International Journal of Automation, Control and Intelligent Systems
Vol. 4, No. 3, 2018, pp. 36-42
http://www.aiscience.org/journal/ijacis
ISSN: 2381-7526 (Print); ISSN: 2381-7534 (Online)

Remote Attestation Technology Based on Identity and Attribute

Dapeng Song[1, *], Lei Peng[1], Yanli Xiao[2]

[1]School of Medical Information Engineering, Taishan Medical University, Taian, China
[2]Department of Graduate, Taishan Medical University, Taian, China

Abstract

With gradually mature and widely used, cloud computing has become the future direction of the information technology. The nature of cloud computing, such as flexibility, openness, and public availability, presents many challenges to application security. It is an urgent problem to be solved that how to build a credible cloud computing environment, ensure the integrity, credibility and security of all parts of the network system. Remote attestation based on identity and attribute is introduced to study the security mechanisms for accessing cloud servers. With the help of trusted third parties, the credibility of the user platform is increased through dual authentication. The identity of the terminal user is confirmed by the authentication of the identity certificate. The credibility of the system and application are confirmed by the authentication of the attribute certificate. A trusted network access is established through the remote attestation technology. Authentication between cloud computing and users is the first threshold for cloud computing security. Secure and effective user authentication can prevent unauthorized users from accessing. Remote authentication is a verification technique for trusted platforms. It provides effective ideas for authentication problems in the cloud computing field, can solve the security measures of the cloud platform, and provides strategies and guidance for users to choose safe and reliable services.

Keywords

Cloud Computing, Remote Attestation, Attribute Certificate, Identity Certificate

Received: September 19, 2018 / Accepted: October 17 2018 / Published online: November 28, 2018

1. Introduction

With gradually mature and widely used, cloud computing has become the future direction of the information technology. The nature of cloud computing, such as flexibility, openness, and public availability, presents many challenges to application security. It is an urgent problem to be solved that how to build a credible cloud computing environment, ensure the integrity, credibility and security of all parts of the network system. In the face of complex network security issues, we need to consider how to ensure the security of data storage and application of users in cloud computing. It is necessary to establish a perfect authentication mechanism for both server and user. Remote authentication technology based on identity and attributes enables the server and the user to authenticate each other's identity. It can effectively prevent the occurrence of security risks such as fake identity and theft of information. The security of the authentication system has been greatly improved. [1-2]

2. Trusted Cloud Platform

2.1. Key for Trusted Cloud Platform

The use of keys and certificates plays a very important role in verifying the integrity of the trusted platform. After the trusted root and the trusted chain are established, each step requires remote attestation. The service can be authorized and

* Corresponding author
E-mail address: dpsong@tsmc.edu.cn (Dapeng Song)

obtained after the remote attestation is successful. Remote attestation is inseparable from keys and certificates. The trusted computing group (TCG) specifies a variety of keys and associated certificates to participate in the authorization process. Keys are mainly divided into signature and encryption. The signature key cannot be used for encryption, and the encryption key cannot be used for signature.[3]

Endorsement key (EK) is a non-migrated decryption key for the trusted platform module (TPM) platform [4-5]. It is a 2048-bit RSA key pair. The EK is the key pair uniquely identified by the TPM when it leaves the factory. It represents the true identity of each platform. EK cannot be used for any signature or encryption. It can only be used to decrypt the owner's authorization data in the platform, and it can also be used to decrypt the AIK-related data. The signing key is never used for data encryption and signing. The primary function of signing key is to generate an identity certificate key AIK and establish the owner of the TPM platform. The owner of the TPM generates a storage root key (SRK), and uses SRK to encrypt and store other keys. When generating an endorsement key, you need to be aware that EK is confidential. It has not been tampered with and does not endanger secret information. Simultaneous operation will not cause leakage of EK.

Attestation identity key (AIK) [6] is a non-migrated key. It is an RSA public-private key pair with a length of 2048 bits. It is used to sign the data generated by the TPM and the value of the platform configuration register (PCR). For security and privacy reasons, the TPM does not use EK to directly encrypt data and authenticate, but uses AIK as the signing key. This is used to prove the identity of the platform and the environment configuration of the platform. The entities signed by AIK have been processed by the TPM. Each user can have multiple AIKs. The generation of each AIK requires the participation of a trusted third party. The trusted platform is bound to the data trusted by the PCR through a set of certificates. The TPM generates a pair of identity keys at the key generator. The AIK is generated by binding the AIK public key with the endorsement certificate, platform certificate, and compliance certificate. Since the AIK key cannot be repeated, it needs to be regenerated each time. When the TPM's EK private key is attacked or the AIK certificate has been compromised, the AIK and the corresponding certificate are revoked, and the revoked certificate list is updated.

Signing key can be either migrated or non-migrated. The signature key is an asymmetric key. It is used to sign application data and information. The migrated signature key can be passed between TPMs. Pass confidential data by migrating keys. Signature keys in the TPM are available in several different lengths. They follow the standard for RSA signing keys. The data is kept secret by the transfer of the migration key. Signature keys in the TPM are available in several different lengths. They follow the standard for RSA signing keys.

Storage Keys are RSA private keys with a length of 2048 bits. It can be either a migrated key or a non-migrated key. The storage key is used to encrypt the universal asymmetric key of data and other keys. The other key can be another storage key, a binding key or a signature key.

2.2. Certificate for Trusted Cloud Platform

The generation and use of keys is inseparable from certificates. Proof of the identity information of the platform requires the protection of the certificate. The AIK certificate is used to determine the legality of the AIK private key that signs the PCR value. AIK certificates are issued by trusted third parties that can verify various certificates and protect client privacy. The AIK certificate includes the public key of AIK and other information that the publisher believes to be useful. The signer judges whether the platform is authentic based on the information it provides. The platform certificate is issued by the platform manufacturer. It is used to confirm the platform's manufacturer and describe the properties of the platform. The platform certificate contains information such as the platform manufacturer name, platform model number, platform version number, endorsement certificate, and verification certificate. The AIK certificate center (ACC) [7-8] issues an AIK certificate to the user platform to verify the validity of the AIK certificate. ACC issues an attribute certificate to the user platform to verify the reliability of the attribute certificate. [9]

3. Remote Attestation of Trusted Cloud Platform

3.1. Remote Attestation

Remote attestation is the current key technology of trusted computing. The purpose of remote attestation is to establish a set of proof system to prove that the operating system of the terminal platform is credible, That is, the verification platform has secure and reliable attributes, providing a real operating environment for the server. Remote attestation is to achieve the credibility of the network environment. It enables trusted communication between the terminal and the server, ensures the credibility of the terminal to be transmitted to the network, and establishes a secure network environment. The remote attestation technique passes the integrity status information of the terminal to the required verifier. After the authenticator obtains the terminal information, it verifies and judges whether the requestor is trusted and meets the communication requirements. In this kind of trusted computing, the process of requesting and verifying the

terminal to the authenticator is the remote attestation. The terminal platform that is remotely proven is a trusted network terminal device that enables credible access control. [10-13]

3.2. Remote Attestation Based on Attribute

Attribute-based remote attestation is a proof process that combines identity and integrity checks. It provides the authenticator with a trusted user platform status report. The attribute-based remote attestation is provided by a trusted third party with an attribute certificate to prove that the components of the user platform satisfy the remote attestation mechanism of certain attributes. The TPM is the trusted root throughout the verification process. It makes a credible report of the integrity metrics of the currently trusted computer. The user platform sends the system configuration to the certificate issuer. The certificate issuer derives the attributes it has based on its system configuration values. It issues the appropriate attribute certificate for the user platform. The user platform sends the relevant attribute certificate to the authenticator to prove the credibility of the platform.

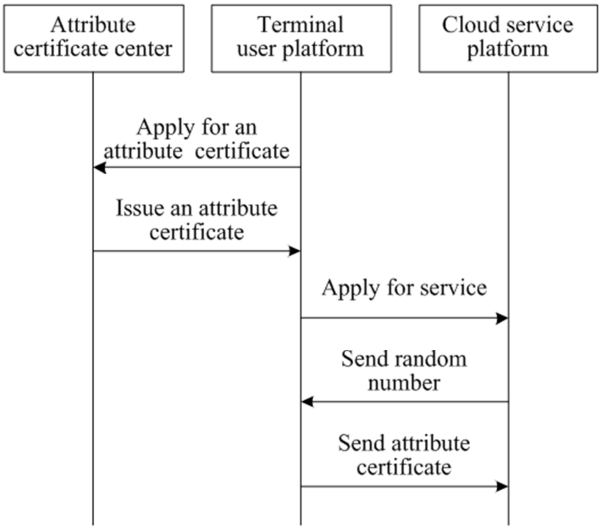

Figure 1. Remote attestation based on attribute.

ACC generates an EK key pair. TPM of the user platform sends the PCR value of the platform to ACC. ACC according to its attribute configuration value, and analyses the corresponding attribute of the user platform. ACC generates an attribute certificate, which is encrypted and issued to the user platform. The user platform requests the cloud platform to provide services. The cloud platform acts as a verifier to send random numbers to the user platform. The user platform signs the attribute certificate and converts it by means of information hiding. It gets a hidden signing certificate. The result is then signed with the ATM of the TPM. The user platform's TPM sends the configuration information, attribute certificate, and random number of the platform to the authenticator. The verifier checks if the random number is equal to the one sent to the user platform. If they are equal, the session is proven to be the current session. The verifier confirms that the configured configuration value is indeed from the specified user platform. The verifier verifies the validity of the attribute certificate. The remote attestation based on attribute is shown in Figure 1.

3.3. Remote Attestation Based on Identity

The remote authentication based on identity authentication is to verify whether the TPM owned by each other is legal and can represent the identity of the other party. The legitimacy of the TPM protects the current state of the platform and the keys in the authentication process. It can effectively verify the status between the two platforms. A series of protections of the platform status and keys by the legal TPM can provide security and credibility guarantee for the proof of the status between the platforms. In identity authentication, the identity of the challenger is prevented from being directly exposed to the challenger, ensuring the security of the challenged platform itself. It is necessary to achieve identity authentication and to maintain anonymity to the greatest extent possible. Avoid platform-sensitive information being compromised and prevent platform users from being tracked.

In the remote certification process based on trusted third parties, both the user platform and the cloud service platform have TPM chips. A trusted third party has a list of EK public keys for all trusted computers. First, the user platform applies for an AIK certificate from a trusted third party, the AIK certificate center. The user platform generates an AIK key pair based on an asymmetric key. Sign the AIK public key with the EK private key. The signed data is then sent to the AIK certificate. The AIK certificate looks up the list of existing EKs and determines if the platform's EK public key can be found. If it can be found, it proves that the AIK signature is valid. The user platform is then issued a certificate that is bound to its AIK public key. When performing remote attestation, the trusted computer signs the PCR value using the generated AIK private key. The signed data and the AIK certificate are then sent to the cloud platform, the authenticator. After receiving the data of the user platform, the cloud platform verifies whether the AIK certificate of the user platform is authentic and valid. If valid, the validity of the content signed by the AIK is verified. Otherwise, the AIK certificate is considered invalid and the verification fails.

The legality of TPM is mainly verified by trusted third parties. The AIK certificate sent by the user platform to the authenticator is different each time. Therefore, the verifier cannot distinguish whether multiple remote certificates are from the same TPM platform. The information of the platform users cannot be tracked, so the identity information of the platform can be protected. The remote attestation

based on identity is shown in Figure 2.

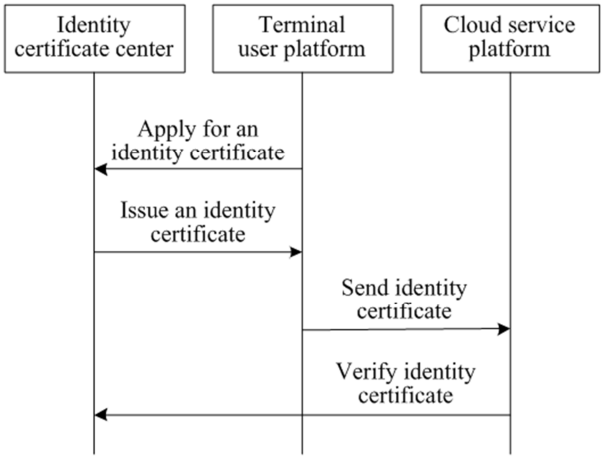

Figure 2. Remote attestation based on identity.

4. Remote Attestation Based on Identity and Attribute

4.1. Remote Attestation Architecture Based on Identity and Attribute

On the basis of attribute-based remote attestation, the identity -based authentication is added. The credibility of the user platform is increased through two-tier authentication. The remote attestation architecture based on identity and attribute includes CA, ACC, user platform, server and manufacturer [14]. CA is the certificate authority. The main function of CA in the remote attestation model is to publish and revoke the identity certificate. ACC is the attribute certificate issuing authority. The main function of ACC in the remote attestation model is to publish and revoke the attribute certificate. User platform includes user terminal and TPM module. Server is a verifier and service provider that provides attribute verification and access services. Manufacturer is responsible for the design and production of TPM chips and the injection of EK key pairs. The remote attestation architecture based on identity and attribute is shown in Figure 3.

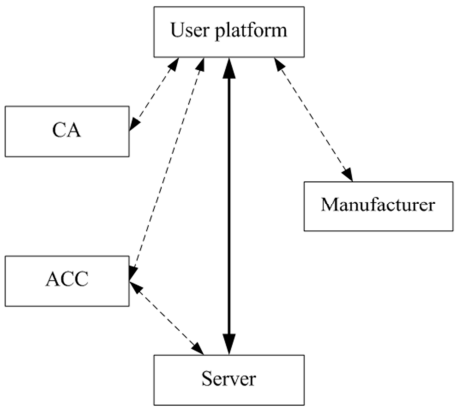

Figure 3. Remote attestation architecture based on identity and attribute.

The user platform first sends an identity certificate request to a certificate authority (CA). After receiving the application, the CA authenticates the platform certificate. After the authentication is passed, CA sends the identity certificate to the user platform. The user platform sends the identity certificate to the server for identity platform authentication. After the certification is passed, the user platform applies for an attribute certificate from ACC. The server signs the platform's attribute certificate. The ACC sends the attribute certificate to the user platform. The user platform then sends the attribute certificate to the server for attribute authentication. The server verifies that the attribute proves successful and the remote attestation process is completed. [15-16]

4.2. Remote Attestation Process Based on Identity and Attribute

The remote attestation process based on identity and attribute certificates includes four processes: application for identity certificate, verification of identity certificate, application for attribute certificate, and verification of attribute certificate. The remote attestation process based on identity and attribute is shown in Figure 4.

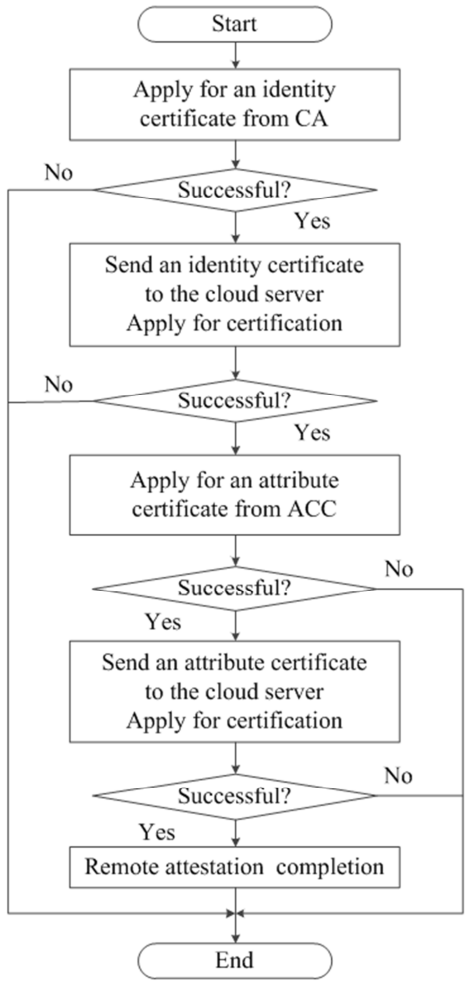

Figure 4. Remote attestation process based on identity and attribute.

The application for the identity certificate refers to the process in which the user platform applies for an identity certificate from a trusted third party CA. CA is the certificate authority for public key infrastructure. It is responsible for issuing identity certificates to the user platform. Certificates issued by CA are a guarantee and proof of trust from other platforms and systems.

The verification of the identity certificate refers to the process of the user platform authenticating to the cloud platform server. After the user platform applies for the identity certificate to the CA, the user certificate is sent to the cloud platform server. In order to prevent information leakage, the identity certificate and the TPM random number need to be signed. After the cloud platform is signed, the signature is verified. After verification, the cloud platform recognizes the user platform. User platform identity verification is complete.

The application for the attribute certificate is that after the user completes the identity authentication, the cloud platform server has recognized the identity of the user platform. However, it is not yet possible to determine whether the systems and applications of the user platform are trusted.

Authentication of the attribute certificate is required. The user platform encrypts and signs the metrics of the host by the TPM. The host forwards it to ACC. ACC decrypts and verifies the data and generates an attribute certificate. ACC encrypts the attribute certificate and sends it to the user platform. The TPM in the user platform decrypts the data to obtain an attribute certificate.

The verification of the attribute certificate is that the user platform sends a request to the cloud platform server, and the cloud platform needs to perform attribute certificate authentication. The TPM of the user platform encrypts and signs the data randomly generated by the host and sends it to the cloud platform server for verification. After the cloud platform is signed, it is decrypted to obtain an attribute certificate. The cloud platform server verifies the attribute certificate. This proves that the user platform is a complete and trusted one. The remote proof of the user platform is complete.

4.3. Security Analysis of Remote Attestation Based on Identity and Attribute

In the scheme of remote attestation based on identity and attribute, it is desirable to ensure the credibility and privacy of the user terminal device. It guarantees security and data confidentiality during the authentication process, and also prevents attacks and replay attacks during the authentication process.

In the process of identity certificate application, you need to use the random number generated by the TPM and the TPM's own private key. After the random number is signed by the private key, it is sent to the third party through the host. These data are kept confidential for third parties. The TPM, along with the host, obtains a valid identity certificate and signature from the third-party CA. However, CA does not know what these specific values mean. The third-party CA only authenticates and signs these data. The TPM, host, and CA sign with a zero-knowledge proof protocol, giving the host a legal signature and proof of identity [14].

During the certificate verification process, the TPM and the host are required to prove to the server. The identity certificate for the host is from a certificate issued by CA. It is a certificate that passes strict certification. The credibility of the identity of the host platform is ensured. In the process of identity authentication, it is necessary to negotiate and encrypt. This makes the interactive data confidential and ensures the security of data transmission.

In the attribute certificate application phase, after the TPM measures the host, the metric value and the identity certificate are cryptographically signed using the private key. Then, the host sends it to the attribute certificate center for attribute certificate authentication. After receiving the data, the ACC first decrypts it with its own certificate private key to get a symmetric key. The metric is obtained by decrypting the symmetric key. The ACC generates an attribute certificate by decrypting the value. The ACC sends the attribute certificate to the user host after being signed and encrypted. The host's TPM is decrypted and verified. In the process of attribute application, the two parties authenticate each other through two-way verification of random numbers. And in the process of communication, all are signature encryption, which ensures the confidentiality of data information transmission.

During the attribute certificate verification phase, the user has obtained an identity certificate from the CA and an attribute certificate from the ACC. The identity certificate has proven the reliability of the identity of the platform. It has been approved by the server to confirm the authenticity of the identity of the user platform. The attribute certificate has ensured the credibility of the user platform and has been certified and certified by a third party. Next, the attribute certificate is needed to be sent to the server for attribute authentication. It ensures that the trusted platform is a secure, trusted, and reliable trusted platform for the server. In the process of attribute authentication, the TPM is required to sign and encrypt the random number and attribute certificate generated by the host. The encrypted data is then sent to the server through the host. The server decrypts it by its own public key and obtains an attribute certificate. Then verify the attribute certificate, and if the verification is passed, the remote certificate is completed. During the attribute

verification process, the TPM encrypts the random number and attribute certificate generated by the host using the private key to ensure the security of the attribute certificate.

The TPM chip in the user platform performs integrity metrics and signatures on the host. This is very secure for data protection. It protects the platform against illegal intrusions. The key used by the TPM signature is preset by the manufacturer. It is secure and confidential. When the ACC receives data sent by the user, there is a possibility of being externally invaded during data transmission. However, because the integrity metric is correct, the intruder cannot crack the TPM key pair and cannot crack its signature authentication process. The ACC private key signature ensures that the attribute certificate cannot be changed, thus ensuring the security of the attribute signature. Due to data interaction between the ACC and the user host, there is no possibility of data tampering and disclosure. The forwarding and delivery of attribute certificates does not affect the integrity of the attribute certificate. Therefore, the forwarding and delivery of attribute certificates is safe.

During the attribute certificate verification phase, the TPM generates encrypted data by encryption to ensure the correctness of the data. Security is guaranteed through secure interaction with the host. The interaction between the user platform and the server can ensure the correctness of the data through the encryption and decryption algorithm of the public key. The encryption of the attribute certificate by the public key password ensures the unforgeability of the attribute certificate. Therefore, the correctness of the attribute verification is guaranteed.

5. Conclusion

The remote authentication scheme based on identity and attribute certificates ensures that the user platform can securely access the cloud server. The cloud terminal ensures that the user accessing the server is secure and trusted according to the configuration mapping relationship between the issued certificates and the server. The remote attestation technology passes the security status information of the terminal to the authenticator. The authenticator establishes a channel for resource sharing by verifying and judging the terminal information. It ensures credibility and reliable communication between the terminal and the server to establish a secure and trusted network environment.

Foundation Items

Shandong Provincial Science and Technology Development Program, China (No. 2014GGX101020)

Safe Production Major Accident Prevention Key Technology Program, China (No. shandong-0021-2015AQ)

References

[1] Botta A, De Donato W, Persico V, et al. Integration of cloud computing and internet of things: a survey [J]. Future Generation Computer Systems, 2016, 56: 684-700.

[2] Almorsy M, Grundy J, Müller I. An analysis of the cloud computing security problem [J]. arXiv preprint arXiv:1609.01107, 2016.

[3] Celesti A, Fazio M, Longo F, et al. Secure Registration and Remote Attestation of IoT Devices Joining the Cloud: The Stack4 Things Case of Study [J]. Security and Privacy in Cyber - Physical Systems: Foundations, Principles and Applications, 2017: 137-156.

[4] Mugisha E, Zhang G, El Abidine M Z, et al. A TPM-based Secure Multi-Cloud Storage Architecture grounded on Erasure Codes [J]. International Journal of Information Security and Privacy (IJISP), 2017, 11 (1): 52-64.

[5] Kashif U A, Memon Z A, Siddiqui S, et al. Architectural Design of Trusted Platform for IaaS Cloud Computing [J]. International Journal of Cloud Applications and Computing (IJCAC), 2018, 8 (2): 47-65.

[6] Song Y, Liao Z, Liang Y. A trusted authentication model for remote users under cloud architecture [J]. International Journal of Internet Protocol Technology, 2018, 11 (2): 110-117.

[7] ZHOU Y, DENG M, CHONG Y, et al. Research and Design of Trusted Computing Platform [J]. 2016.

[8] Xu G, Tang Y, Yan Z, et al. TIM: A trust insurance mechanism for network function virtualization based on trusted computing [C]//International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Springer, Cham, 2017: 139-152.

[9] Gonzales D, Kaplan J M, Saltzman E, et al. Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds [J]. IEEE Transactions on Cloud Computing, 2017, 5 (3): 523-536.

[10] Brasser F, Rasmussen K B, Sadeghi A R, et al. Remote attestation for low-end embedded devices: the prover's perspective [C]//Design Automation Conference (DAC), 2016 53nd ACM/EDAC/IEEE. IEEE, 2016: 1-6.

[11] Carpent X, Rattanavipanon N, Tsudik G. ERASMUS: Efficient remote attestation via self-measurement for unattended settings [J]. arXiv preprint arXiv:1707.09043, 2017.

[12] Knauth T, Steiner M, Chakrabarti S, et al. Integrating Remote Attestation with Transport Layer Security [J]. arXiv preprint arXiv:1801.05863, 2018.

[13] Gong B, Zhang Y, Wang Y. A remote attestation mechanism for the sensing layer nodes of the Internet of Things [J]. Future Generation Computer Systems, 2018, 78: 867-886.

[14] Liang Y. Tth trusted platform design based on cloud computing [D]. Chengdu: University of Electronic Science and Technology of China, 2013.

[15] Fu D, Peng X. TPM-based remote attestation for Wireless Sensor Networks [J]. Tsinghua Science and Technology, 2016, 21 (3): 312-321.

[16] Zhao J, Liu J, Qin Z, et al. Privacy protection scheme based on remote anonymous attestation for trusted smart meters [J]. IEEE Transactions on Smart Grid, 2016.