SPIKE REPLY is the specialist for IT security within the Reply Group. Spike Reply specializes in secure IT and the protection of personal data. Spike Reply has created a comprehensive, integrated and consistent offering to identify, minimize and maximize all aspects of the risk associated with an information system.
These range from the identification of threats and weak points to the planning, design and implementation of the corresponding technological, legal, organizational, underwriting and risk-limiting countermeasures.
Spike Reply provides vendor-independent security services through a broad network of partnerships. Spike Reply can therefore provide in-depth knowledge of the most widely used security technologies on the the most appropriate technology.

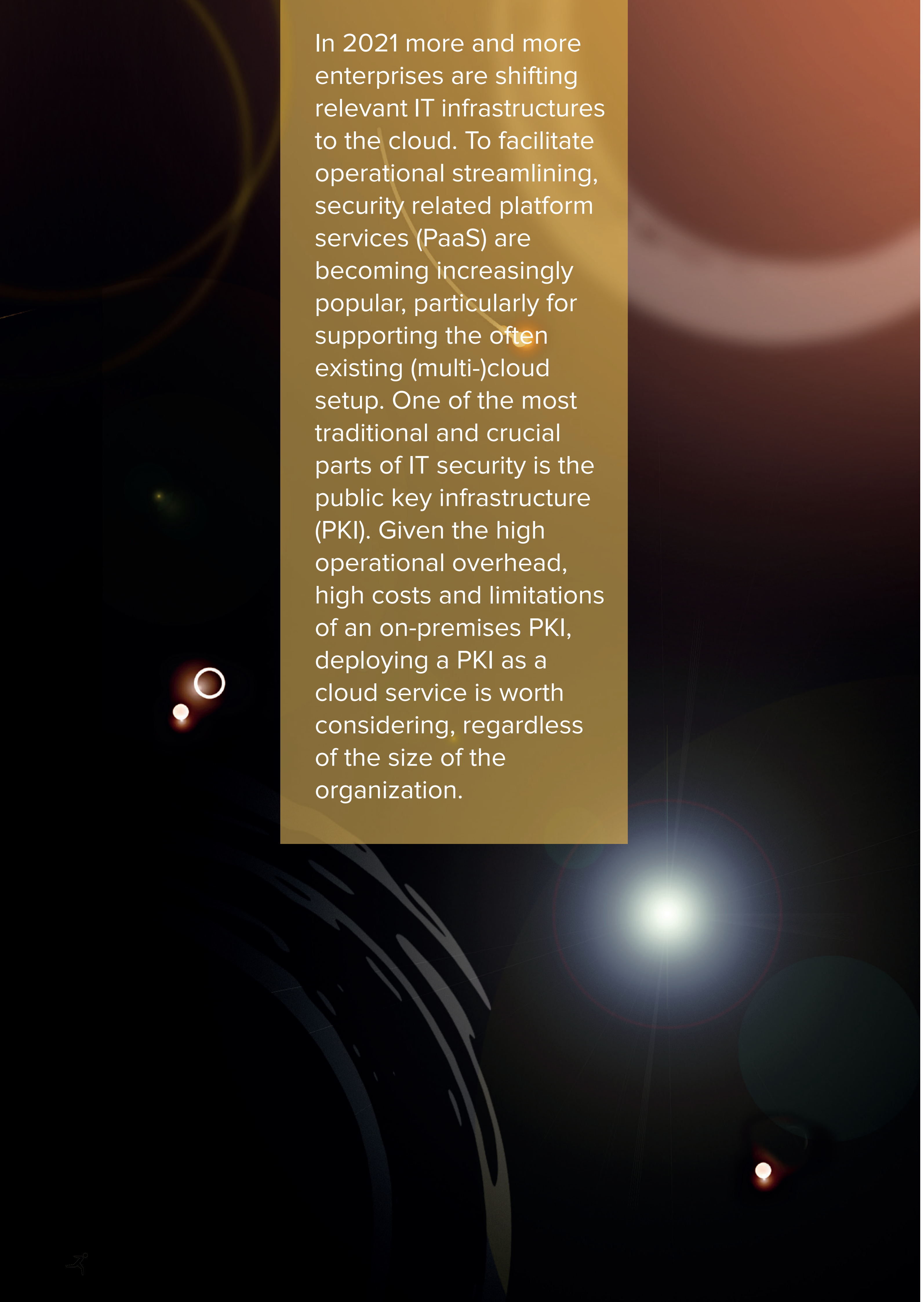
www.reply.com

REPLY
SPIKE

PUBLIC KEY INFRASTRUCTURE (PKI)

PKI GOES CLOUD

Spike Reply outlines the advantages and disadvantages of a cloud-based Public Key Infrastucture.



In 2021 more and more enterprises are shifting relevant IT infrastructures to the cloud. To facilitate operational streamlining, security related platform services (PaaS) are becoming increasingly popular, particularly for supporting the often existing (multi-)cloud setup. One of the most traditional and crucial parts of IT security is the public key infrastructure (PKI). Given the high operational overhead, high costs and limitations of an on-premises PKI, deploying a PKI as a cloud service is worth considering, regardless of the size of the organization.

CONTENT

INTERNAL PKI GOES CLOUD

More and more enterprises are shifting relevant IT infrastructures to the cloud. Initially driven by the need for flexibility and security-by-design approaches, the number of cloud migration projects continues to increase. Likewise, to facilitate operational streamlining, security related platform services (PaaS) are becoming increasingly popular, as means to support the often existing (multi-) cloud setup.

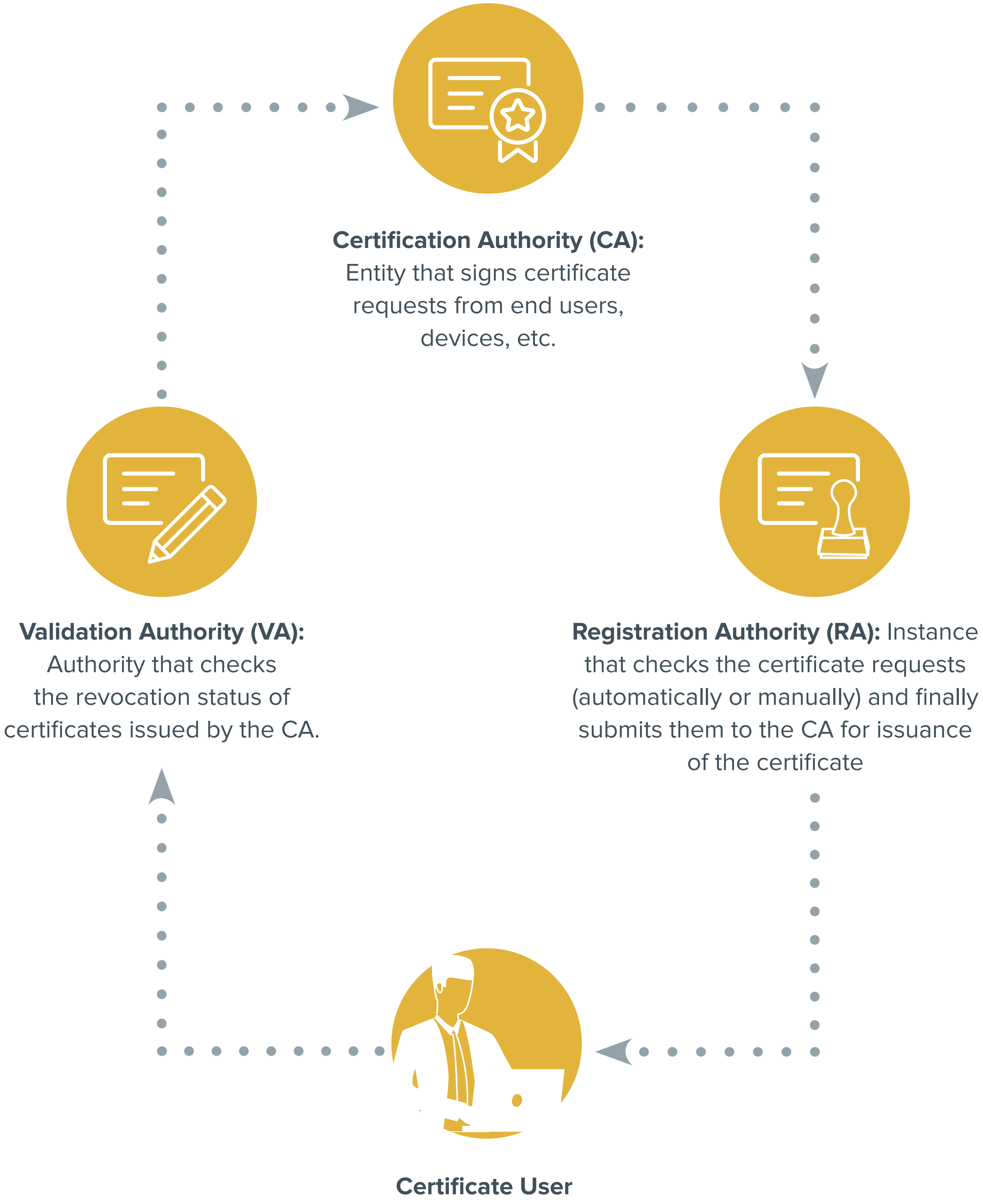
As a result, cloud providers are now offering services for internal PKI as PaaS services. These are services that represent a key security pillar of any enterprise structure. Given the high operational overhead, high costs and (intrinsic) limitations of an on-premises PKI, deploying a PKI as a cloud service is a considerable motivator for organizations, regardless of size.

Ensuring the very high availability of this central infrastructure component is typically a major challenge for companies. While such objectives still need to be taken into consideration when integrating a PKI into the wider enterprise architecture, the operation of the PKI service itself can be handed over to professionals at the cloud provider.

One enormous operational advantage of the PKI PaaS becomes visible in regard to key ceremonies. This is a procedure performed for generating the initial set of root keys inherited for the entire environment. In traditional setups this is usually documented and audited to ensure the confidence in the generated root keys. In the cloud, this process is simplified. With the Managend Service, the Certification Authorities can be created via the Console with a couple of clicks.

Despite the simplified key generating process in a cloud setup the cloud customer remains the owner of the keys, meaning that even in a cloud scenario, security managers do not have to transfer more trust to the cloud than necessary.

In the following, a cloud-based PKI service, the Amazon Web Services Certification Manager Private Certification Authority (ACM PCA), is presented and compared with traditional deployments.

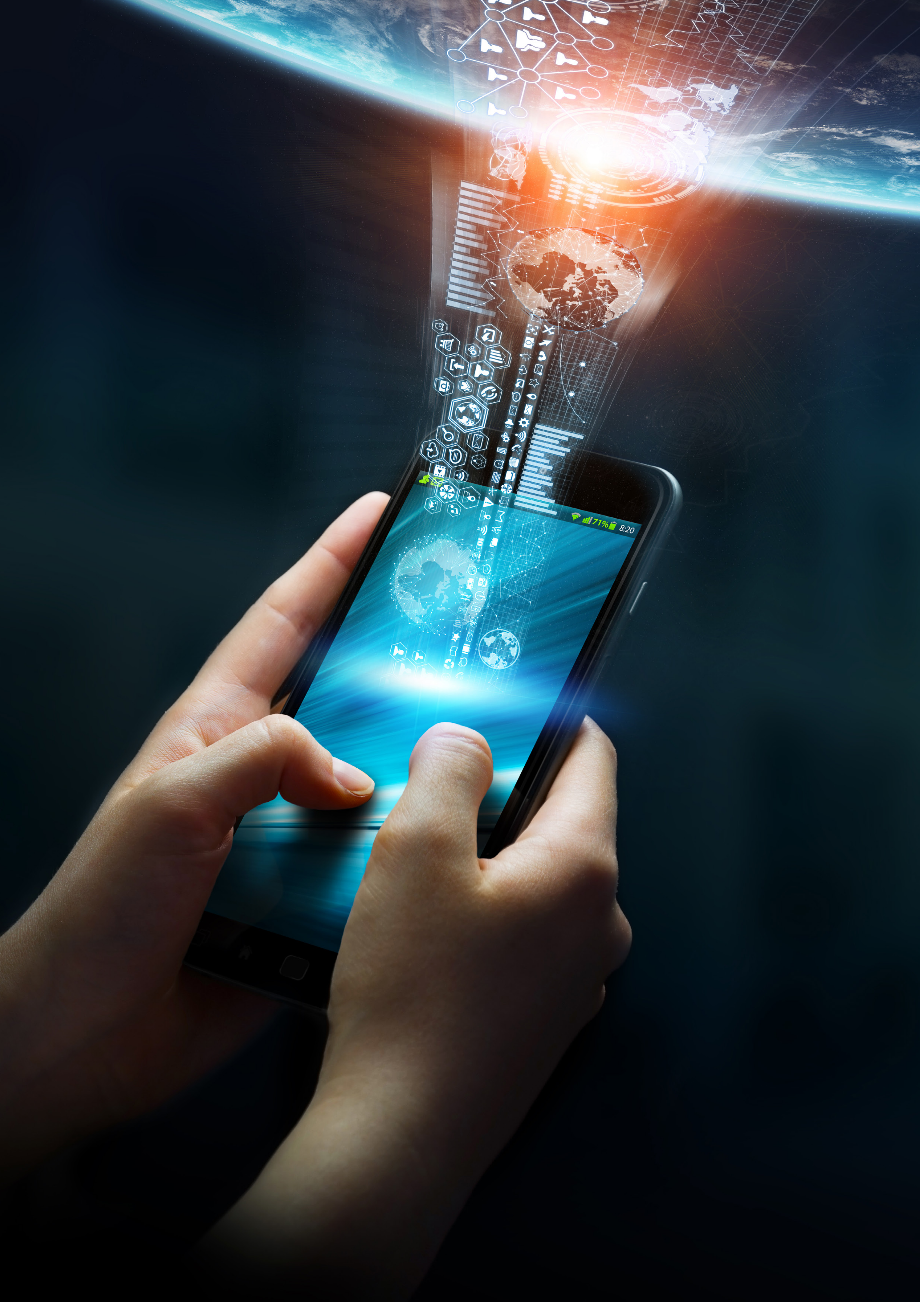


Certification Authority (CA): Entity that signs certificate requests from end users, devices, etc.

Registration Authority (RA): Instance that checks the certificate requests (automatically or manually) and finally submits them to the CA for issuance of the certificate

Certificate User

Validation Authority (VA): Authority that checks the revocation status of certificates issued by the CA.



CLASSIC PKI TASKS WITH THE AWS SERVICE ACM PCA

Before highlighting the main changes the Cloud PKI service brings, let's take a step back and look at the pillars of a PKI.

First, let's look at the Validation Authority. The VA service is crucial in day-to-day operations. This usually means providing a Certificate Revocation List (CRL) and/or providing an OCSP responder, both to verify the status of a single certificate issued by the CA.

The AWS ACM PCA service offers automatic integration for Validation Authority. CRLs are automatically distributed to buckets – all as part of the service and fully automated. An OCSP integration is currently not available, but there are solutions to solve this with serverless Lambda functions to provide OCSP state in addition to the CRL list.

RA is noot active available with AWS. ACM PCA offers no functionality in this direction. This is not particularly surprising, since the design of RA is often very specific and sometimes adapted to the company processes by different software. It is to be expected that some cloud native implementations will appear in the near future (e.g. through AWS Lambda functions). In the end, the core business of ACM PCA is Certification Authority as a Service (CAaaS), meaning its main task is certificate creation. For this task the native cloud version is way superior than traditional on-premises or Infrastructure-as-a-Service implementations.

ADVANTAGES AND DISADVANTAGES OF A CLOUD PKI COMPARED TO TRADITIONAL DEPLOYMENTS

Public Key Infrastructures have long been used as anchors of corporate infrastructures ensuring trust. Established technologies, procedures and have proven themselves and should therefore serve as a reference for a comparison with a cloud-based PKI.
The following section will compare both approaches.

1) Regions and availability:
The availability of a CA, especially the validation authority services, are crucial for enterprise environments. Ensuring this is a significant problem in on-premises environments and the best argument to think about a cloud-based PKI.
The selected region defines where the used services will be deployed. On-premises environments are bound to the location of their data center and offer little flexibility here.Cloud provider like AWS allow to deploy the service in several regions. The regional bound Certificate Authority service offers high availability, which is ensured by the cloud providers via contractual agreements. As the service relies on hardware security modules (HSM) in the backend, it is not possible to move a running PKI to another region. However, it is possible to set up a multi-region architecture across the different PKI tiers to ensure cross-regional availability.

2) Multi-tier architecture: going beyond
It is quite easy to map a multi-tier architecture in the cloud, orchestrated in a console. Of course, multi-tier architec-tures can also be built in traditional deployments, but this significantly increases the operational effort.
Following the cloud approach, tiers from the root CA for example can be used by other sources. This can be on-premises resources or resources that are located in a different region or maintained by a different account or provider. This does not only apply to the Root CA, but also to all of the potential subordinate CAs. Therefore, it is possible to create architectures that combine the advantages of the different services and spread the risk.

3) Certificate templates:
Certificate Templates are used to introduce attributes when signing certificates by the CA. It is used as a container of parameters and variables the CA uses to sign a certificate. These include information like Extended Key Usage – but also information about Client Authentication, Server Authentication, Secure Mail, Code Signing, Time Stamping etc. Additional key length restrictions, signing algorithms and validation endpoints can also be defined in the template. Depending on the CA Software which is used for the PKI, the on-premises or IaaS implementation may offer the full range of features. Considering the widely used Microsoft AD Certificate Service, there is a fully configurable CA template profile for all of the use cases mentioned, which is hard to meet current PKI in the market. But having the complete set of features is not the focus point of PaaS. It is having a robust, low effort and easy deployable service which is suitable for most use cases.
In ACM PCA users can choose between the following templates: Code Signing, End Entity, Client Auth, Server Auth and templates for PKI infrastructure certificates. The template will use a predefined set of certificate attributes like Key Usage or Extended Key Usage and will sign the submitted certificate signing request (CSR) accordingly. All of these are error resistant and suitable for most use cases.
One highlight available for each template is called Passthrough templates. Simply put, this option would sign attributes that were defined during the certificate request without any additional control by the CA and will be included in the certificate. This offers increased. However, there is a risk using this (optional) template.
Another point to highlight is that every API which signs a CSR will need an attribute to define the validity of the certificate. Given the various integration options, especially if there is no registration authority available, it is difficult to control which validity period of the certificate is applied when it is issued.

4) Automation: useful for a PKI?
Automation is a field where typically API based cloud services outperform on-premises environments. Automation at this point is limited to the provisioning of the infrastructure and the operating processes. Unlike rapidly changing application types, a PKI is typically subject to very few changes. However, it still makes sense to represent the infrastructure with infrastructure as code in order to know the clear status of an environment at all times (e.g. accountability, auditability etc.) and to verifiably prevent authorizations for personal users for many aspects. This then leads to the question of authentication in general.

5) Authentication: each request is critical
Since a PKI is all about trust, the authorization is crucial. There are several principles that should be observed when operating one.
First, the principle of least privilege should apply. The user interacting with the PKI should therefore have only the rights that are absolutely necessary.
Second, with minimal rights, there are multiple roles for different purposes (e.g., issue certificate, CA administration, audit). These tasks need to be separated. Additionally, these tasks should be performed using the 4-eyes-principle.
Finally, a multifactor authentication should be used by people with proper rights interacting with the PKI to raise the integrity level for the request.

6) Monitoring and Auditability
Taking a closer look at the topic of monitoring, it quickly becomes clear that cloud services have a clear advantage. All interaction with the respective API can be logged, and aggregated and evaluated by common methods of the cloud provider. This is a major simplification compared to traditional PKIs. This also applies explicitly to the accountability of log traces. All ACM PCA API calls are captured by Cloudtrail. The ACM PCA service also provides audit reports on demand or on schedule to provide information about the certificates issued.

7) Certificate Management
The ability to integrate the PKI into the corporate infrastructure depends on several factors. Starting with the validation service, it must be ensured that the status of the issued certificates can be retrieved at any time. It is therefore a question of the availability and accessibility of the various clients. Cloud services can be used to build up a robust service in line with the company's infrastructure.
What about the issuing service itself? As already illustrated, the certificate templates are comparatively limited with respect to on-premises CAs and corresponding software. However, these are geared towards most use cases and can be used for many common use cases. Flexible application possibilities are gradually being added,
Automation can be another reason for using a cloud-based PKI. Still, many things need to be taken into account in the design. Since there is currently no out-of-the-box registrar functionality for the services, measures must be taken to ensure residual issuance. This is particularly relevant for direct integrations into DevOps processes. This does not necessarily mean that separate software is required in every case, but an appropriate solution should be found for a risk-based analysis approach.

8) Price models
Finally, it must be considered whether operating a cloud-based PKI solves the challenges of maintaining and operating a highly available internal PKI but is also worth considering from a commercial perspective. AWS has a uniform pricing model for all CA types. In addition to the cost per certificate, each CA charges a monthly fee.

CONCLUSION

There are many reasons to operate a PKI in the cloud. The main driver is, as expected, the need for operational stability and low-effort operation of the PKI. Also, topics such as automation and basic monitoring of API calls are available in cloud deployments can't offer thus enable enormous advantages over the years of on-prem practice.

But the key question remains: Can we trust a PKI in the cloud? This question currently poses a barrier for a lot of security managers. Spike Reply can answer it in good conscience: Yes, a PKI in the cloud can be trusted. There are many reasons to trust the professional, audited, certified and also standardized approaches of the cloud providers.

However, good IT security always means minimising risks. At this point, it is worth considering the various options from a risk-based point of view and to weigh each of them against the advantages.

Spike Reply developed a PaaS-internal PKI service which is superior to on-premises PKI in terms of operational efficiency, cost-savings and flexibility.

The solution is a state-of-the-art, future-proof PKI for the IT security setup of tomorrow: supporting multicloud scenarios, API based architectures, microservices and much more. Furthermore, the solution is tested and proven, currently being operated on a handful of Best-Practice-Enterprises.