Cloud Certificate Authorities

The security considerations of moving your Public Key Infrastructure to the cloud

Research Presentation - Commissioned by Deloitte (Itan Barmes, Colin Schappin)

Anand Groenewegen
University of Amsterdam
agroenewegen@os3.nl

Maurits Maas
University of Amsterdam
mmaas@os3.nl

1 February - 2021

Introduction

- A survey held by Statista on IT Outsourcing informs that respondents are outsourcing components of their overall infrastructure because it will provide them access to skills not available in-house. ComputerWeekly describes that IT leaders experience difficulties 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.

- Research Questions
  - **RQ: How does the adoption of a Cloud Certificate Authority (CCA) benefit/impact an organization?**
  - SQ1: How does a CCA differ from the classical CA/on-premise and IaaS implementation?
  - SQ2: How does the current landscape impact user experience in terms of a CCA?
  - SQ3: How does a transition from an on-premise CA to a CCA impact the organizational considerations?

Context

- Private CA
  - On-premise or IaaS found Certificate Authority managed by an organization or service provider
- Cloud CA
  - Cloud Certificate Authority fully managed by a (cloud) service provider (CSP)
- Bring your own encryption
  - Feature for organizations to use their own encryption software and manage their own encryption keys. CSPs allow organizations to optionally import their own key pairs.
- Hardware Security Module
  - Hosts encryption keys and performs cryptographic operations
- Certificate Revocation List
  - Ability to manage and keep track of revoked certificates

Background and Related Work

- No academic research was found on the subject Cloud Certificate Authorities. The goal of this paper is to inform readers on how a cloud CA service impacts the stature of an organization.

- Tech websites reporting on the subject
  - The Register: Google catches up to AWS and steals a march on Azure with introduction of cloudy Certificate Authority Service
  - SSL247: Choosing between On-premise PKI Vs. Cloud-based PKI
  - ComputerWeekly: Outsourcing PKI to the cloud: What enterprises need to know

- (Cloud) Service Providers publishing blog posts on the subject
  - Google Cloud: Introducing CAS: Securing applications with private CAs and certificates
  - Amazon Web Services: AWS Certificate Manager Private Certificate Authority
  - Venafi: Venafi Cloud Private Certificate Authority

Methodology

- Preliminary Research
  - Initial consensus on subject, gathering of related work
- Scope Defining
  - Terminology, diagrams and use cases
- Literature Research
  - Reviewing online available articles and published articles
- Hands-on Reviewing
  - Validation of literature research on selected cloud platforms
- Write-up
  - Formulating findings, results and transforming these into a paper

Data Gathering and Experiments

- Processing Literature..
  - Google Scholar, IEEE, ResearchGate and UvA's database
  - Terms: "Certificate Authority as a Service", "Cloud Certificate Authority", "PKI as a Service" and more specifically related to the X-as a Service and/or Cloud CA

- Platform Reviewing..
  - Ability to host a Cloud CA
  - Ability to create, manage and re-deploy a CA
  - Ability to make use of the 'Bring your own encryption' principle
  - Ability to host and manage a certificate revocation list

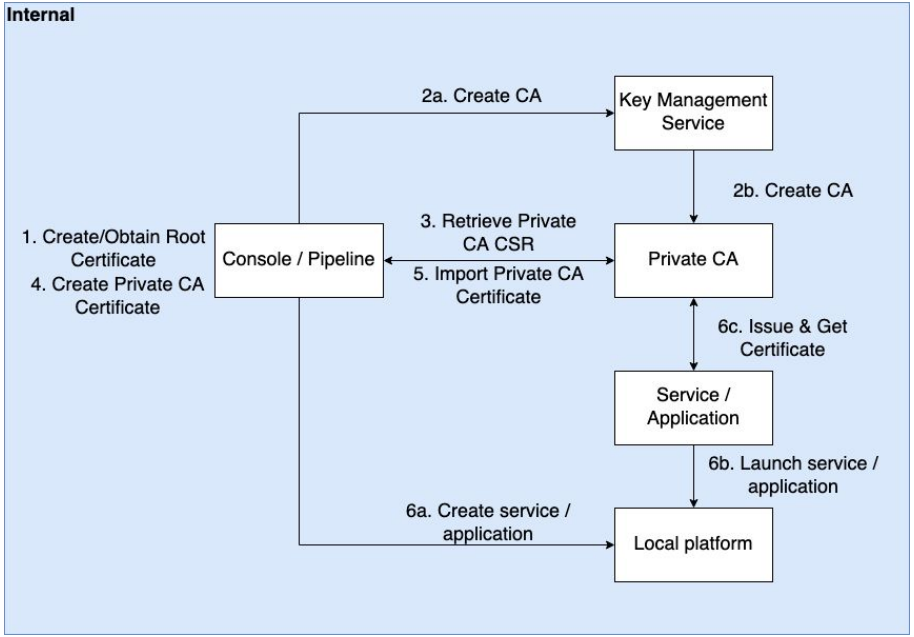
Results: Infrastructure Models

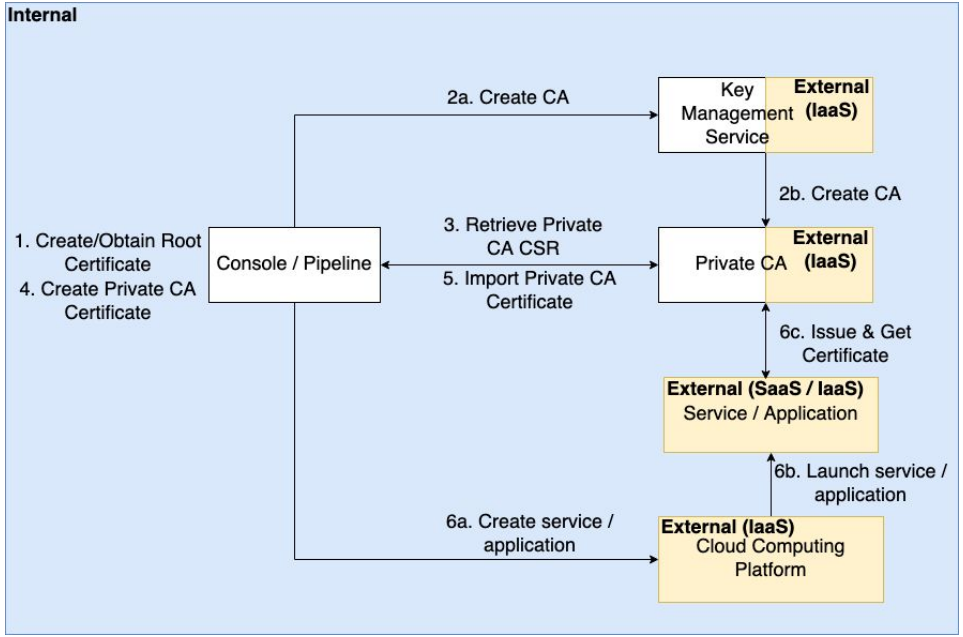
- SQ1: How does a CCA differ from the classical CA/on-premise and IaaS implementation?
  - Fictional Company used for exploration
  - Diagrams

- Shifting occurs between..
  - Online versus Offline
  - Internal trust versus External trust
- Increase or decrease seen in..
  - In-house expertise
  - Cost management

- Example..
  - Private CA transforms into a Cloud CA

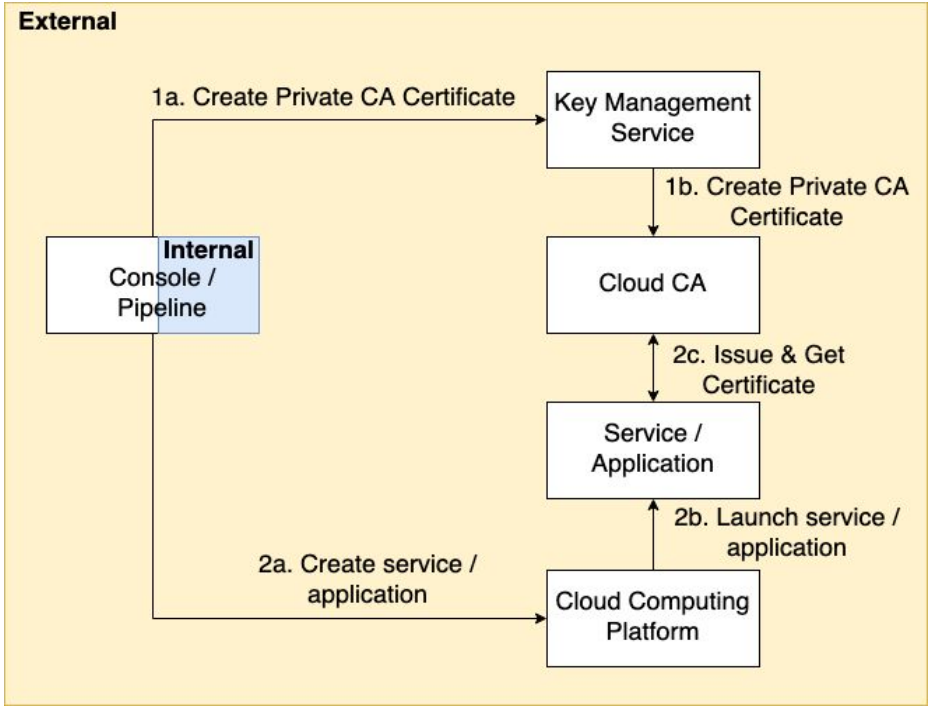
On-Premise and IaaS

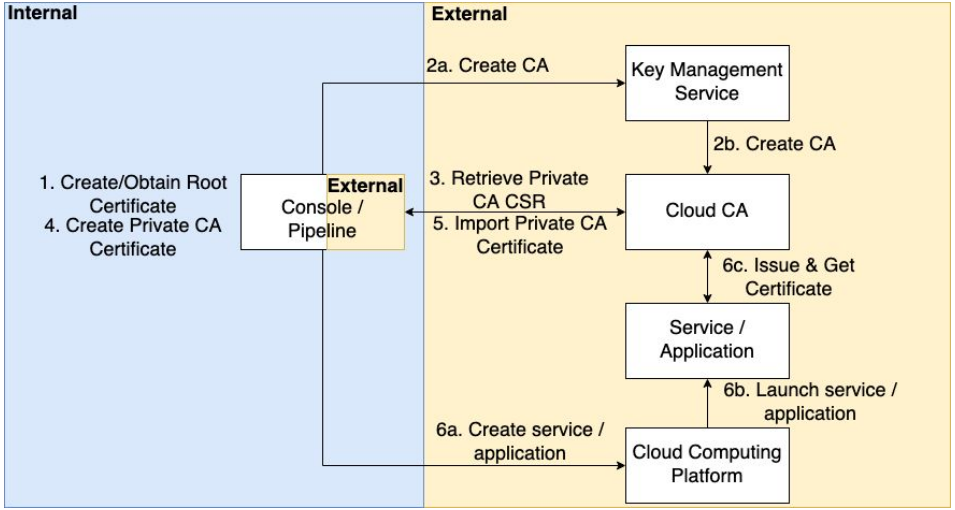




Initial draft of diagrams based on “Setting up a Private Certificate Authority on AWS” written by Frederik Willaert

Certificate Authority Service in the Cloud





*Bring your own encryption principle

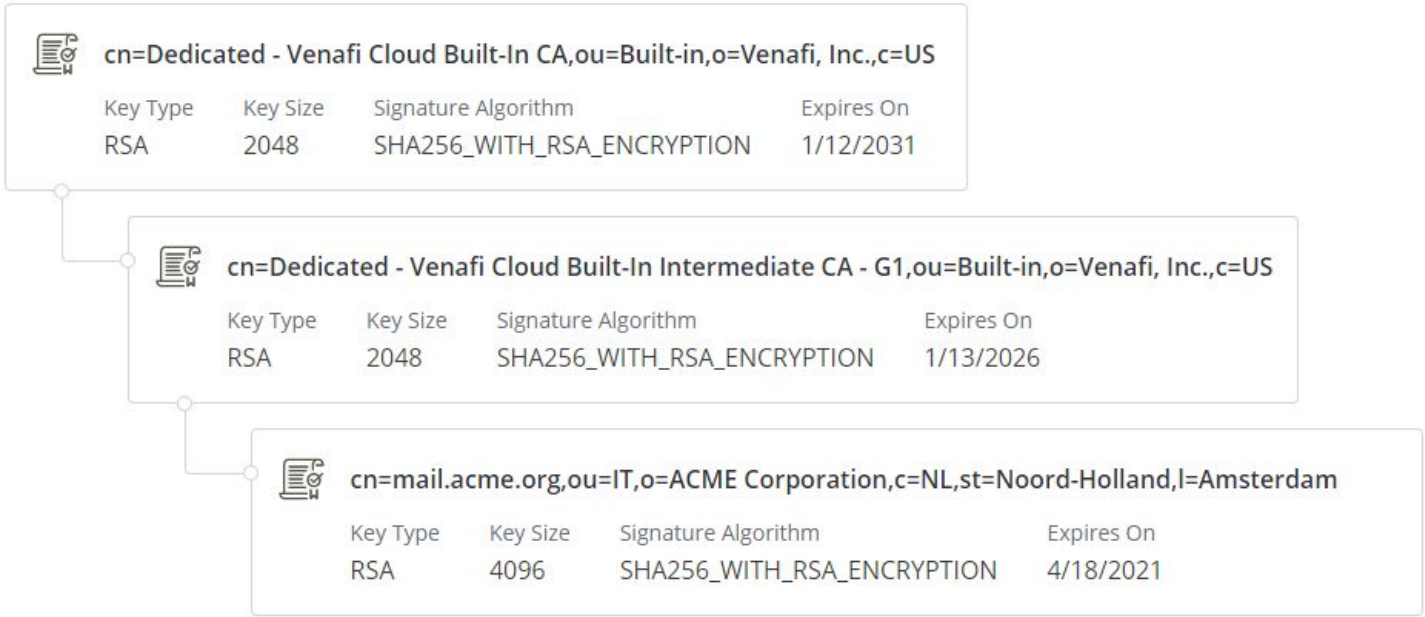
Results: (Cloud) Service Providers

- SQ2: How does the current landscape impact user experience in terms of a CCA?
  - Service comparison based on public available documentation
  - Hands-on Platform Reviewing

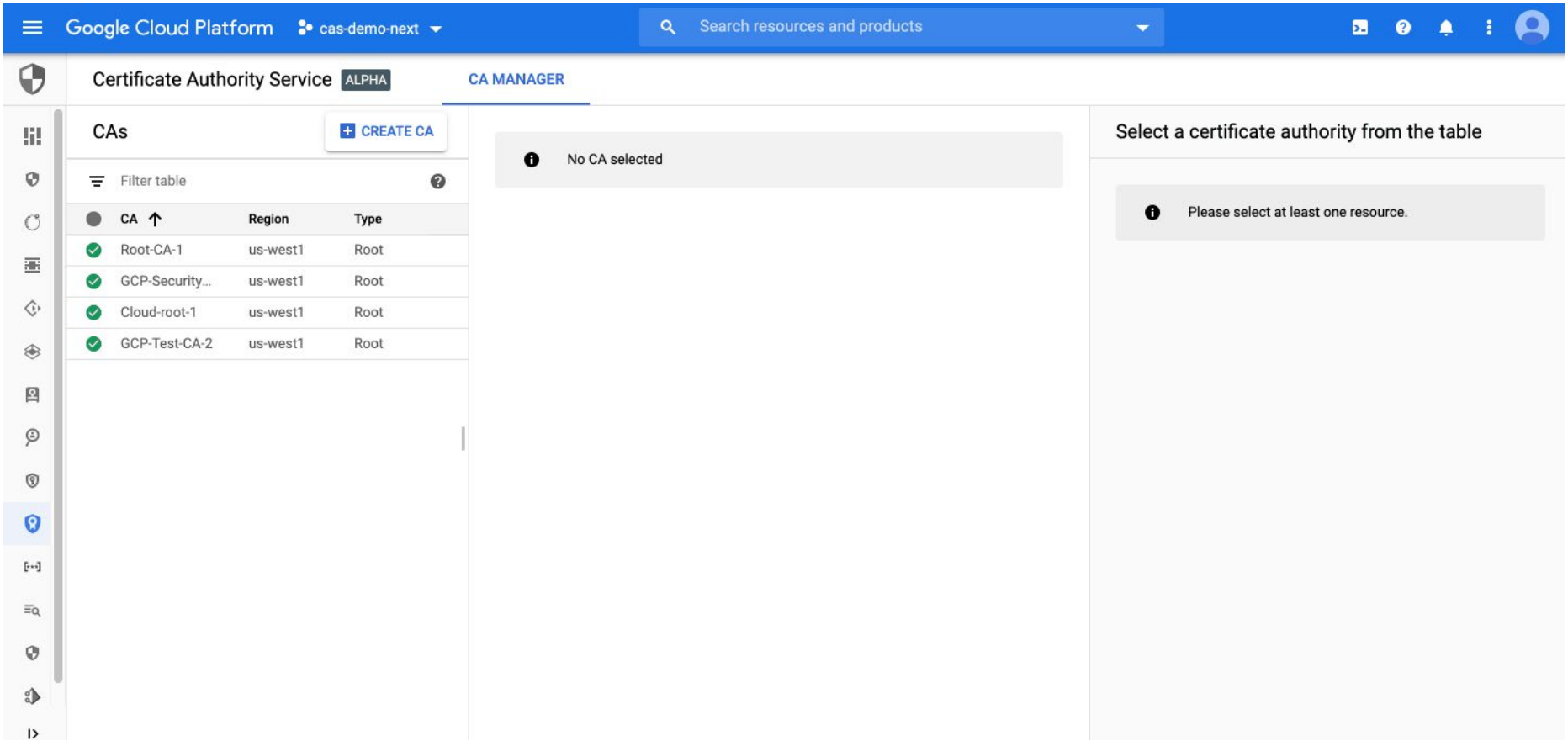
- Amazon Web Services
  - ACM Private CA
- Google Cloud
  - Certificate Authority Service
- Microsoft Azure
  - none, but sort of Key Vault
- Venafi
  - Cloud Private CA

	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

Auto generated root CA and sub CA at Venafi

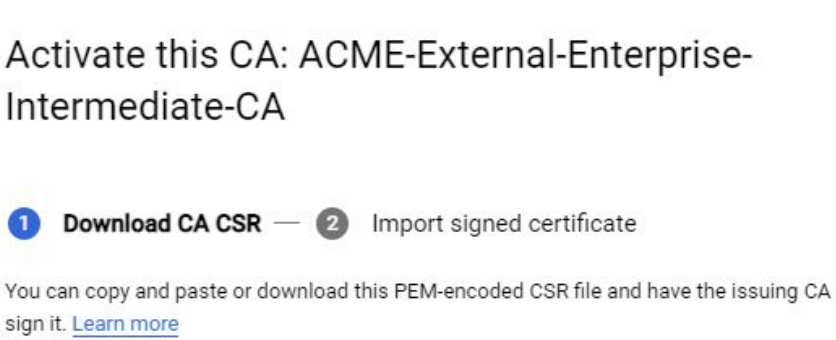


Setting up a Cloud CA…



Source is “Introducing CAS: Securing applications with private CAs and certificates” by Google Cloud

Bring your own encryption principle at Google Cloud



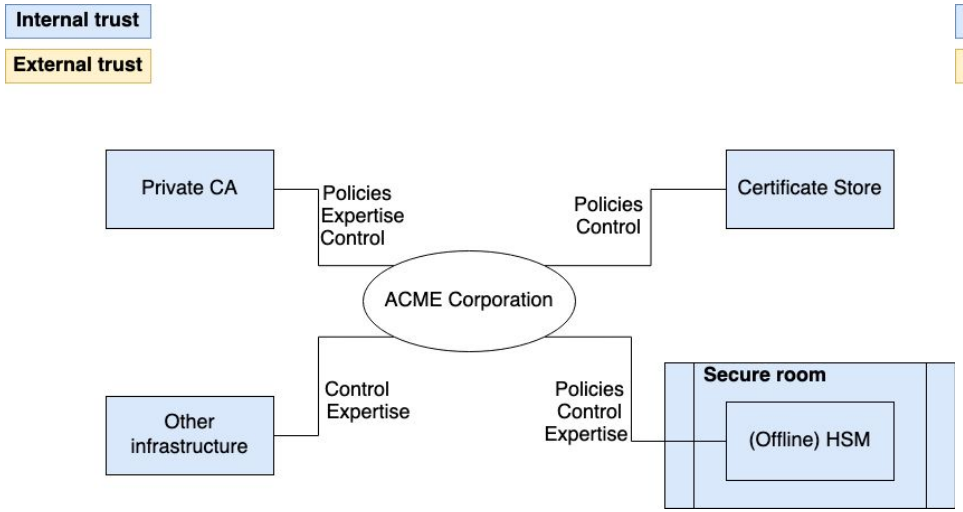
Results: Transition towards Cloud

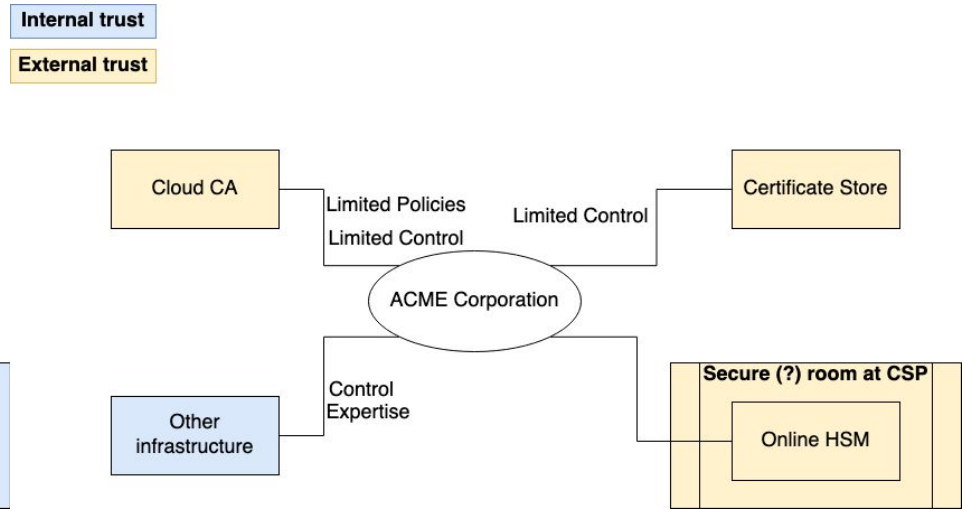
- SQ3: How does a transition from an on-premise CA to a CCA impact the organizational considerations?
  - Use Cases for exploration
  - Diagrams

- Shifting occurs at..
  - Defining policies
  - Managing risks
- Increase or decrease seen in..
  - Control of PKI

- Example..
  - Hardware Security Module

On-premise versus Cloud





Conclusion

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

- Technical
    - Online versus Offline
    - Internal trust versus External trust
    - In-house expertise
    - Cost management
- Organizational
    - Defining policies
    - Managing risks
    - Control of PKI

- 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.

Discussion

The research team acknowledges limitations of the paper and discusses them with..

- Related Work Validity
  - Multiple databases were exhausted, there is a possibility that related papers were overlooked. The fact that no previous research was found guided the way on how the related work section is currently formed.
- Conclusion Validity
  - Guided by existing and newly found knowledge via specific methodology
- Internal and External Validity
  - Peer reviewing of the document by internal and external security experts

Future Work

- Microsoft Azure Key Vault
- Physical and juridical changes
- Offline environment with a Cloud CA

Summary

- We've researched..
  - .. the changes within a company when transitioning to a Cloud CA service
  - .. what (cloud) service providers currently offer in terms of a Cloud CA service
  - .. the set of impact and benefits when using a Cloud CA Service
- We've concluded..
  - .. that technical and organizational changes occur after transitioning in regards to shifting control, risks and policies
  - .. Amazon Web Services and Google Cloud are offering a full fledged Cloud CA service whereas Venafi is trying to compete in their own way
  - .. that each shift in control, risk and policy when moving to a Cloud CA service organizational specific is, whereas it can be said that a benefit for company A can be a risk for company B