White Paper

Hardware-based cryptographic key management in the Cloud

Introduction

The present study is a holistic bird's view on the security requirements for critical data imposed by modern information technology deployment models and trends. Its aim is to give the reader an overview of the various technology deployment models and to list the potential attack vectors introduced by such models. Applicable best practices are suggested aiming at minimizing the risk and achieving compliance when it comes to the security requirements of critical data.

Cloud Computing

If there is one concept dominating discussions about the deployment of infrastructure and applications nowadays then it is cloud computing. The basic building blocks of cloud computing are

1. Virtualization, although often mistaken as a synonym for cloud computing, it is only one of the key technologies for cloud computing.
2. Automation is an equally important building block which, together with
3. Standardization, gives cloud computing its key success characteristics.

Those characteristics are:

- On demand self-service: The automation capability minimizing the necessity for human interaction when it comes to commissioning and decommissioning of computing resources; the latter being required for services and applications to meet service level agreements and to maintain and expand the business value of an organization.
- Resource pooling: The ability to concentrate and share computing resources between multiple users in a secure manner. This minimizes Opex for both providers and consumers, and maximizes the positive investment results for organizations.
- Rapid elasticity: Together with the previous two characteristics of cloud computing, rapid elasticity enables organizations to quickly and automatically allocate and deallocate computing resources as needed to meet demand.
- Broad network access: Cloud computing resources are broadly accessible over the network through various client types and protocols.
- Measured service: The ability to monitor and measure delivered services and resources enables the provision of pay per use models ultimately leading to the concept of Technology as a Service.

Having reviewed the unique characteristics of cloud computing it is time to examine the diverse service models as they are offered and can be classified today. The three main service models through which cloud computing resources are offered to consumers are:

- IaaS or Infrastructure as a Service where major bare metal providers can deliver rack-space, power, cooling and computing and network resources on a global and redundant scale. In such service models the providers' responsibilities are limited to provisioning the resources and making sure those resources are available upon demand.
- PaaS or Platform as a Service refers to the provisioning of frameworks and development environments which enable consumers to write and deploy applications without having to care about the necessary infrastructure underneath. PaaS providers can be but not necessarily are also IaaS providers.
- SaaS or Software as a Service refers to the offering of specific applications via the cloud. Online CRM (Customer Relationship Management) tools are a typical example of such offerings. As before, SaaS providers can be but usually are not IaaS and PaaS providers at the same time.

The reader might already have observed that cloud computing is introducing a variety of stakeholders into cloud based infrastructures as various parties can offer different services or can even bundle their offerings into packages. As such, one has to be careful when it comes to assessing security risks and making assumptions about who is responsible for which data and at which stage, security-wise.

As cloud computing has reached maturity and more and more organization move to and depend on it, the trend shows that providers of cloud computing resources specialize on one of the above described service offering models. We will revisit this point later when talking about the potential new risks and attack vectors introduced by cloud computing that any organization thinking of moving to the cloud has to carefully assess. Before doing so, let's have a horizontal look at the different cloud deployment models available.

Cloud deployments can be classified in three categories. While public cloud deployments refer to the utilization of cloud computing resources which are off-premise and shared between multiple clients, Private cloud deployments can be either outsourced to third parties dedicating resources to their clients or operated within premises of big organizations. A third variant are hybrid cloud deployments, which reflect cases where organizations mirror their internal infrastructure in the cloud for mainly capacity and redundancy purposes. Or where organizations outsource their infrastructure to a provider but keep business critical data, applications or work-flows within premises.

There is no doubt that organizations can massively benefit from cloud computing as they can rapidly deploy resources as needed, outsource non business-critical knowhow and make use of high quality services provided by highly specialized vendors and providers. At the same time though, cloud computing has introduced a completely new landscape when it comes to the security requirements of the data and applications for which all this infrastructure can be utilized. Cloud computing has, on the one hand, eliminated the traditional perimeter of organizations upon which security personnel used to focus to ensure a security baseline. And on the other hand, it has introduced multiple vertical actors when it comes to infrastructure, software platforms, applications and eventually the data, both in motion and at rest.

Data in the Cloud

When it comes to securing data in the cloud, three distinct states the data can be in have to be examined separately. Data will always either be at rest, in motion or in processing. Organizations can utilize cloud computing for either of these possible data states. It is therefore critical to understand that risk exposure and attack vectors differ depending on the data state, the delivery and the service model of cloud computing.

An IaaS provider will be responsible for the hardware and its availability but not for the security of the data and applications he is hosting and that are running upon those resources. PaaS providers on the other hand will be accountable for the security of the virtualization and container resources made available, or for the integrity of the available development environments, but not necessarily for the hardware infrastructure underneath, nor for the data stored and processed within those virtual machines or containers. A SaaS provider in turn outsources the security concerns to the underlying IaaS and PaaS providers as far as hardware infrastructure and platforms are concerned and assumes responsibility for the data he is storing and processing on behalf of his clients.

Cryptographic techniques for Cloud deployments

Irrespective of the delivery or service model used by an organization, cryptography and in particular encryption and digital signature techniques can play a crucial role in securing data, the platforms upon which data is stored and the applications processing this data. Based on this idea, we will examine nine different layers at which cryptographic techniques can serve as the cornerstone of any successful security policy. Regardless if the respective data is in motion, at rest or in processing, the following briefly described techniques can help the most in safeguarding this data.

1. Enforce multi-factor authentication whenever administrative or user access to sensitive data is required. Various multifactor authentication products and techniques are widely available nowadays. Pin-protected smartcards, the combination of passwords and biometrics or one-time password generating tokens are just a few examples. Depending on your deployment, they can provide secure access to critical data and applications by securely identifying entities requesting access.
2. Role based access control (RBAC) complements multi-factor authentication and has proven to be very practical and efficient. It is a way of enforcing the “need to know” principle and restricting access to applications and data by assigning specific pre-configured roles to users.
3. Encrypt and digitally sign virtual machines & containers. Ensuring integrity and authenticity of virtual machines and containers by digitally signing them and by allowing deployment only after integrity and authenticity have successfully been verified.

4. Securely manage workstations by enforcing code signing. Code integrity and authenticity can be guaranteed by digitally signing code before deployment. Code signing should be utilized when installing applications and hardware drivers or patching operating systems and applications.
5. Run critical applications in secure environments. Organizations should safeguard the execution environment of critical applications by securing the booting process of operating systems hosting such applications. This can be achieved by means of digital signatures.
6. Enable database encryption. Whenever sensitive data is stored in databases, an organization should ensure those data is only stored in an encrypted form by deploying database encryption. Lots of database vendors provide database encryption as a build-in functionality.
7. Protect data in transit by deploying build-in data encryption techniques or virtual private network technologies. Furthermore, information communicated via mail can be encrypted and digitally signed.
8. Enforce file and folder level data encryption. Instead of encrypting the sensitive data themselves it might be more efficient to deploy encryption techniques on a file or folder level. This approach is particularly useful in environments where the application hosting platform is not under the control of the organization using it.
9. Utilize PKI technologies. By deploying Public Key Infrastructures (PKIs), organizations can authenticate users and devices, real or virtual, and securely exchange encryption and signature keys in a manageable manner.

We have briefly examined nine security domains utilizing cryptography which can be applied at different layers and help organizations in addressing the critical security requirements for their data and applications. Cryptography though is only as robust as the applied cryptographic algorithms and as secure as the respective keys are safeguarded and managed.

Hardware-based key management and storage

As we have seen in this paper, cloud computing has introduced a series of benefits that organizations can use to meet demanding requirements. And it has nonetheless also diminished the classical security perimeter once and for all. Multiple layers and parties involved in this ecosystem have introduced new attack vectors and have made data security an even more challenging task. We have also investigated how cryptography – and in particular encryption and digital signatures – can have a major impact on safeguarding sensitive data and applications. When it comes to the deployment of cryptographic techniques, the most critical issue is safeguarding and managing the cryptographic keys. It is exactly this issue which is addressed in the best possible way by utilizing Hardware Security Modules.

There are four possibilities to efficiently deploy HSMs in modern IT infrastructures and in particular in the context of cloud computing. These are the following:

1. On premises deployment. HSMs can be deployed as classical IT infrastructure components within the organizational data center and serve as safe key stores for the entire set of applications employing encryption and digital signatures.
2. Co-location deployment. HSMs can also be deployed in collocation scenarios in which either the entire or only parts of an organization's infrastructure have been outsourced to third-party cloud service providers. This way the entire set of applications and data

hosted by a provider can be securely controlled from within the organization and by trusted staff members.

3. Trust center deployment. An organization thinking of moving to the cloud can consider using HSM resources made available by trust centers around the globe, or by deploying its own HSMs within the trust center facilities. Managed public key infrastructures are typical examples of such deployments.
4. Last but not least, HSMs are perfectly fit for purpose when it comes to running applications in completely insecure environments. Organizations can use HSMs as a secure platform for developing and running custom application. Road fee collection projects are a typical example for such deployments. HSMs in such cases serve as both secure execution environments for critical applications and as safe key and data stores.

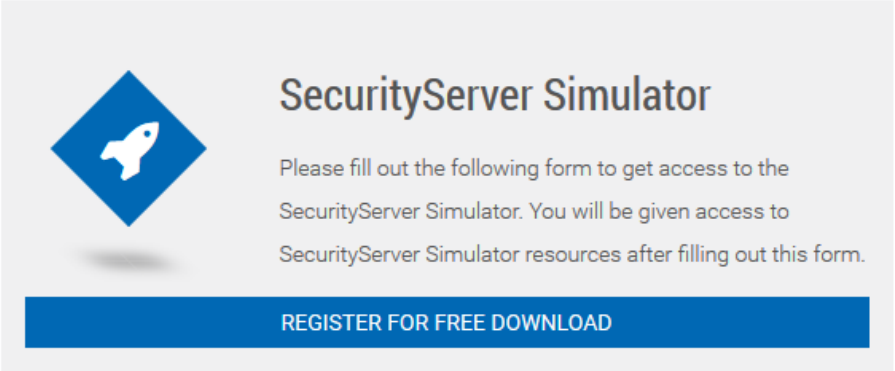
In a nutshell, we have seen how cloud computing has introduced a series of advantages but also security concerns for organizations. Cryptography can play a major role in addressing a variety of security requirements but is only as safe as the respective cryptographic keys are. HSMs can help with almost all of the above stated requirements by introducing the root of trust in your infrastructure.

About Utimaco

Utimaco is a leading manufacturer of hardware security modules (HSMs) that provide the Root of Trust to the IoT. We keep cryptographic keys and digital identities safe to protect critical digital infrastructures and high value data assets. Our products enable innovations and support the creation of new business by helping to secure critical business data and transactions. Founded in 1983, Utimaco HSMs today are deployed across more than 80 countries in more than 1,000 installations. Utimaco employs a total of 170 people, with sales offices in Germany, the US, the UK and Singapore. For more information, visit hsm.utimaco.com

Download the Utimaco Software HSM Simulator to get started immediately learning about HSM devices. It is a FREE fully functioning Software version of the Hardware HSM. The download package includes documentation on our product. Here is the link to register for the download.

https://support.hsm.utimaco.com/hsm-simulator



The Simulator download includes tools for creating user accounts, sample code and libraries for PKCS#11 Microsoft CNG, Java JCE and the Utimaco CXI API to link and test your code. The Simulator will run on a Windows or Linux platform. This is your opportunity to try out the Utimaco HSM technology easily and without initial cost.