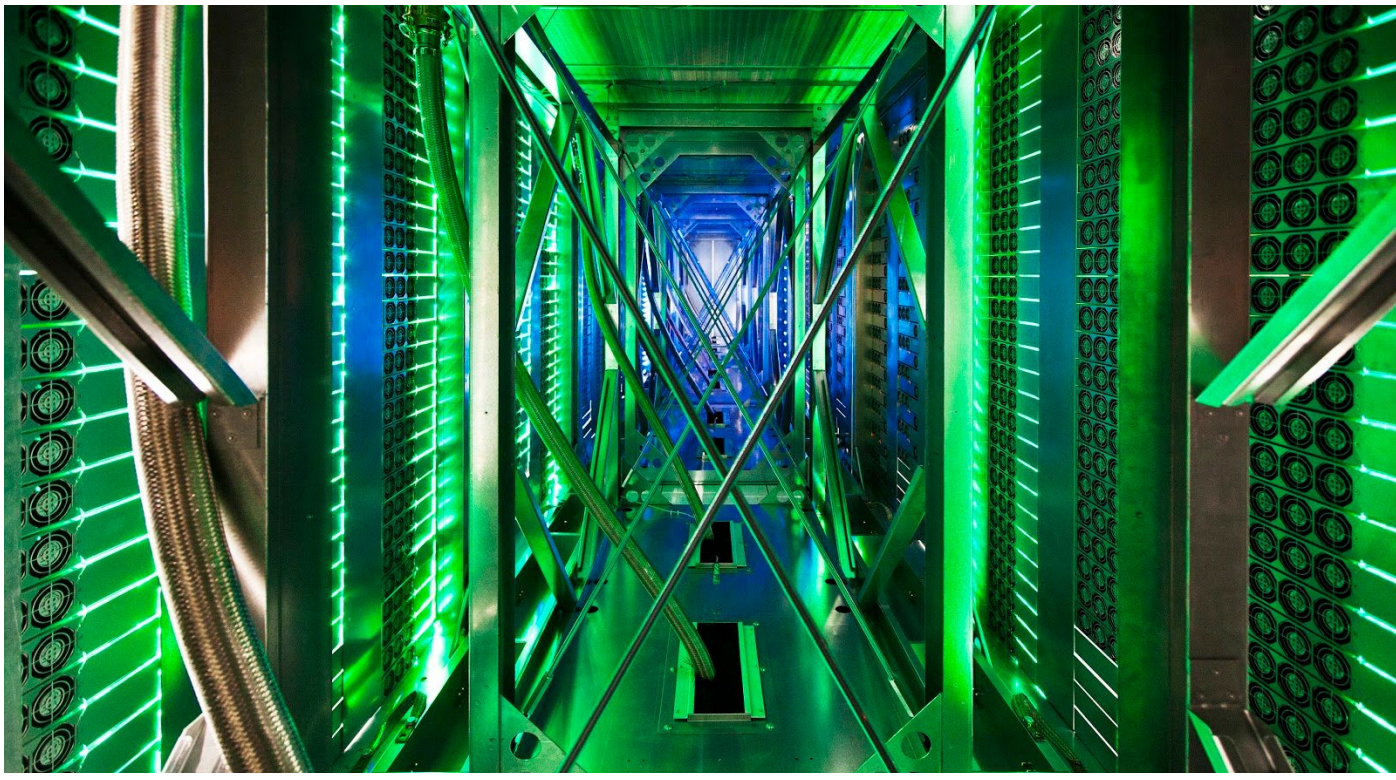
Google Cloud

Google Cloud Whitepaper
February 2021

Scaling certificate management with Google Certificate Authority Service



Authors:
Andrew Lance, Founder & Principal, Sidechain
Dr. Anton Chuvakin, Head of Security Solutions Strategy, Google Cloud
Anoosh Saboori, Product Manager, Google Cloud

Google Cloud

Google Cloud

Table of Contents

Certificates in a cloud-ready world **4**

New demands require a new approach **7**

Global scalability 7

Cloud-native, cloud-ready 8

Strong resilience and reliability 9

Support multi-cloud use cases 9

Logging and auditability 10

Key use cases **11**

Certificates in a DevOps world 11

Certificates for Internet-of-things hyperscale 12

Modernizing traditional IT 13

A new CA for a new world **13**

DISCLAIMER: This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Google Cloud

Certificates in a cloud-ready world

The digital world is experiencing unprecedented growth and interconnectivity due to a perfect storm of conditions over the past few years. Achieving almost a flywheel effect, the advent of many technological innovations - the rise of cloud computing, the emergence of 5G, the proliferation of Internet-of-things (IoT) smart devices - has created immense market opportunities for digital products that interconnect our lives and workplaces. At the center of this explosion of connected devices and software-defined-everything is the ability for these interconnected devices to verify their *identity* with each other.

Digital identity, a critical part of any system infrastructure, is how systems prove they are who they claim to be. Humans use things like usernames and passwords to *authenticate* to the services we use day-to-day. When a computer needs to interact with another computer, usernames and passwords have been used, but there's a more secure way of proving identity that is vastly more common - digital certificates. These digital fingerprints are cryptographically secure, and enable devices to authenticate with each other in an increasingly automated world where systems talk with other systems, as part of a sometimes massive web of interconnected devices.

Imagine that a company manufactures a smart home thermostat that connects back to a cloud infrastructure to report various conditions and enable the device to be managed remotely. These devices each have a unique *certificate* embedded inside that is used when they connect to the cloud that ensures they are in fact the device they claim to be. If this company is manufacturing hundreds of thousands of devices *every month*, a lot of digital certificates need to be generated, and in an automated way that integrates with the build process.

With over 40 billion IoT devices in use by 2027, and at a rate that is increasing dramatically, the need for digital certificates that are securely generated, integrated, and managed for those devices is immense.

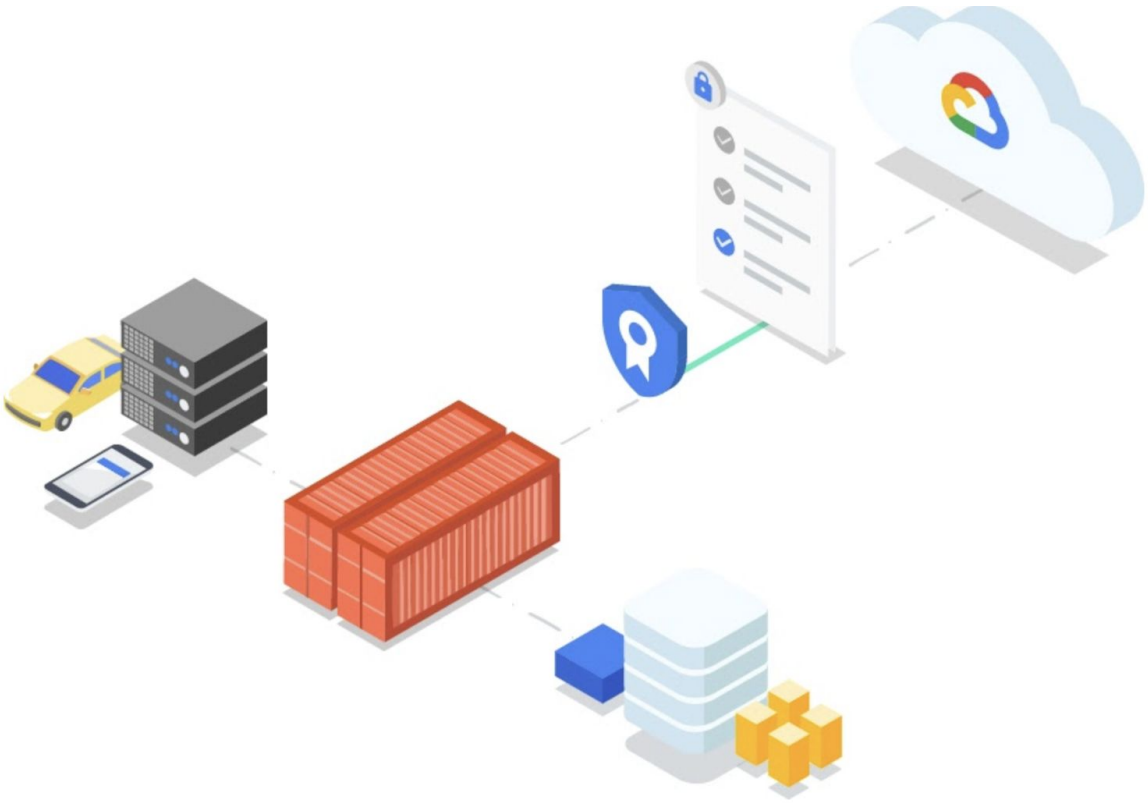
IoT devices are just the beginning though. As digital transformation grips every industry, the use of software, cloud, and integrated systems is becoming ubiquitous. Public cloud services like Google Cloud Platform (Google Cloud) have created a wholesale migration of on-premises infrastructure to the cloud for countless reasons, but agility and speed of deployment and time to market are commonly cited as primary drivers. All of these systems must also be digitally fingerprinted with certificates in order to maintain the security of interconnected systems. The hyperscale growth of digital infrastructures have expanded not only from the data center to the cloud, but have embraced sophisticated multi-cloud strategies, and hybrid strategies that seamlessly integrate clouds and on-premise workloads. Digital certificates underlie the system integrity of all of it, the scale of which has become frighteningly massive.

The sheer scale of digital identities provided by certificates is not the only complicating factor at play. As system architectures shift from monolithic long-living systems (most IT pro's can probably remember computers that ran for years, if not decades!) to microservices and auto-scaling systems, the mean time-to-live for these systems has decreased significantly. Applications are increasingly architected with containerized building blocks that are rapidly rebuilt and redeployed when changes are necessary, further decreasing the overall uptime of these systems. CI/CD pipelines auto-provision systems as part of their orchestration processes, spinning up virtual machines to perform various tasks along the way, then destroying them as those specialized tasks are completed, all of which need certificates provisioned even for their short existence to verify that rogue systems aren't introduced into the pipeline. For every one certificate a long-running legacy application may have needed, now dozens of certificates are required, even if temporarily, during the application lifecycle.

The digital world has changed - systems are built more rapidly than ever, integrated into large networks of other devices where identity and security are paramount. These networks exist globally, and require resilience and scalability. They are increasingly automated and cloud-native.

This is the new reality.

Google has introduced Certificate Authority Service (CAS) to address these, and many other, challenges organizations face as they use their digital certificates in a new age. CAS is not only a cloud-ready platform for hyperscaling certificate management, but is already aligned with the development methodologies of cloud-native applications, as well as fully API-enabled.



As we will see, a solution like Google Certificate Authority Service is absolutely necessary for organizations to meet their growing demands for digital certificate management.

Google Cloud

New demands require a new approach

Traditional certificate management systems - often referred to as Certificate Authorities (CA's) - are not equipped to handle these new demands. They are traditionally buried deep inside corporate networks, locked down with monolithic hardware devices (appropriately called *hardware security modules* or HSM's) which manage the critical foundational master signing keys from which all of the generated certificates are generated.

These systems, which often require specialized skill sets and dedicated staff to manage, are also guarded by gatekeepers and processes for how certificates are generated and distributed across an organization. It is very typical that certificate requests are manual, often requiring days if not weeks turnaround time. Legacy enterprise environments already contain an overwhelming amount of certificates to manage - easily hundreds of thousands — to secure things like SSL/TLS connections among the many, many thousands of machines that make up an enterprise infrastructure, email security, single-sign on technologies, and code signing.

New demands being placed on digital certificates and PKI systems are often at-odds with these traditional deployments.

Global scalability

The workforce for many organizations has continued to be distributed globally, and applications that at one time could remain safely running behind centralized corporate firewalls are no longer possible. These applications now must be available to employees across the globe. As the Covid-19 pandemic marches on, a record number of employees are connecting to corporate systems remotely using VPN (which themselves are provisioned with certificates) while the emerging zero trust remote access approaches also grow. This places demands on how CA's must be architected in order to reach the distribution requirements of the modern workplace.

Likewise, applications of all sorts have grown to global scale, often reaching across data centers, on-premise infrastructure, and public clouds to achieve the levels of operations necessary to support growing customer demands. IoT devices sold to consumers across the globe must all connect back centralized (but cloud-based) infrastructure, distributed regionally to minimize latency and reliability issues. The "connected car" is becoming ubiquitous across vehicle manufacturers, resulting in a fleet of millions of automobiles that must securely communicate to management applications. The adoption of 5G will undoubtedly result in countless new use cases where global distribution of connectivity becomes the norm. All of these use cases require CA's as the backbone of security.

Microservices are now scaling at a tremendous pace, requiring huge levels of automated certificate generation to keep up. In a large scale deployment, for example, an entire system may run over 100,000 nodes. Assuming that each node needs 10 different certs, renewed twice a day, results in a whopping 730M certificates generated per year! Such is the enormous scale of modern global applications.

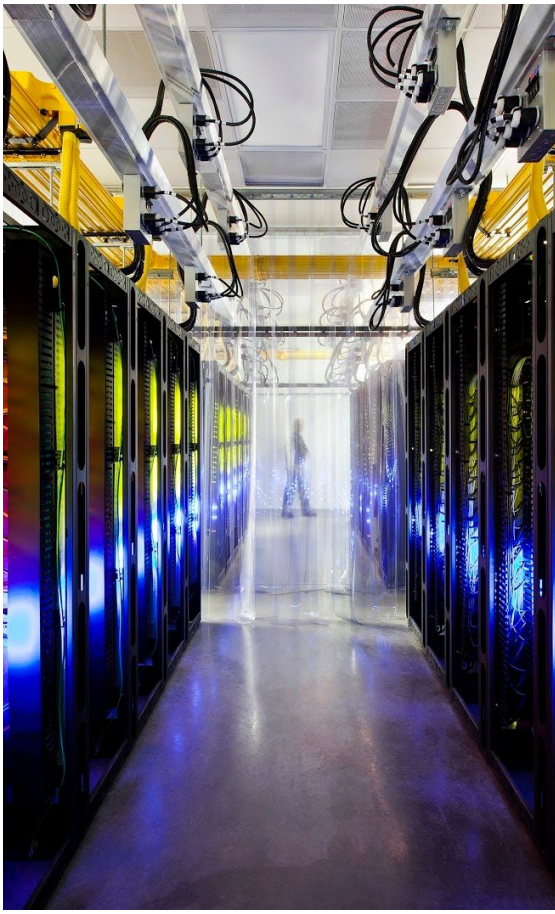
Traditional deployments of CA's are not suitable for these kinds of architectures at this kind of scale, but Certificate Authority Service is. CAS can be deployed globally, across the Google Cloud, ready for workloads wherever certificates are required. It also implements all of the guardrails and identity and access controls required for global scale.

Because traditional CA's are usually anchored to physical hardware devices for key management, they are difficult to scale without replicating that hardware in additional data centers. CAS is backed by Cloud KMS, so it's trivial to create keys that are stored in Cloud HSM in regions across the globe.

CAS also has the capability of issuing millions of certificates, all with an enterprise-grade service level agreement.

Cloud-native, cloud-ready

As more organizations are developing applications and technology infrastructure cloud-first, it simply doesn't make sense to keep tying back to on-premise infrastructure like certificate authorities. Because traditional certificate authorities and PKI are typically anchored in hardware security modules, they are (almost by definition) on-premise systems.



CAS, on the other hand, is natively integrated into Google Cloud and other services in the cloud. This means that certificate management operations are seamlessly integrated and automated, providing stronger security. Cloud-first applications using orchestrated development automation and CI/CD pipelines can avoid the overhead of manual certificate requests, which can often defeat the purpose of automation in the first place.

For example, as applications scale during peak usage times, and more systems are replicated to handle traffic, a service account constrained by Cloud Identity and Access Management controls can be authorized to make certificate request operations to CAS. This, of course, can be fully automated as part of the scale out process. In this way, every system that is provisioned can have certificates generated for them. As these systems are decommissioned, certificate revocation requests can take place to clean them up.

Certificate enrollment processes typically take hours or days to complete, and according to Venafi, 75% of DevOps professionals are concerned that policies for issuing certificates slow down the development process, and over a third (39%) believe developers should be able to circumvent these processes to main service-level agreements.

Integrating into orchestrated toolchains is a vital demand by organizations today, one fulfilled by a cloud-native CA like CAS.

Strong resilience and reliability

As systems continue to grow in complexity and interconnectivity, their demand for high resilience and reliability has increased dramatically. The reason is that with large, sophisticated interconnected systems, for example a cloud-based management service that operates a half-million field devices, a failure means a half-million devices stop working. For a large software-as-a-service platform that receives millions of requests per day, a system-wide failure means millions of failed requests.

In other words, failures are amplified. They are also incredibly difficult to troubleshoot. This is why organizations rely on cloud platforms like Google Cloud to deliver *reliability* - to work as designed and deliver incredible stability. Cloud-dependent organizations also demand *resilience* - the ability for the system to continue to withstand certain types of failures and still remain functional.

Resilience and reliability don't "just happen" - they are the result of smart cloud-first architecture that enables an application or system to leverage the high uptime and stability that cloud platforms like Google Cloud deliver.

Because digital certificates play a central role in the operations of most modern interconnected systems, they are notorious for causing system outages. An expired certificate can cause systems to reject connections, thinking they are untrusted, and when communications start failing, applications fail. These kinds of failures are usually the result of human error, a failure to find expiring certificates, or the inability to renew a certificate in an acceptable time before expiration.

No certificate authority can automatically fix these problems, but it does enable systems to use certificates in an automated manner, thus reducing manual steps prone to error.

Support multi-cloud use cases

Organizations are continuing to develop multi-cloud infrastructures to support a variety of use cases. They require best-of-breed toolsets and services found among the leading cloud providers, and are also distributing applications across cloud platforms. Traditional CA's don't support modern API's expected to ease integration across services. CAS is queryable through standardized RESTful interface calls, as well as convenient client libraries for Google Cloud. This enables distributed applications, even services in other platforms and private clouds, to easily integrate with CAS for certificate issuance.

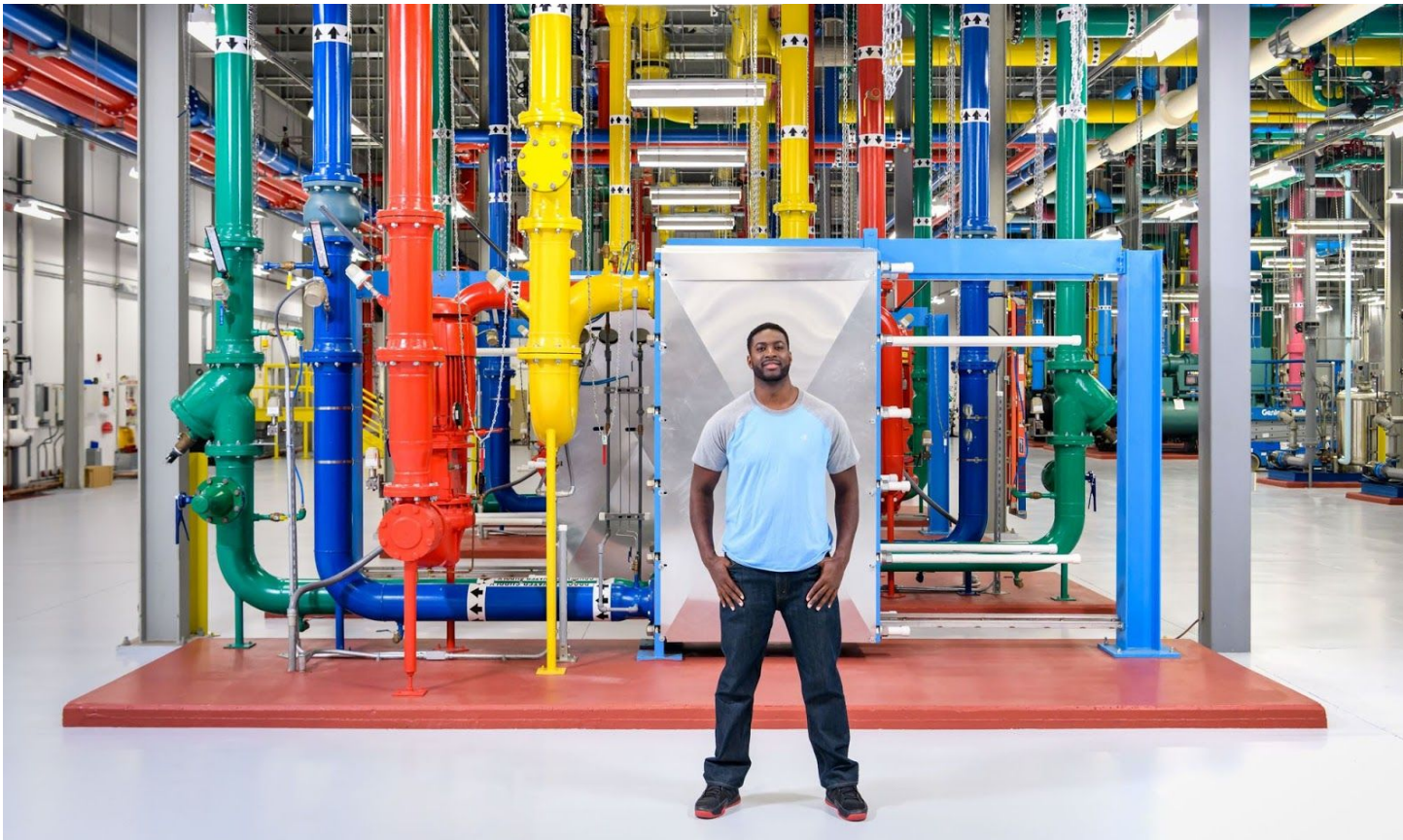
For example, a best practice is that every connection to, from, and within a container, and between applications that comprise a system, should use SSL/TLS to enable end-to-end encryption and mutual authentication. Since containerized applications may be deployed to run on a variety of endpoint platforms, certificates can be issued from a centralized cluster of CAS instances and then shipped to whatever destination environment is required.

Logging and auditability

A further demand by modernized applications and cloud-native infrastructure is *integrated logging* and visibility across services. Google Cloud equips customers with powerful visibility capabilities and services that provide insights not about systems in isolation, but within the context of their entire cloud environment.

As mentioned above, certificate-related errors that cause application downtime can be like trying to find a needle in a haystack, often being eclipsed by vast other system errors, or never showing up in the right logging aggregation systems in the first place.

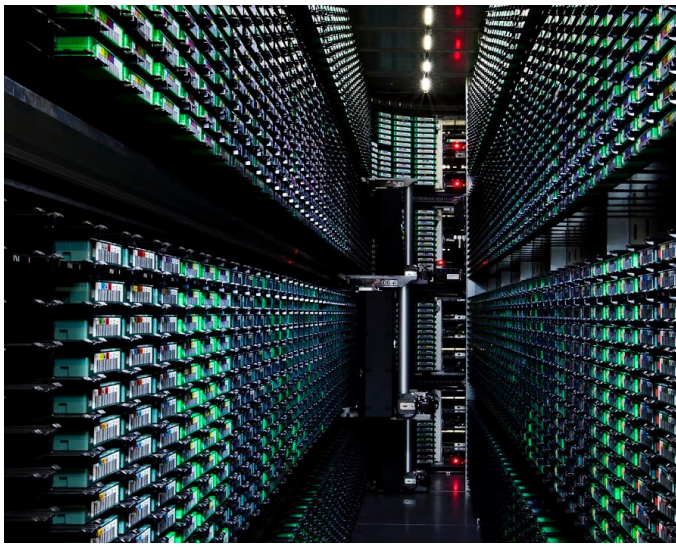
Since CAS is already integrated into the Google Cloud platform, logging is integrated as well, and can be processed using the native log analytics tools available within Google Cloud. This happens automatically as CAS instances are created, so there's never a risk that logging of a CA didn't get configured correctly.



Google Cloud

Key use cases

Certificates in a DevOps world



DevOps has become the new normal in terms of release cycles and application development paradigms, primarily because it has decreased time to market and increased agility for engineering teams.

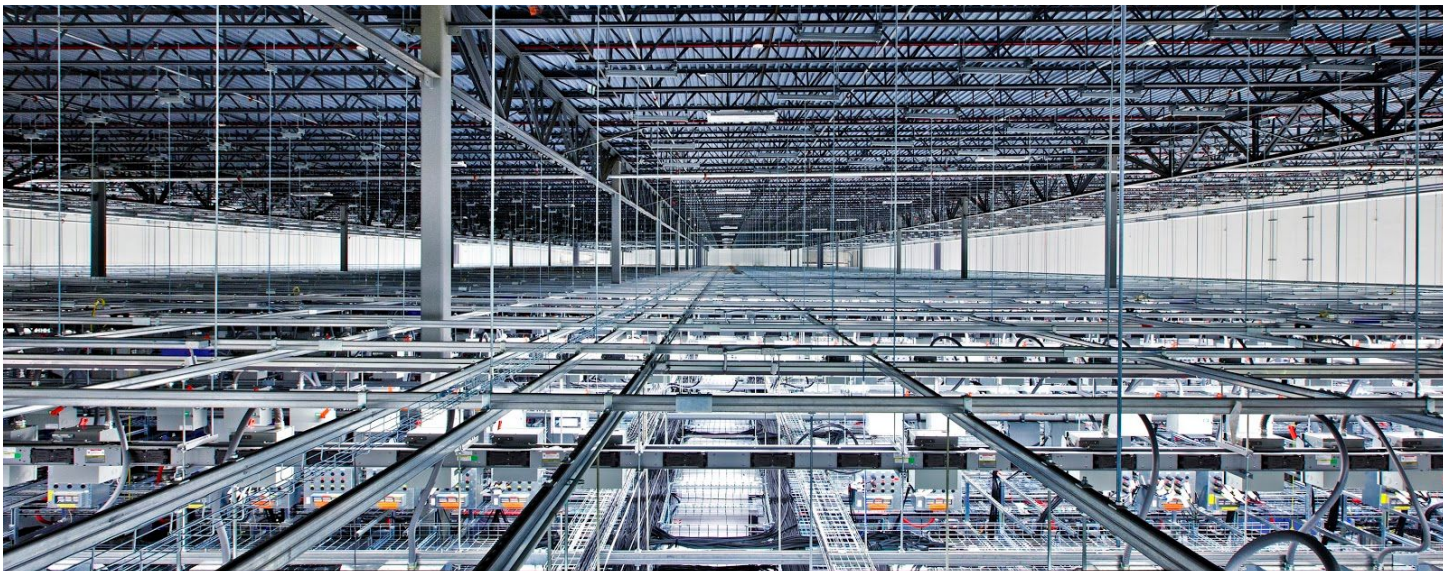
As application architectures shift from monolithic stacks to microservices stitched together to provide scalable functionality, so too have systems increased in agility to support this rapid-fire development mindset. Code is not promoted from source-to-production in fully automated CI/CD pipelines and toolchains.

This has affected systems in countless ways, including:

Shorter system life-span -- systems now scale on-demand and as needed, sometimes being provisioned and destroyed all through automation. Google Cloud, for example, supports automatica instance scaling with App Engine containers. But these systems, as short as they may live, serve a core part of the application and while why exist, must be secure. Their communications to other systems must be protected by certificates, and these must too be automated within the cloud.

Containerized deployment -- Containers make deploying application components easy and fast. By creating modular components that can be combined to create application stacks and full systems, containers offer a way to quickly deploy packaged applications. Things get complicated when adding certificates. Certificate renewal usually happens at a different cadence than application updates, and traditional CA systems are managed by completely different teams requiring lengthy manual requests to fulfill certificate issuance. CAS, on the other hand, can enable developers to securely manage certificates within their containerized applications through automation and standardized API's.

Cloud-ready -- because CAS is already a service integrated into the same platform developers are building cloud-native applications in, it can serve as a powerful tool to add secure, yet convenient, certificate issuance for applications that otherwise wouldn't have it.



Certificates for Internet-of-things hyperscale

With over 40 billion IoT devices are estimated to be deployed across the globe by 2027, the scale of certificates required to secure device communication can't really be overstated. But the challenge with managing huge device infrastructures that IoT demands isn't just issuing these certificates. It's about managing their complete lifecycle.

Compounding the sheer expansion of devices is also the growth of the IoT market, especially the entrance of smaller vendors innovating in the field. While these smaller organizations employ crackshot engineers that are solving new problems within the IoT space, they are also being tasked by their respective standards body's to deliver on security and compliance requirements.

Because of the unprecedented scale of these infrastructures, lifecycle demands for certificates are magnified enormously. Not only are certificates issued in the millions, but they require timely monitoring and renewals, lest an expired certificate causes application or device downtime. And this all assumes normal operations. If a security incident occurs, those same volume of certificates may need to be revoked and reissued.

These operations at scale are impossible without automation and a tightly integrated certificate-management process.

Many smaller vendors in the IoT space are now seeing the need for PKI and certificate management as standards body's such as the Wireless Power Consortium now require authentication frameworks that involve certificate-based identities and other security requirements. Many smaller companies do not have the skillsets or other resources to manage their own traditional PKI infrastructure. CAS is a service that enables smaller engineering-centric organizations to manage certificates much easier than traditional CA's would be.

Modernizing traditional IT

Digital certificates are not only pervasive in high-scale use cases like IoT and globally-distributed applications, they are also present in many more traditional IT functions. As IT organizations shift their functions from the data center to the cloud, a cloud-ready solution like CAS is a natural solution.

Issuing certificates for cloud-based infrastructure or SSL becomes routine using a cloud-native CA like CAS. Certificates are also issued for VPN, a very common use case as more workers are based remotely. Digital certificates are also commonly issued to provide passwordless wifi access for laptops and other devices. These functions are commonly performed manually by PKI teams, resulting in requests that can take days or even weeks to turn around. IT teams can take on these functions themselves using CAS, a CA service that requires minimal training.

Many IT organizations are also establishing a “zero trust” model for network-based security, all of which relies on the concept of trusted identity rooted in digital certificates. IT teams are now establishing trusted identities for applications, operating systems, smartphones and other BYOD devices, and workstations. Network access is governed by identity, but managing certificates to this scale, especially as the lifespan of certificates has been shrinking, can create significant overhead. CAS offers an intuitive service for IT teams to scale their efforts with zero trust models.

A new CA for a new world

Traditional CA’s just aren’t designed for the demands of the new world of cloud-level scaling and agility. Cloud Authority Service is a CA to enable application builders to deploy security aligned with their development processes: with automation, resilience, global scale, and cloud-integrated.

Start planning your transition to a cloud-ready CA platform that CAS enables. As you continue modernizing your applications to take advantage of cloud-native services and integrations, evaluate how to make CAS work for your applications and certificate management processes within the cloud. Getting started with CAS is easy, and spinning up a CA that you can integrate with takes only minutes. See for yourself how easily you can integrate certificates within your cloud-ready applications.