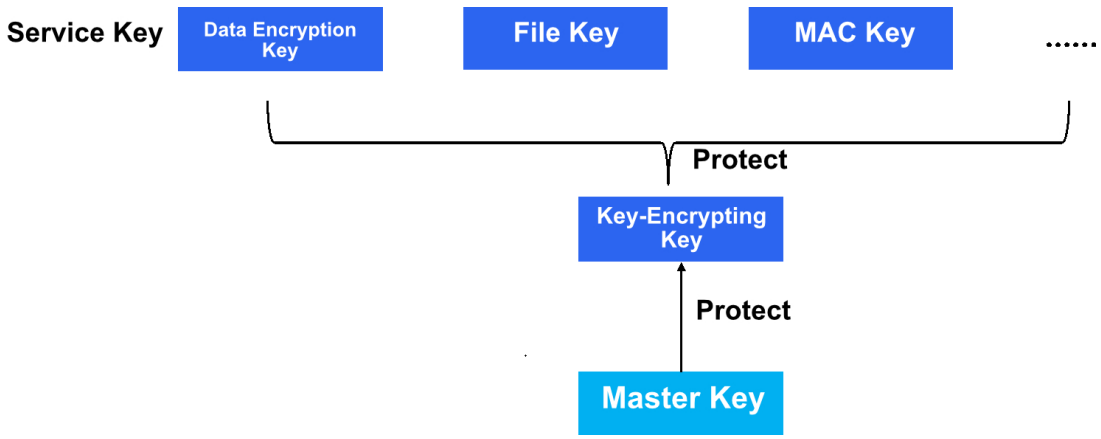


Fig 4-1 Secret Key Architecture

4.4 Data Security

Password Security

- Password Generation

Password need to be entered manually. It should contain at least 8 characters, and at least 2 types of the following characters should be contained: digits, lowercase letters, uppercase letters, and special characters. Users are required to set passwords that meet the security standard to replace the default password when activating the device.

- Password Storage

User's original password will not be stored in the device. The password entered when activating the device will be hashed based on the secure random generated by the device, then it will be allowed to be transmitted, stored and authenticated by the device.

- Password Transmission

HTTPS protocol has been adopted in network transmission so as to ensure the security of user data.

- Password Authentication

Invalid login attempts are monitored, and the account will be locked if multiple login failed so as to prevent brute force attack. Setting the maximum consecutive failed login attempts and the lock duration are supported.

- Password Destruction

Original password will be destroyed when user changes the password, and user password will be destroyed when the device is restored to factory settings.

Certificate Security

1、Person Data

Person management is the core element of access control system. To ensure the security of user information, Hikvision access control devices have stored all user information in non-volatile memory. In this way, the critical data can remain integral even during power outages or system failures.

- Person Data Application

Person data is inputted on the platform software by the user in accordance with local laws and regulations. Sensitive user information in person data, such as employee ID and PIN, will be desensitized by the platform when transmitted from the platform to the device (see 4.2 *Transmission Security*) so as to prevent it from being captured during transmission. In addition, an exception warning mechanism has been established on the device and platform. If person data fails to be applied, the cause of the exception can be displayed on the platform.

During the process of person data application, access control device will perform protection on the stored data to prevent it from being corrupted by exceptions such as power outage, network outage, etc.

- Duplicate Person Data Filtering

The employee ID of the user is the only identity in person data stored in the device. Applying or storing duplicate employee ID is not allowed.

- Privacy Configuration of Person Recognition Visualization Results

During the process of person recognition, access control device equipped with screen can showcase authentication information directly. To protect user privacy and security, the showcased information, such as face picture, name, employee ID, etc. has been desensitized already. Through configuring the software, the system administrator can decide whether to showcase the sensitive information on the screen or not. In this way, both the convenience of use and the user privacy security can be ensured.

2、 Desfire Card

Hikvision works to perform the research on access controller through the years. To ensure user information security, Hikvision researches Desfire application system and has developed Desfire smart card based on the security attributes of Desfire card.

- Issuing Desfire Card

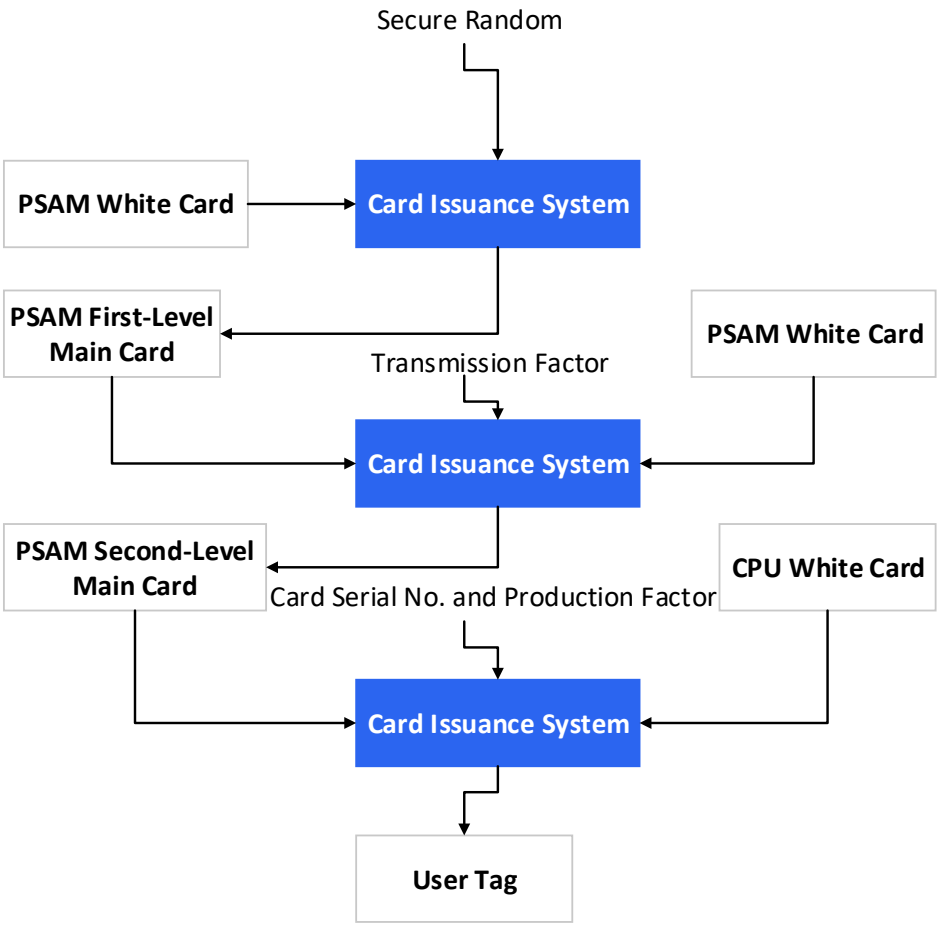
Hikvision supports encryption issuance of Desfire card. Independent secret key is created for each card based on the dispersion characteristics of AES algorithm secret key.

The card issuance system adopts a multi-level management mechanism, where the secret key of the next level is derived from the secret key of the upper level based on specific dispersion factors, making it impossible to recover the upper-level secret key from the lower-level secret key.

The original secret key of the card is obtained from the security chip within the device when the card issuance system powers on. The entirely random number inside the secure device is unpredictable. It is stored in the device's memory and lost when the card issuance system powers off. The original secret key is stored on the Desfire card in encrypted form, relying on the security mechanisms of the Desfire card to prevent the secret key of the card from being read or recovered.

During transmitting the secret key of the card, the key is always exported from the upper-level card to the lower-level card in encrypted form, making it impossible to obtain the original content by packet capture. AES 128 encrypted channel is adopted during the transmission to ensure the data is secure and reliable.

The terminal user's secret keys of the card are derived based on the card serial number and production factors. In Hikvision card issuance system, cards with the same serial number are filtered to ensure that each terminal user's card is independent, ensuring that the secret keys of each card are different.



- Recognizing Desfire Card

When recognizing users' cards, Hikvision access control devices require secret key authentication of the Desfire card. A security chip is embedded in the access control reader terminal, with the secret key pre-installed by Hikvision card issuance system. During the authentication process, AES 128/256 algorithm is adopted to ensure channel security.

3、 Fingerprint

Hikvision has deeply engaged in biometrics realm, owning advanced fingerprint imaging technology and fingerprint recognition technology based on detailed features. Also, we have developed fingerprint recognition algorithm integrating fingerprint collection and recognition characterized by high security, strong stability and high recognition rate.

- Fingerprint Collection

Fingerprint can be collected by fingerprint recognition device or fingerprint collector, both of which collect fingerprint pictures via the front-end fingerprint sensor. The pictures will be algorithmically processed to become fingerprint templates and then being stored as user data. Hikvision never stores any fingerprint pictures. All of them will be destroyed when fingerprint features are successfully generated.

- Footprint Storage

Fingerprints are stored as eigen values in the device. AES 128/256 is adopted to encrypt the access and the access permission has been limited so as to ensure the security. Fingerprint pictures cannot be restored from fingerprint features.

- Fingerprint Recognition

Through fingerprint sensor on the device, fingerprint pictures can be collected, which will be algorithmically processed to generate the fingerprint

features for comparison in fingerprint library. In addition, template learning strategy has been adopted in recognition function so as to enrich fingerprints information and improve fingerprint recognition speed and the recognition rate.

- Fingerprint Recognition Rate

Hikvision has provided 5 security levels to adjust fingerprint recognition rate. The security level can be set on web.

Security Level	False Acceptance Rate (FAR)	False Rejection Rate (FRR)
1	0.1%	0.005%
2	0.003%	0.01%
3	0.001%	0.1%
4	0.0003%	0.5%
5	0.0001%	1%

4、Face Picture

- Face Picture Collection

After being captured by front-end camera sensor on access control device, face pictures will be processed by face algorithm, including live target verification, face picture analysis, etc. In this way, it can be ensured that the captured face pictures are reliable. Generated from face pictures through algorithmic picture analysis, face features will be stored as a part of user information. Before stored and accessed, face features will be algorithmically encrypted by AES 128/256, which is similar to face picture data. With the

encryption, together with access permission limitation, the security of face features can be ensured.

As the process of generating face features is irreversible, face pictures cannot be restored from face features.

- Face Picture Storage

To fully ensure user data security, face features instead of face pictures are stored by default during the process of collecting, registering, and recognizing face pictures. Face pictures can be configured to be stored in the device or not through access control management terminal software.

Before being stored in the memory, face pictures have been desensitized by the device with AES 128/256.

- Facial Recognition

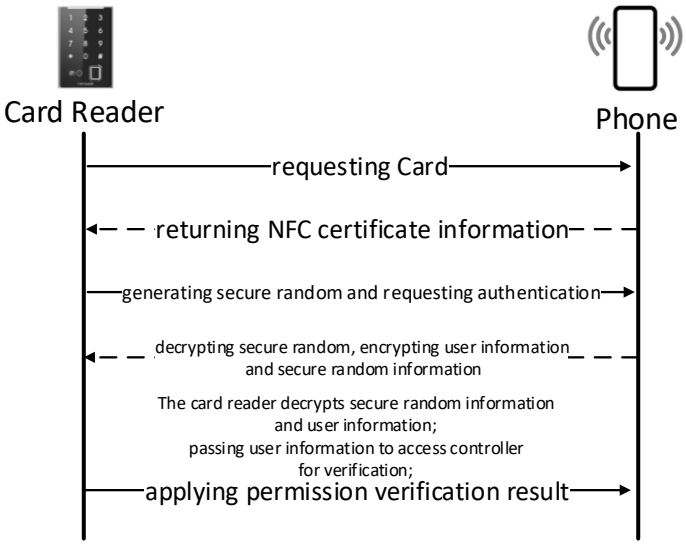
After being collected by the front-end camera sensor on the device, face pictures will be algorithmically processed to generate face features for comparison in feature library. During facial recognition, captured face pictures will not be stored in Hikvision access control device by default. Instead, the user can decide to store the pictures or not with the terminal software.

5、Electronic Credential

- NFC

With the development of wireless communication technology and mobile Internet, together with the popularity of smart phones, mobile applications have been widely used across all industries. Among the applications, NFC communication technology is increasingly used in access control sector. Users admire it for its convenience and high-efficiency. At the same time, however, users are also concerned about the security of electronic credentials. In light of that, Hikvision explored NFC transmission mechanism and has launched a secure transmission and verification scheme of NFC electronic credential which is compatible with Android system.

NFC encrypted electronic credential is supported by Hikvision access control devices. Each system owns a separate encrypted secret key, which is generated by HCP / Hik-Connect platform and passed to app and devices via HTTPS. When the card reader on mobile phone or access control device recognizing NFC, AES 128/256 is adopted to encrypt NFC information so as to prevent data from being stolen.



- Bluetooth

Like NFC, bluetooth electronic credential is also a product of IoT era. Bluetooth credential recognition is supported by Hikvision access control device (with bluetooth function). To ensure bluetooth transport security, Hikvision has adopted AES 128/256 to encrypt communication data.

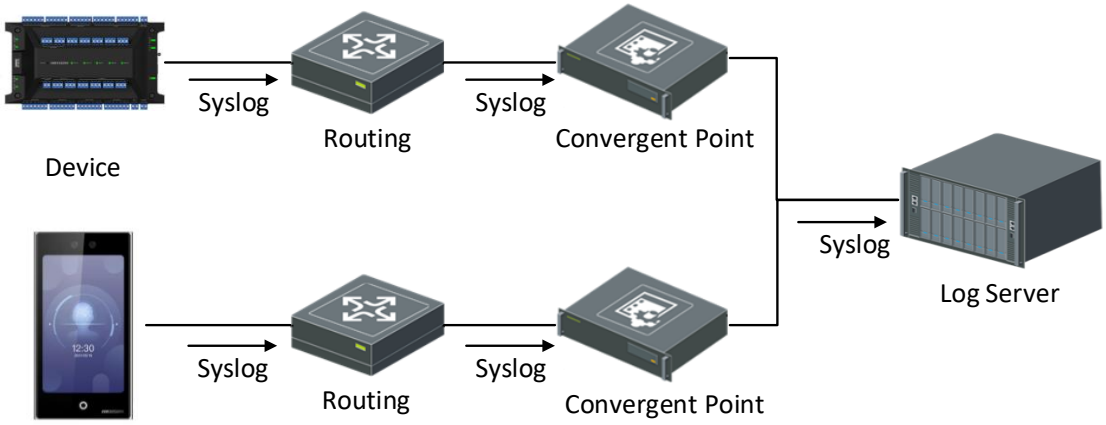
Event & Log Record

1、Log Audit

The security audit log of Hikvision includes detailed record of security-related activities of products, such as information required for audit, and recognizing various types of exception events, etc. All data and activities can be seen on the result report, such as login failed, configuration changes, user management, upgrade and maintenance of the device, access failed, etc. All user operations can be checked on the report.

In addition, canceling the audit process, or deleting, editing or covering the audit record is not allowed. The exception events alarm function is equipped at the same time.

PIN technology has been applied to prevent the locally-stored logs from being illegally viewed or tampered. At the same time, with syslog protocol, the logs can be securely uploaded to the log server in real time for centralized storage.



The syslog Log Management Service

Transport-layer encryption and authentication for the syslog protocol via TLS is supported in log transmission, ensuring the security of network transmission.

2、Event Record

- Event Storage

Event records, such as storage device authentication, exceptions, etc. are supported by Hikvision access control devices. Events including IP address of the user, users, and the occurrence time, etc. can still be recorded even if they have been authorized on the platform. All records can be viewed on the management terminal software of access control devices.

- Event Cleanup

Due to the limitation of the storage capacity of Hikvision access control devices, events will be cleaned up if the number of them reaches the limit. The cleanup mechanism can be divided into three types: overwriting, periodical deletion, and specified time deletion

Overwriting The earliest events will be deleted when the system detects the stored events has been full of the space.

Periodical Deletion All events will be deleted according to the time period. Setting the time period is allowed.

Specified Time Deletion All events will be deleted at the specified time. Setting the time is allowed.

4.5 Security Authentication

With the intricate and constant changing global legal environment, together with the increasingly complex regulatory requirements especially the cybersecurity laws of the industry, many countries and regions have launched laws and regulations in recent years. For example, China has enacted *the Cybersecurity Law, the Data Security Law*, and *the Personal Information Protection Law of the People's Republic of China*.; European Union has issued *General Data Protection Regulation*. It can be seen that security and compliance have become major challenges for IoT service providers. Hikvision has been committed to building a high-impact internal security-control system. Following the compliance requirements of different industries, sectors and countries, Hikvision works to improve compliance from perspectives of institutions, procedures and activities control. To expand the business worldwide, better meet the compliance requirements globally, and promote the standardized management across countries and regions, Hikvision optimized internal compliance organization schema in 2018 and has established the compliance department, which is responsible for the construction of global compliance system of the company.

There is an internal team of professional lawyers in Hikvision to investigate, recognize and track the laws and regulations applicable to the operation of the company. We have also established long-term cooperation with well-known law firms at home and abroad with rich experience in the industry. At the same time, to recognize and control legal risks in all processes including product

development, manufacturing, delivery and service, Hikvision has formed special work groups to integrate applicable laws and regulations with business practices to provide suggestions and support of compliance. New employees, middle and senior managers, and key personnel in cybersecurity of Hikvision are continuously provided with specialized training on newly enacted laws and hot regulations to enhance compliance awareness.

Hikvision is committed to improving and perfecting product security. Based on compliance with all applicable national and regional security regulations and reference of best practices for industry, we have established a sustainable and trustworthy security guarantee system from company policies, organizations, processes, technologies and specifications.

Hikvision supports mainstream international standards and actively contributes to their formulation. At the same time, we have also participated in the formulation and promotion of industry security standards to further open up our core security technologies and cooperate with different industry experts and national standards organizations so as to jointly improve the security standard system related to IoT.

Hikvision also cooperates with independent third-party assessment facilities and persons to conduct fair security assessment and certification of our products.

Supply Chain Security

Given the fact that the supply chain system is characterized by complex and diverse participants, numerous processes and cross-regional products transfer, it is vulnerable to internal negative factors and external threats. The security threats faced by the supply chain system include unauthorized production, tampering, stealing, malicious software and hardware implementation, and defective manufacturing and developing practices in supply chain. The vulnerabilities of supply chain might remain undetected for several years, and it is often difficult to determine whether a security incident is directly resulted from a supply chain vulnerability. Given that, the security threats might cause continuous negative impacts on the supply chain.

To prevent manufacturing security risks and ensure the integrity of hardware and software, Hikvision has taken security control measures of tamper protection, implant protection, and switch protection at key production stages, including software providing, chip burning/verification, software loading and production testing. In this way, the risks of replacing unauthorized hardware, implanting or tampering software, and infecting virus can be prevented. The software that the device needs to burn is downloaded to a secure manufacturing distribution system by the Product Data Management system. Before burned, the software has undergone multiple verifications in terms of the integrity.

Network for burning and loading software, assembly and testing is isolated from IT system in the office and the public network.

In addition to taking technical measures, Hikvision also conducts management system construction to ensure the supply chain security. ISO 28000 Supply Chain Security Management System aims to improve overall supply chain security. With the system, the organization is able to review security risks and take measures to control and mitigate potential threats in supply chain. Given that ISO 28000 is compatible with ISO 9001 Quality Management System and ISO 14001 Environment Management System, the three systems can be integrated within one organization.

Based on a clear understanding of the supply chain operating environment, recognizing threats at each stage, and conducting risk assessment and response, Hikvision has established a supply chain security management system that fully conforms to ISO 28000. Through PDCA Management Cycle, the supply chain security management system can be continuously updated and improved.

Hikvision has launched a secure and strict maintenance process, with which the product integrity can be ensured. The information throughout the process is recorded in the manufacturing and barcode system, presenting detailed execution records and logs for R&D, procurement, manufacturing (chip burning, software loading, assembly, testing, etc.), warehousing, and logistics to ensure the traceability.

ISO/IEC 27001

ISO/IEC 27001 Information Security Management System is the most authoritative, strict, and widely accepted and applied system certification standard in the field of international information security. Obtaining the certification means

that a company has established a scientific and effective information security management system to align its development strategies with information security management, ensuring that the information security risks are appropriately controlled and correctly addressed. Hikvision has established the information security management system in 2012. After 10 years of innovation and improvement, the information security management system 3.0 was officially released in 2021, which covers management requirements for cybersecurity, information security, and privacy protection, adhering to the continuous improvement policy of PDCA, thus providing reliable support and protection for Hikvision's business. In January 2023, Hikvision was certified by the British Standards Institution (BSI), an international authoritative audit organization, becoming one of the world's first companies to obtain the ISO/IEC 27001:2022 certification. The fact marks that the information security management capability of Hikvision has been in the world's leading ranks.

ISO/IEC 27701

As the privacy extension of ISO/IEC 27001 Information Security Management Standard, ISO/IEC 27701 is applied to help the organization protect and process personal information in compliance. The standard is considered as the world's most authoritative privacy protection standard, serving as an internationally recognized guide for best practices in privacy protection. It also provides guidance on "appropriate technical and organizational measures" mentioned in GDPR,

becoming an important reference and support for privacy-related legal compliance.

Hikvision has obtained the ISO/IEC 27701:2019 certification awarded by BSI in December 2021.

ISO/IEC 29151

ISO/IEC 29151 standard aims to resolve the threats in personal information security in the context of the rapid development of global IT technology. With a focus on protecting personal information, it regulates data operation behaviors in various stages, including the collection, storage, processing, use, and disclosure of personal information, to perform accurate assessment of risks of personally identifiable information and take effective control measures accordingly. It aims to enhance the security and reliability of business processes and minimize the risks of personally identifiable information in IT operations, thereby protecting users' legitimate rights and the public interest to the greatest extent.

Hikvision has obtained the ISO/IEC 29151:2017 certification awarded by BSI in December 2021.

CMMI5 Software Maturity Level Certification

CMMI, namely Capability Maturity Model Integration, is a framework for enterprise-level process management. It represents the best practices of the world's leading companies and is recognized as an authoritative standard for measuring enterprise products and service capabilities. It also serves as a method

for improving the process, helping enterprise achieve their business goals, ensure the quality, guarantee delivery, and enhance customer satisfaction. There are five ascending levels of process improvement capability of enterprises being set in CMMI standard for software, with the fifth level (CMMI5) being the highest.

Hikvision has obtained CMMI5 certification in April 2016.

5 Security Commitment

Hikvision has been committed to protecting customers' personal information with leading technologies in terms of security protection and personal information protection, and has adopted an overall approach to protect user data.

Hikvision applies a unified integrated security infrastructure throughout the ecosystem of access control system application. In addition, there is a professional security team in Hikvision providing security audits and tests for both in-development and released access control products. The team also conducts security training and actively monitors new security risks and threats. To learn how to report issues to Hikvision and subscribe to security notifications, see

https://www.hikvision.com/cn/support/CybersecurityCenter/。

见远 行更远

See Far, Go Further