Cloud Certificate Authorities

The security considerations of moving your Public Key Infrastructure to the cloud
Commissioned by Deloitte Netherlands

Anand Groenewegen
University of Amsterdam
agroenewegen@os3.nl

Maurits Maas
University of Amsterdam
mmaas@os3.nl

ABSTRACT

Organizations around the world are experiencing an increase use of an internal public key infrastructure (PKI). Surveys inform that IT leaders are outsourcing components of their overall infrastructure because it will provide them access to skill not available in-house. This is sidelined by articles describing that IT leaders are experiencing a struggle in finding and employing experienced staff to oversee their public key infrastructure. With this, the service model Certificate Authority as a Service (in the Cloud) was introduced by (cloud) providers. The goal of this paper is to inform readers on how a cloud CA service impacts the stature of an organization and to possibly serve as the seminal paper towards the subject. The main research question is divided into several sub-questions.

The sub-questions have explored the differences between infrastructure models when hosting a certificate authority, what providers currently offer in terms of a Cloud CA service and what organizational aspects are to be considered during a transition from on-premise to the cloud. This paper can answer the main question, "How does the adoption of a Cloud Certificate Authority (CCA) benefit/impact an organization?", by concluding that an organization will need to evaluate their in-house capabilities, such as cost management and internal PKI expertise, against diminishing their control over policies and risks to an external vendor.

Index Terms: *Certificate Authority as a Service, Cloud Certificate Authority, PKI as a Service*

February 9, 2021

1 INTRODUCTION

A survey held by Statista about IT Outsourcing in 2018 informs that over their 3,958 respondents, almost half of them are outsourcing components of their infrastructure because it will provide them access to skill not available in-house [1]. According to an article written for ComputerWeekly, IT leaders experience difficulties in finding and employing experienced staff to oversee their public key infrastructure [2]. Because of this, cloud computing service providers are empowering a new trend where an entire on-premise public key infrastructure is moved towards their hosted environment. A simple set up of a public key infrastructure would contain a Root Certificate Authority (CA) which is encrypted by a key pair stored on a hardware security model (HSM). From this root CA, intermediates or subordinates CA are issued and the these CAs will issue certificates for services/applications. A certificate authority in the cloud is capable of doing the same, issuing and managing private certificates for services hosted in the same environment, or in a local environment. With this, cloud and local machines are capable of validating in-house certificates. This can be seen as Software-as-a-Service (SaaS), or an entire new acronym namely Certificate Authorities-as-a-Service (CAaaS). This research will focus on the cloud part of CAaaS, whereas it is possible to see CAaaS solely as managed PKI this is not the main focus of the research. By exploring the differences between infrastructure models when hosting a certificate authority, what providers currently offer in terms of a Cloud CA service and what organizational aspects change during transition will this paper be capable of informing the reader of the impacts and benefits of moving a Public Key Infrastructure to the cloud.

2 CONTEXT

To ensure cohesion between the paper and reader, a few of the used terminology will be given extra context. A private CA is an organization built certificate authority which functions like a root of trust for an internal network and is hosted within that network or via an Infrastructure as a Service (IaaS) solution. The organization behind this private CA is either responsible for the hardware, software or both. With a cloud CA, this paper will define this as private CA but now completely hosted and managed by a (cloud) service provider. An organization can subscribe to such a cloud CA service whereas it will operate as a black-box connected to the organization's environment through a web interface or API to issue and manage private certificates. This intervenes with the terms cloud-based PKI and managed PKI whereas this paper defines the former as Certificate Authority as a Service (CAaaS) in the cloud, a true cloud CA service, and the latter as solely CAaaS. With this, the paper is indicating that it is possible for a managed provider to deploy and maintain a private CA for a client on-premise or through IaaS without the functionality that a Cloud CA service offers extra. Such as a complete front-end, e.g. a web console.

Important is to comprehend the bring your own encryption (BYOE), root (BYOR) or key (BYOK) principle, as this will return quite often. With BYOE, the understanding is that an organization is capable of using their own encryption software and manage their own encryption keys. Cloud Service Providers (CSP) allow customers to optionally import their own key pairs. With this model, the root CA of an organization is kept outside the cloud CA and a subordinate CA is placed in the cloud from which certificates are issued. With BYOR and BYOK, the understanding is that an organization is capable of using their own encryption keys without managing the encryption software. CSPs allow customers to optionally import their own key pairs. With this model, the root CA of an organization is placed inside the cloud CA and certificates are issued from this root. The cloud service customers have a copy of the root encryption keys themselves and are not vendor locked by this.

Last but not least is the defining of online versus offline and internal trust versus external trust. Online is defined as connecting to external services, including the Internet or another organization's internal network over which you do not have control. Offline is connecting to internal services over which you have full control. Internal and external trust has a lot of overlap with online and offline. Services that are offline can be seen as services with internal trust because no other organization has access to them. Online services will have external trust as third parties also have access to them.

The appendix includes more terminology, larger versions of demonstrated diagrams, a versus service comparison and formulated use cases.

3 PROBLEM STATEMENT

During the collection of related work, no academic research was found on the Certificate Authorities service in the cloud subject. This is exactly what this paper will try to solve and to possibly serve as the seminal paper towards the overall subject and influence later developments. The goal of this paper is to inform readers on how a cloud CA service impacts the stature of an organization.

3.1 Research Questions

The main research question of this paper is:

"How does the adoption of a Cloud Certificate Authority (CCA) benefit/impact an organization?".

This paper focuses on answering the main question by addressing the following set of sub-questions.

- How does a CCA differ from the classical CA/on-premise and IaaS implementation?
- How does the current landscape impact user experience in terms of a CCA?
- How does a transition from an on-premise CA to a CCA impact the organizational considerations?

4 RELATED WORK

Though no academic research was used as related work to further this research on, articles written by (tech) journalists and blog posts of the respective (cloud) service providers were used.

Tim Anderson from The Register wrote an article mid-2020 informing his readers on the cloud CA services of Amazon, Google and Microsoft. His conclusion was as to that Amazon Web Services was the first, which led to Google Cloud becoming the second while leaving Microsoft Azure behind with no service [3]. This article fundamental for the initial research into which providers should be researched.

PKI re-seller SSL247 wrote an article on why an organization would want to consider moving their public key infrastructure to the cloud. SSL247 states that cloud-based PKI is a cost effective solution for all critical business transactions, which means organizations do not have to choose between expensive security or a costly breach any longer [4]. Arti Loftus for ComputerWeekly wrote an article giving an abstract answer as to why a company would want to outsource their PKI [2]. This article, combined with the article of SSL247, gave the research team a direct insight into why these matters are a subject in the current day.

As was found in the early stage of this research, Microsoft Azure is not offering a Cloud CA Service while Amazon Web Services and Google Cloud are. The blog posts from the providers on what they are actually offering helped start the research. Amazon Web Services has been offering a Certificate Authority as a Service since mid-2019. Their certificate manager, called AWS Certificate Manager (ACM), is now supplied with the option of deploying a Private Certificate Authority which is capable of managing online root certificate authorities and with this a full online public key infrastructure hierarchy [5]. Google describes their Certificate Authority Service (CAS) in detail, which at the moment is a service available as beta. They claim to offer a highly scalable and available service that simplifies and automates the management and deployment of private CAs [6].

During the search of related work, a non-cloud provider was found offering a Cloud CA services, namely Venafi. Their focus is on providing companies cyber security products where they specialize in managing a public key infrastructure. Because of this, they have released an early version of a Cloud Private Certificate Authority into their integration suites [7].

5 METHODOLOGY

The following steps were utilized to research the given subject:

- Preliminary Research: Deep dive into the overall subject, CAaaS/PKI, and which (cloud) service providers are to be researched including what part of their infrastructure is to be taken into consideration.
- Scope Defining: With the help of defining a set of terminology, diagrams and use cases to reach a common understanding of the subject within the research team.
- Literature Research: Reviewing documentation written by (cloud) service providers and other (security) experts related on the given subject.
- Hands-on Review: Practical reviewing how (cloud) service providers deploy a certificate authority in the cloud.
- Write-Up: Report findings, formulating results and transforming these into a paper.

6 DATA GATHERING AND EXPERIMENTS

This research was mainly based around literature study. It started with a preliminary research into related work in various databases, such as Google Scholar, IEEE, Research Gate and UvA's database. These databases were searched with the terms "Certificate Authority as a Service", "Cloud Certificate Authority", "PKI as a Service" and more terms specifically related to the X-as-a-Service and/or Cloud CA. The literature study was complemented by hands-on platform reviewing each cloud CA solutions from the different providers. This was done by requesting trials to verify any claimed feature and to deep-dive into them further. A total of three trials were requested, at Google Cloud, Amazon Web Services and Venafi. In each environment experiments executed towards hosting a cloud CA, to create an own CA, implementing the bring your own encryption principle and having full control over the certificate revocation list.

7 RESULTS

The results section is divided into three section, based on the sub-questions. The first section focuses on the various implementation techniques of setting up a public key infrastructure. In the second section, cloud CA solutions of providers are highlighted to see what functionalities they offer. The last section discusses the considerations that take place at an organizational level when moving from a private CA on-premise to a cloud CA.

7.1 Infrastructure Models

During the mid-90s companies experienced an increased need of having a public key infrastructure. An article written for ComputerWorld in 2001 gives insight into the dilemma of housing a public key infrastructure locally or at a trusted PKI vendor [8]. The article states that outsourcing your PKI is only valuable when it is more expensive to run a certificate authority in-house. Though running a local certificate authority entails high costs such as soft- and hardware maintenance, specialistic PKI knowledge and constant evaluating risk this could be outsourced. With this a company is relieved from these burdens but in return will need to trust an external vendor with them. Evaluating the difference between on-premise, Infrastructure as a Service and in the Cloud in means of a certificate authority can be done in two ways, namely the technical side and the organizational side. This part of the paper will focus on the former.

Let's introduce A Company that Manufactures Everything (ACME) Corporation. ACME will face three scenarios in which they need a certificate authority for their public key infrastructure but have different requirements, such as PKI expertise in-house, software/hardware resources and more. These requirements will be described in the respective scenarios.

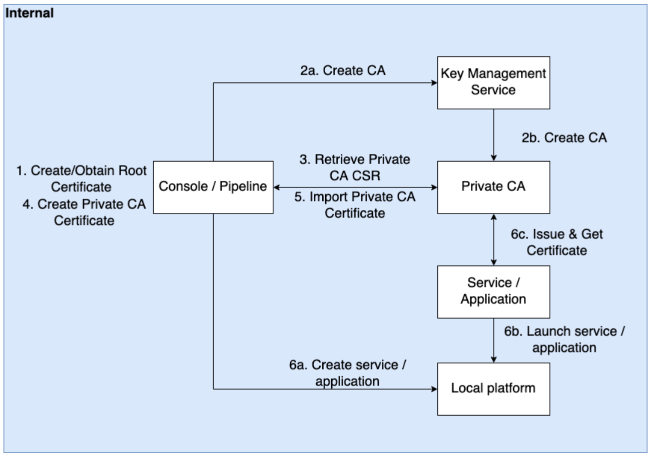

Internal
2a. Create CA
Key Management Service
2b. Create CA
1. Create/Obtain Root Certificate
4. Create Private CA Certificate
Console / Pipeline
3. Retrieve Private CA CSR
5. Import Private CA Certificate
Private CA
6c. Issue & Get Certificate
Service / Application
6b. Launch service / application
6a. Create service / application
Local platform

Figure 1: Initial PKI set up on-premise

To evaluate the difference between an on-premise CA versus a CA hosted external using IaaS versus a CA service in the cloud a baseline needs to be defined as to what each model exactly means. This will be done according to figures, whereas the initial drafts of the figures were based on an article written by Frederik Willaert [9]. Figure 1 defines the on-premise CA situation. ACME Corporation has an internal IT department with a system administration team responsible for the entire internal and external PKI. They will most likely make use of the Active Directory Certificate Services when using Windows Server or the OpenSSL library when working with Unix. According to Globalsign, a PKI vendor, this will burden the company with hardware costs, maintaining software validation services and the need of internal PKI expertise [10]. This is outlined by an article written by Encryption Consulting, which shares that having an on-premise PKI cost organizations approximately $305,000 more than cloud-based or Managed PKI services [11]. Though having a private CA on-premise does come with advantages such as being able to work with an offline root certificate authority, e.g. stored on a hardware security module or such as utilizing the bring your own encryption, key and root. With this, no question arises as to who is responsible. In this scenario, ACME is in full technical control of its PKI, with all of the advantages such as ownership and disadvantages such as high cost.

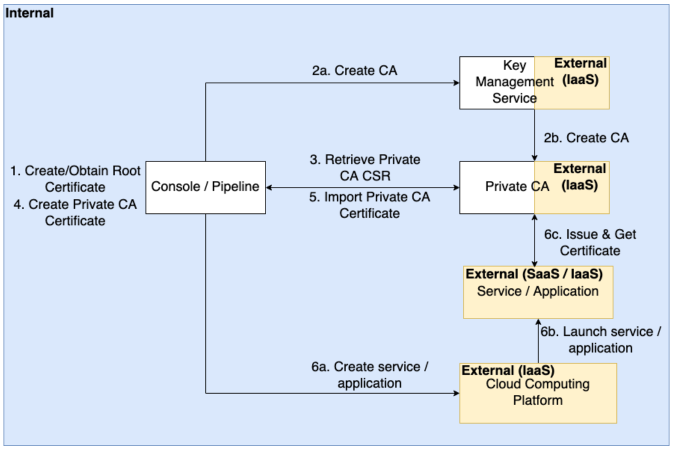

Internal
2a. Create CA
Key Management Service
External (IaaS)
2b. Create CA
1. Create/Obtain Root Certificate
4. Create Private CA Certificate
Console / Pipeline
3. Retrieve Private CA CSR
5. Import Private CA Certificate
Private CA
External (IaaS)
6c. Issue & Get Certificate
External (SaaS / IaaS)
Service / Application
6b. Launch service / application
6a. Create service / application
External (IaaS)
Cloud Computing Platform

Figure 2: Initial PKI set up with Infrastructure as a Service

In 2010 a rising trend [12] started where companies moved their core components of their infrastructure to the cloud to enable cost savings and provide scalability, with this came the now well known X-as-a-Service models. One of them is PKI-as-a-Service (PKIaaS) [2], which can be divided into cloud-based PKIaaS, managed PKIaaS or simply a private CA externally hosted using IaaS. Let us consider the latter for now, which is demonstrated in figure 2. ACME has decided to modernize their way of working by offloading all of its infrastructure to a cloud service provider. With this, they transfer their on-premise certificate authority server to a server hosted within the cloud computing platform of the CSP. ACME is now only in control of what is running on that server, their private CA. They have lost the ownership over the hardware but with this came the advantage of not having to worry about maintenance and costs. Internal PKI expertise is still needed, as the software around the private CA is still in full control of ACME, and when wanting to work with a local root certificate, a hardware security module is still necessary. The main advantage of hosting a private CA with the Infrastructure-as-a-Service model is to have a sole focus from the system administration team on existing software services such as PKI which will increase their time investment into reducing human errors and being capable of fine tuning their certificate landscape by orchestration and automation. With this model, a company will need to invest less into system administration and can decrease and shift budget to their development team, or work with the DevOps principle.

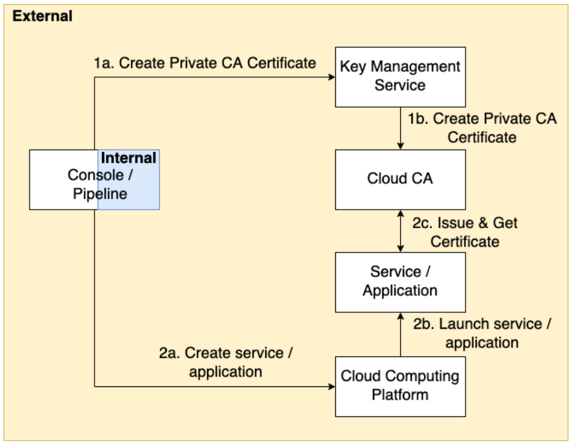

External
1a. Create Private CA Certificate
Key Management Service
1b. Create Private CA Certificate
Internal
Console / Pipeline
Cloud CA
2c. Issue & Get Certificate
Service / Application
2b. Launch service / application
2a. Create service / application
Cloud Computing Platform

Figure 3: Initial PKI set up with CA as a Service in the Cloud

As of 2019, CAaaS has entered the vastly growing X-as-a-Service market. So let us consider ACME again, but now in a scenario in need of a cloud CA service. ACME has no in-house PKI expertise, their IT department is quite large and has their hands full with ongoing DevOps projects. They do need a public key infrastructure and they certainly need a fast way of obtaining certificates for their projects. For ACME, a fast way of implementing an entire PKI hierarchy would be to set up a new Cloud CA at one of the providers. This is illustrated in figure 3. No soft- and hardware maintenance, minimal PKI knowledge and vast insight of costs. Though outsourcing all of this does come with risks that need to be accepted, such as having a root CA hosted online or if the cloud service provider has downtime which results in certain (or a complete) blackout of ACME's public key infrastructure. When considering the first issue, it is known that cloud service providers offering a CA service in Cloud are implementing the bring your own encryption principle, which ensures that you can keep hold of your root certificate and store it offline. This can be seen in figure 4.

Smaller companies, or not marketed as cloud service providers, such as Venafi are starting to introduce similar services where they offer a CA Cloud Service whereas other companies have stripped off the cloud part. It is critical to get a clear definition difference between CAaaS and CAaaS in the cloud. It is possible for companies to start offering merely a Certificate Authority as a Service whereas the company will function as a managed provider implementing and maintaining a private CA hosted on a local platform or within a cloud computing platform. With this you revert back to managed PKIaaS which can be seen in figure 5.

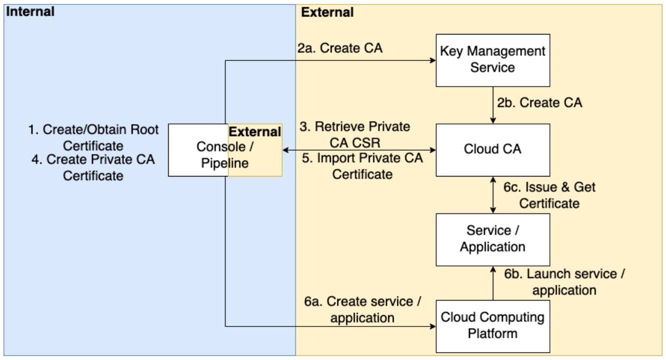

Internal
External
2a. Create CA
Key Management Service
2b. Create CA
1. Create/Obtain Root Certificate
4. Create Private CA Certificate
External
Console / Pipeline
3. Retrieve Private CA CSR
5. Import Private CA Certificate
Cloud CA
6c. Issue & Get Certificate
Service / Application
6b. Launch service / application
6a. Create service / application
Cloud Computing Platform

Figure 4: Initial PKI set up with CA as a Service in the Cloud including bring your own encryption principle

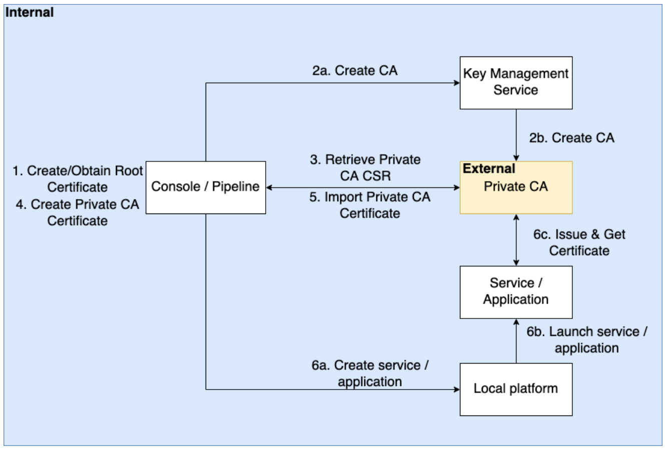

Internal
2a. Create CA
Key Management Service
2b. Create CA
1. Create/Obtain Root Certificate
4. Create Private CA Certificate
Console / Pipeline
3. Retrieve Private CA CSR
5. Import Private CA Certificate
External
Private CA
6c. Issue & Get Certificate
Service / Application
6b. Launch service / application
6a. Create service / application
Local platform

Figure 5: Initial PKI set up with CA as a Service

The actual difference between on-premise, IaaS and CAaaS reveals itself on the decision regarding the need of in- or outsourcing hardware/software and specific expertise. When looking at an on-premise PKI solution, all components of a PKI infrastructure are kept within the ownership of a company. This means that the knowledge but also the hardware facilities within an organization are required to be present. With an on-premise solution, you keep the trust part completely offline, which offers a high degree of own control and security in a PKI infrastructure. When using a X-as-a-Service infrastructure model to run a certificate authority, all hardware resources are provided by a cloud service provider. A company will still need to have the knowledge in-house to set up a PKI infrastructure. The advantage of this solution is that a company does not have to incur any hardware costs, unless they decide to keep the root CA offline within a local HSM of the organization. This keeps the security and control of the organization's root certificate internal and does come with minimal costs compared to an on-premise certificate authority solution. And finally, you have the CA service in the cloud, where you hand over all the burdens, including hardware, trust, knowledge and storage. A cloud service provider supplies the solution with all the means to set up a PKI infrastructure. The trust of your root CA with this solution usually lies with the CSP, but a number of providers offer the possibility to bring your own encryption with their Cloud CA, whereby the root CA can still be kept outside the cloud.

Having looked at three different scenarios whereas a certificate authority has been implemented, it can be concluded that the difference between them is the level of placing a trust. This should not be mistaken with the organizational part of the dilemma, which is in regards to managing risks can be read later in this paper. Ownership, technical control, hardware/software costs and PKI expertise are the main takeaways when explaining the differences. With this, the first sub-question, "How does a CCA differ from the classical CA/on-premise and IaaS implementation?", has been answered.

7.2 (Cloud) Service Providers

During the research, cloud CA solutions from different service providers were compared to get an idea of what each solution offers in terms of functionalities. The solutions of the three largest cloud service providers were investigated and the solution of a cyber security company was also examined. This part of the paper will elaborate on the functionalities of the CA solutions per provider. Ultimately, the results of the experiments will be highlighted in table 1 to provide a quick overview of the different CA solutions and to answer the second sub-question, "How does the current landscape impact user experience in terms of a CCA?".

Amazon Web Services

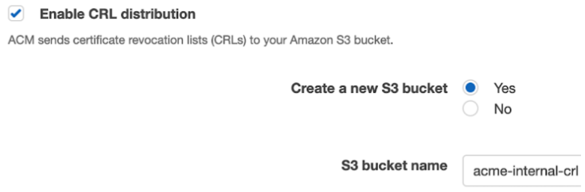
Amazon Web Services was the first on the market to offer a Certificate Authority as a Service in the Cloud, they did this through an addition to their AWS Certificate Manager by adding the feature Private Certificate Authority [13]. This addition was done mid-2019 and by adding this feature, the manager is now able to create, deploy and manage private certificates issued from a customer created CA.

When subscribing to the ACM Private CA service, Amazon Web Services provides a cloud CA with which a complete PKI hierarchy can be set up or expanded. If a company already has a root CA, the root certificate can be stored outside the ACM Private CA service by means of the bring your own encryption principle. The cloud CA acts as a subordinate / intermediate CA of the already existing root CA to expand a hierarchy.

Amazon Web Services provides three different communication methods for communicating with a cloud CA namely their cloud console, command line (AWS CLI) and a REST API. Via these methodologies, the hierarchy can be set up or expanded as described above, but it is also able to manage, validate and issue certificates below the root and or intermediate certificates. A cloud CA from Amazon Web Services is able to handle 25 requests per second.

Services that are often subscribed together with the ACM Private CA feature are the AWS Key Management Services for managing the certificates and the AWS CloudHSM for securely storing the encryption keys/certificates. AWS's cloud HSM complies with FIPS 140-2 Level 3. In addition, Amazon Web Services also keeps track of events using CloudTrail, where all API calls from the ACM Private CA console, from the CLI or from code saved in a S3 bucket. The S3 bucket is also used within ACM private CA to store the certificate revocation list, this can be seen in figure 6.

Amazon Web Services offers a complete cloud CA service. This makes them one of the front runners of cloud service providers with a Certificate Authority as a Service in the Cloud. In addition to being the first, they want to stay in pole position which can be seen when analyzing what has been added after release. It should be an interesting fact as to if Amazon Web Services can stay in this position for the upcoming time.



☑ Enable CRL distribution

ACM sends certificate revocation lists (CRLs) to your Amazon S3 bucket.

Create a new S3 bucket ● Yes ○ No

S3 bucket name: acme-internal-crl

Figure 6: Enable certificate revocation list at Amazon Web Services

Google Cloud

Google Cloud introduced their Certificate Authority Service in beta as of early August 2020 [6], almost a year after Amazon Web Services released their Certificate Authority in the Cloud service but Google is still ahead of Microsoft Azure in the ‘race’. Being in beta, Google's developers are rapidly adding new features to the service such as supporting the bring your own encryption principle or upping the API/CLI queries per second threshold to withstand environments with a high-volume of short-lived certificates.

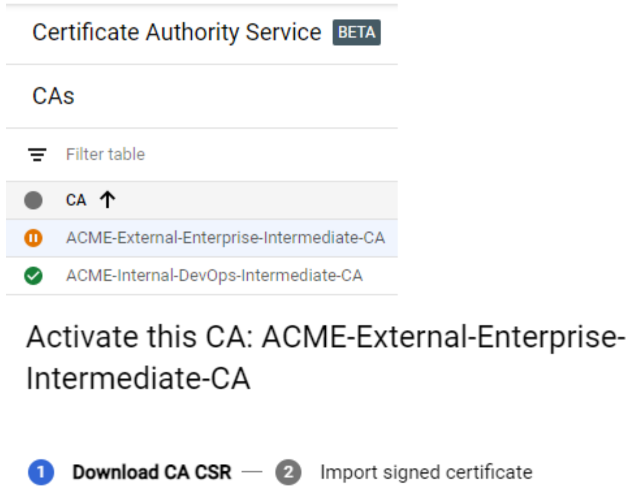
After signing up for Google's Certificate Authority Service (CAS), Google provides the mean to create a cloud CA with which a complete PKI hierarchy can be set up or expanded. Google CAS supports the ability to generate a root certificate as the start of a new hierarchy but also supports to create a subordinate certificate to withstand an already existing hierarchy. This enables the administrator to work with the bring your own encryption model and can be seen in figure 7.

Google Certificate Authority Service (CAS) includes all other relevant services if needed such as their Cloud Key Management service to manage any of the certificates, their Cloud HSM service, abiding to the FIPS 140-2 Level 3 standard, to store any of the encryption keys, Cloud Audit Logs to keep track of events and Cloud Identity Access Management (IAM) to ensure authentication and authorization. Besides this, CAS is reachable via the Google Cloud web platform, a REST API and Google's own gcloud command line interface tool. Furthermore, CAS allows customers to store their certificate revocation list externally or internally within a Cloud Storage Bucket.

While still in a beta phase Google's Cloud CA service can keep up with functionality compared to its direct competitors. Google seems to want to attract new customers to its cloud platform by being one of the first to offer a full fledged Certificate Authority as a Service in the Cloud and perhaps see this as their way to increase their lesser market share.

Microsoft Azure

When reviewing the initial comparison between Amazon, Google and Microsoft [3], Microsoft is still not offering a Cloud CA service. Though multiple feature requests have come in via the Azure feedback forum [14], Microsoft is yet to reply to any.



Certificate Authority Service BETA

CAs

Filter table

CA ↑

ACME-External-Enterprise-Intermediate-CA

ACME-Internal-DevOps-Intermediate-CA

Activate this CA: ACME-External-Enterprise-Intermediate-CA

1 Download CA CSR — 2 Import signed certificate

Figure 7: Bring your own encryption principle at Google Cloud

Microsoft published a comparison table between Azure and Amazon Web Services in which Microsoft claims to offer an alternative service to AWS Certificate Manager. While in some cases this is true, Microsoft is not capable of setting up a full Cloud CA service for its customers. This can neither be reached via their App Service Certificates nor their Key Vault service. The similarity between the solutions of Azure and Amazon lies within the capability of setting up a partner subscription with an external CA, such as DigiCert or GlobalSign, or a private CA hosted external via IaaS. Therefore it can be concluded that Microsoft Azure does not offer anything in terms of a Cloud CA service. A conclusive answer as to why they are not offering such a service is unknown. One can speculate and say that Microsoft has their focus on offering Active Directory Certificate Services as a feature for their Windows Servers.

While still in the second position as biggest market share in Cloud Computing [15], the question is if Microsoft will start to decline to other cloud service providers while customers are in suspense of a Cloud CA Service.

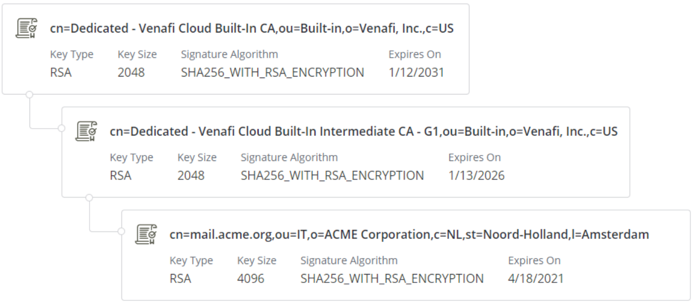
Venafi

Venafi is as of writing the only company that is not a cloud provider but does offer a Cloud CA solution. Their solution is Venafi Cloud Private Certificate Authority [7]. Venafi is a cyber security company that focuses on improving the security of DevOps processes offering products specialized within the public key infrastructure domain.

When subscribing to the Venafi Cloud CA service, a Cloud CA with a built-in root CA is set up for each customer, along with an intermediate CA from which certificates can be issued. Customers are unable to create their own CA, this is automatically done by Venafi, the CA certificates can be seen in figure 8. Besides this, the customer is unable to delete the existing CA or create a new one operating next to it. Customers are limited to the Venafi generated CA but are also limited in managing issued certificates because the control over the certificate revocation list is solely in control of Venafi. The Cloud CA can be accessed via the included cloud interface, API or command line utilities. Venafi provides a software development kit (SDK) for their solution in various programming languages such as Java, GO, Python and more. This distinguishes Venafi from the other three providers because they are very focused on the integration of DevOps tools, such as Kubernetes, Ansible and Terraform, to better secure DevOps processes within organizations. Besides offering a personal Cloud CA solution, Venafi offers a similar service as Azure Key Vault where it is possible to set up a partner subscription with external CAs such as Globalsign and DigiCert.

Venafi Cloud CA allows customers to create private certificates but limits the certificate key pair to only RSA 1024, 2048 and 4096. They do not offer issuing templates to ensure faster deployment but they offer templates to limit what can be inserted in a certificate. For example, if a project exists where only certificates may be issued with a country code in The Netherlands, this would be set in a template. When handling certificate requests, Venafi declares itself a high-speed issuance, but a specific speed cannot be confirmed. The same goes with many other criteria, Venafi remains unclear on how they deliver in areas such as HSM, logging and IAM.

As a cyber security company, Venafi is a frontrunner in providing a Cloud CA with integration for many DevOps tools. This makes them a worthy competitor for the Cloud CA solutions of cloud service providers. However, there are still many points where Venafi is unclear how they handle it.



cn=Dedicated - Venafi Cloud Built-In CA,ou=Built-in,o=Venafi, Inc.,c=US

Key Type	Key Size	Signature Algorithm	Expires On
RSA	2048	SHA256_WITH_RSA_ENCRYPTION	1/12/2031

cn=Dedicated - Venafi Cloud Built-In Intermediate CA - G1,ou=Built-in,o=Venafi, Inc.,c=US

Key Type	Key Size	Signature Algorithm	Expires On
RSA	2048	SHA256_WITH_RSA_ENCRYPTION	1/13/2026

cn=mail.acme.org,ou=IT,o=ACME Corporation,c=NL,st=Noord-Holland,l=Amsterdam

Key Type	Key Size	Signature Algorithm	Expires On
RSA	4096	SHA256_WITH_RSA_ENCRYPTION	4/18/2021

Figure 8: Auto generated root CA and sub CA at Venafi

	AWS	GC	MA	VEN
Cloud CA	✓	✓	X	✓
Create your own CA	✓	✓	X	X
BYOE	✓	✓	X	X
Control over HSM	X	X	X	X
Control over CRL	✓	✓	X	X

Table 1: Results of experiments

AWS = Amazon Web Services, GC = Google Cloud, MA = Microsoft Azure, VEN = Venafi, BYOE = Bring your own encryption

7.3 Transition towards Cloud

To get a better understanding as to how a transition would proceed, a set of use cases are defined and can be found in appendix B.

These use cases were used to aid the research and to receive a good overview on which dilemmas companies encounter during such transition.

A transition from having an on-premise CA to a Cloud CA does not only contain technical changes, but also organizational changes. This part of the paper will focus on the latter. In the PKI landscape, a number of aspects are affected during a transition to the cloud to which an organization will need to adhere at a higher level for managing risks.

Once again the fictitious company ACME Corporation is used to demonstrate the transition. The current situation is an on-premise CA and the end goal is a cloud CA. To map the current PKI situation, the research specifically looked into the following PKI components: Private CA, HSM and a certificate store. The private CA at ACME is maintained by the team of system administrators who have full control over the CA and can regulate all policies themselves so that their security rules are enforced. The root CA of ACME is encrypted with encryption keys stored in their HSM, which is located in a secure room which ACME has full control over and can only be accessed if all predefined policies are met. The same applies to the storage of the certificates issued by the private CA of ACME, the storage is fully controlled by ACME itself, as is the access to it. Figure 9 shows a diagram in which the current situation of ACME is outlined with the aspects of a PKI and the required resources (knowledge, control and / or policies). In short, with an on-premise CA, ACME Corporation has full organizational control over their PKI but also requires in-house expertise and predefined policies that allow them to continue running their public key infrastructure. With this, ACME corporation has started their journey into managing risks. For this scenario, they have decided to take all potential risks on themselves which in turn results in having ACME to uphold their organizational needs, such as in-house policies. But how would this scenario change when ACME decides to move towards a Cloud CA service for their PKI?

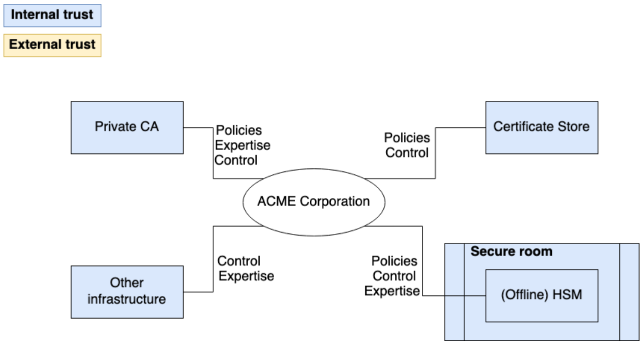


Figure 9: Organizational representation of a PKI on-premise

Moving your PKI landscape to the cloud entails the necessary risks because parts with internal trust are replaced with external trust, as already mentioned in the Infrastructure Model chapter. For an organization like ACME Corporation, it is important to consider the risks that can arise from it. The private CA becomes a cloud CA where the system administration team loses their full control over it because it is maintained by the cloud service provider. Losing control means that ACME can no longer withstand company policies on the CA itself. For example, if ACME has a policy in regards to only deploying servers running Windows Server 2016 or higher, a service provider can decide to deploy and run the CA on a server with a different operating system. ACME has only limited control over the cloud CA, or in some cases with certain providers no control at all. The same limitation applies to regulating the policies at the cloud CA, ACME relies on the configuration options made available by the CSP. One of the major changes when moving to the cloud is the situation regarding the HSMs, whereas ACME chooses to go completely in the cloud, so without the bring your own encryption principle. They will utilize an always online HSM that ACME no longer has control or even the ability to access it. This results in what some may say are advantages and other disadvantages, because ACME will not be able to set up policies to access the HSM containing their key pair. This is now fully decided by the chosen provider. The storage of the issued certificates is also arranged by the cloud service provider, though with a certificate storage can be said that certain aspects are still in control of ACME such as the certificate revocation list. This can be seen as limited control. Now having full cloud fledged certificate stores and HSMs, ACME does not have control in regards to physical security. This can once again be seen as an advantage or disadvantage as it comes down to weighing up the risks. Though some providers do over adequate Identity Access Management in which logical access control can be set up. This plays an important role in the distinction of responsibilities for the ACME administrator team. Figure 10 provides a visual representation of the PKI landscape as it has changed from an on-premise CA to a cloud CA.

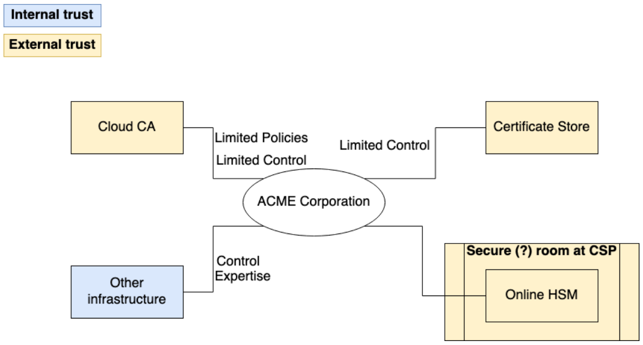


Figure 10: Organizational representation of a PKI in the Cloud

When looking at all aspects of the PKI landscape, it can be seen that there has been a decrease in organizational control as with needed in-house expertise and predefined policies when comparing to an on-premise CA situation. By relinquishing these aspects, the trust is placed in the hands of a CSP, with all of the corresponding risks. This means that ACME's management has an important role to play in weighing up the risks in order to ensure a tolerable amount for their company. Their weighing points rely on if they should accept less risks and in-source, but increase their cost or should they outsource their risks and increase their available resources into business areas. This dilemma is company specific to which it is unable to give a complete answer in this paper although it all comes down to the musts, shoulds and coulds of a company. With this, the third and last sub-question, "How does a transition from an on-premise CA to a CCA impact the organizational considerations?", has been answered.

8 CONCLUSIONS

This paper has explored the differences between infrastructure models when hosting a certificate authority, what providers currently offer in terms of a Cloud CA service and what organizational aspects change during a transition from on-premise to the cloud. By reviewing these results the following can be concluded.

The technical side of the research has shown that when shifting between infrastructure models, a company will need to rethink how they handle their online versus offline matters. As in with an on-premise CA, a root certificate can be held offline completely whereas this is partly the case with IaaS and only in certain cases when using a Cloud CA service. This latter can be accomplished when using the bring your own encryption principle. This furthers into shifting of internal trust versus external trust whereas when moving from an on-premise model a company starts with a full internal trust model and will gradually transform into an external trust model, whereas a (cloud) provider will take over technical aspects of the certificate authority. This can be seen as disadvantages but as seen in the research can come out of the need to outsource because of missing in-house PKI expertise or having reviewed the cost management of the infrastructure models. This latter generally concludes in that having a cloud CA service lowers direct cost. When comparing the infrastructure models head-to-head, hosting a certificate authority via an IaaS solution seems to be worst. An organization will give away some control but still require in-house expertise. This solution is only valuable when vendor locked when using IaaS, for whatever reason, without a cloud CA service but still requiring a internal public key infrastructure. A practical example to this conclusion would be the Diginotar hack in 2011. This Dutch certificate authority was hacked due to various security failures. This caused a great loss in reputation which resulted in the the company's closing. These two facts are unacceptable risks for companies such as Amazon and Google. This results into them investing a lot of resources into mitigating and controlling these risks. This is the exact technical consideration an organization should take. As to is it still realistic and feasible to protect an on-premise Certificate Infrastructure against such hacks while (cloud) service providers with a much higher level of resources already do this.

This research was capable of identifying two cloud service providers (Amazon and Google) offering a true cloud CA service. Besides this, software cyber security company (Venafi) was found offering a limited cloud CA service. Each of them has their own quirks and ultimately the decision between lies in which platform has already been invested within an organization. The main takeaways were the ability to host a cloud CA, to create an own CA, including the bring your own encryption principle and having full control over the certificate revocation list. Amazon and Google are offering this within their service whereas Venafi is missing some essential parts such as the ability to create an own CA or to manage a certificate revocation list. The odd bird in the story here is Microsoft Azure. Based on the amount of feature requests within their Azure Feedback Forum, they either do not seem to worry about the fact of not offering a cloud CA service or they are silently working on integrating it into their Azure Key Vault solution. If we compare the early stages of AWS Certificate Manager, Amazon was offering the same as what Microsoft is currently offering with Azure Key Vault. Namely to set up partner subscriptions with external CAs. This research can only speculate but with the fact that Microsoft added the ability to include non-partnered CAs in Azure Key Vault, they might introduce a cloud CA service in the future. It should not be forgotten that Microsoft offers Windows Server features such as Active Directory Certificate Services, allowing them to rely on the IaaS model.

When looking at the organizational considerations, this research was capable of defining changes in company policies and the way a company manages their risks as takeaways. When shifting from an on-premise CA to a cloud service, this paper can conclude that a company is no longer in full control of creating and maintaining policies. Examples are not being able to set up an own secure room with a hardware security model or imply organizational requirements to software, such as operating systems or certificate limitations. During this research the aspect of losing the fact of having an on-premise secure room with a HSM was brought up more than any of the other aspects. A HSM is seen as the root of trust of the certificate authority, and the way to stay in full control. When moving towards a cloud CA, this responsibility is in most cases handed over to the (cloud) service provider in which a customer will need to place full trust. Like the earlier mentioned technical consideration on the fact that a CSP is able to invest more resources into protecting the infrastructure. This can be shifted into the organizational consideration as to is it possible to put trust into an external vendor handling these responsibilities. A company will have to review their potential risks and decide whether they want to in-source or out-source these to a service provider.

When looking at the main research question of the paper, "How does the adoption of a Cloud Certificate Authority (CCA) benefit/impact an organization?", the research can conclude that each impact and benefit that comes with moving to a cloud CA service is organizational specific. This results into the fact that each company should review their portfolio into the matters of having PKI expertise in-house, the capability of hosting the soft- and hardware themselves and in what matters they want to manage risks. Security advantages that come with on-premise are having full control over the infrastructure but with this comes a higher level of risk into infrastructure responsibility. This latter can be out-sourced to a service provider where they are now responsible for ensuring security of the infrastructure but with this comes less control over the, now turned into, cloud CA. Even if all the requirements are found in-house, a company can still decide to use a cloud CA service since some may assume that the biggest cloud service providers out there meeting all the requirements might do the job better than in-house. This once again, all comes down to evaluating the stature of the company and the exact needs. For companies looking to do such an evaluation, this paper could be used as a starting point.

9 DISCUSSION

This section will discuss the limitations of the paper.

Related Work Validity: During the collection of related work for the research, no academic papers were found on the given subject. The research team acknowledges that there is a possibility that even though multiple databases were exhausted, such papers were overlooked. The fact that no previous research was found guided the way on how the related work section is currently formed. The research team speculates that this is the first academic paper on the CA Cloud Service provider.

Conclusion Validity: The research team acknowledges that parts of the conclusion can be subjective. This is because the conclusion of this paper has been formed around the experiences and knowledge that the research team had, and gained during the research. In addition, discussions were held between the research team and the stakeholders which could have directed parts of the conclusion. This could mean that when another person utilizes a different methodology founded on different knowledge and experience, could result in parts of the conclusion to differ. If the same approach is used to perform the research again, the authors expect the conclusion to withstand.

Internal and External Validity: To ensure no internal and external conflict of interest occurs, the paper has been peer reviewed by two experts of the commissioning company, Deloitte, and two external security experts.

10 FUTURE WORK

The research team acknowledges that the paper is currently set on a broad subject and that if more time had allowed for the project, the research team would have liked to investigate further into the means of what Microsoft Azure truly brings to the table with their key management service. The current research draws conclusions based on publicly available documents and blogs posts written by external person. For some reason, Microsoft is not feeling any pressure in regards to release a Cloud CA service and appraise their Key Vault as alternative. Why is this the case?

Besides this the researchers agree that a specific research towards the changes into the physical security that occur when you move from an on-premise CA to a Cloud CA service would be valuable. This would be a very practical research whereas on-site touring and interviewing would be needed besides literature research. Besides physical changes, a research into the juridical field as to who is accountable for what will be beneficial for organizations.

As last addition, the research team thinks that a noteworthy research could be done in regards to completely offline environments while still implementing a Cloud CA service. A lot of aspects come to mind, such as cloud and local security including the way how such an air-gapped network should be build.

ACKNOWLEDGMENTS

This work was supported by Deloitte, in specific by Itan Barmes PhD and Colin Schappin MSc. Additional resources were provided by the University of Amsterdam and the master's study System and Network Engineering (OS3). We also thank the external reviewers for contributing.

REFERENCES

[1] Statista Research Department. *Top reasons why companies outsource information technology (IT) services worldwide in 2018.* URL: https://www.statista.com/statistics/948977/technology-outsourcing-top-reasons-globally/. (accessed: 23.12.2020).

[2] Arti Loftus. *Outsourcing PKI to the cloud: What enterprises need to know.* URL: https://www.computerweekly.com/feature/Outsourcing-PKI-to-the-cloud-What-enterprises-need-to-know. (accessed: 23.12.2020).

[3] Tim Anderson. *Google catches up to AWS and steals a march on Azure with introduction of cloudy Certificate Authority Service.* URL: https://www.theregister.com/2020/08/05/google_introduces_cloudy_certificate_authority/. (accessed: 30.12.2020).

[4] SSL247. *Choosing between On-premise PKI Vs. Cloud-based PKI.* URL: https://www.ssl247.com/kb/mpki/cloudvslocal. (accessed: 25.11.2020).

[5] Todd Cignetti Josh Rosenthol. *How to host and manage an entire private certificate infrastructure in AWS.* URL: https://aws.amazon.com/blogs/security/how-to-host-and-manage-an-entire-private-certificate-infrastructure-in-aws/. (accessed: 25.11.2020).

[6] Anton Chuvakin and Anoosh Saboori. *Introducing CAS: Securing applications with private CAs and certificates.* URL: https://cloud.google.com/blog/products/identity-security/introducing-cas-a-cloud-based-managed-ca-for-the-devops-and-iot-world. (accessed: 25.11.2020).

[7] Venafi. *Venafi Cloud Private Certificate Authority.* URL: https://www.venafi.com/venaficloud/devopsaccelerate/capabilities/privateCA. (accessed: 25.11.2020).

[8] ITworld staff. *Companies warming up to PKI.* URL: https://www.computerworld.com/article/2797542/companies-warming-up-to-pki.html. (accessed: 21.01.2021).

[9] Frederik Willaert. *Setting up a Private Certificate Authority on AWS.* URL: https://medium.com/@frederik.willaert/setting-up-a-private-certificate-authority-on-aws-b220154cf98. (accessed: 21.01.2021).

[10] Julien Olenski. *What is Active Directory Certificate Services and Why Should I Use It?* URL: https://www.globalsign.com/en/blog/what-is-active-directory-certificate-services. (accessed: 21.01.2021).

[11] Parnashree Saha. *What is Cloud-based PKI Architecture?* URL: https://www.encryptionconsulting.com/cloud-based-public-key-infrastructure-architecture/. (accessed: 21.01.2021).

[12] Bradley Knapp. *IaaS (Infrastructure-as-a-Service).* URL: https://www.ibm.com/cloud/learn/iaas. (accessed: 21.01.2021).

[13] AWS. *AWS Certificate Manager Private Certificate Authority.* URL: https://aws.amazon.com/certificate-manager/private-certificate-authority/. (accessed: 28.01.2021).

[14] Azure. *Private CA (Certificate Authority) certificate issuing capability.* URL: https://feedback.azure.com/forums/906355-azure-key-vault/suggestions/41007625-private-ca-certificate-authority-certificate-iss. (accessed: 28.01.2021).

[15] Katy Stalcup. *AWS vs Azure vs Google Cloud Market Share 2020: What the Latest Data Shows.* URL: https://www.parkmycloud.com/blog/aws-vs-azure-vs-google-cloud-market-share/. (accessed: 28.01.2021).

[16] Azure Microsoft. *What is a cloud service provider?* URL: https://azure.microsoft.com/en-us/overview/what-is-a-cloud-provider/. (accessed: 4.01.2021).

[17] TechTarget. *registration authority (RA).* URL: https://searchsecurity.techtarget.com/definition/registration-authority. (accessed: 4.01.2021).

[18] Wikipedia. *Public key infrastructure.* URL: https://en.wikipedia.org/wiki/Public_key_infrastructure. (accessed: 4.01.2021).

[19] Patrick Grubbs. *Managed PKI VS Private PKI.* URL: https://www.securew2.com/blog/managed-pki-vs-private-pki. (accessed: 4.01.2021).

[20] Patrick Nohe. *The Difference Between Root Certificates and Intermediate Certificates.* URL: https://www.thesslstore.com/blog/root-certificates-intermediate/. (accessed: 4.01.2021).

[21] Jason Soroko. *Private CA (private PKI).* URL: https://searchsecurity.techtarget.com/definition/private-CA-private-PKI. (accessed: 4.01.2021).

[22] Wikipedia. *Hardware security module.* URL: https://en.wikipedia.org/wiki/Hardware_security_module. (accessed: 4.01.2021).

[23] TechTarget. *BYOE (bring your own encryption).* URL: https://whatis.techtarget.com/definition/BYOE-bring-your-own-encryption. (accessed: 4.01.2021).

[24] TechTarget. *Infrastructure as a Service (IaaS)*.
URL: https://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS. (accessed: 4.01.2021).

[25] TechTarget. *BYOE (bring your own encryption)*.
URL: https://www.salesforce.com/ap/saas/. (accessed: 4.01.2021).

Below is a complete overview of appendixes used to complete the research successfully.

A TERMINOLOGY

Cloud Service Provider (CSP): A third-party company offering a cloud-based platform, infrastructure, application, or storage services [16]. This research will be focused on Amazon Web Services (AWS), Google Cloud (CG) and Venafi.

Certificate Authority (CA): A certificate authority is a company or organization that handles the validation and issuing of digital certificates.

Registration Authority (RA): A registration authority is an authority in a network that verifies user requests for a digital certificate and tells the certificate authority to issue it [17].

Public Key Infrastructure (PKI): Roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public key encryption [18].

On-Premise/Private PKI: A PKI that is maintained by an internal team of an organization. A private PKI is usually also “on-premise”, meaning that the physical hardware is on-premise and also being maintained internally. It is possible to have a private PKI that is hosted in the cloud and maintained internally [19].

Managed PKI: A PKI that is maintained by an external company. This can be either hosted in the cloud or on-premise but the maintenance is always outsourced.

Cloud-Based PKI: A PKI that is fully maintained in the cloud by a company external to your organization.

Online vs Offline: Online is connecting to external services, including the Internet or another organization’s internal network over which you do not have control. Offline is connecting to internal services that you have full control over.

Internal vs External Trust: Internal and external trust has a lot of overlap with online and offline. Services that are offline can be seen as services with internal trust because no other organization has access to them. Online services will have external trust as third parties also have access to them.

Air gap: A component, such as the CA server, which is isolated from unsecured networks such as the internet and any other components connected to the online services. This can be achieved physically or when done correctly, with the help of firewalls. The firewall would need to be configured to only allow one-way traffic towards the disconnected environment under supervision of a system administrator. There is no traffic ongoing without supervision.

Root CA: A Root CA is a Certificate Authority that owns one or more trusted roots [20]. Root CAs can be found in many operating systems and web browser trust stores by default while also being pushed towards trust stores within a local network by a system administrator.

Subordinate CA: A subordinate CA is created as soon as the root CA issues certificates to other CAs. A subordinate CA that only issues certificates to users, and not CAs, is also known as a leaf CA.

Intermediate CA: An intermediate CA is created as soon as a subordinate CA has issued certificates to other CAs. While an intermediate CA is subordinate to the root CA, it is considered superior to those subordinate CAs to which it issued certificates.

Cross-signed: A cross-certificate is a digital certificate issued by one Certificate Authority that is used to sign the public key for the root certificate of another Certificate Authority. Cross-certificates provide a means to create a chain of trust from a single, trusted, root CA to multiple other CAs.

Private CA: A private CA is an organization-specific certification authority that functions like a publicly-trusted CA. Essentially, an organization creates its own private base certificate which can issue other private certificates for internal servers and users. Certificates issued by a Private CA are not publicly trusted and should not be used outside of the organizations trusted members and infrastructure. Private CA is also known as Private Public Key Infrastructure (Private PKI) or internal Certificate Authority. [21]

Cloud CA: A private CA that is fully hosted by a cloud service provider and thus owning all the hardware, such as the HSM, that the PKI is being hosted on. In sense, an external trust is made towards another company which delivers internal trust.

Hardware Security Module (HSM): A physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions [22].

Key Management Service (KSM): A component which creates and manages cryptographic keys and controls the use of them for services and applications.

Cloud-KMS: A cloud-hosted key management service that lets you manage cryptographic keys for your cloud services. You can generate, use, rotate, and destroy cryptographic keys.

Cloud-HSM: A Cloud-HSM is a cloud-hosted Hardware Security Module (HSM) service that allows a company to host encryption keys and perform cryptographic operations in a cluster of certified HSMs owned by a cloud service provider. Providers such as Google and AWS manage the HSM cluster for the company, so the company doesn’t need to worry about clustering, scaling, patching, (physical) maintenance, procedures and specialistic knowledge. Cloud-HSM and Cloud-KMS are components which often work together.

Bring your own encryption: A cloud computing security marketing model that purports to help cloud service customers to use their own encryption software and manage their own encryption keys [23]. CSPs allow customers to optionally import their own key pairs. With this model, the root CA of an organization is kept outside the cloud CA and an intermediate CA is placed in the cloud from which certificates are issued.

Bring your own key / root: A cloud computing security marketing model that purports to help cloud service customers to use their own encryption keys without managing the encryption. CSPs allow customers to optionally import their own key pairs. With this model, the root CA of an organization is placed inside the cloud CA and certificates are issued from this root. The cloud service customers have a copy of the root encryption keys themselves and are not vendor locked by this.

IaaS: Infrastructure as a service is a form of cloud computing where the infrastructure is offered virtually. The hardware including servers, network equipment and the workstations are owned by the cloud service provider [24].

SaaS: Software as a service is a way of delivering applications over the Internet, as a service. Instead of installing and maintaining software, you simply access it via the Internet, freeing yourself from complex software and hardware management. SaaS applications run on a SaaS provider's servers. The provider manages access to the application, including security, availability, and performance [25].

CAaaS: Certificate Authority as a service is a way of setting up a CA by a third party so that the burden of an organization is taken over by the third party. In this way, a third party sets up the CA on premise at an organization, allowing you to keep the root CA offline.

CAaaS in the Cloud: With Certificate Authority as a service in the cloud, the PKI infrastructure is set up or moved from on-premise to the cloud. A third party is responsible for hosting CAs in the cloud, including the company's root CA. In this way, the organization's root CA will be available online.

B USE CASES

Use case 1: Initial setup of CAaaS in the Cloud Basic flow: "A new cloud CA needs to be set up by the PKI Administrator. The administrator will access the cloud service provider through the respective certificate authority portal or via the key management service. Via this portal, a new cloud CA will be generated whereas the CA type will be set to root CA. With this, the administrator has chosen to have the root certificate stored on the cloud-HSM of the CSP. After this, the administrator is capable of generating subordinate/intermediate certificates which in turn can generate X.509 certificates to be used for services / applications."

Use case 2: Initial setup of CAaaS in the Cloud with bring your own encryption Basic flow: "A new cloud CA needs to be set up by the PKI Administrator. The administrator will access the cloud service provider through the respective certificate authority portal or via the key management service. Via this portal, a new cloud CA will be generated whereas the CA type will be set to subordinate CA. This subordinate certificate will have a generated key pair and CSR in the cloud whereas the CSR will be signed by an on-premise root CA. With this, the administrator has chosen to work with the bring your own encryption principle and thus staying in control of the root certificate by not storing the corresponding private key within the cloud CA. The key of this certificate can now remain offline. After this, the administrator is capable of generating X.509 certificates with the subordinate certificate which in turn can be used for services / applications."

Use case 3: Moving a private CA (on-prem) to cloud CA Basic flow: "An existing private CA is to be transformed into a cloud CA. The PKI administrator will generate a new cloud CA within the respective cloud service provider certificate authority portal or key management service. While following the generation steps, the administrator will export the keypair of the existing on-premise root certificate whereas the key pair will be imported into the certificate authority portal or key management service and will continue to operate as a cloud CA. This can be seen as the bring your own key or root principle. After this, all existing X.509 certificates are exported from the private CA and imported into the newly generated cloud CA. The root certificate will be stored on the cloud-HSM of the CSP and thus losing the fact that this certificate can be stored offline. This entails moving your trust from internal to external. The administrator is now capable of generating X.509 certificates with the root certificate or any newly generated subordinate/intermediate certificates."

Use case 4: Moving a private CA (on-prem) to cloud CA with bring your own encryption Basic flow: "An existing private CA is to be transformed into a cloud CA. The PKI administrator will generate a new cloud CA within the respective cloud service provider certificate authority portal or key management service. The administrator has decided to stay in control of the root certificate, with the bring your own encryption principle. Because of this, the administrator will generate a new subordinate certificate within the cloud platform, this will ensure a new key pair online including a CSR which is then signed by the on-premise root certificate. Only the subordinate certificate and the public part of the root certificate will be stored in the cloud CA, capable of generating X.509 certificates, while keeping the root certificate offline. After this, all existing X.509 certificates are exported from the private CA and imported into the newly generated cloud CA. The administrator is now capable of generating X.509 certificates with the subordinate certificates while still being able to validate any imported."

Use case 5: High-volume deployments (e.g. DevOps, IoT, Blockchain) Basic flow: "With the increase of Internet of Things devices and the trends in DevOps and Blockchain, the amount of certificates has significantly risen. Because of this automation within the public key infrastructure is wanted to keep up with the amount of short lived certificates. The system administration team is lacking overall PKI experience and in turn incorporates the use of a cloud CA within their environment where APIs from cloud service providers can be called to retrieve, generate and recovate certificates within a much faster timespan. This is possible because there is no upkeep of soft- and hardware of the certificate authority itself and merely is used for the high amount of needed certificates."

Use case 6: Offline environment while using private certificates issued by a cloud CA Basic flow: "A system administrator wishes to use a cloud CA while his entire environment operates offline due to an increased level of risk. In-house PKI experience on building and maintaining a private CA is missing and company policies define the need of outsourcing as many services as possible. Within the environment an air gapped key management service will be set up (e.g. Vault or Venafi TPP) which is isolated with the help of firewalls and one directional traffic. Because of this, the KMS will be capable of obtaining/generating certificates and retrieving the certificate revocation list via the cloud CA as they will be pushed under supervision of the system administration to ensure an offline environment. With this, the environment is capable of using private certificates issued by the cloud CA certificates while remaining almost fully offline."

C COMPLETE SERVICE COMPARISON

The CA solutions of the each provider has been compared on the basis of the below criteria. The research team made a textual description of what the different providers offer for each criteria. This comparison was a preliminary study for answering sub-question 2, which concerns the different (cloud) service providers.

Cloud CA: When looking at the cloud service providers who currently offer a CA service in the cloud, you will find Amazon Web Services (ACM Private CA) and Google Cloud (Certificate Authority

Service). A third, officially not a CSP but a software cybersecurity company, is Venafi (Cloud Private Certificate Authority). All three providers claim to deliver a highly available cloud CA, whereas AWS and Venafi have released programs including pricing but GC is currently in a beta program without pricing. With their CA service in the cloud, clients will be capable of renting a 'blackbox' environment in which they can send queries via different paths to issue, request, revoke and delete their private certificates. With this an entire private hierarchy can be set up in which there is one root CA and several subordinate / intermediate CAs all for internal use of an environment but all hosted in the cloud. As of writing Microsoft Azure does not have a CA Service in the Cloud nor a CA as a Service (e.g. a private CA managed externally in the form as SaaS) yet. Azure made a comparison in which they state to offer a somewhat similar service where Azure Key Vault can be implemented which can set up a partner subscription with an external CA (i.e. DigiCert or Globalsign) in which customers can request and revoke certificates. In essence, Microsoft Azure is offering a Key Management Service versus an actual CA Service in the Cloud of the other providers. Naturally all cloud service providers give the option to deploy a Windows Server including the Active Directory Certificate Services installed. This can be seen as a private CA hosted on a cloud computing platform, which makes it IaaS, or with an MSSP/CSP in between, making it SaaS. This might be the reason why Microsoft has not released a dedicated cloud CA service.

Cloud-KMS: All providers offer a cloud KMS in which customers can create, manage and store certificates. When looking at key management services that come together with a CA Service such as with Amazon (AWS KMS), Google (Cloud Key Management) and Venafi (Cloud), then it is only used for storage and management. As soon as a KMS receives a certificate from the CA, it is sent to the cloud-HSM and stores it securely. For the management part, the KMS is responsible for the life cycle of a certificate. Azure has Key Vault as their KMS and is also responsible for requesting certificates from an external CA (i.e. DigiCert or Globalsign), it has this extra responsibility because Azure does not have its own cloud CA. The requested certificates are managed by the KMS and stored in a dedicated HSM.

Cloud-HSM: Each Cloud Service Provider is providing a Cloud-HSM service to store encryptions. AWS has CloudHSM, Google Cloud has Cloud HSM and Microsoft Azure has Dedicated HSM. Amazon and Google automatically offer their HSM service as soon as a customer decides to use their respective CA Service in the Cloud. Encryption keys generated or imported will be stored within this service. Azure does the same when a customer decides to use their Key Vault service, which is a KMS and not a CA Service. Venafi is the odd one out here which does not exactly share how their cloud CA stores encryption keys. They themselves promote Thales as a Cloud-HSM service which gives the assumption that they outsource this service entirely. This part can be cleared up with a hands-on review of the environment. Each of them are working with a FIPS 140-2 Level 3 processing standard, which seems to be the way to go within the Cloud-HSM service world. None of the providers seem to go below, or higher, with their standards.

Bring your own encryption: With the feature to bring your own encryption, the provider allows you to use your own root CA that is stored outside the provider's cloud. From this root, you can further expand the hierarchy in the cloud using subordinate / intermediate CAs. Both Amazon Web Services and Google Cloud provide this feature for their CA Service in the Cloud. This differs from the bring your own root / key model as they do not allow external root certificates to be imported. Microsoft Azure supports both features for their KMS when storing private certificates while not supporting this feature in case of an external CA. Venafi does not have the option of bringing your own encryption or key. At Venafi, a built-in root CA is created for each cloud service customer, along with an intermediate CA, from which the customer certificates can be issued.

Audit Logs: All cloud service providers have a different way of logging. Amazon uses CloudTrail, this captures API calls from the ACM Private CA console, from the CLI, or from your code, and delivers the log files to a S3 bucket. With the collected data it can be determined what kind of request has been made, but also from which IP address it came and many other parameters can be retrieved. Google Cloud uses Cloud Audit Logs for the Certificate Authority Service, which uses four different log types: Admin Activity, Data Access, System Event and Policy Denied. Azure uses Key Vault logging to record all operations on a Vault. With every action performed on a Vault, a JSON object is created that contains information about the operation such as date, type of operation, duration, IP address, identity, etc. Venafi only logs per account the certificate requests and logons, although only visible for the account logged in at that moment.

IAM: All cloud service providers have their own Identity Access Management (IAM) system in regards to their CA Cloud service. At Amazon Web Services, ACM private CA, IAM policies are used, where various policies can be set up so that a distinction can be made between administrators (create and configure CA) and user / developers (issue and revoke certificates). Google Cloud, like Amazon Web Services, works with IAM policies, which makes it possible for them to set up different policies. In addition, with Google Cloud IAM it is also possible to distinguish based on roles or groups. Microsoft Azure arranges access and identity at Key Vault in a different way than the other cloud services providers. The access to a key vault is handled using two interfaces, namely the management plane and the data plane. The data plane is especially important for the research because it is responsible for adding, deleting, and modifying keys, secrets, and certificates. The management plane is more focused on managing the Key Vault itself, such as creating and deleting Key Vaults, retrieving Key Vault properties, and updating access policies. As an access control mechanism, two different mechanisms can be chosen for the data plane. The first is Key Vault access policy where different policies can be set as with the other cloud services providers and the other way is Azure RBAC which looks at the role of the users. The second way is the only option that can be used as an access mechanism for the management plane.

Communication Methods: There are several ways to communicate with the Cloud CA solutions of all cloud service providers. Amazon Web Services, Google Cloud and Microsoft Azure all provide a cloud console, command line and API to communicate with the cloud CA. All three of these communication methods can achieve the same goals, namely the creation, management and issuing of instances (CA / Key Vault / Certificates). The only difference between the communication methods is the name that the cloud services providers have given the command line interface, namely AWS CLI (Amazon Web Services), gcloud (Google Cloud) and az keyvault (Microsoft Azure).

Queries per second: With queries / requests per seconds, the cloud service providers indicate how many certificates can be issued per second. Amazon Web Services indicate that they have increased the limit of requests from 5 to 25 requests per second. This was done to give better support for use cases that require a large number of certificates in a short period of time. Google Cloud also gives a clear indication of the queries that can be handled per second. They can also handle 25 queries per second, but mention that this can only be achieved in DevOps mode (vs Enterprise mode, unclear how many queries per second). Microsoft Azure itself does not have a cloud CA, so the speed of queries per second depends on the partner subscription between an external CA such as DigiCert or GlobalSign. Venafi indicates to their cloud CA that it complies with a high-speed certificate issuance. However, they do not mention which speeds can be achieved per second.

Cross-signing: When migrating from on-premise or IaaS to a CA Service in the Cloud, it is interesting to review if it is possible to cross-sign intermediate certificates so that you can bring your own encryption / root while ensuring multiple validation paths for active certificates. This will ease the migration so to say that old and new certificates are valid on-premise and in the cloud and to not lose any existing compatibility. A third party vendor, Hashicorp, claims that for their Consul application it is not possible to cross-sign other CAs when using the Cloud CA services of Amazon Web Services. Although during hands-on reviewing it seemed as though Amazon Web Services and Google Cloud offer cross-signing for root and subordinate certificates. Venafi does not support this. As Microsoft Azure does not offer a Cloud CA, this feature is dependent on an external CA or an internal private CA.

Certificate Revocation List: Both Amazon Web Services and Google Cloud include the option of hosting a certificate revocation list within their cloud platform when using their CA service, though Google Cloud only offers it with their Enterprise (vs DevOps) tier certificates. Amazon Web services will utilize a S3 bucket to store it in while Google Cloud offers the customer a Cloud Storage Bucket to store their certificate revocation list in. With the help of these two storage methods, the cloud CA is capable of keeping track of active and revoked certificates to ensure a valid environment. Since Microsoft Azure's Key Vault is dependent on external CA's, they do not offer a certificate revocation list option themselves and differ to using the CRL's pushed by the external CA. Venafi is solely in control of the CRL and does not offer this option to the user.

Certificate Properties: When comparing, this is one of the few criteria that aligns quite well. The providers with a Cloud CA service, Amazon Web Services and Google Cloud, offer the same in terms of strictness around the subject name, the expiration date and encryption keys. Only Amazon Web Services strife past Google Cloud in terms of utilizing certificate templates, as they do offer it when using their API or CLI. Venafi does work with issuing templates perse but only to limit what sort of certificates can be issued. So it does not enforce faster issuing but if a specific project is only allowed to utilize a specific component of in the key pair, such as the country code. Amazon Web Services and Google Cloud offer the feature to generate the CSR and private key for a customer whereas with Venafi a customer always has to supply an own CSR when requesting a certificate. Microsoft Azure is dependent on external CAs, which according to the CA/B forum require CAs to not issue certificates with a lifetime that exceeds 13 months. This can be seen as a limitation within internal environments.

D DIAGRAMS

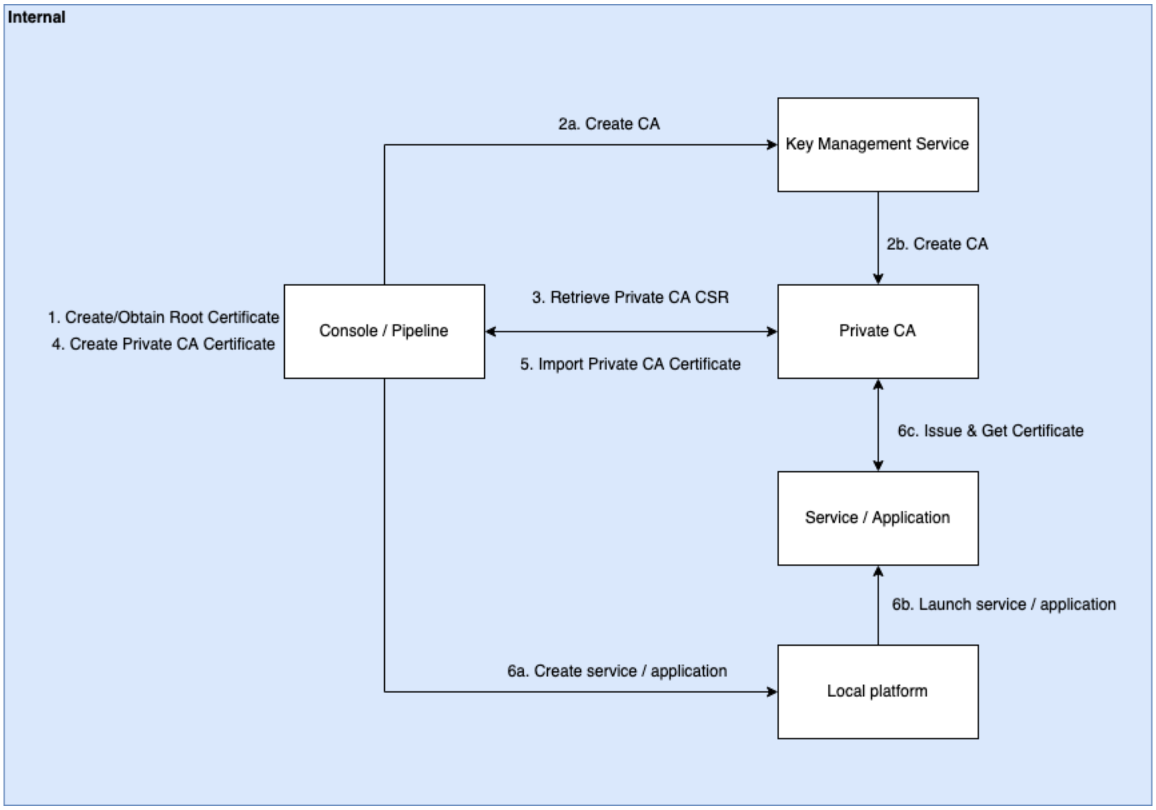

Internal
2a. Create CA
Key Management Service
2b. Create CA
1. Create/Obtain Root Certificate
4. Create Private CA Certificate
Console / Pipeline
3. Retrieve Private CA CSR
5. Import Private CA Certificate
Private CA
6c. Issue & Get Certificate
Service / Application
6b. Launch service / application
6a. Create service / application
Local platform

Figure 11: PKI on-premise

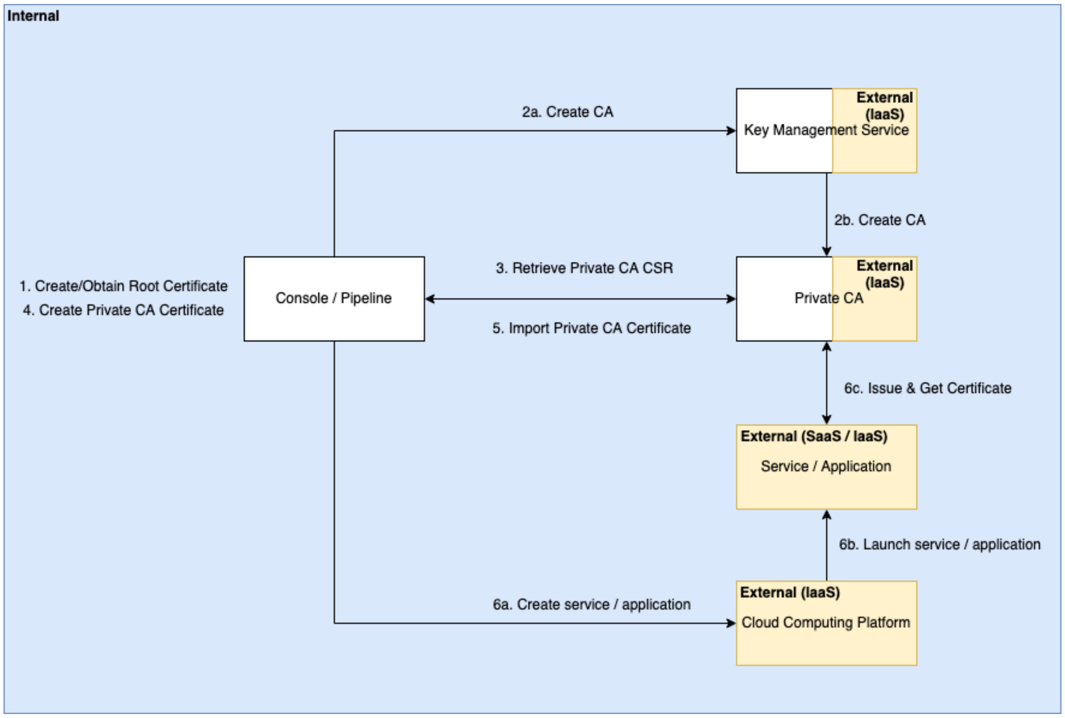

Internal
2a. Create CA
Key Management Service
External (IaaS)
2b. Create CA
1. Create/Obtain Root Certificate
4. Create Private CA Certificate
Console / Pipeline
3. Retrieve Private CA CSR
5. Import Private CA Certificate
Private CA
External (IaaS)
6c. Issue & Get Certificate
External (SaaS / IaaS)
Service / Application
6b. Launch service / application
6a. Create service / application
External (IaaS)
Cloud Computing Platform

Figure 12: PKI with Infrastructure as a Service

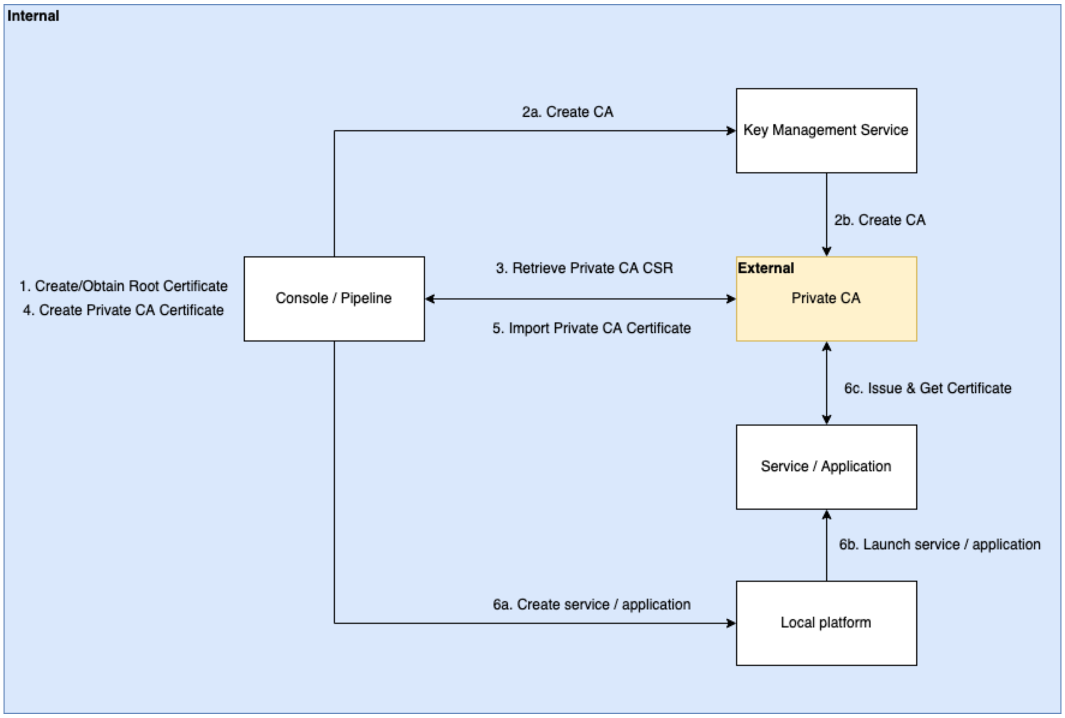

Internal
2a. Create CA
Key Management Service
2b. Create CA
1. Create/Obtain Root Certificate
4. Create Private CA Certificate
Console / Pipeline
3. Retrieve Private CA CSR
5. Import Private CA Certificate
External
Private CA
6c. Issue & Get Certificate
Service / Application
6b. Launch service / application
6a. Create service / application
Local platform

Figure 13: PKI with CA as a Service

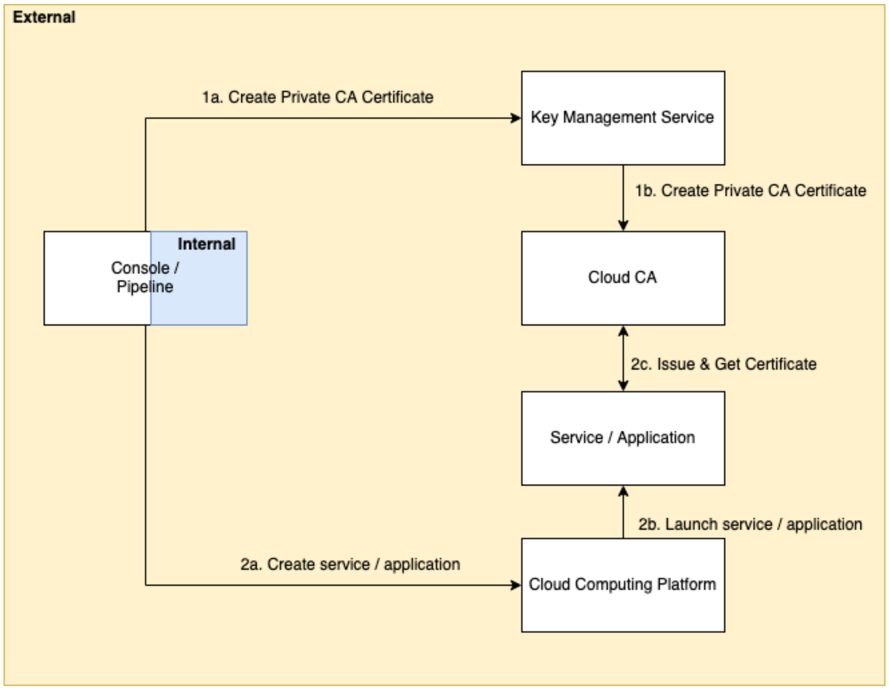

External
1a. Create Private CA Certificate
Key Management Service
1b. Create Private CA Certificate
Internal
Console / Pipeline
Cloud CA
2c. Issue & Get Certificate
Service / Application
2b. Launch service / application
2a. Create service / application
Cloud Computing Platform

Figure 14: PKI with CA as a Service in the Cloud

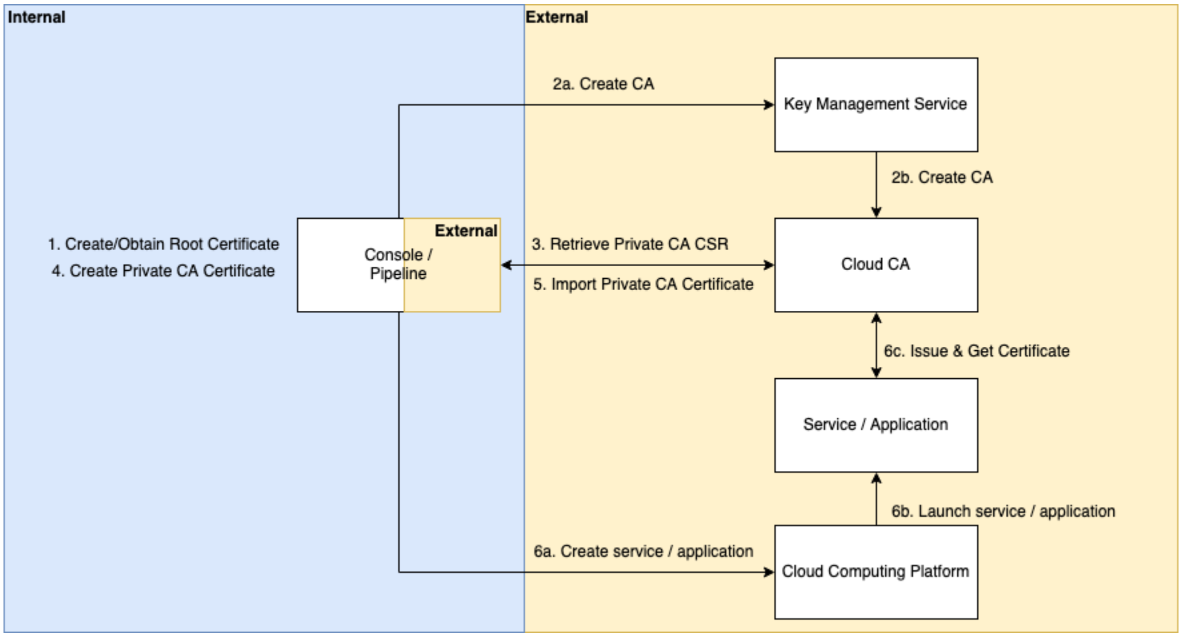

Internal
External
2a. Create CA
Key Management Service
2b. Create CA
1. Create/Obtain Root Certificate
4. Create Private CA Certificate
External
Console / Pipeline
3. Retrieve Private CA CSR
5. Import Private CA Certificate
Cloud CA
6c. Issue & Get Certificate
Service / Application
6b. Launch service / application
6a. Create service / application
Cloud Computing Platform

Figure 15: PKI with CA as a Service in the Cloud including bring your own encryption principle

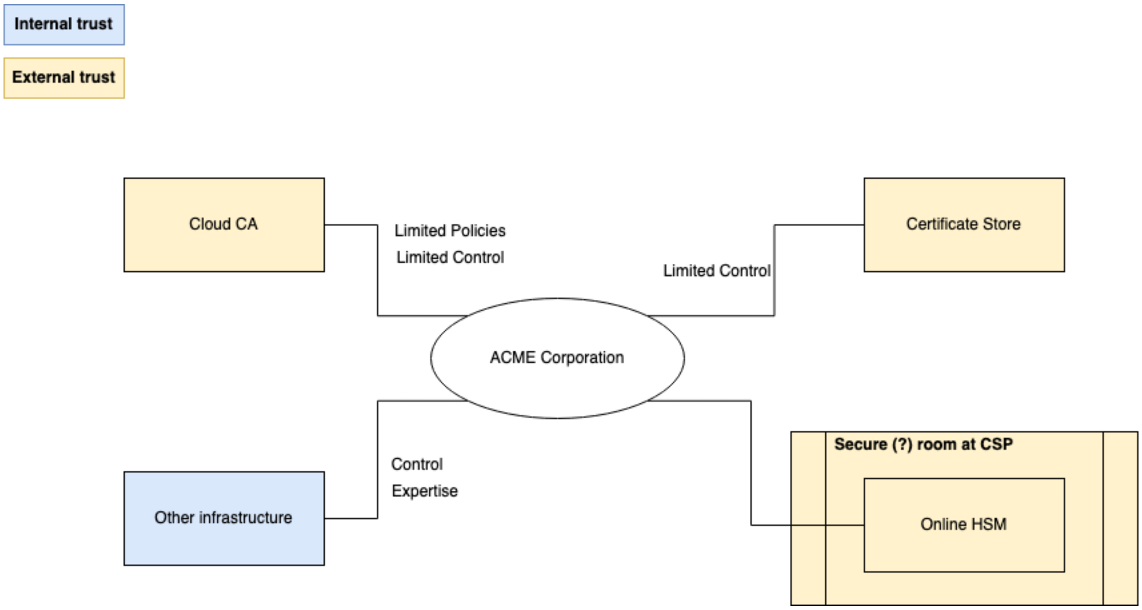


Figure 16: Organizational representation of a PKI on-premise

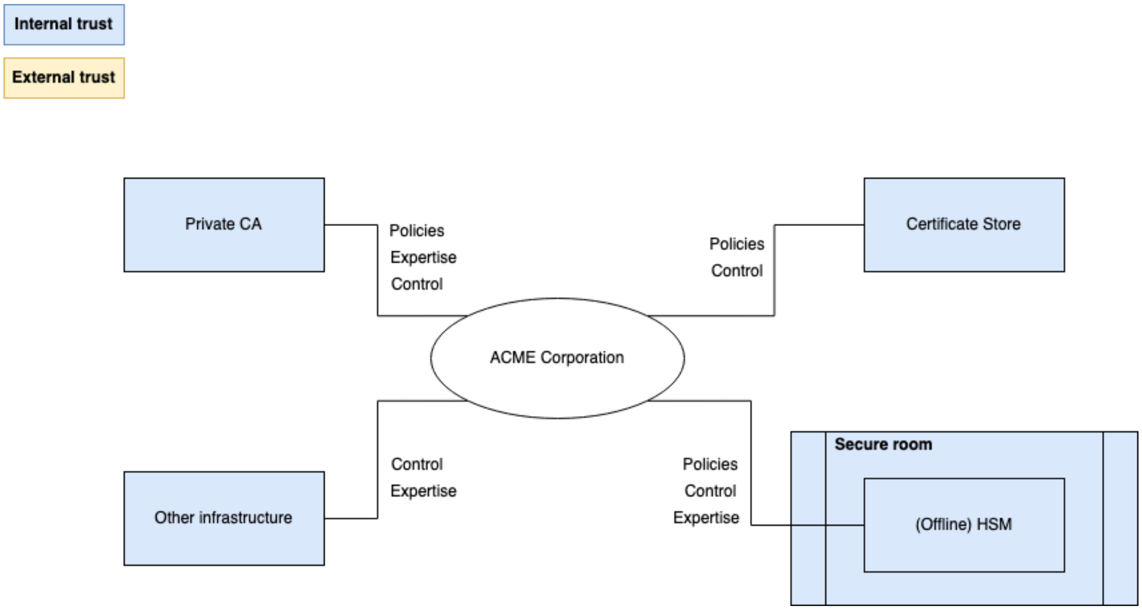


Figure 17: Organizational representation of a PKI in the Cloud