ISSN: 2664-9640

Application of Cryptography in Intelligent Connected Vehicles

Wen Shao[1, a], Baizheng Wang[1, b] and Xiong Zhao[1, c]

[1] CATARC Software Evaluation (Tianjin) Co., Ltd, Tianjin 300300,China.

[a] shaowen@catarc.ac.cn, [b]wangbaizheng@catarc.ac.cn, [c] zhaoxiong@catarc.ac.cn

Abstract

With the promulgation of the Password Law of the People's Republic of China and the Administrative Measures for the Construction of National Government Information Projects (GBF (2019) No. 57), the importance of network security with password as the core has become increasingly prominent. As the foundation and core technology of the network security of ICV, the password technology is described from the aspects of the application architecture, core technology, protection capability, application field of solution, password application practice, etc. At the same time, the password products of ICV industry are analyzed, focusing on the application of password technology in ICV.

Keywords

Password; Certification system; Key; CA.

1. Introduction

Driven by a new round of scientific and technological revolution and industrial revolution, ICV has become an important strategic direction for the development of the global automotive industry. At present, ICV has gone out of the laboratory, and the carrying rate of some auto drive system on passenger vehicles has gradually increased, and it has begun to move towards the stage of open road actual testing and commercial demonstration.

China vigorously promotes the construction of new infrastructure. The new infrastructure includes a new round of network construction and data information related services, such as 5G, big data center, cloud computing center, artificial intelligence, etc. It is essentially the infrastructure of information digitization and the information infrastructure supporting the development of traditional industries in the direction of networking, digitization and intelligence. It is not difficult to find that digital infrastructures such as 5G, big data center, artificial intelligence, cloud computing, etc. involved in the new infrastructure are closely related to the Internet of Vehicles, which will certainly promote the rapid development of the Internet of Vehicles.

Made in China 2025 has set a clear development goal for ICVs, that is, by 2020, master the overall technology and key technologies of intelligent assisted driving, and initially establish an independent research and development system and production supporting system for ICVs. By 2025, master the overall technology and key technologies of automatic driving, establish a relatively complete independent research and development system, production supporting system and industrial cluster of intelligent connected vehicles, and basically complete the transformation and upgrading of the automobile industry. Like new energy vehicles, automatic driving technology and intelligent connected vehicles have reached the height of national strategy.

Cryptography is the core technology to ensure the security of the Internet. The control of cryptographic algorithms and products is the top priority to ensure the information security of our country. At present, our country adopts many encryption algorithms developed abroad, and there are uncontrollable factors of the amount of encryption. Once the encryption algorithm is

ISSN: 2664-9640

attacked by illegal distribution of profits, the losses will be immeasurable. It is the most effective method to prevent backdoor loopholes and the ultimate measure to ensure the security of the network to realize the national production and replacement of the main controllable software and hardware of password products. Guomi algorithm has the main intellectual property rights, which is in line with the national information product localization strategy. With the further strengthening of the domestic substitution trend, the Guomi algorithm is expected to accelerate the substitution of international algorithms such as RSA in the stock market. This paper mainly analyzes the password products of the intelligent network connected automobile industry, focusing on the service supply relationship, and comprehensively analyzes the upstream and downstream of the industrial chain.The architecture of digital certification center is shown in Figure 1:

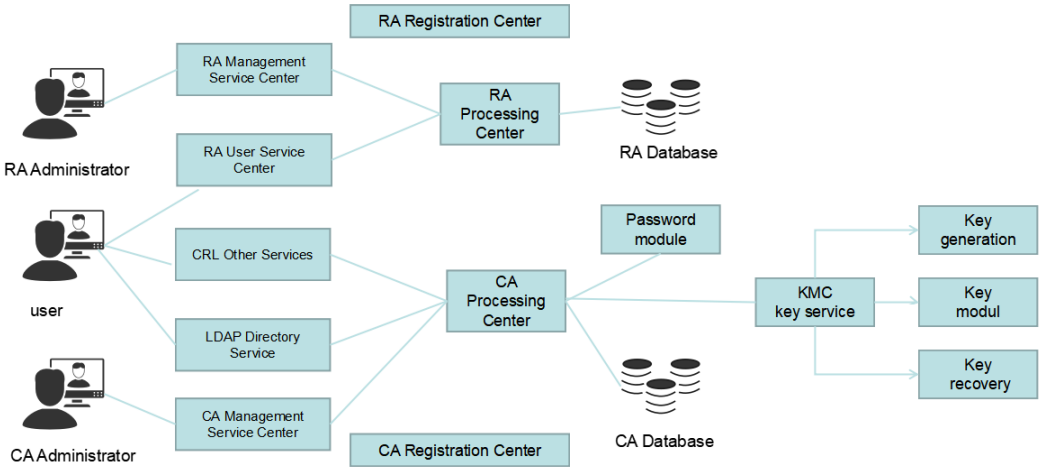

Fig.1 The architecture of digital certification center

The CA system is the main service system of the digital certificate authentication system. It is used to initialize the user's digital certificate authentication system, configure the digital certificate policy template, edit and set the types and quantities of certificates that can be issued, including single key pair digital certificates, double key pair digital certificates, file digital certificates, USBKey digital certificates, mobile digital certificates, etc., standardize the registration content of digital certificates, and publish digital certificates to LDAP services, Issuing and managing user digital certificates, issuing and managing CRL publishing, providing OCSP service interfaces, etc. In addition, the secondary CA root certificate is saved and managed by the CA system. The CA system will also register and authorize the RA system. Only the authorized RA can apply for and issue certificates to the CA system. At the same time, it controls the types and quantities of certificates that can be issued by the RA. It is the most core functional system in the digital certificate authentication system, except for the key.

RA system is a system for digital certificate authentication system to register and audit users. It is an important bridge between users and CA system. It is mainly responsible for information entry, registration and audit of users, and submitting the results to CA system. After CA system issues a digital certificate, the digital certificate is transmitted to the end user through RA system for downloading. In addition, it also provides a variety of certificate application and download methods, including online application, offline application, mobile phone application and other functions. It supports a variety of interface applications, downloading digital certificates. It is the most front-end digital certificate authentication system for users and applications, and can be expanded.

Lightweight Directory Access Protocol (LDAP) service is another important service provided by digital certificates in actual operation management and application. LDAP provides a fast search and query service for users' digital certificates, which can facilitate users to quickly search and query any digital certificate issued by the digital certificate authentication system

ISSN: 2664-9640

and its corresponding public key. For a digital certificate, users can first determine whether it is issued by a trusted authority and whether it can be searched in a trusted digital certificate authority. In addition, LDAP can also regularly receive the update service of the CA system, provide external search, query and download of certificate revocation list (CRL), and provide blacklist for the authentication service in the digital certificate application to help the application authenticate the further validity of the user's digital certificate.

The certificate real-time status query (OCSP) service is an important service provided by digital certificates in the actual operation management. It can provide users with real-time certificate status query. After users provide the search information of digital certificates, they can feed back the current real-time status of the certificate, including revocation, freezing, validity, expiration, and invalidity. It can provide accurate status feedback for effective and sensitive applications of digital certificates.

Lightweight Directory Access Protocol (LDAP) service is another important service provided by digital certificates in actual operation management and application. LDAP provides a fast search and query service for users' digital certificates, which can facilitate users to quickly search and query any digital certificate issued by the digital certificate authentication system and its corresponding public key. For a digital certificate, users can first determine whether it is issued by a trusted authority and whether it can be searched in a trusted digital certificate authority. In addition, LDAP can also regularly receive the update service of the CA system, provide external search, query and download of certificate revocation list (CRL), and provide blacklist for the authentication service in the digital certificate application to help the application authenticate the further validity of the user's digital certificate.

2. Key management system

The key management system is used to manage the whole process of data encryption and decryption key generation, use, storage and backup recovery in the entire security system, to ensure the security of the key in its full life cycle, that is, to maximize the security of data content (the algorithm is much more difficult to crack than the attack key). The management of various keys in the key management system shall uniquely determine the corresponding key according to the key identification, key version number and key type for processing. The key must be transmitted in a secure message.

2.1. Key generation and storage update

Use the internal physical noise source (such as WNG4) to generate hardware random numbers. The random numbers after passing 15 tests (frequency test, sequence test, autocorrelation test, poker test, run test, etc.) are used as key materials. The key is a piece of data selected from the key material library. The key must be stored securely. Key transmission process, key management system database and other environments, and the key exists in the ciphertext state. The storage carrier of the key can be a mobile storage device, a hard disk, a floppy disk, a CD, etc. All application keys have certain attributes, including type, version, index, validity, etc. The key of each version is given a certain validity period. When the validity period of the key expires, the key of the next version can be easily enabled.

2.2. Identification management system

Backing up various keys is a necessary key management work. The key management system must provide the means of key backup/recovery operation. Only when the system key is lost or the system is damaged can the system be restored to its original state and return to normal operation. The key must be backed up when it is changed or added.

Use the password algorithm and encryption equipment certified by the National Cryptographic Administration, comply with the requirements of the Certificate Authentication System

ISSN: 2664-9640

Password and Related Security Technical Specifications issued by the National Cryptographic Administration, and provide technical and policy security for PKI application fields together with the Certification Center system.

The key management system is mainly applied to the business scenarios that require the generation, distribution and use of symmetric and asymmetric keys, and can provide external key management of multiple cryptographic algorithms. For example, it provides asymmetric key service to CA system and symmetric and asymmetric key service to data encryption application system.

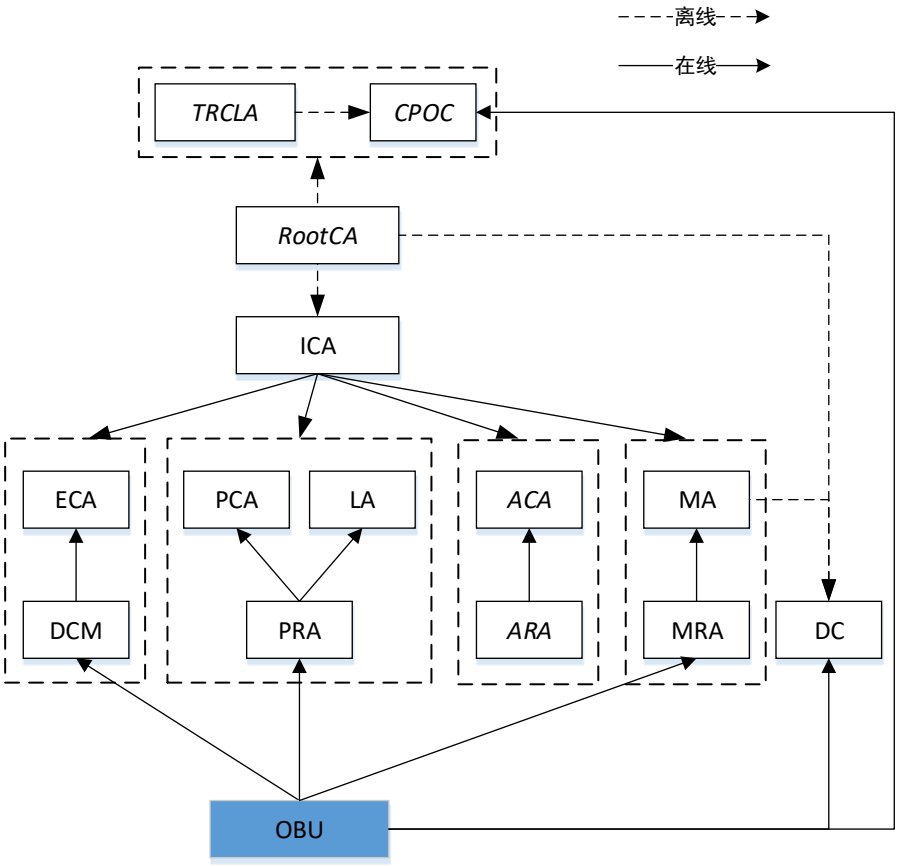

Fig. 2 The authentication system

3. Application of Password in Intelligent Network Connected Vehicle

3.1. Intelligent transportation digital certificate system

The intelligent transportation certificate authentication system is a certificate security management system suitable for intelligent connected vehicles. The design of the intelligent transportation certificate authentication system conforms to the specification of Technical Requirements for LTE based Internet of Vehicles Wireless Communication Technology Security Certificate Management System, and realizes the process management of the whole life cycle of V2X certificate.

The intelligent transportation certificate authentication system uses the cooperation of multiple subsystems, such as root CA, registration CA, pseudonym CA, application CA, abnormal behavior management system, link value management system, to build a set of V2X Internet of Vehicles network trust support platform, which shields communication differences and supports docking vehicles of different enterprises. The intelligent transportation certificate

ISSN: 2664-9640

authentication system realizes the identity authentication in the process of vehicle, road, cloud and terminal communication, ensures the confidentiality and integrity of communication data and the privacy of vehicle information in the Internet of Vehicles scenario, and provides a handle for the network security management of intelligent connected vehicles.The authentication system is shown in Figure 2:

3.2. On board password module

The on-board password module can be divided into hardware password module, software password module and firmware password module according to different password boundary division methods.

Hardware password module

The password boundary is defined as the hardware boundary. Firmware and software can be included within the hardware boundary, which can also include operating systems, such as security chips.

Software password module

The password boundary refers to pure software parts (one or more software parts) and data components executed in a modifiable operating environment. The computing platform and operating system included in the running environment of the software password module are outside the defined password boundary. Modifiable operating environment refers to the configurable operating environment that can add, delete, and modify system functions, such as Windows/Linux/MAC/Android/iOS and other general operating systems.

Firmware password module

The password boundary delimits the boundary for pure firmware components that are executed in a restricted or unmodifiable operating environment. The computing platform and operating system included in the operating environment of the firmware password module are outside the defined password boundary, but are explicitly bound to the firmware module. Restricted operating environment refers to software or firmware modules that allow controlled changes, such as TEE operating system based on trusted execution environment technology.

3.3. Specific application of password module at vehicle end

The password requirements for vehicle terminal security are mainly embodied in key management, safe startup, security upgrade, identity authentication, user privacy data encryption, etc. Specific applications include but are not limited to the following functions:

(1) Key Management

The password module provides key generation, key storage, key use and other functions. Key generation includes the generation of preset key and symmetric/asymmetric key of vehicle terminal; The key storage needs to be encrypted, and strict security measures should be taken to prevent the key from being illegally obtained; Key usage provides data signature and signature verification, data encryption and decryption, hash and verification and other computing services for upper security measures to ensure data confidentiality, integrity, availability and non repudiation.

(2) Safe start

Safe startup refers to enabling the trust source mechanism in the vehicle terminal. The root certificate is embedded in the password module of on-board equipment to verify the signed boot loader. Then, the signed boot loader verifies the signed kernel or the signed second level boot loader to realize the trusted startup function of the vehicle terminal.

(3) Security upgrade

The password module provides the ability to self check the upgrade and update request of the on-board terminal. When the on-board operating system updates its own partition or transmits

ISSN: 2664-9640

update files and update commands to other devices, it declares its identity and authority through security technology. During the upgrade operation, verify the identity of the server and identify forged servers or high-risk links. During the transmission of the upgrade package, the message signature and encryption are used to prevent the upgrade package from being tampered with and forged.

(4) Identity authentication

When the on-board terminal communicates with the service network, it provides two-way authentication between the on-board terminal and the service network to confirm the legitimacy of the other party's identity. During data transmission, it encrypts and protects the communication data to ensure that the information is not eavesdropped, forged, tampered with, or replayed during transmission. In the process of direct connection communication, provide on-board terminal to authenticate the message source to ensure the legitimacy of the message; Support message integrity and anti replay protection to ensure that messages are not forged, tampered with and replayed during transmission; Support the confidentiality protection of messages, ensure that messages are not eavesdropped during transmission, and prevent the disclosure of user sensitive information; It supports hiding the real identity and location information to prevent users from disclosing their privacy. It can resist the forgery, tampering and other security attacks of illegal subjects, and ensure the safe and reliable operation of the vehicle terminal system.

(5) User privacy data encryption

The configuration data, log data, collected data and other sensitive data of the on-board terminal can be secured through the password module, including hash value calculation, symmetric encryption, asymmetric encryption and other technical means to ensure that the stored information will not be stolen by a third party through physical methods.

3.4. Function of on-board password module

The new energy and intelligent connected vehicle password application industry chain has established a standard specification system and an operation and maintenance management system. Clarify the requirements for the password application system involved in the information security of ICV, and establish a password application system standard and operation and maintenance management system covering the whole life cycle process of data generation, transmission, storage, use, interaction and destruction of ICV, including the vehicle, vehicle cloud, vehicle person, vehicle road and in vehicle business scenarios on the cloud end.

The on-board password module has become an important direction to strengthen the security protection of intelligent connected vehicles. Through the password module, identity authentication and password services are provided to securely store identity identification, key and other sensitive data. Local control security and data security of key components at the vehicle end, configure a secure communication channel, verify the encryption key, issue control instructions, perform security upgrades and audits, etc., and open up the new energy of vehicle terminals and the password application industry chain of intelligent connected vehicles in the security application field. Based on the life cycle of vehicle terminal data and centering on the data life cycle, an attack defense and communication security protection system covering cloud, network and end based on cellular network and short distance network communication protocol is established, and a software and hardware integrated protection system matched with the evolution of the new electronic and electrical architecture of intelligent networked vehicles is built to form an information security system of intelligent networked vehicles throughout their life cycle.

ISSN: 2664-9640

4. Conclusion

This paper focuses on the analysis of key management system, vehicle application, authentication system and vehicle password module from the perspective of password technology, and analyzes their principles and functions from a technical perspective, making great contributions to the high-quality development of password products in the intelligent connected automobile industry. The importance of network security with password as the core has become increasingly prominent.

References

[1] Blockchain-Based Decentralized Trust Management in Vehicular Networks. [J] . Zhe Yang,Kan Yang 0001,Lei Lei 0004,Kan Zheng,Victor C. M. Leung. IEEE Internet of Things Journal . 2019 (2).

[2] A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks [J] . Gao Feng,Zhu Liehuang,Shen Meng,Sharif Kashif,Wan Zhiguo,Ren Kui. IEEE Network . 2018 (6).

[3] LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem [J] . Huang Xiaohong,Xu Cheng,Wang Pengfei,Liu Hongzhe. IEEE Access . 2018.

[4] An Anti-Quantum Transaction Authentication Approach in Blockchain [J] . Yin Wei,Wen Qiaoyan,Li Wenmin,Zhang Hua,Jin Zhengping. IEEE Access . 2018.

[5] Blockchain-based secure firmware update for embedded devices in an Internet of Things environment [J] . Boohyung Lee,Jong-Hyouk Lee. The Journal of Supercomputing . 2017 (3).

[6] An Efficient Revocable Group Signature Scheme in Vehicular Ad Hoc Networks. [J] . Zhen Zhao,Jie Chen,Yueyu Zhang,Lanjun Dang. KSII Transactions on Internet and Information Systems （TIIS）:KSII Transactions on Internet and Information Systems（TIIS） . 2015 (10).

[7] A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks. [J] . Khaleel W. Mershad,Hassan Artail. IEEE Trans. Vehicular Technology . 2013 (2).