*Proceedings of CECNet 2021*
*A.J. Tallón-Ballesteros (Ed.)*


*doi:10.3233/FAIA210426*

# A Master Station and Terminal Data Exchange Method Based on Symmetric and Asymmetric Algorithms

Fan HE [a], Zhengquan ANG [b], Guanglun YANG [a], Qingqin FU [a1], Ling YI[c], Pingjiang XU [c], Jia LIU [c], Zhaoqing LIANG [c], Changsheng NIU [c] and Jianying CHEN[a]
[a] *ZhongGuanCun XinHaiZeYou Technology Co.Ltd, Beijing 100094, China*
[b] *Beijing aerospace flight control center, Beijing 100094, China*
[c] *Beijing Chip Microelectronics Technology Co., Ltd., Beijing 100192, China*

**Abstract.** This paper analyzes the disadvantages of the traditional method of data security between the master station and the terminal, and proposes a new method of data exchange between the master station and the terminal. This method improves the security of data interaction. In the process of using it, symmetric algorithm and asymmetric algorithm are combined, involving security mechanisms such as signature, certificate, MAC and symmetric encryption, so as to establish a secure link between the master station and the terminal, so as to protect the communication security between them.

**Keyword.** Master station, terminal, data interaction, symmetric algorithm, asymmetric algorithm

## 1. Introduction

In recent years, the State Grid Corporation has comprehensively promoted the construction of power consumption information collection systems. This system can achieve comprehensive coverage of all power users and gateways, realizing on-line monitoring of devices and real-time collection of important information such as user load, power, voltage, etc. Provide complete and accurate basic data for relevant systems, provide support for analysis and decision-making of all aspects of business management, and provide information foundation for intelligent two-way interactive services. This requires a large number of terminals to participate in the collection of data information. These power information's collecting devices can implement energy meter data collection, data management, data bidirectional transmission, and devices that forward or execute control commands.

To establish a comprehensive user power information collection system, it is necessary to construct a system main station, a transmission channel, an acquisition device, and an electronic energy meter. At present, most terminal data upload communication channels use GPRS communication. In order to ensure the safe and stable operation of the power user's electricity information collection system, to prevent the power supply interruption of the user, and to prevent a greater range of security

[1] Corresponding author, email: fuqingqin@icrus.cn

risks caused by the public network and the user terminal invading the primary station, the primary station and the terminal need to perform authentication when performing data interaction with the terminal. And encryption, which requires a method and rules for specifying data transmission between the primary station and the terminal [1-7].

## 2. Data exchange method between traditional primary station and terminal

The traditional method is: when the primary station interacts with the terminal data, the symmetric external authentication is performed first, and after the authentication is passed, the communication data is encrypted to ensure the secure transmission of the data.

The traditional method of interaction between the primary station and the terminal data, although there is an authentication operation before the data interaction, the symmetric algorithm is easy to be cracked and replayed, so the overall security is not high [8-20].

## 3. Master station and terminal data exchange method based on combination of symmetric and asymmetric algorithms

In order to overcome the problems caused by the traditional methods, this paper proposes a new data exchange method for the primary station and terminal for power. This method divides the interaction between the primary station and the terminal into three steps:

1) The first step is the establishment of a session between the primary station and the terminal;

2) The second step is to use the session key negotiated in the session for data encryption operation;

3) The third step is to resume the session between the two if the communication reaches the limit of the number of times. After the session is restored, the second step can be repeated.

These three steps use a combination of symmetric and asymmetric algorithms in the process of use, involving security mechanisms such as signature, certificate, MAC, and symmetric encryption, so as to establish a secure link between the primary station and the terminal, thereby achieving the communication between the two is secure.

The specific implementation of this method is as follows.

### *3. 1. Master station and terminal session establishment*

The specific process of session establishment is shown in Figure 1.

The specific method of session establishment is:

1. The primary station end group message 1, the specific organization message method is as follows:

1） Take the random number R1;

2） using a cipher machine to encrypt the random number R1 to obtain the ciphertext EKs1 (R1);

3) The version number represents the version of the protocol and the encryption algorithm used;
4) The session ID, initially initiated as 0, must be initialized to 0 once a day;
5) Take the master station certificate CM;
6) The MAC1 field is mainly used to use the last session key, the initial initiation, the field is filled with 0;
7) Digitally sign the version number, session ID, master certificate, MAC, and R1 to form signature S1.

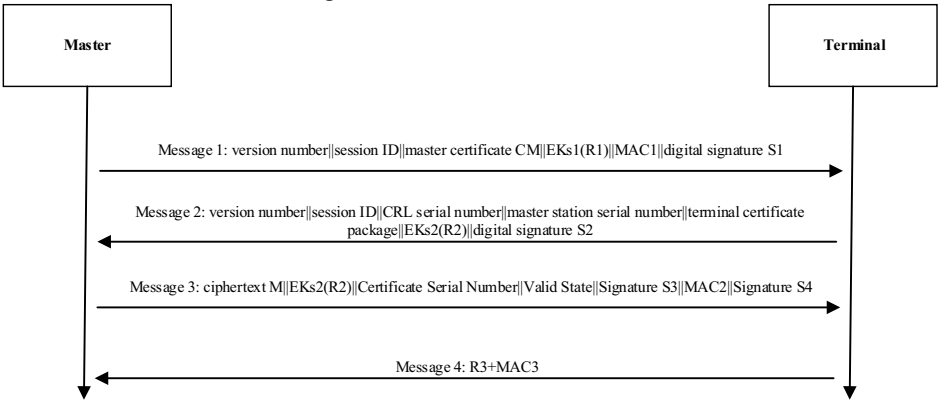


**Figure 1.** Master station and terminal session establishment process

2. The terminal receives the message 1 and performs the following operations:
1) Verify the validity of the master certificate CM;
2) decrypt EKs1 (R1) to get R1;
3) Verify the legality of signature S1;
4) The terminal ESAM chip generates a random number R2;
5) Decrypting R2 with key EKs2 to generate EKs2(R2);
6) Sign the S2 by using the terminal signature private key (version number, session ID, master certificate serial number, terminal certificate package, R2, R1).

3. The master station receives the message 2 and performs the following operations:
1) Verify the validity of the terminal digital certificate;
2) using the key EKs2 to solve the random number R2;
3) verify the signature S2 using the terminal signature public key;
4) The master station generates the master key K, and obtains the ciphertext M1 by using the terminal encryption public key encryption;
5) Upload the EKs2 (R2) obtained in the message 2 and its serial number to the certificate server;
6) using the master key K derived MAC key and initial vector, calculate the MAC for {(EKs2 (R2) + certificate serial number + valid state) + signature S3}, generate MAC2;
7) Sign the previous part using the master private key to form the signature S4.

4. The terminal receives the message 3 and performs the following operations:
1) Verification signature S4

2) Verify its signature information, certificate serial number and generated EKs2(R2) to determine if the master certificate is correct;
3) Using the terminal private key to unlock the ciphertext M1, and obtaining the master key K;
4) calculating a master key, a data encryption key, a MAC key, and an initial vector according to a key derivation algorithm;
5) Verify the correctness of MAC2;
6) The terminal generates a random number R3 (for the MAC initial vector used for subsequent data interaction encryption);
7) Calculating MAC3 with R3 using the MAC key and the initial vector;
8) Send message 4 to the master station.

5. The primary station receives the message 4 and performs the following operations:

1) Take R3 as the initial vector for subsequent data interaction;
2) Verify the correctness of MAC3 using the MAC key and the initial vector.
3) After the verification is passed, the session is successfully established, and the subsequent message uses the master key K, the data encryption key, the MAC key, the initial vector, and the random number R3 calculated in the interaction process.

### *3.2. Data Encryption Processing*

In order to ensure the security of the session between the primary station and the terminal, the session key has a lifecycle limit when encrypting data using the negotiated session key (including: master key, data encryption key, MAC key, initial vector). When the session key expires after reaching a certain number of times, the session recovery process must be initiated by the primary station to renegotiate the new session key.

For example, if the session key lifetime is set to 10,000 times, the session key can be used up to 10,000 times. After 10,000 times, the session ID is set to 1. At this point, session recovery is required to communicate again, thus ensuring the timeliness and security of the session key.

### *3.3. Session Recovery*

If the primary station side session ID flag is 1, the session recovery process is performed. The specific process and method of session recovery are as figure 2:

The specific method of session recovery is:

1. The primary station group message 1, the specific organization message method is as follows:

1) Take the random number R1;
2) using a cipher machine to encrypt the random number R1 to obtain the ciphertext EKs1 (R1);
3) The version number represents the version of the protocol and the encryption algorithm used;
4) The session ID is 1;
5) Take the master station certificate C M;

6) using the MAC key generated by the last session and the initial vector to perform MAC calculation on the session ID and EKs1 (R1) to obtain MAC1;
7) Digitally sign the version number, session ID, master certificate, MAC1, R1 to form signature S1.

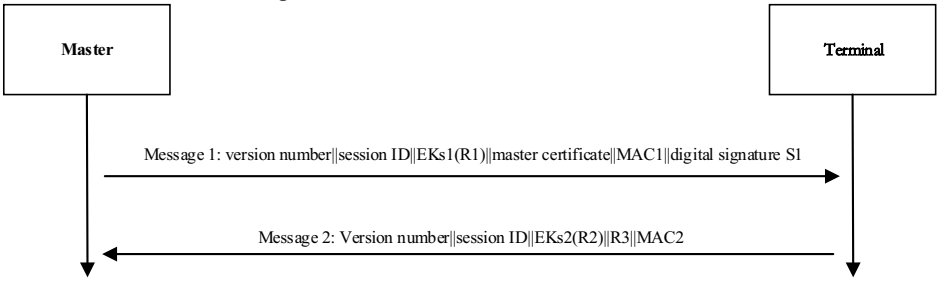


**Figure 2.** Master station and terminal session recovery process

2. The terminal receives the message 1 and performs the following operations:
1) Take out the master station certificate CM in message 1, verify its validity, and expire;
2) Verify the signature S1;
3) Verify the MAC value in message 1;
4) The terminal ESAM chip generates random numbers R2 and R3;
5) using the preset key EKS2 to encrypt it to generate EKS2 (R2);
6) Deriving a new master key, a data encryption key, a MAC key, and an initial vector using the new R1, R2, and the original master key K;
7) performing MAC calculation on the session ID, EKS2 (R2) and R3 by using the newly generated MAC key and the initial vector to obtain MAC2;
8) Send message 2.

3. The primary station receives the message 2 and performs the following operations:
1) decrypt EKS2 (R2) to get R2;
2) using the new R1, R2 and the original master key K to derive a new master key, data encryption key, MAC key and initial vector;
3) Verify the correctness of MAC2;
4) After the verification is passed, the registration is successful, and the subsequent message uses the newly calculated master key, data encryption key, MAC key, initial vector and random number R3.

### *3.4. Comparison of advantages between primary station and terminal data exchange methods*

This paper proposes a new data exchange method for the primary station and terminal for power. This data exchange method has the following advantages:

1) This article expands the method of establishing the connection between the primary station and the terminal into two types, one is the new session establishment, and the other is the session recovery in the case that the session has been established.

2) After the master station and the terminal session are established, symmetric data and asymmetric algorithms can be used in subsequent data interaction, which improves the security of data interaction.
3) This paper proposes to limit the number of times the session negotiation key is used. When the number of communication between the two reaches a limited number of times, session recovery is required to ensure the security of the session.
4) The session key proposed in this paper has multiple key types such as master key, encryption key, MAC key, initial vector, etc., which are used in different occasions to meet the application requirements of different scenarios.
5) This paper proposes to use the negotiated master key to decentralize multiple keys such as encryption key, MAC key and initial vector, which ensures the randomness and diversity of key generation.

## 4. Conclusion

In this paper, the method of data exchange between the master station and the terminal based on the combination of symmetric and asymmetric algorithms is realized. The security of data interaction is improved because the security mechanism such as signature, certificate, MAC, and symmetric encryption is used in data interaction. At the same time, the interaction between the primary station and the terminal is divided into three steps: session establishment, data encryption, and session recovery. The user can select different steps according to the actual application situation to meet the application requirements of different scenarios and enhance the application diversity.

## References

[1] Li Tao, Zeng Ying. A New Remote Bidirectional Authentication Based on Dynamic Password[J]. Microcomputer Information, 2007, 11(3): 38-40.
[2] Wu Jianwu. A remote password authentication scheme based on smart card[J]. Computer Engineering and Applications. 2007, 43(33): 158-160.
[3] Kong Mengrong, Zhu Guohua. Remote authentication system based on smart card[J]. Computer Engineering and Design. 2008, 29-3: 606-608.
[4] Wang Aiying. Smart Card Technology [M]. Beijing: Tsinghua University Press, 2009.
[5] Xu Pingjiang. Design of smart card file system based on linked list method [J]. Microcomputer Information, 2011, 27 (11): 49-50.
[6] Zhao Dongyan, Wang Yubo. Implementation of a smart card write protection mechanism [J]. Electronic Technology Application, 2014, 12: 32-34.
[7] Lai Yuyang. A high security network data transmission implementation [J]. Information Security and Communication Confidentiality, 2016, 2: 109-112.
[8] Xu Pingjiang. State machine based chip access control implementation [J]. Microelectronics and Computer, 2019, 36(7): 98-102.
[9] Xu Pingjiang. Implementation of a high reliability read/write mechanism for security chips [J]. Computer Application Research, 2019 (increase): 280-282.
[10] Du Shuwei, Zhao Dongyan. Smart grid chip technology and application [M]. Beijing: China Electric Power Press, 2019.
[11] Fu Qingqin. Implementation of an improved smart card authentication method [J]. Computer Engineering and Science. 2014, 36 (1), 94-98.
[12] Yuyang LAI. A grey lock method to support once pre-freezing mechanism in IC card[J]. Institute of Electrical and Electronics Engineers Inc. 2014, 1411-1414

[13] Weibin LIN. A mechanism for patching ROM smart card[J]. Institute of Electrical and Electronics Engineers Inc. 2014, 1415-1417
[14] Chen Huajun. An implement of the digital certificate on electrical IC card[J].CRC Press/Balkema, 2015,725-727
[15] Fu Qingqin. A grey lock method to support multiple pre-freezing mechanism in IC card[J]. CRC Press/Balkema, 2015,1395-1400.
[16] Qing-qin FU. A Novel Power-down Protection Mechanism for Secure Chip Based on CRC Check[A].EETA2017[C],2017,48-52.
[17] Jia Liu. Implementation of IC Card Authentication Method Based on Self-defined Algorithm[A]. EETA2017[C],2017.
[18] Fu Qingqin. A method for realizing secure chip multi-algorithm processing application[A]. Fuzzy Systems and Data Mining IV.2018,743-748.
[19] Fu Qingqin. A new secure chip file access method based on security level information[A]. Fuzzy Systems and Data Mining IV.2018,749-756.
[20] Pingjiang Xu. An Implementation of a Chip Security Mechanism[A]. Fuzzy Systems and Data Mining IV.2018,763-770.