DSS Security Instruction

V2.0

Zhejiang Dahua Technology Co.,Ltd

Legal Notice

Copyright Statement

Without the prior written permission of Zhejiang Dahua Technology Co., Ltd. (hereinafter referred to as "Dahua"), no one may copy, transmit, distribute or store any content in this document in any form.

The products described in this document may contain software copyrighted by Dahua and other third parties. No one shall copy, distribute, modify, extract, decompile, disassemble, decrypt, reverse engineer, lease, transfer, sublicense or otherwise infringe the copyright of the software in any form except with the permission of the relevant owner.

Trademark Statement

- alhua, alhua, alhua TECHNOLOGY, alhua TECHNOLOGY, HDCVI are trademarks or registered trademarks of Dahua.
- HDMI HIGH-DEFINITION MULTIMEDIA INTERFACE: This statement applies to all products. For example, our products utilize HDMI technology, HDMI, HDMI High-Definition Multimedia Interface, HDMI trade dress, and the HDMI logo. These are either trademarks or registered trademarks of HDMI Licensing Administrator, Inc. Rest assured that our products have been licensed by HDMI Licensing Administrator, Inc to use HDMI technology.
- VGA is the trademark of IBM.
- The Windows logo and Windows are trademarks or registered trademarks of Microsoft.
- All other company names and trademarks mentioned herein are the properties of their respective owners.

Responsibility Statement

- To the extent permitted by applicable laws, in no case will the company compensate for any special, attached, indirect and secondary damages caused by the relevant contents and products described in this document, nor for any loss of profits, data, goodwill, documents or expected savings.
- The products described in this document are provided “in accordance with the status quo”. Unless required by applicable laws, the company does not provide any express or implied warranties for all contents in the document.

Export Control Compliance Statement

Dahua complies with applicable export control laws and regulations and implements requirements related to the export, re-export and transfer of hardware, software, and technology. With regard to

the products described in this manual, kindly fully understand and strictly abide the applicable domestic and foreign export control laws and regulations.

About This Document

- The products, services or features you purchase shall be subjected to the company's commercial contracts and terms. All or part of the products, services or features described in this document may not be within the scope of your purchase or use.
- If the operation is not carried out according to the instructions in this document, any loss caused thereby shall be borne by the user.
- If the obtained PDF document cannot be opened, please upgrade the document reader software being used to its latest version or use other mainstream reading tools.
- The company reserves the right to modify any information in this document at any time, and the modified content will be added in the new version of this document without notice.
- This document may contain technical inaccuracies, inconsistencies with product functions and operations, or typographical errors, subject to the company's final interpretation.

Foreword

Overview

With the maturity of technologies like IoT, AI, and big data, an increasing number of companies embrace AIoT as a core pillar of their development strategies. Responsible, open, professional, and systematic cybersecurity and privacy protection have become important guarantees and foundations for promoting the long-term and healthy development of the industry. Dahua has always placed a high priority on cybersecurity and privacy protection. We continuously allocate special funds to ensure steady progress in product R & D, delivery, key security technology research, security compliance, and emergency response systems. At present, Dahua has achieved significant accomplishments in security technologies like trusted computing, data security, privacy protection, and attack and defense testing. These advancements have been integrated into a wide range of our software products.

Scope

This document aims to provide an open and transparent view of Dahua's exploration and practices in security issues, enabling users, partners, industry organizations, and government agencies understand Dahua's security capabilities.

This document will elaborate the security measures of software platform products, covering aspects such as security engineering practices, security technology applications, security compliance and security emergency response.

Definitions

Term	Note
AIoT	The Artificial Intelligence of Things
AK	Access Key ID
DoS	Denial of Service
GDPR	General Data Protection Regulation

KDF	Key Derivation Function
RBAC	Role-Based Access Control
sSDLC	secure Software Development Lifecycle
SK	Secret Access Key
SSL	Secure Sockets Layer
TLS	Transport Layer Security

Revision History

No.	Version	Revision	Release Date
1	V1.0	First release.	2020.10.30
2	V2.0	Add the new security baseline and the latest results of security technology research.	2023.9.8

Contents

1 Security Threat

The rapid integration of cutting-edge technologies like AI, IoT, cloud computing, and big data with the real economy is driving significant advancements. This integration, known as a new round of scientific and technological revolution led by the digital economy, is reshaping the world at an unprecedented pace. By developing an IoT platform that integrates "IoT access, vision intelligence, and data intelligence," Dahua has achieved the seamless aggregation of vision data and IoT data, which unleashes the data value and creates new industry value.

The application of new technologies to expand services in various scenarios brings about the integration of virtual and physical space, the access of numerous devices, the aggregation of large volumes of data, and the micro-service business. However, these advancements also pose significant security challenges to software platforms, leading to various threats:

- Data Breach: Sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used without authorization.
- Virus Intrusion: It is attacked by viruses such as miner virus and ransomware, which damages or affects the system business and function.
- Weak Password: Using weak passwords or weak identity authentication mechanisms makes software platforms vulnerable to attackers.
- Vulnerabilities: The complexity and diversity of business scenarios call for complex platform design and extensive amount of code, which makes it easier for defects and vulnerabilities to emerge.
- .....

2 Security Organization

2.1 Security Organizational Structure

With a systematic and professional security team, Dahua ensures that cybersecurity work is deeply integrated into every execution unit through a hierarchical structure. This comprehensive implementation covers areas such as research and development (R & D), marketing, supply chain, delivery, and services.

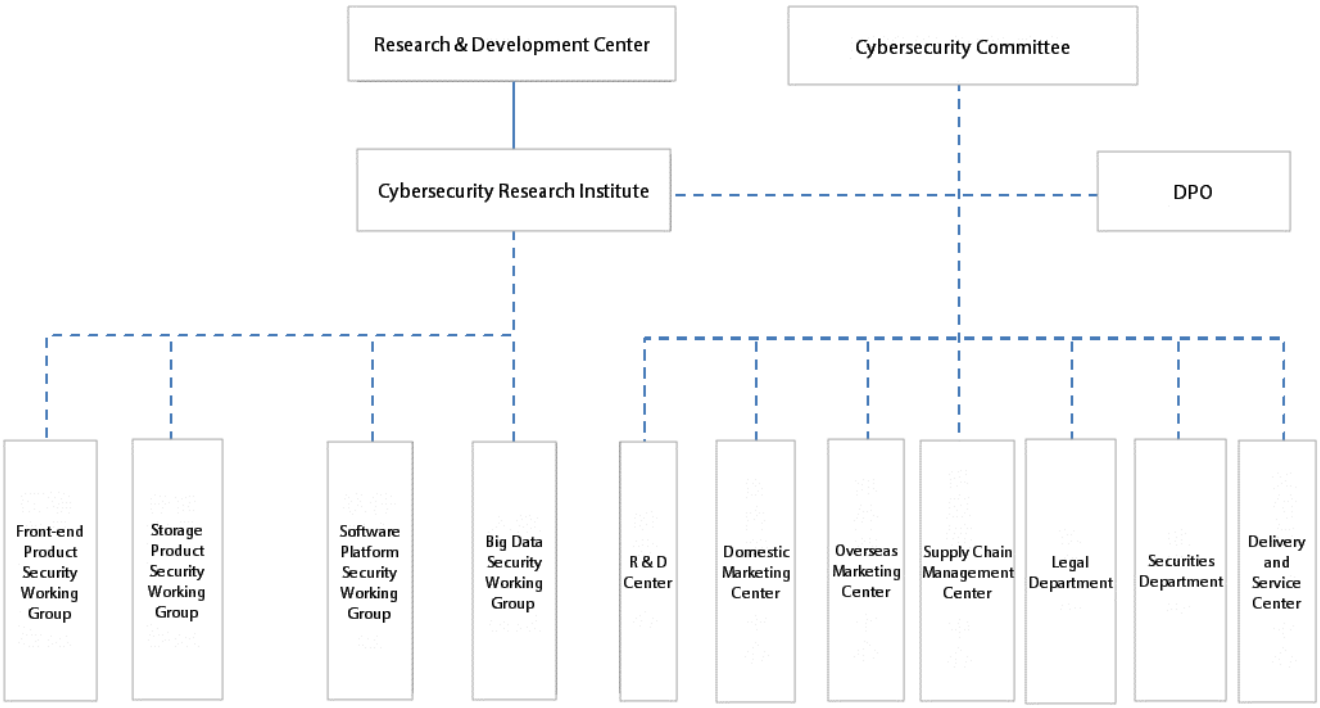

Figure 2-1 Security organizational structure

- The Cybersecurity Committee is the highest decision-making organization, which comprehensively plans, coordinates, guides and supervises the cybersecurity work from the strategic level.
- The Cybersecurity Execution Team is a joint execution team across business teams. At the policy level, this team takes the lead in discussions and devises mechanisms and strategies pertaining to cybersecurity. At the implementation level, they are responsible for executing, monitoring, and managing daily cybersecurity operations. The organization consists of various departments, including R & D, marketing, supply chain, delivery and

service, legal matters and more. This ensures that decisions related to cybersecurity can be efficiently implemented across all business systems through the organization.

- The Cybersecurity Research Institute is an entity organization that undertakes key research in security and privacy technologies, builds security engineering capabilities, and develops security ecosystems. The institute assumes responsibility for security and privacy requirements, security and privacy risk assessment, security and privacy design, penetration testing, vulnerability management, emergency response, and formulation of security process system and security compliance system.
- The Cybersecurity Engineering Team is set up for each product line. This team interacts closely with the Cybersecurity Research Institute, which enables the swift implementation of security standards and specifications, security and privacy technologies, and vulnerability repair and disposal in each product.

2.2 Security Training

The construction of cybersecurity requires the active participation of all departments. For this reason, Dahua places significant emphasis on security training, and continuously carries out a range of activities aimed at enhancing security awareness and capabilities, including:

- Security Training for New Employees: To enhance the cybersecurity awareness of new employees, Dahua employs a systematic learning approach. Specifically, targeted security training courses are designed for employees in key positions. Only after successfully completing the training and passing relevant examinations, are they officially employed.
- Daily Email: Tips on cybersecurity. To remind employees of cybersecurity issues, Dahua regularly sends common problems in the form of pictures and descriptive text by email.
- Cybersecurity Awareness Month: A series of engaging activities are conducted both online and offline, including poster publicity, security knowledge Q&A, security risk collection, signature wall, photo contests with likes as a voting mechanism, theme training and more.
- Cybersecurity Coding Empowerment Plan: Dahua conducts at least 2 sessions of security coding training and evaluation per year. Additionally, the company regularly shares related articles to enhance developers' understanding and proficiency in security coding practices.

- Cybersecurity Technology Challenge: Participants are encouraged to utilize their security skills comprehensively. This includes engaging in tasks such as in-depth vulnerability mining, evidence collection and analysis, as well as attack and defense. Along with the growth of attack and defense mechanism, participants have also demonstrated significant improvements in their capabilities.

3 Security Engineering Guarantee

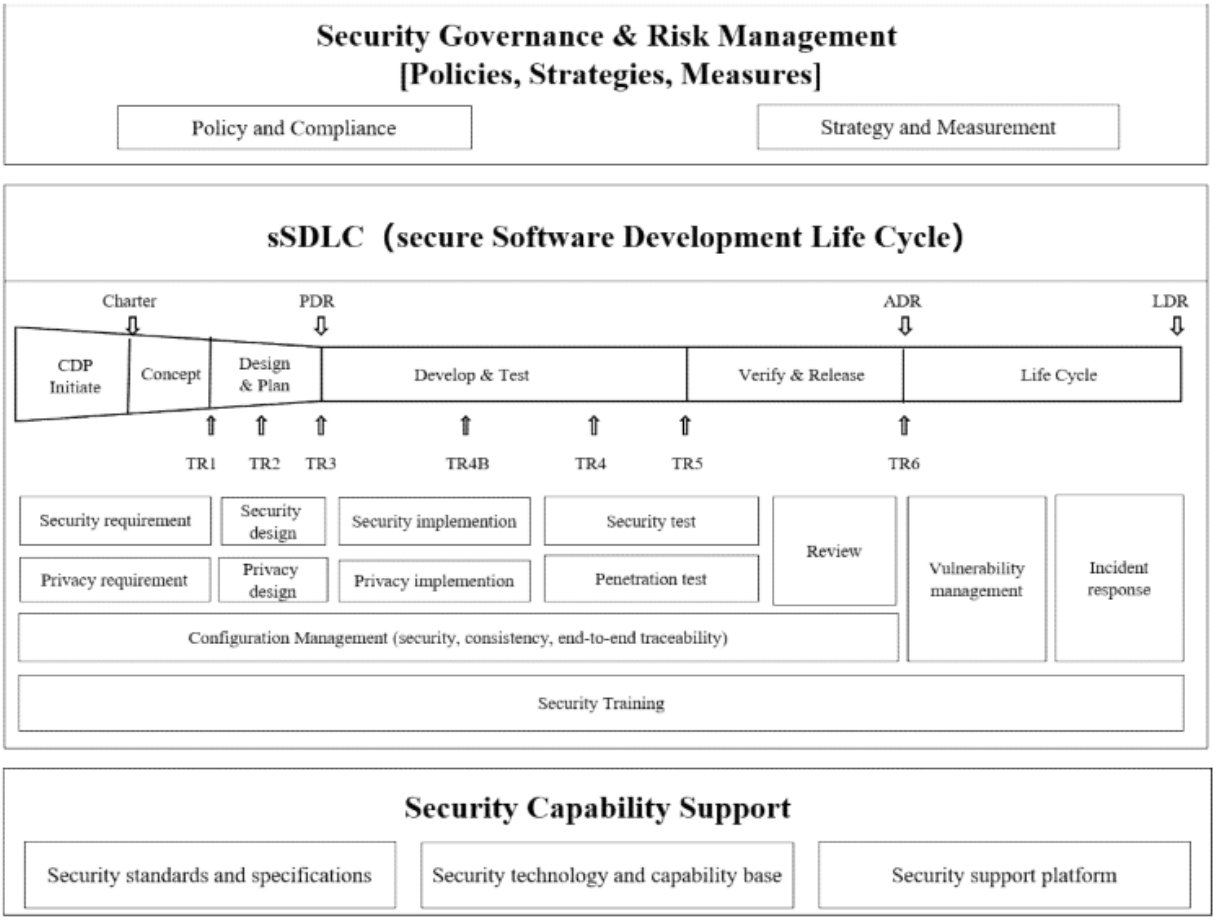

Figure 3-1 Secure software development life cycle

With ongoing efforts in construction of Secure Software Development Life Cycle (sSDLC), Dahua is dedicated to standardize and control the software development process. By conducting a comprehensive and thorough security activity maturity assessment, the security software development suitable for Dahua is further refined and optimized.

- In the definition stage, security baseline and privacy baseline are taken as the most basic requirements of the software platform, then the security and privacy risk assessment is carried out. Requirements and strategies in risk response are tailored precisely fitting the risk assessment results.
- In the design phase, core security design principles such as attack surface minimization, permission minimization, default security, and defense in depth are strictly followed.

Collaborating extensively with cybersecurity experts and product business experts, our approach incorporates concepts such as Security by Design, Privacy by Design and Privacy by Default. Furthermore, threat modeling is adopted and mitigation measures are developed.

- In the development phase, we strictly follow the security code specifications, and perform static code security testing and defect repair on the basis of code cross-review. Additionally, references to open-source software strictly comply with relevant control requirements.
- In the verification stage, comprehensive security activities such as virus scanning, host scanning, Web security scanning, known vulnerability scanning, mitigation measures verification, penetration test, and fuzz testing are carried out.
- Upon reaching the release stage, the review of consistency between security requirements and security design follows, where attention focuses on checking the implementation of security measures and the completeness of security data.
- In the full lifecycle of product development, we conduct regular trainings on security design principles, security code specifications, security testing methods and the use of various security tools, thereby cultivating everyone's safety awareness and capabilities.

4 Security Technology Guarantee

4.1 Security Baseline

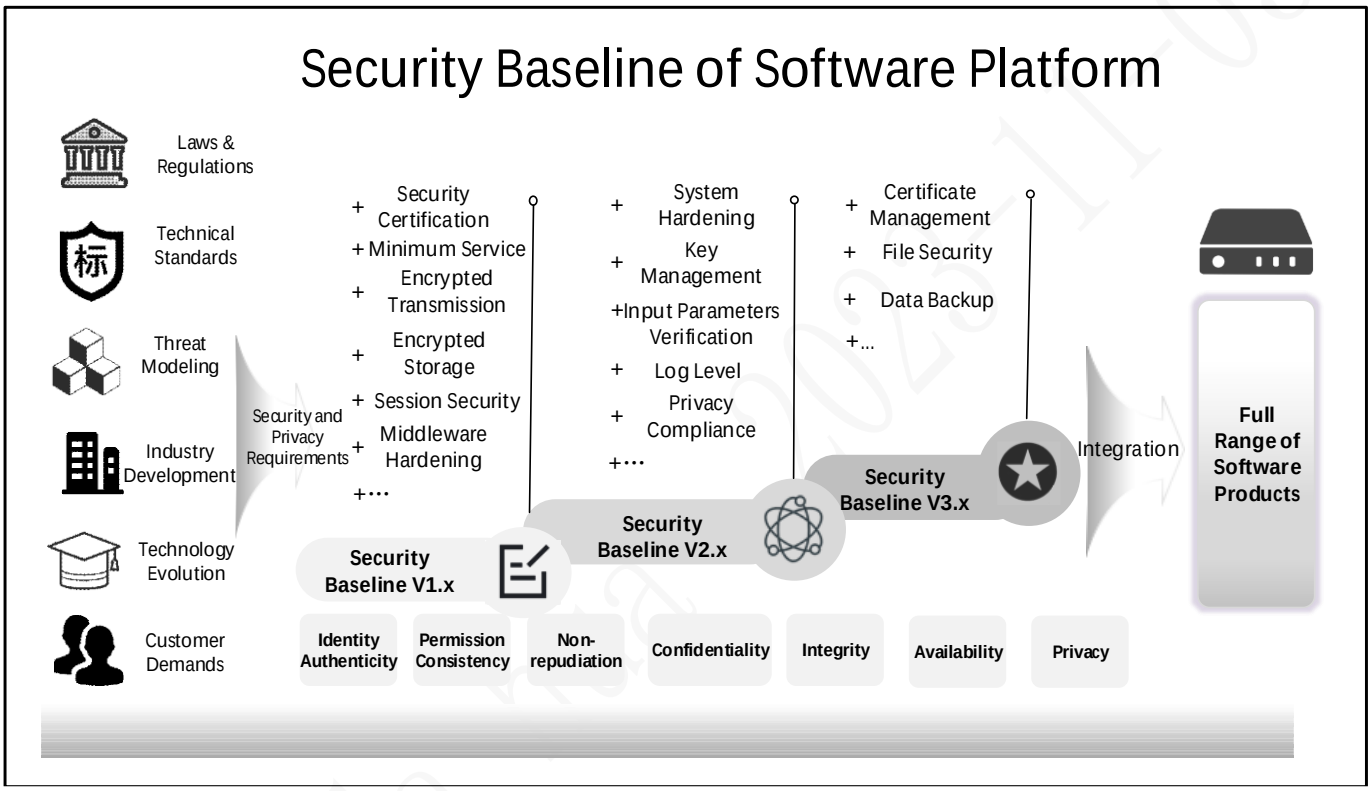

Figure 4-1 Security baseline of software platform

Dahua meticulously follows the "security baseline" and adheres to the core concepts of Security by Design, Security by Default, Privacy by Design and Privacy by Default. With long-term commitment into product security and privacy protection technologies, it delivers safe and private online experiences for users.

The security baseline is designed on principles of security and privacy. With identity authenticity, permission consistency, non-repudiation, confidentiality, integrity, availability and privacy being incorporated as security elements into its architecture, a systematic protection framework covering host security, service security and data security is formed.

To keep pace with the ever-evolving industry and the changing landscape of technology and attack methods, Dahua consistently conducts a range of activities. These include tasks such as compliance with laws and regulations, standard specification study, industry dynamic tracking,

threat modeling and analysis, key technology pre-research, and security demand research. Additionally, Dahua continuously iterates its security baseline standards, ensuring that they remain adequate and at the cutting edge of security protection.

As an important enterprise standard of Dahua, the security baseline is an integral part within the entire lifecycle of security development. It has been integrated into the quality assurance system, thereby enabling the technical guarantee of default security.

4.2 Security Technology

4.2.1 Host Security

4.2.1.1 Firewall

The firewall utilizes network packet filtering technology. It examines the characteristics of received and sent network packets based on preset filtering rules, ultimately determining whether to allow them to pass. The firewall also supports domain-based management, allowing for the centralized management of cluster resource node ports and the establishment of reasonable policies. This enables the division and management of cluster domains and user domains. Cluster domains support exclusive communication among service nodes within the same domain, while user domains support access and communication among authorized users within the domain.

By default, the firewall mechanism is enabled on the software platform. Once the deployment completes, the system automatically generates firewall policies for the cluster domain by considering the internal relationships between services. We recommend that you further divide the scope of user domains based on actual scenarios to improve the firewall policy.

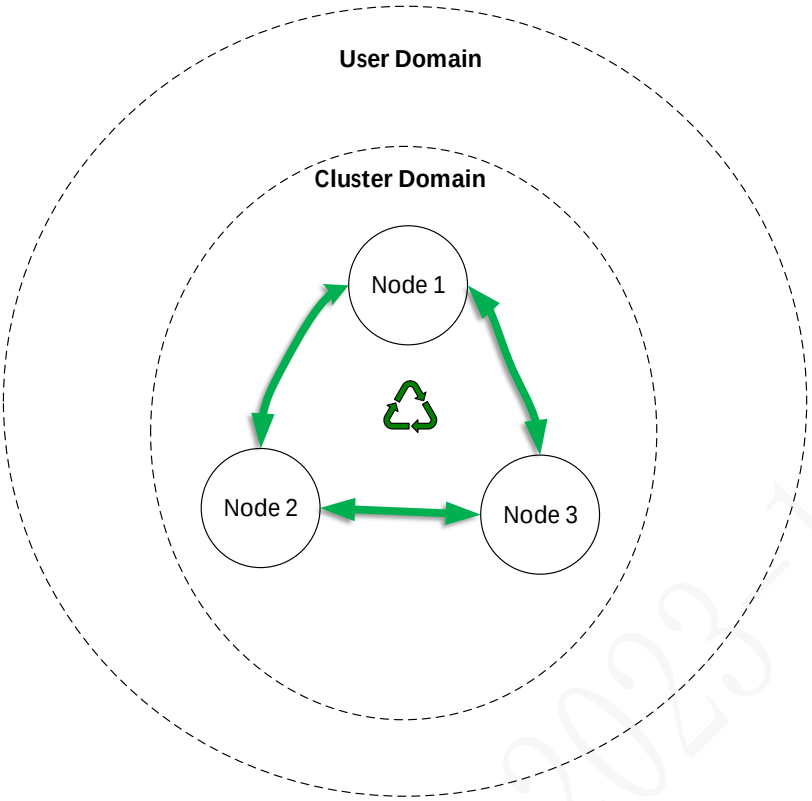

Figure 4-2 Internal firewall domain management

4.2.1.2 Trusted Upgrade

When upgrading a program on the software platform, the upgrade service performs trusted verification on the target package. This verification guarantees that only legitimate and untampered packages are allowed onto the platform.

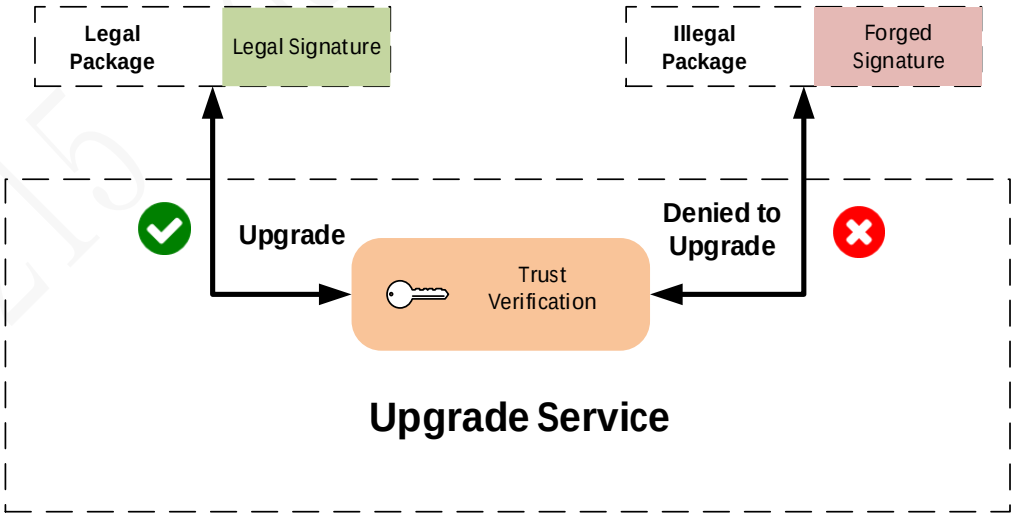

Figure 4-4 Trusted upgrade principle

4.2.1.3 System Hardening

In accordance with CIS Benchmarks best practices, the operating system is hardened to enhance its defense capabilities. This involves implementing a variety of measures, including but not limited to the following:

- Set the system configuration to defend against DoS attacks.
- Configure the system password policy, including the password length, complexity, number of historical repeats, and number of failed password attempts before being locked.
- Configure the minimum access control for key files, such as etc/passwd and etc/shadow.
- Remote login from root account is prohibited.
- An empty password account is prohibited.
- Delete or lock a useless account.
- .....

4.2.2 Service Security

4.2.2.1 Identity Authentication

4.2.2.1.1 Digest Authentication

Digest authentication technology is a challenging authentication method based on HASH algorithm on passwords and random numbers (valid once) to ensure the confidentiality and non-repeatability of the authentication. Digest is mainly applied in the identity authentication of client users on the software platform. The steps are as follows:

- The client with a username requests a login from the server.
- The server returns the status code 401 and generates parameters such as realm and nonce.
- The client calculates the digest based on information such as realm, nonce, user name, and password, and requests the server to log in again.
- The server verifies the received digest with the same calculation based on the locally stored password.

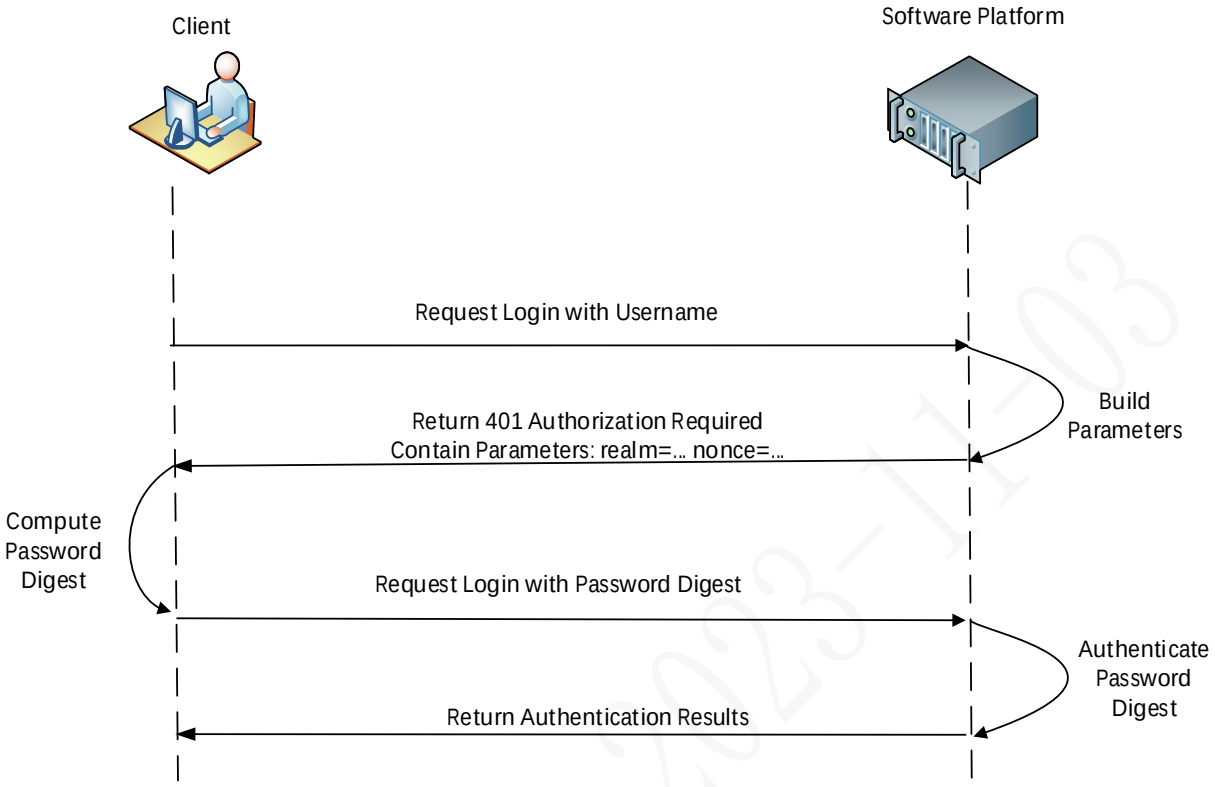

Figure 4-6 Digest authentication process

4.2.2.1.2 AK/SK Authentication

AK/SK authentication is a mechanism that relies on shared keys between two parties. The AK serves as the identity of the requester. The SK is a unique key paired with the AK, which is used for signing and authentication. AK/SK is mainly used in the communication between internal services within the software platform. The steps are as follows:

- The requester builds a message body with AK, timestamp and more. The SK is used to sign the request.
- Upon receiving the request, the responder verifies the validity of the timestamp and uses the corresponding SK to authenticate the signature. Only when the verification is successful will the party respond to the business request.

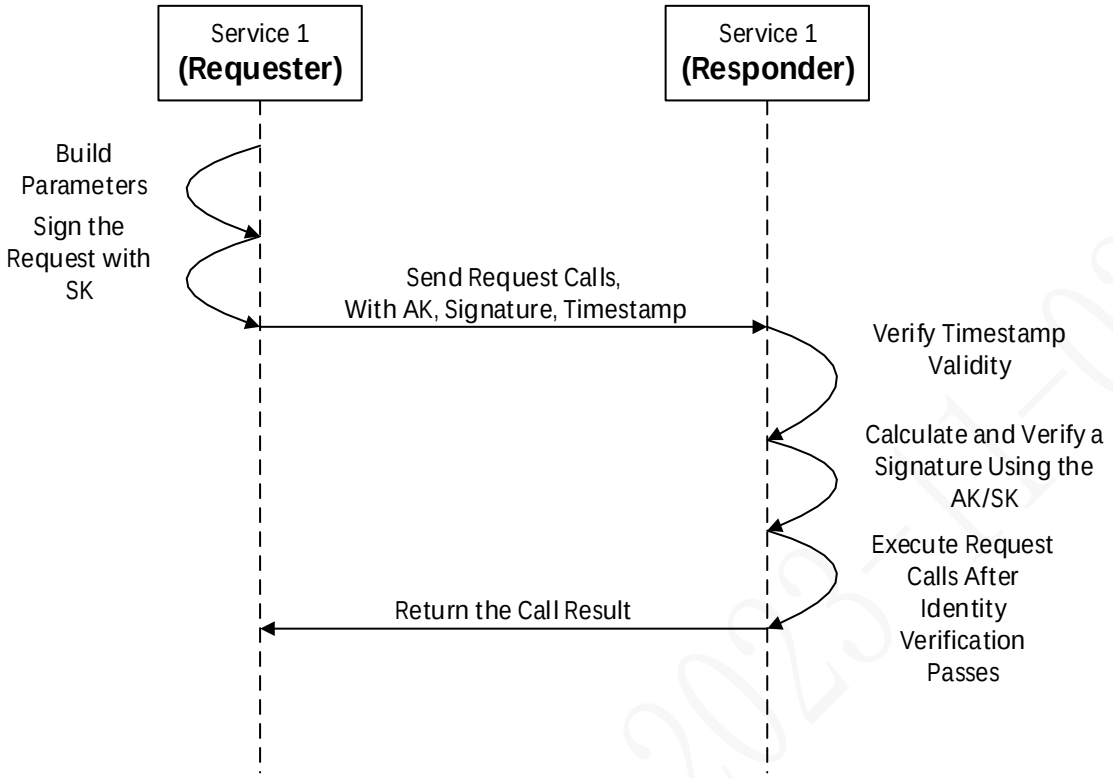

Figure 4-7 AK/SK authentication process

4.2.2.1.3 Digital Certificate Authentication

Digital Certificate Authentication is an identity verification mechanism used in the Public Key Infrastructure (PKI) system. It verifies the identity validity at both ends of a link through trusted certificates. This technology is mainly applied in machine-to-machine interaction. Its main principles are as follows:

- The requester and responder create their own digital certificates and private keys, and preset the range of trusted certificates.
- The requester initiates negotiate authentication and carries a random challenge A generated by itself.
- When the responder receives challenge A, it uses its own private key to sign it. It randomly generates challenge B, and sends its own certificate, signature and challenge B to the requester.
- The requester receives the response and verifies the returned certificate based on the trusted certificate. If the certificate is a trusted one, the public key in the digital certificate

is used to verify the signature of challenge A. If the verification succeeds, it confirms that the responder has a valid certificate and private key. The responder is a valid server.

- The requester uses its own private key to sign challenge B and sends its own certificate and signature to the responder again.
- The responder verifies the validity of the requester's certificate with the range of trusted certificates. It then uses the public key in the requester's certificate to verify the signature of challenge B. If the verification succeeds, it confirms that the requester is a valid client, and subsequently returns the result after negotiate authentication completes.

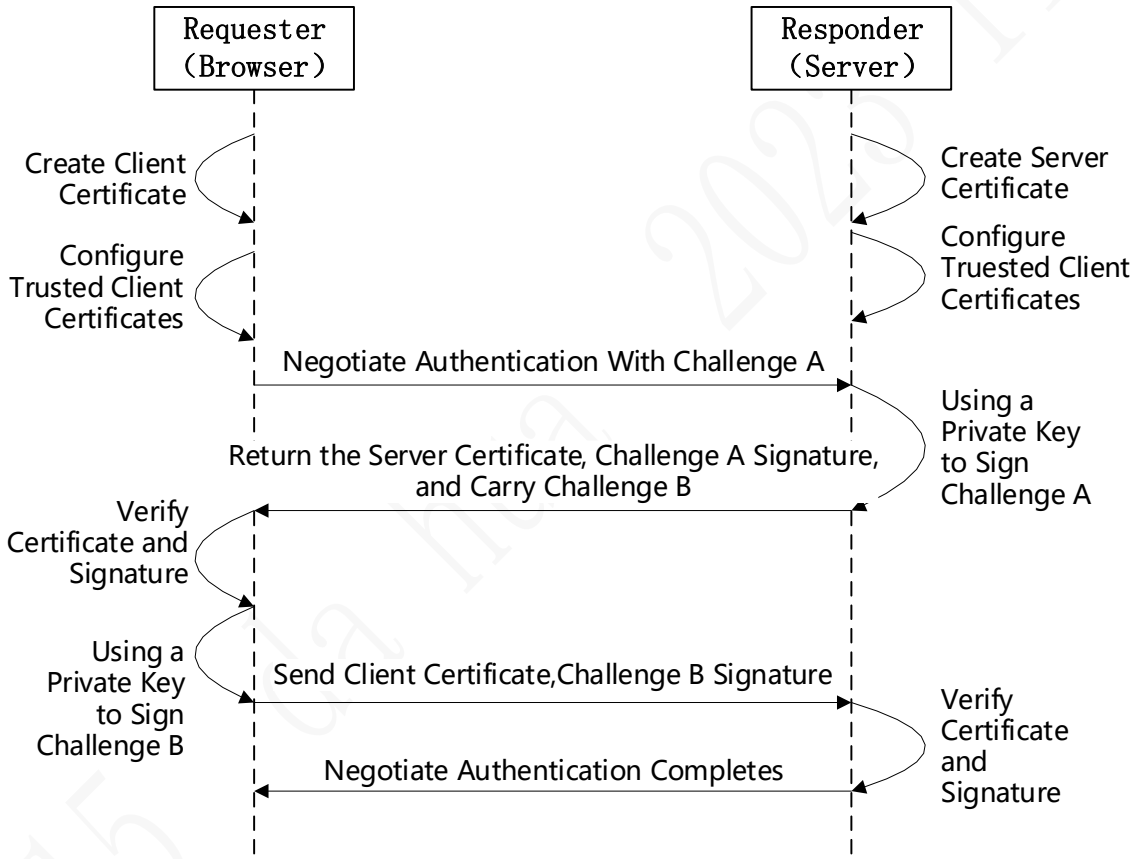

Figure 4-9 Digital certificate authentication process

4.2.2.2 Account Security Management

The user's account password is a key credential for operating the application, so it is important that it is not guessable. Therefore, for the first time, the software platform has adopted the policy of forced password changes to avoid the use of default password. At the same time, the complexity and validity period of the password set by the user are limited as follows:

- Passwords must be at least 8 characters in length and contain no less than two types.
- The weak password library and the rule detection ability are introduced to prohibit users from setting weak passwords with low strength.
- The password validity period can be set. Users are prompted to change their password before it expires. The old password cannot be used to update the validity period.

4.2.2.3 Authority Control

Based on the Role-based Access (RBAC) model, the platform builds a flexible and efficient authority control system. Different roles can be configured with different permissions based on needs, and different users can be flexibly assigned different roles based on needs to meet business needs in different scenarios.

4.2.2.4 Session Security

The platform services support session interaction based on short connection. The protection strategies are as follows:

- Use highly complex, strongly random session credentials, and the length is not less than 32 characters.
- After the account password is changed, actively log out all online users of the account.
- Automatically log off long inactive sessions.
- After the authentication passes, the session credentials are updated.

4.2.2.5 Secondary Authentication for Key Operations

When a user leaves the operation interface without logging off timely, in order to prevent any security risks caused by malicious operations, secondary authentication is required. Users are prompted to re-enter their password before performing any key operations such as factory restoration or system restart. Only after the identity is successfully verified can these operations be performed.

4.2.2.6 Log Specification

The platform records detailed operations of user login, configuration modification and resource access. The log content contains the following important factors:

- Operation Source
- Operation Target
- Operation Details
- Operation Time
- Operation Results

4.2.2.7 Network Log

The software platform supports Syslog network log. This function enables the synchronization of user operation logs, allowing them to be saved to a log server for unified management and analysis.

4.2.2.8 Certificate Management

The software platform supports unified certificate management. It adopts the X.509 standard digital certificate. It prohibits the use of default certificates and private keys. Users can install the certificate during deployment and use. Here is the installation:

- The software platform creates certificates and private keys independently. The certificate signature algorithm used is at least SHA256-RSA2048 and above.
- The software platform supports the import of certificates and private keys issued by a third-party Certificate Authority (CA). Users can install and replace these certificates through the certificate management.

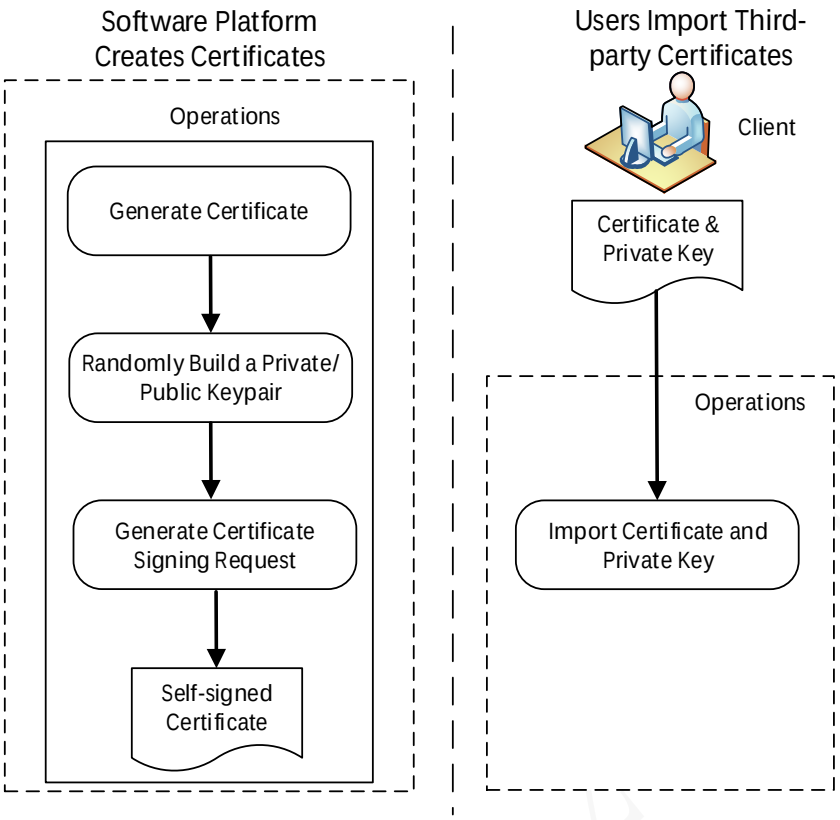

Figure 4-10 Certificate management

4.2.2.9 Web Security

To ensure the Web service security of the software platform, the built-in security protection policy is as follows:

- Restrict Web service resource access paths to prevent cross-directory access.
- It is forbidden to deploy Web services in the root directory of the system.
- Web code is prohibited from saving platform-related passwords to local disks.
- It is forbidden to store passwords in cookies.
- Enable security attributes such as http-only and secure for Web cookies.
- .....

4.2.2.10 Middleware Hardening

Following the principles of minimum permissions, default security, attack surface minimization, and combined with the CIS Benchmarks best practices, the middleware and database are systematically hardened. Some measures include, but are not limited to the following:

- If password authentication is involved, the password should be randomly generated during initial deployment to ensure that one machine has one password.
- The password must be 15 characters in length and must contain at least two character types.
- Different middleware of the software platform must use different passwords.
- The middleware should be started as a non-root user and the remote login permission should be prohibited.
- Restrict the access to the installation directory and configuration files.
- Enable or configure security configurations.
- .....

4.2.3 Data Security

4.2.3.1 A/V Encryption

To ensure the security of audio and video data, the software platform provides full-link security protection for its transmission, storage and download (export).

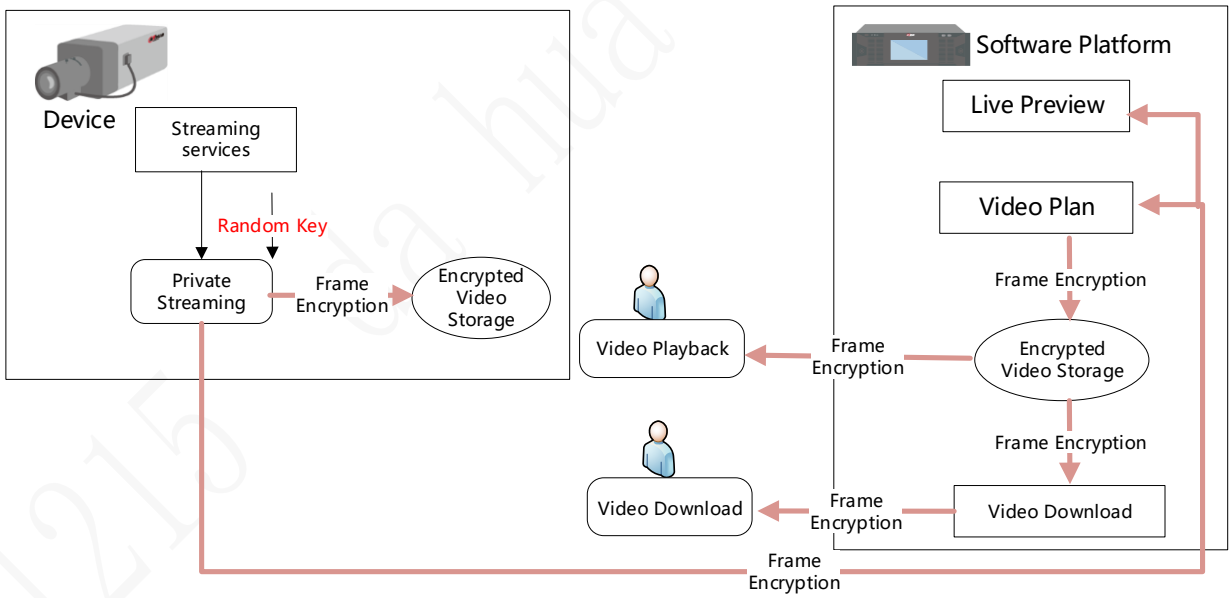

Figure 4-11 A/V full-link encryption

4.2.3.2 Configuration Encryption

4.2.3.2.1 Password Irreversible Encryption

For account password storage, the software platform adopts an irreversible HASH storage mechanism:

- Using a random salt for hashing passwords to ensure that the storage values for the same password are different.
- The salt length is not less than the HASH output length.

4.2.3.2.2 Configuration Data Encryption

To protect sensitive configuration data, the software platform supports the Key Derivation Function (KDF) technology to generate a key for encrypted storage. The basic principle is shown in the figure.

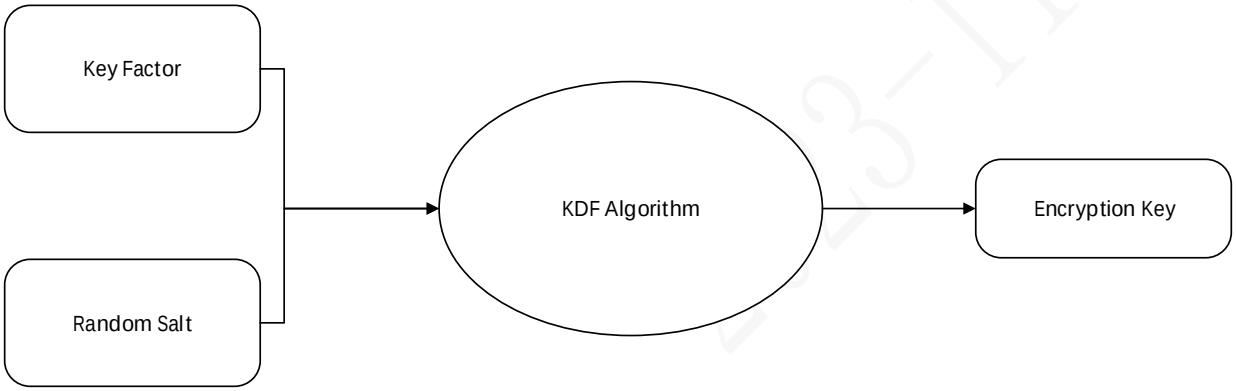

Figure 4-12 Key derivation process

4.2.3.3 HTTPS

HTTPS is enabled by default on the platform, and HTTPS is forcibly redirected when users use HTTP access. HTTPS follows the following security configuration:

- Disable insecure cipher suites, such as TLS_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_RC4_128_MD5.
- Disable insecure versions of SSLv3.0 and below, turn off TLS1.0 by default. TLS1.2 is supported.
- Disable renegotiation.

4.2.3.4 Backup and Restoration

To ensure business continuity and availability, the software platform offers multiple database backup mechanisms, including:

- Manual backup: Export database backups through related operations.
- Automatic backup: Set the backup period. The platform regularly performs the automatic

database backup.

- Remote backup: Configure remote backup servers for remote database backup.
- Hot standby: Configure hot standby to synchronize data in real time to improve system robustness.

5 Security Compliance

5.1 Legal and Regulatory Compliance

With the implementation of China's Cybersecurity Law, Data Security Law, Personal Information Protection Law and EU's General Data Protection Regulations (GDPR), the supervision of cybersecurity, data security and privacy protection has become increasingly stringent worldwide. In response, Dahua has adopted pragmatic attitudes and approaches.

Dahua takes the compliance of cybersecurity and privacy protection as top priorities. Upholding the concept of being active, open, cooperative and responsible, Dahua has established a full-fledged security and privacy management system. With mature ability in security engineering, strict security and privacy controls permeate into every stages of its platform planning, design, development and delivery. This ensures the security and privacy compliance of platforms.

5.2 Testing and Certification

ISO27701 Privacy Information Management System Certification

ISO/IEC 27701: 2019 was lately launched in August 2019 by the International Standardized Organization (ISO) and the International Electro technical Commission (IEC). Based on ISO/IEC 27001 and ISO/IEC 27002, the privacy information management system (PIMS) is formed by expanding the information security management system (ISMS) in terms of privacy information management.

ISO/IEC 27701 sets high requirements for information security and privacy information management through establishment, implementation, maintenance and continuous improvement. By means of audits, it verifies the organization's compliance. Initially, the GDPR Act, as well as ISO/IEC 29100, ISO/IEC 29151 and other privacy-related standards are taken into

account in its construction. It is a recognized authority of guiding standard for the PIMS construction in the industry.

Dahua receives full recognition of its privacy safety management and protection capabilities as it passes the ISO/IEC 27701 PIMS certification. The passing is significant for Dahua to improve product data security and privacy protection capabilities, as well as accelerate the construction of a global security compliance system.

ETSI EN 303645 Certification

The GDPR has been recognized as one of the most stringent data protection regulations to date. It has set strict and high-level requirements for data security and privacy protection, covering a wide range of aspects. Based on GDPR, the European Telecommunications Standards Institute (ETSI) has collaborated with product manufacturers, academia and government agencies to develop ETSI EN 303645. This standard aims to address significant and widespread cybersecurity vulnerabilities and protect user privacy.

In line with regulations such as GDPR, the Personal Information Protection Law, Dahua has developed and continually improved the Dahua Personal Data and Privacy Protection Standard. This standard also incorporates guidelines from ETSI EN 303645, as well as other industry standards such as the Personal Information Protection Specification. The software platform adheres strictly to the standard for design, development and implementation. Dahua also invites third-party evaluators like France Bureau Veritas (BV) to conduct testing and evaluation. As a result of this diligent approach, Dahua has successfully obtained the ETSI EN 303645 certificate. This certification signifies that Dahua software platform is well-equipped to assist customers to comply with GDPR regulations.

6 Security Emergency Response

Dahua has established the Dahua Product Security Incident Response Team (Dahua PSIRT) to receive, handle and disclose security vulnerabilities related to its products and solutions. It serves as the exclusive channel for disclosing vulnerabilities.

Dahua places utmost importance on product safety and vulnerability management. Drawing from standards such as ISO/IEC 30111 and ISO/IEC 29147, Dahua has established a comprehensive vulnerability management process. This process enables Dahua to effectively fix any identified vulnerabilities, thereby enhancing its product security.

Figure 6-1 Vulnerability management system

Dahua follows the principles of openness and transparency when it comes to disclosing vulnerabilities in the following two forms:

- Security Advisory (SA): Release information about security vulnerabilities related to Dahua products and solutions, including but not limited to vulnerability descriptions and patch fixes.
- Security Notice (SN): Respond to security topics related to Dahua products and solutions, including but not limited to vulnerabilities and security incidents.

Dahua PSIRT actively engages in industry and public activities. At of the end of 2022, we have joined several authoritative vulnerability organizations, including International CVE Numbering Authorities (CNAs), China National Vulnerability Database (CNVD), China National Vulnerability Database of Information Security (CNNVD), China National Industrial Cyber Security Vulnerability Database (CICSVD), and China National APP Vulnerability Database (CAPPVD). Give full play to the role of member units, we have established a collaborative sharing mechanism of cybersecurity threats. As a result, we have been honored with “Outstanding Unit in Vulnerability Emergency Response” award by CNVD, and ”Advanced Enterprise in Vulnerability Management” award by

CAPPVD and CICSVD.

7 Security Commitment and Recommendation

Dahua places great emphasis on cybersecurity and privacy protection. We continuously allocate special funds to enhance employees' awareness and capabilities in security, and ensure sufficient security protection for our products. Dahua has established a professional security team to provide comprehensive security empowerment and control throughout the entire product lifecycle, including design, development, testing, production, delivery, and maintenance. Dahua products adhere to the principle of minimum necessary data collection, service minimization, strict prohibition of backdoors, and the disabling of unnecessary and insecure services (such as Telnet). We continuously introduce innovative security technologies to bolster the security capabilities of our products. Additionally, we go above and beyond by providing global users with security alarm and 24/7 security emergency response services. This approach ensures that we are better safeguarding their security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report potential risks or vulnerabilities to the Dahua PSIRT. They can do so by visiting the cybersecurity section on the Dahua website.

The security of software platforms not only relies on the continuous attention and efforts from manufacturers throughout R & D, production, and delivery, but also requires active participation from users. Users should remain attentive to the environment and methods to ensure its secure operation. To this end, we suggest users to safely use the software platform, including but not limited to:

1. Account Management

1.1 Use Strong Passwords

- The length should not be less than 8 characters.
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
- Do not contain the account name or the account name in reverse order.
- Do not use continuous characters, such as 123, abc, etc.
- Do not use overlapped characters, such as 111, aaa, etc.

1.2 Change Password Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

1.3 Assign Accounts and Permissions Reasonably

According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.

1.4 Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

1.5 Set and Update Passwords Reset Information Timely

The platform supports password reset function. To reduce the risk of being attacked, please set up related information for password reset in time. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

1.6 Enable Account Binding IP/MAC

It is recommended to enable the account binding IP/MAC mechanism to further improve access security.

2. Service Configuration

2.1 Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

2.2 Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.

3. Network Configuration

3.1 Enable Firewall Allow list

We suggest you to enable allowlist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the allowlist.

3.2 Network Isolation

The network should be isolated by partitioning the video monitoring network and the office network on the switch and router to different VLANs. This prevents attackers from using the office network to launch Pivoting attacks on the video monitoring network.

4. Security Auditing

4.1 Check Online Users

It is recommended to check online users irregularly to identify whether there are illegal users logging in.

4.2 View the Platform Log

By viewing the log, you can get the IP information of the attempt to log in to the platform and the key operation information of the logged-in user.

5. Physical Protection

We suggest that you perform physical protection to the device that has installed the platform. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware.

6. Perimeter Security

We suggest that you deploy perimeter security products and take necessary measures such as authorized access, access control, and intrusion prevention to protect the software platform security.

【让社会更安全 让生活更智能】

ENABLING A SAFER SOCIETY AND SMARTER LIVNG