WHITE PAPER

Secure Communication Technology

i-PRO Video Surveillance Systems

Table of contents

© i-PRO Co., Ltd.. All rights reserved.

1. Introduction

Cyber attacks on IoT devices are on the rise in recent years, with video surveillance systems connected to the Internet also being the target of cyber attack. Resistance to cyber attack is thus becoming an important factor to look at when selecting the appropriate video surveillance system. Some models of i-PRO's i-PRO series cameras ship with digital certificates preinstalled, and they can encrypt communications, detect alteration, and prevent spoofing right after being set up. By equipping with data encryption functions, countermeasures against data leakage can be performed end-to-end.

This white paper explains i-PRO series security functions of communications encryption and falsification detection using digital certificates as well as data ciphers.

2. Cipher technology and certificates

Ciphers, digital signatures, and digital certificates are some of the basic technologies of cyber security. This chapter explains the basic details of those technologies.

2.1. Cipher technology

Encryption means to rearrange information of text and digital data following set rules to prevent the content from being understood by third parties. Modern encryption is usually separated into algorithms that are exchanged and data called keys applied to those algorithms, with just the key ordinarily kept secret. Cipher systems are classified into the two major types according to properties of the keys and how they are used.

- Symmetric-key cryptography
- Public-key cryptography

Symmetric-key cryptography can be compared to a house key, with the key for encryption and the key for decryption being the same. In cyberspace, data can be snooped on relatively easily in a communication path, so how to share the key between the sender and receiver becomes an issue. DES, 3DES, RC4, and AES are examples of cryptography using the symmetric-key cryptography system, and they usually have higher speeds compared with public-key cryptography.

© i-PRO Co., Ltd.. All rights reserved.

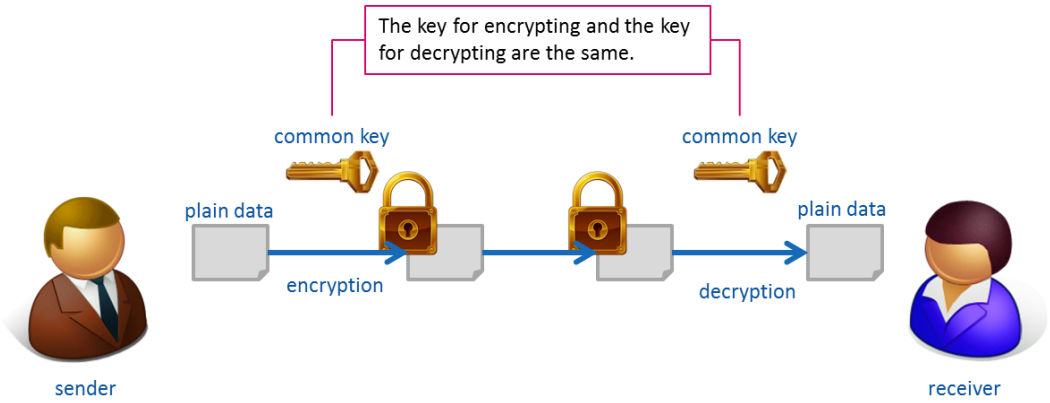


Figure 1: Symmetric-key cryptography

Public-key cryptography uses a pair of different keys called a public key and a private key. Data encrypted by one of the keys can only be decrypted by the other key, and it is difficult to guess one key from the other key. The method of communication is by the receiver first generating a pair of keys and sending the public key to the sender. The sender uses the public key to encrypt the data to send, and the receiver decrypts the cipher text with the private key. Data encrypted by the public key can only be decrypted by the private key, so safe communications is possible unless the private key is leaked. This method does not require the private key to be shared, so the issue of key sharing with symmetric-key cryptography is overcome. RSA is an example of a cipher using the public-key cryptography system.

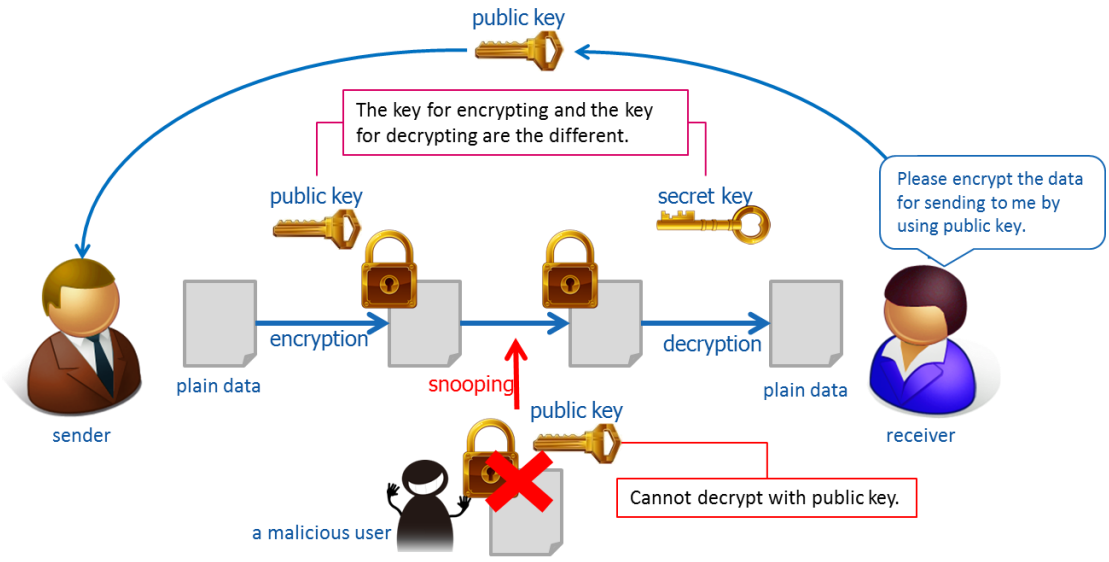


Figure 2: Public-key cryptography

© i-PRO Co., Ltd.. All rights reserved.

2.2. Digital signature

Digital signatures are technology to certify that data is created by the person it is purported to be from. Specifics of the certification method are as follows.

[At creation of data (signature)]

I. The data creator (sender) generates public and private keys and sends public key to receiver.
II. The creator calculates hash value (message digest).
III. The hash value is encrypted by creator's private key. This is the digital signature.
IV. The digital signature is added to the data, and the data is sent to the receiver.

[At data verification (certification)]

I. The receiver calculates the hash value (A) of received data.
II. The receiver extracts the digital signature from received data and decrypts by the public key (B) received from creator.
III. If A and B are match, B is confirmed to be encoded by the private key known only by the creator, and the data is certified as being created by the creator.

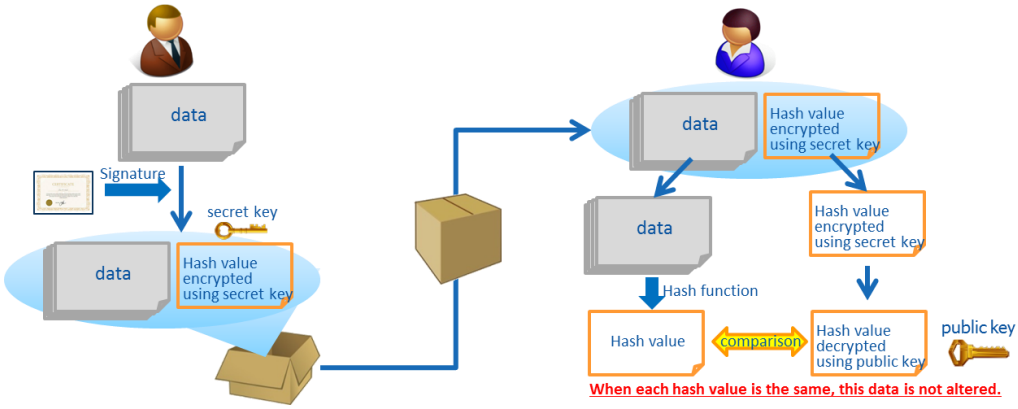


Figure 3: Digital signature

© i-PRO Co., Ltd.. All rights reserved.

2.3. Digital certificates

2.3.1. Overview of digital certificates

A digital certificate uses the aforementioned public-key cryptography and digital signature technologies, and it has the following three roles.

I. Storing the public key and the owner information of the private key paired with that
II. Accreditation by a third party that the data is true
III. Certification that the data is not falsified.

Certificates fulfill these roles by third parties digitally signing public keys and owner information.

2.3.2. Types of digital certificates

Digital certificates are classified into two major types according to who the signer is.

- CA-signed certificates
- Self-signed certificates

The following section explains the features and differences of those.

2.4. CA-signed certificates

2.4.1. Procedures for issuing CA-signed certificates

A CA-signed certificate is a digital certificate signed by a Certification Authority (CA) acknowledged to be socially correct. CA-signed certificates are ordinarily generated by the following procedure.

I. A pair of public and private keys is generated in the device.
II. A certificate signing request (CSR) is generated in the device based on the pubic key and its owner information.
III. The device owner sends the CSR to the CA by means such as e-mail.
IV. The CA checks to see if information of the CSR received is correct.
V. If information is acknowledged to be correct, the CA's private key is signed and a certificate is generated.
VI. The CA sends the certificate back to the device owner.
VII. The device owner installs the certificate to the device.

When installing CA certificates to security devices, the persons who set up those devices must conduct the procedure above for each device. Steps Ⅲ to Ⅵ take a few minutes to a few weeks, as described in the next section, leading to increased time-related costs in setting up.

© i-PRO Co., Ltd.. All rights reserved.

2.4.2. Types of CA-signed certificates

CA-signed certificates are classified into the three types below according to the difference in examination method employed in step Ⅳ, above.

Type	Examination method	Usual time required for examination	Features	Price
Extended validation certificate (EV)	Confirmation of existence of company's legal address	A few weeks	Address bar turns green when accessed by a browser.	High
Organization validation certificate	Confirmation of company's legal existence	A few days	Company name can be noted on the certificate.	Medium
Domain validation certificate	Confirmation of name that domain is registered under	A few minutes	Low cost and fast time to issue	Low

Digital signatures of certificates are screened by CAs acknowledged to be socially correct to verify the owner of the key, but care needs to be taken regarding the differences in the examination methods above.

With the lowest-costing domain validation, a certificate can be issued as long as the applicant has ownership rights to the domain (common name) noted on the certificate. A domain can be obtained by anyone for a few tens of US dollars a year and an "official" CA certificate can be easily obtained even by someone with malicious intent. In actual online banking phishing, CA certificates obtained in this way are used to put on a show of being safe.

2.4.3. Trustworthiness of the CA itself

Digital signing of a CA-signed certificate is done by a private key owned by a CA, so if that private key should be leaked, all the certificates the CA signed in the past will no longer be trustworthy. For this reason, how the CA stores private keys needs to be noted. There have been cases in the past where private keys were leaked due to cyber attack and unauthorized CA-signed certificates were issued. Certificate authorities deemed to be highly trustworthy put much time, effort, and money into preventing leakage.

© i-PRO Co., Ltd.. All rights reserved.

2.5. Self-signed certificates

With a self-signed certificate, the digital certificate is signed by the device itself, not a third party. Ordinary methods of generation are as follows.

I. A pair of public and private keys is generated in the device.
II. A certificate signing request (CSR) is generated in the device based on the pubic key and its owner information.
III. The CSR is signed by the aforementioned private key generated in the device.

Being able to sign by oneself allows examination by a third party to be omitted, so a certificate can be generated instantly and expenses for issuing are not incurred. But as there is no guarantee of the identity by a third party, there is no function to accredit that certificate information is true, one of the three roles in 2.3.1. This means that if a person with malicious intent intercepts the certificate when it is being sent to the other party and replaces that with another self-signed certificate, there is no way to verify it, so there is risk of spoofing. Self-signed certificates should only be used for encrypted communications if the identity of the data sender is guaranteed by another method. Many video surveillance system devices have a function to generate self-signed certificates, but caution is needed because this point is not often explained.

2.6. Selecting a certificate

As shown, the roles of digital certificates of storing public key and owner information and of preventing falsification of content written in the certificate are the same for all types of certificates, but trustworthiness varies greatly between digital certificates in the role of certifying the owner. In order to prevent spoofing with network cameras, organization validation certificate or stronger CA-signed certificates should be introduced; however, it takes time to issue those certificates and the price is high. Moreover, installing a certificate for each camera when tens to hundreds of network cameras are set up leads to increased setup expenses.

© i-PRO Co., Ltd.. All rights reserved.

3. Preinstalled certificate with i-PRO series cameras

Some models of i-PRO series cameras will ship with certificates preinstalled at time of manufacture, starting in April 2016. That way, customers who purchase those devices will be able to use various security functions that employ certificates right away without having to go through the process of issuing certificates at time of setup. With i-PRO cameras with Secure function, private and public keys are generated at manufacture in the factory and certificates installed at the factory. As there is no way to obtain the private key from the camera externally, there is no risk of the private key being leaked. Also, certificates are signed by a trusted third party, and the private key used for signing is managed strictly by the authority.

As for examination at time of issuing certificates, only certificates for which a request for issuing is appropriately made at manufacture in a i-PRO factory are signed, and stringent measures are taken to prevent unauthorized issuing of certificates. In order to identify certificates issued in this manner, special root CA certificates (digital certificates owned by certificate signer) are used. These root CA certificates are only signed for i-PRO video surveillance system devices, so spoofing can be easily uncovered when the root CA certificate is checked.

4. i-PRO's secure functions

4.1. SSL/TLS communications

Currently, much communications between video surveillance system devices (for example, network cameras) and clients (PCs, recorders, mobile terminals) is by unencrypted plain text. If packets flowing in switching hubs, routers, and the like between servers and clients can be observed, the content of the communications can easily be snooped on. This includes not just the video data in the communications, but also the IDs/passwords for logging into the cameras, so persons with malicious intent can easily take control of the cameras if they can get inside. And by altering the path information and packets themselves, it would be possible to spoof the server.

Such problems are solved by using digital certificates preinstalled in i-PRO cameras and communicating by SSL/TLS. Things that can be done by SSL/TLS communications are as follows.

© i-PRO Co., Ltd.. All rights reserved.

4.1.1. Protection of contents of communications

This explains the mechanism by which contents of communications is protected using SSL/TLS. With SSL/TLS communications, the client first receives a certificate from the server, and the private value that the common key is based on is encoded by the public key included in the certificate. That value is then sent to the server, and the server extracts the common key from the value decrypted by the private key only the server has. Afterward, data to be transmitted based on this common key is encrypted and transmitted. For that reason, even if packets are observed by someone on the transmission path with malicious intent, the data cannot be understood by parties who do not have the private key. SSL/TLS communications can be achieved by entering https:// in the address bar of a browser.

4.1.2. Guarantee that communications is with the correct server

Next, we explain the mechanism for guaranteeing that the party being communicated with is correct. Judgment of whether or not the party being communicated with is correct is done by signing of a certificate received from the server at start of SSL/TLS communications. As explained in 2.4 what Certificate Authority is signed by is very important. First of all, with a self-signed certificate, signing is done by oneself, so no identify confirmation can be done. Therefore, spoofing cannot be prevented. And with CA-signed certificates, CA identity and evaluation method need to be confirmed well, and spoofing cannot be prevented with some signers. On the other hand, i-PRO cameras preinstalled certificates are signed by a highly trustworthy method as explained in 3, so spoofing cannot be done.

In this way, conducting SSL/TLS communications using preinstalled certificates with i-PRO cameras provides two kinds of safety in that eavesdropping on the communications path and spoofing of devices are prevented.

4.2. Detecting falsification

Another way of using certificates is to prevent falsification of video and audio data recorded by cameras. Data recorded directly to an SD card or other media from the camera and exported data of recordings by recorders can be falsified when carrying the media. In using recorded data as evidence, the need to prove that data is not falsified is an issue.

That issue is solved by using certificates preinstalled in i-PRO cameras. First, recording data is signed by the private key in the camera when recording video on the SD memory card. When detecting falsification after that data is transported, the camera’s certificate is input in advance and signing is verified by the public key included in the certificate. If verified to be correct, the data is proven not to be falsified.

Detection of falsification can be done by signing when the recorder or other recording device

© i-PRO Co., Ltd.. All rights reserved.

receives the data, but detection is not possible if falsification was done between the camera and recorder in this case. For that reason, it is important to sign within the camera.
Also, there is a risk of spoofing in detection of falsification as well with some types of certificates. For example, if someone with malicious intent falsifies data while it is being transported and signs the data with their own certificate then replaces the original certificate with their own, signing is successfully verified and it is judged that there is no falsification. With certificates preinstalled in i-PRO cameras, a root CA certificate is unique, so by confirming the signer of the certificate, it is known that the certificate was signed within the camera, thereby preventing spoofing.
In this way, detecting falsification using preinstalled certificates with i-PRO cameras provides two kinds of safety in that falsification of recorded data and spoofing of signed devices are prevented.

4.3. Data cipher

With network camera systems, there is risk of private information being leaked due to incidents such as video data from the network stream being eavesdropped on and loss or theft of media on which video is recorded, but video data is encrypted with
i-PRO cameras to protect from such threats.

4.3.1. Stream protection

The H.264 stream, which is video data, is encrypted in real time and delivered by a network. Video is encrypted by the network camera that generates it, so the video cannot be viewed even if the communications route to connected devices is eavesdropped on. Unlike with SSL/TLS communications, video data is encrypted, so data can be transferred by ordinary video data communications protocols (RTP, etc.) without relying on the communications protocol. Also, special equipment does not have to be equipped to the connected devices.

4.3.2. Recorded data protection

i-PRO cameras can record video data to SD cards in H.264 format, and recording encrypted video data is possible. Even if the SD card in use is stolen or a stored SD card is lost, third parties will not be able to view the video even if they play back MP4 files on the SD card if the data is encrypted.[*1]
And in a system configuration where video data is recorded on a recorder, server, or other recording device, encrypted data can be generated even if the recording device does not have an encryption function by encrypting video data by the network camera. There is no need to decrypt in the interval from generating and encrypting video data on the network camera to saving to a recording device, and the data is constantly encrypted, so there is no risk of decrypted video leaking from the recording device even if the recording device is infected by a virus or comes under cyber attack.
*1: Authorized viewers can play back video with a dedicated viewer after being authenticated.

© i-PRO Co., Ltd.. All rights reserved.

4.3.3. Encryption method

Encryption is by a high-speed cipher system that combines a secret sharing scheme using a i-PRO proprietary high-speed algorithm with a symmetric-key cryptography system. The following covers the features of that.

4.3.3.1. Strength of cipher

Unlike simple cipher systems made lightweight for embedded devices, the cipher has strength equal to or greater than ordinary symmetric-key cryptography systems. The secret sharing scheme has computationally security greater than AES-256 bit, and by combining a symmetric-key cryptography system that uses key length of 256 bits, cipher strength is equal to or greater than AES-256 bit.

4.3.3.2. Load

Processing load is reduced compared with ordinary symmetric-key cryptography systems (AES-256 bit), so delay due to encryption is miniscule.*2 Theoretically, greater reduction effects can be expected the more the data volume increases due to high bit rate and high resolution, so this can be applied to 4K cameras as well.

And in contrast to encryption processing by connection destination when encrypting by communications protocol, there is no increase in encryption load when encoding video data, even if the number of videos distributed increases (at the same resolution).

*2: See Figure 4

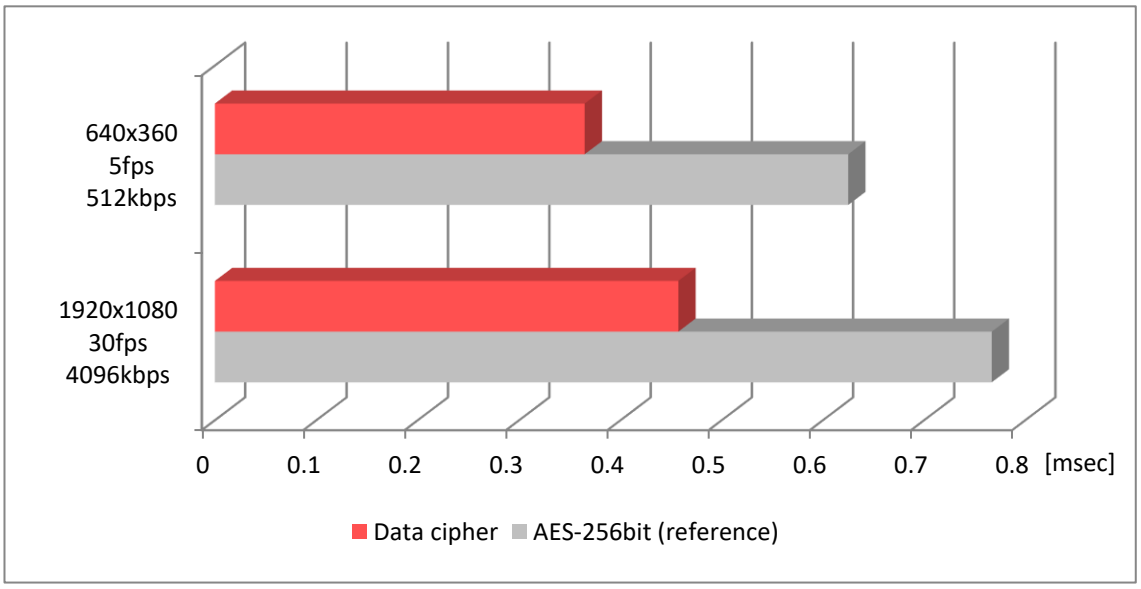


Figure 4: Encryption processing time (calculated for WV-SPN631)

© i-PRO Co., Ltd.. All rights reserved.

4.3.3.3. Data size

Increase in data volume due to encryption is kept to about 2%, so there is almost no effect on communications band and storage capacity.

4.3.3.4. Software implementation

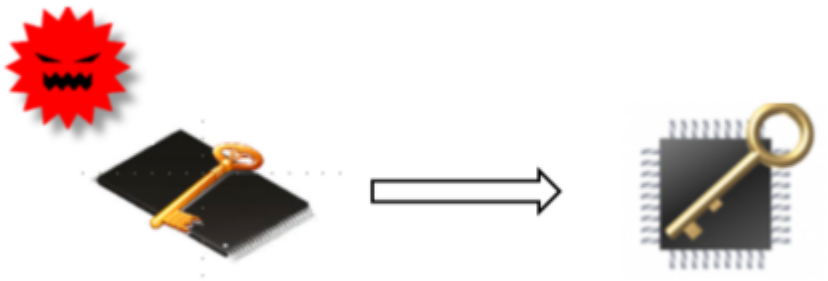
Encryption processing is implemented by software, so encryption functions are enabled even for i-PRO cameras that are already set up by updating software. Also, special hardware is not needed for video data playback, and the data can be decrypted by software.*3

*3: Symmetric-key cryptography system used in combination uses ordinary cipher hardware assist to enable further increase in processing speed.

4.4. FIPS 140-2/140-3 Level 3 with Secure Element

4.4.1.1. Objective

Encryption Algorithm can be roughly classified into symmetric key cryptosystem and the public key cryptosystem. SSL/TLS realizes encrypted communication by combining these 2 cryptosystems. The communication can be invaded and disclosed by a third party who intercepts and decrypts the transmitted content if these security keys are disclosed. Thus, protecting the keys from being exposed is the most important role of the cyber security schemes. It is often the case that these private keys are stored in a non-volatility memory such as flush ROM of a built-in device. However, this flush ROM is vulnerable to external invasions into the device and that the risk of compromising confidential information is rather high. On that account, storing private keys in a tamper-resistant IC (TPM, secure element etc.) is more effective to protect a device. i-PRO provides device with embedded Secure Element to protect private keys.



© i-PRO Co., Ltd.. All rights reserved.

4.4.1.2. Secure Element

Secure Element and CPU are connected via bus, in which the communication contents are encrypted in between. RSA private key used for public key encryption is stored in Secure Element and more than one RSA private key can be stored. Application that provides RSA operation requests RSA operation to the Secure Element via CPU, then the Secure Element will return the outcome of the operation. This makes it difficult to know RSA private key from outside as RSA private keys stored in Secure Element cannot be reached through CPU.

4.4.1.3. FIPS 140-2/140-3

FIPS（Federal Information Processing Standard） is an information processing standard standardized by NIST in the U.S. In this standard, security requirement for encrypted module is specified in the section FIPS 140-2/140-3. There are 4 security levels from level 1 to 4 stated in FIPS 140-2/140-3 where level 4 is the highest. Secure Element that is certified as level 3 is used for i-PRO devices. i-PRO will now be transitioning to FIPS 140-3 compliant secure elements. Please refer to NIST website (www.nist.gov) to learn more about FIPS.

4.4.1.4. Applying Secure Element to i-PRO devices

Applying Secure Element to i-PRO devices

The i-PRO device features listed below uses Secure Element.

HTTPS・SRTP (Used in RTSPS for SRTP)

SD tamper detection

HTTPc（to be supported in near future）

The features mentioned above will need a pre-installed license or externally generated CA license in the device. Secure Element can protect RSA private keys that is paring with such licenses. RSA private keys are generated at the same time when this license is created.

The license created by GrobalSign K.K is pre-installed in i-PRO devices. RSA private key is generated within Secure Element before the device leaves our factory to be paired with the public key included in the pre-installed license.

5. Conclusion

As previously noted, there are potentially many threats to video surveillance systems, such as eavesdropped and falsification of data and spoofing of devices, and resistance to those threats will probably become even more important in the future with advances in IoT. i-PRO is continuously working to improve security to achieve a safe and secure society from the perspective of cyber security by quickly identifying and overcoming those threats.

© i-PRO Co., Ltd.. All rights reserved.

Akihiro Nawata

Expert Engineer-Embedded Software

The Power of Truth

i-PRO Co., Ltd.. All rights reserved

7-9-66 Hakozaki, Higashi-ku, Fukuoka-shi, Fukuoka, 812-0053 Japan

i-pro.com/corp/jp/

© i-PRO Co., Ltd.. All rights reserved.