

Interpretation of the RSA Master's PPT-"Cryptography as a Service"

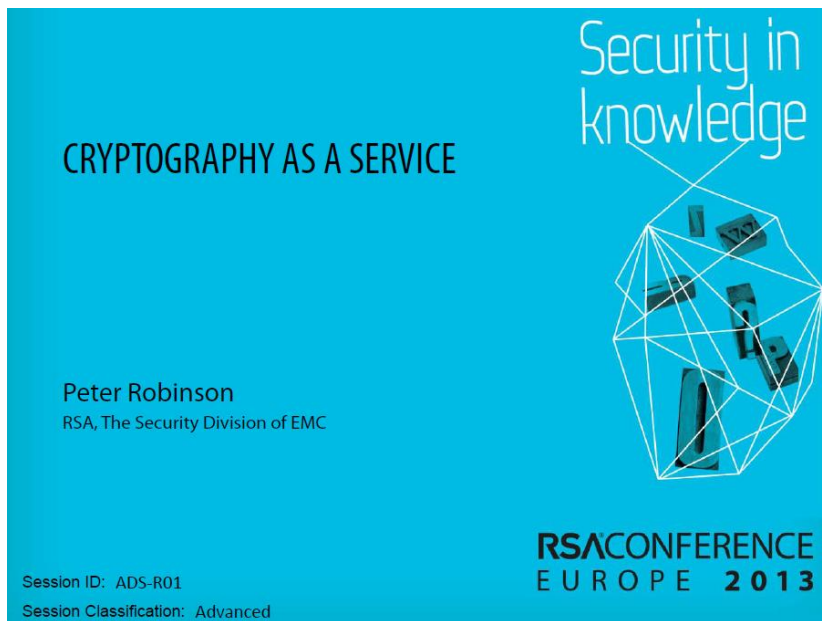
(May 06, 2021)

Cryptography as a Service is becoming a hot service of cloud computing services. Not only Amazon Cloud, Microsoft Azure, Google Cloud, Alibaba Cloud, Tencent Cloud, Huawei Cloud, etc. have already provided cloud cryptographic services, and cryptographic equipment manufacturers, cryptographic system developers, and CAs have also begun to provide cloud cryptographic services, which shows that everyone has realized that to protect the security and trusted of cloud data, cryptographic technology must be used. Turning the cryptographic capabilities of cryptographic technology, cryptographic equipment and cryptographic systems into a resource in cloud computing services to provide services, this is cloud cryptographic service.

However, after studying these cloud cryptographic services, the author seems to be a little confused and feel that most of the cloud cryptographic services are shared rental services of the cryptographic equipment and cryptographic systems, a bit like the early stages of cloud computing services that only provide virtual hosting service and server rental services. If my understanding is correct, it can be analogized that cloud cryptographic services are still in the early stages, and they are all being explored. The purpose of writing this article is also to discuss with the cloud cryptographic service industry and users how we should develop cloud cryptographic services and which cloud cryptographic services should be provided to meet the needs of users for cryptographic applications.

With this research topic, the author found the PPT of "CRYPTOGRAPHY AS A SERVICE" on the Internet. This is the first PPT used by RSA Senior Engineering Manager Peter Robinson at the RSA Conference European 2013 on October 29-31. For the first time, the concept of "Cryptography as a Service" was proposed. The author carefully read each page of the PPT. Although the PPT only lists the general content of the speech but can basically understand the

core ideas of Peter. This article will share the author's thoughts with you.



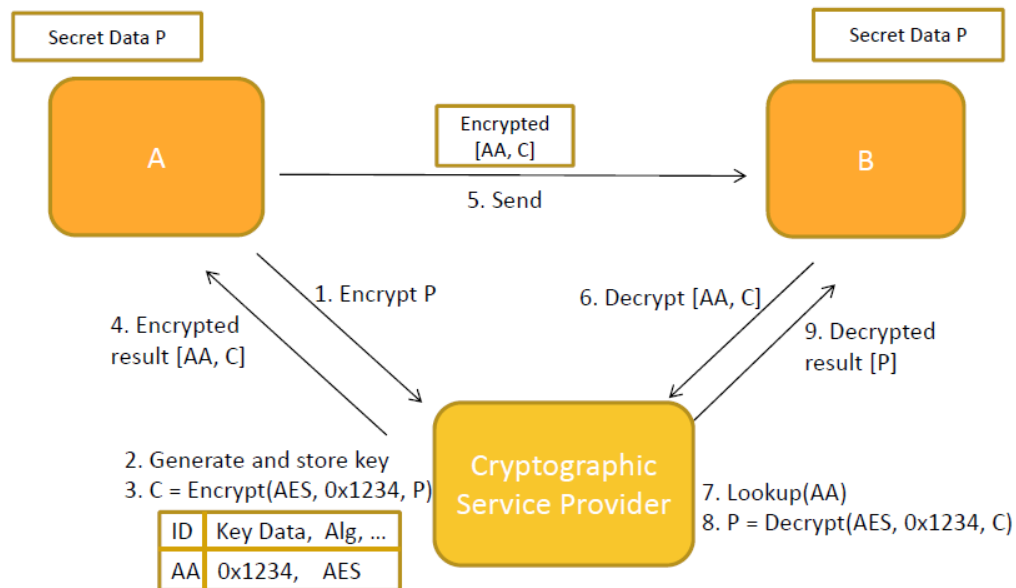
On the first page of the PPT, Peter explained why "Cryptography as a Service" was proposed. He believes that deploying cryptographic keys to end points such as smartphones, virtual machines in the public cloud and smart grid equipment is risky. Therefore, this speech proposes a Cryptography as a Service (**CaaS**) model which allows cryptographic operations to be performed without exposing cryptographic keys and recommends how to overcome the pitfalls associated with this technology. This is the first time recognized by the industry that the concept and application scenarios of "Cryptography as a Service" have been proposed at a large-scale security professional conference.

Peter clearly defines the Cryptography as a Service on page 23 of the PPT: Keyed cryptographic operations, such as encryption and decryption, are performed by a CaaS provider on behalf of a device via web services APIs. The cryptographic keys used to perform these operations are stored within the CaaS provider, so devices do not possess these keys at any time.

The following figure shows the encryption and decryption diagram shown one page 31 of the PPT. User A wants to send Secret Data P to user B, and user A posts data P to the cryptographic service provider to request encryption P, the cryptographic service provider generates and store key and encrypt the data using the key, then return the encrypted data to user A. User A sends

the encrypted data to user B. After receiving the encrypted data, user B posts it to the cryptographic service provider for decryption. The service provider decrypts the encrypted data and returns the original data P to the user B. The whole process is that users A and B do not possess the encrypting key, and this method solves the security problem of the encrypting key on the endpoint.

Cryptography as a Service



Peter also analyzed the possible impact of adopting Cryptography as a Service. The advantages are that the security is improved. No important cryptographic keys on end points. Important cryptographic keys stored and backed up in one place, in a key management system. And possible improved performance due to scalable web services. Its disadvantages are the cryptographic service provider must have a cryptographic infrastructure that increased architectural complexity; latency due to web calls; possibly reduced performance due to overhead of making web calls; possibly more hardware required to host the CaaS provider; Denial of Service: causing a loss of connection between an endpoint and the CaaS provider results in the end point not being able to perform cryptographic operations. The major challenge is the authentication of the end point requesting cryptography services, and the other challenge is network connectivity, it is required to allow the end point to have the CaaS provider perform the required action when required.

Regarding cryptographic algorithms, Peter suggests combining multiple cryptographic

services, such as digital signatures and encryption, in one Web service call. And it is recommended to use Cryptographic Message Syntax (CMS/PKCS#7) standard to realize secure messaging which offers a range of standard encapsulation types, for instance signed and enveloped.

Peter also used sending signed email as an application example to illustrate how to use cryptographic services to implement digital signatures of email. At the same time, Peter also proposed a solution for how the smart grid manages keys. This is a cloud key management and key distribution to the terminal solution. It not only solves the key management problem for users, but also solves the problem of relying only on the cloud that the service is too inefficient and the higher network connection quality. At the same time, Peter also pointed out that in this way, entropy from CaaS can be mixed into an endpoint's entropy to dramatically improve the quality of entropy on the end point. This will greatly improve the quality of end point produced keys.

Peter finally summarized several key points of Cryptography as a Service: (1) End points are bad places to generate and store keys. (2) CaaS allows cryptographic services to be performed on behalf of end points without exposing important cryptographic keys to the end points. (3) CaaS when combined with strong authentication can greatly improve the security of a system. (4) CaaS does not apply to all cryptographic operations. (5) Some environments, such as embedded devices, are challenging for CaaS. However, CaaS can still be used in these situations to improve the security.

In other words, Peter's original idea of "Cryptography as a Service" was designed to solve the problem of key security and to solve the problem of key management. It now appears that the key management solution for MeSign email encryption automation is very innovative, although we have not seen Peter's PPT when using cloud key management technology to solve the problem of email encryption there years ago. MeSign Technology can realize automatic email encryption because it uses cloud key management technology and uses different key management methods for different type certificates, which not only makes it convenient for users to obtain encrypting key anytime and anywhere to decrypt the encrypted email, which

completely solves the problems of key management by users. And because the digital signature is legally effective, the signing key is generated locally under the cooperation of the cloud key management system and store it in local device securely. MeSign App will distribute the encrypting key after validating the user's email control, so that users can quickly decrypt encrypted emails locally without relying on cloud cryptographic service, because users have a large number of emails to decrypt every day. Relying on cloud cryptographic service is too inefficient and requires relatively high network bandwidth, which will affect user experience and is not suitable for managing encrypted emails in smart phones. This is the first gain after the author reads Peter's PPT, and more firmly believes that MeSign automatic encryption solution based on cloud key management is scientific, advanced and innovative.

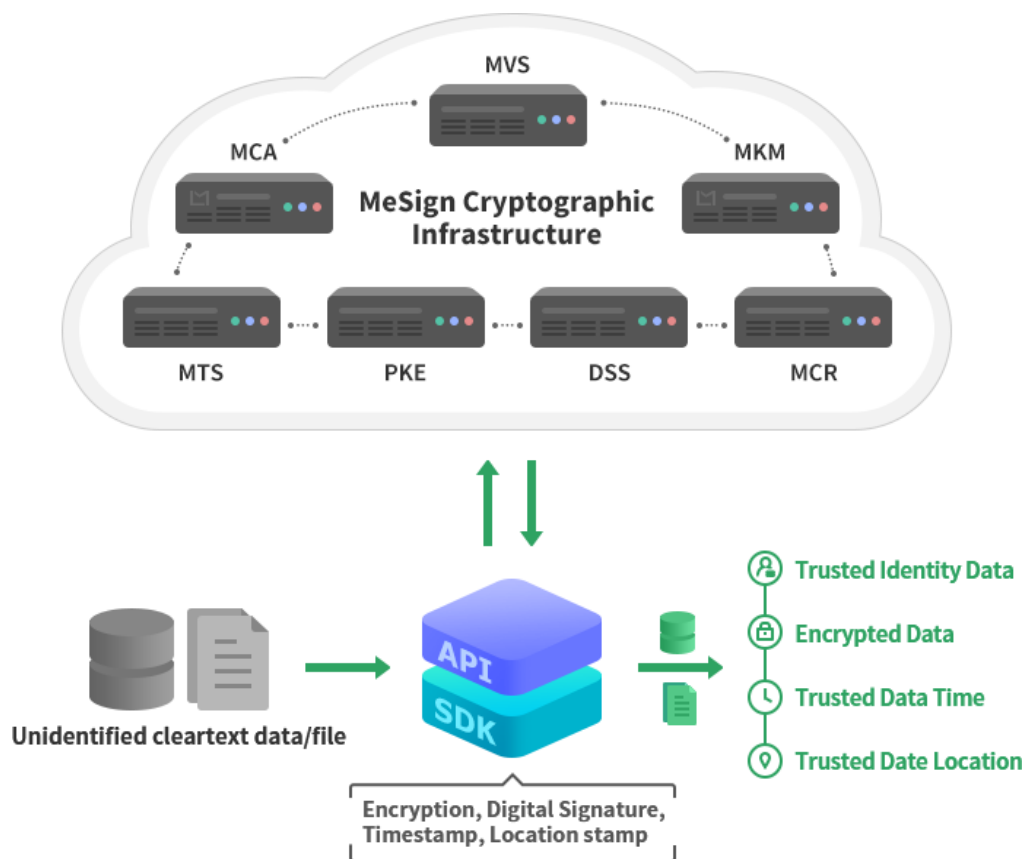
It has been more than 7 years since Peter first proposed the concept of "Cryptography as a Service" in 2013. During this period, both theoretical research and application practices of the Cryptography as a Service have done a lot of exploration and achieved certain results, it has become an important part of the cloud computing service, so all cryptographic-related services are called cloud cryptographic services. MeSign did some market research before planning to provide cloud cryptographic services, and found that users do need cryptographic technology to ensure the security and trust of the data in the cloud, but most users do not understand cryptographic technology, and do not know how to program to achieve encryption, digital signature and timestamp applications, how to do?

In other words, what kind of CaaS is the service that users need? The author believes that the provision of cryptographic equipment and system rental services cannot solve the user's cryptographic application needs. It not only involves the different technical docking requirements of different manufacturers, but more importantly, the user does not know how to program the cryptographic function to achieve digital signature and encryption. What the user needs is to input "unsigned and unencrypted data" and output "signed and encrypted data" with one click. This is a real service, the CaaS service that the user really wants.

MeSign Technology built a cloud cryptographic infrastructure 3 years ago, empowering its own client software-MeSign App, the cloud and client are closely coordinated to provide users

around the world with fully automated email encryption and document digital signature services. The service realizes various functions that are impossible with traditional independent client software, this is a technological innovation and the future development direction of cloud computing and client software. Now, MeSign Technology has opened the mature cloud cryptographic infrastructure as a cloud cryptographic service to all Internet application developers and service providers, turning cryptographic capabilities into a resource service for cloud computing, empowering all client software and Internet applications , so that all developers and service providers do not need to repeatedly invest in the cloud cryptographic infrastructure, but can purchase cryptography as a services on demand according to their application needs.



MeSign Technology delivers cryptographic services in the form of SDK or API, which can meet user’s cryptographic applications need such as data encryption (certificate encryption), data identity trust (digital signature), data generation and use time trust (time stamping), and data generation and use location trust (location stamping), and users do not need to understand cryptographic programming technology at all, only need to know the simple Web service calls.



[MeSign Cryptography as a Service](#) allows users to quickly use cryptographic capability and help business data to be secure and trusted. This not only meets users' cryptographic application compliance requirements, but also protects users' valuable data resources and data assets, which greatly enhances the enterprise core competitiveness. Welcome to choose MeSign Cryptography as a Service.

----- END -----



Want to contact me to discuss this topic? Please use [MeSign App](#) ( - ) to scan the QR code and send me an encrypted email, I will reply to your encrypted email ASAP.