Vanguard Report

November 2023

Centralized Trust for Decentralized Uses

Revisiting Private Certificate Authorities

Commissioned by

aws

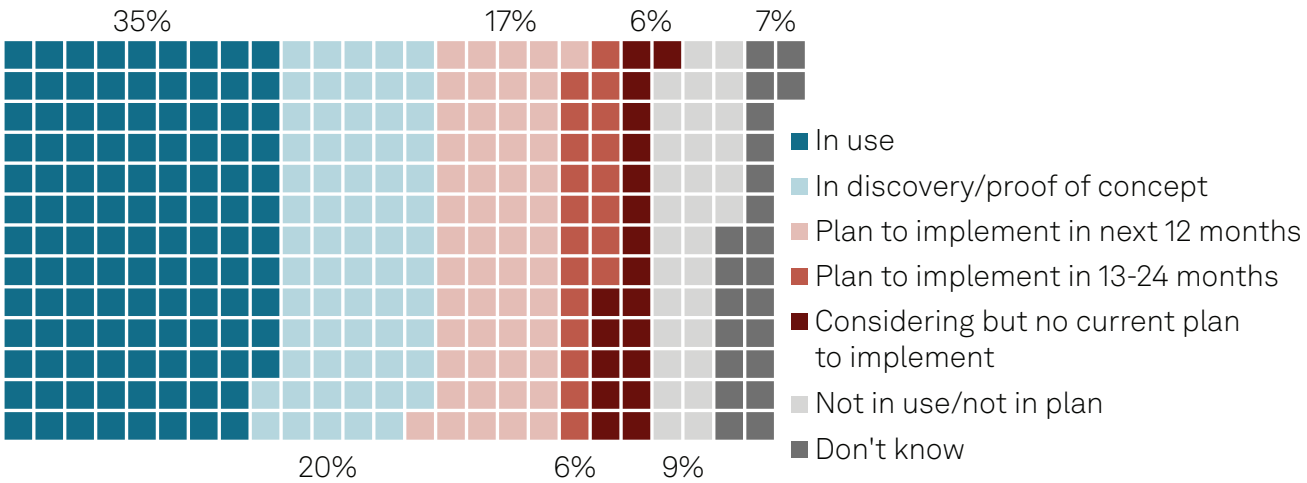
S&P Global
Market Intelligence

Introduction

Strong cryptographic controls, such as certificate-based authentication, are mature and broadly implemented today, with more than 95% of all internet traffic protected by hypertext transfer protocol secure (HTTPS) and its underlying certificate-based authentication. Certificate authorities (CAs) create hierarchies of descending public trust between root certificates, issuers and clients. This descending public trust is typically "one way" — a client can verify and authenticate the website with its issued certificate. However, the website typically does not authenticate its clients or anonymous visitors.

New computing architectures such as Kubernetes, service meshes and internet of things (IoT) networks are creating complex and decentralized processes at a significant scale. According to 451 Research's Voice of The Enterprise: Cloud Native, Adoption and Usage 2023 study, service mesh architectures are proving to be especially popular, with 72% of respondents having implemented or planning to implement in the next 12 months.

Figure 1: Service mesh adoption



Q. What is the state of your organization's adoption for each of the following cloud-native technologies? - Service mesh.
Base: Respondents whose organizations are using or discovering cloud-native technologies for application development or deployment (n=327).
Source: 451 Research's Voice of the Enterprise: Cloud Native, Adoption and Usage 2023.

The underlying services, devices and identities provisioned to these architectures are highly modular and dynamic, with little or no hierarchy. From a security perspective, zero-trust principles have become essential because the underlying environments are always changing in scope or function. This report revisits certificate authorities for these zero-trust environments and private CAs that facilitate mutual authentication of every service or device. For security practitioners familiar with CAs, this report looks at some of the wider business implications for establishing trust in highly decentralized and dynamic environments.

The Take

Decentralized architectures such as service meshes and IoT initiatives are driving the need to modernize one of the "last miles" in cloud and digital transformation — the CA. Flexible zero-trust principles require each device or service to be independently and dynamically trustworthy. Yet historically, organizations deploying CAs have incurred significant capex and up-front costs before the CAs deliver any certificates or value. As enterprises continue their digital transformation, supporting services and infrastructure should scale to follow the same development, cost models and developer enablement to minimize opportunity costs and maximize innovation.

For public-facing applications, certificate authorities still play a role in enabling any client or browser session to authenticate and verify a visited website within the context of a hierarchy of trust — all the way to a global publicly known and trusted root certificate authority. Public CAs are hosted in trusted environments. On the other hand, private CAs enable trust for resources and devices on an internal or private network; securely hosting private CAs needs to be done either by the enterprise or the enterprise's cloud service provider. Cloud service providers solve one of the last-mile challenges in digital transformation — the simplification of obtaining private CA services without the burden of building and maintaining them.

The transformation of private certificate authorities no longer requires a trade-off between resources for maintaining infrastructure and delivering code for new projects and products. Both development of the architectures and the architectures themselves are decentralized and rapidly iterated upon with minimized opportunity costs and the freedom to experiment quickly. Dynamic certificate-based authentication enables deeper integration to ultimately support new architectures and trust models.

As enterprises build more disparate services and devices, each service or device has become part of a broader supply chain that will upend conventional business models and require greater levels of both flexibility and control. Centralized trust for these decentralized use cases via technologies such as private certificate authorities will be paramount.

Why change? Why now?

New computing architectures such as service meshes and IoT networks are creating complex and decentralized processes at a significant scale. The underlying services, devices and identities deployed to these architectures are highly modular and dynamic, with little or no hierarchy. Developers and operators of these environments must factor in security and trust with each new change. Whether that is a new device, new service or even new classes of services or devices, security and trust must be provisioned with developer and operator experience in mind.

From a security perspective, zero-trust principles become essential because the underlying environments are always changing in scope or function. Methods of mutual authentication, such as mutual Transport Layer Security (mTLS), use certificate-based authentication to simultaneously verify the "client" and "server" for any given communication. In these scenarios, the trust model differs significantly from conventional authentication approaches such as when a user's browser communicates with a website via HTTPS. With conventional authentication, the user's browser verifies the authenticity of the website in the context of a hierarchy of trust all the way to a global root certificate authority in a descendant, one-way motion.

For service meshes or IoT networks, trust is continuously and mutually verified between components without requiring the context of an external public trust hierarchy. Zero-trust principles mean every component authenticates every other component with a bidirectional motion. All communications within a service mesh or IoT network become completely private. Certificate authorities that establish constant trust for private, decentralized communication and authentication are *private certificate authorities*.

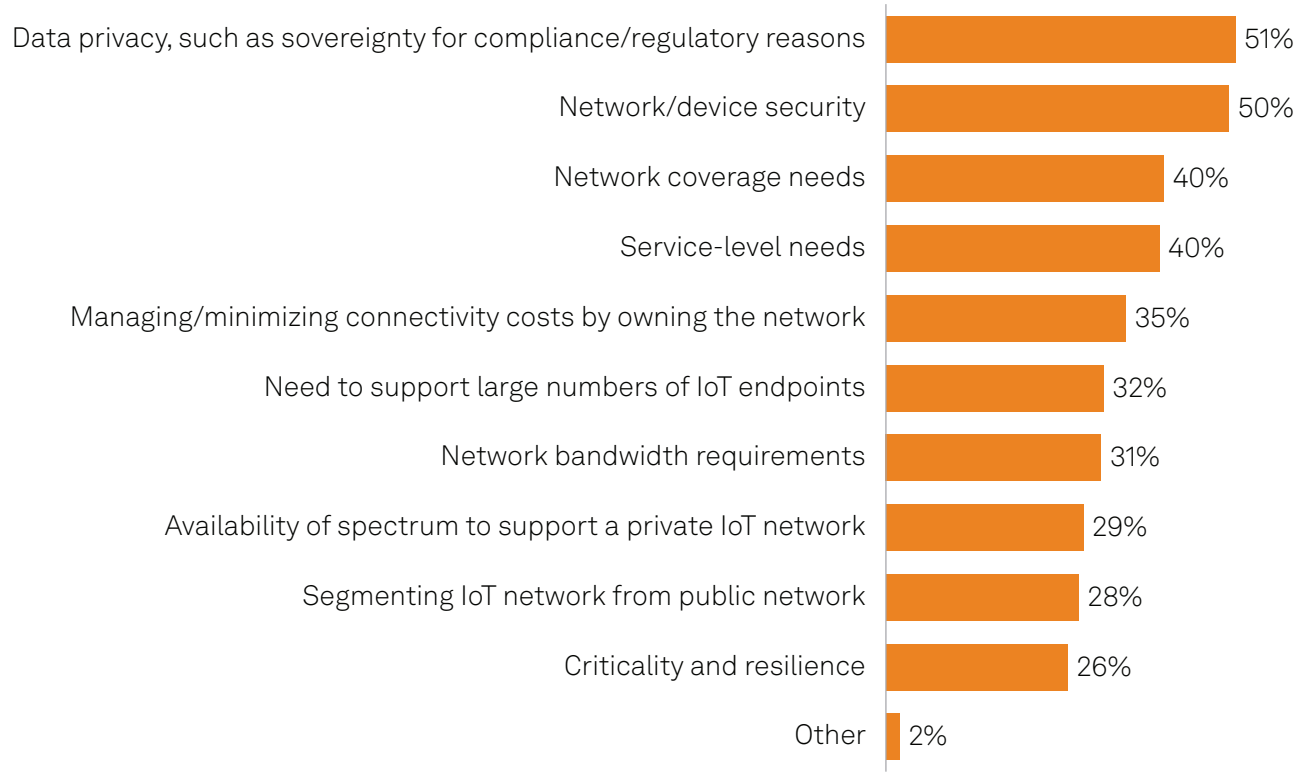
Service mesh architectures provide scale and unify services to operate as a more logical group without sacrificing microservice modularity or flexibility. Given the constant changes, there are no hierarchies of devices or services; each piece must be able to trust other components and prove trustworthy.

Releases, markets and end-user customer adoption are getting faster. According to Voice of the Enterprise: DevOps, Developer Experience 2023, 84% of enterprises have some level of DevOps, with 31% adopting DevOps exclusively. Slightly more than half (51%) of respondents deploy to production weekly or more often. Generative AI is allowing developers to iterate and release even faster. Developers and designers can spend less time searching for, assembling and editing code and infrastructure and more time improving end-user experiences. Other innovations include immediately building in production-level controls for prototype releases. For example, within Kubernetes, private CAs generate certificates for TLS authentication and encryption rather than rely on the default Kubernetes self-signed CA.

Increasing adoption of cloud native means applications are becoming further decentralized to iterate innovation. According to the same study cited above, 59% of respondent companies have architected more than 50% of their applications with cloud-native technologies. Furthermore, 77% of respondents expect most of their applications will be cloud native two years from now, and half the respondents believe that more than three-fourths of their apps will be so. Service mesh makes deploying services even faster, with infrastructure communication tasks such as observability, authentication, resilience and authorization decoupled from any individual service.

The ultimate decentralized and distributed trust model is IoT environments that may have few or no other defenses. Data privacy, network and device security are the top ranked drivers of private IoT network deployments, according to the Voice of the Enterprise: Internet of Things, IoT Connectivity – Private Network 2022 survey.

Figure 2: Drivers of private IoT network deployment



Q. Which of the following drivers, if any, are most critical in influencing your organization's decision to deploy a private IoT network? Please select all that apply.
Base: Current or planned private IoT network users (n=307).
Source: 451 Research's Voice of the Enterprise: Internet of Things, Connectivity-Private Network 2022.

New business models in IoT are driving privacy and security requirements. According to 451 Research's recent Technology & Business Insight report, IIoT Reaches the Mainstream: Benchmarking Digital Maturity of the Manufacturing Sector, manufacturers are heavily embracing industrial IoT, with initiatives in production monitoring, quality assurance and inventory management. Moreover, multiple manufacturers' IoT devices can be combined or reassembled into another finished product. Manufacturers creating these complex systems in fields ranging from automotive to aviation must be able to incorporate trust from their suppliers and their devices. Suppliers in turn must provide a trusted means of servicing their components that honors the security and privacy of their downstream partners and customers.

While decentralized architectures require significant developer agility and scale, private certificate authorities must respond in kind, and their operations must fit the architectures. For many enterprises, IT operator expertise remains in short supply. Cloud security and cloud platform architects are the most common existing cloud-related personas among enterprises surveyed in 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Organizational Dynamics 2023 study. In empirical interviews with senior technology leaders during a similar study, participants expressed concerns about enterprises pursuing multicloud strategies, given the dearth of operator expertise.

By definition, private certificate authorities furnish trust to services and devices beyond any single cloud provider's network, so there is little reason to provision separate private certificate authorities among different clouds or even on-premises.

The most critical requirement for any certificate authority is the safeguarding of private signing keys used to generate any certificate. This "last mile" of digital transformation has required heavy up-front investments for hardware security modules that usually must be clustered locally and regionally to avoid uptime failures or minimize key loss altogether. Operators must expend significant effort in establishing this infrastructure. Moreover, the opportunity cost for developers to wait for any initial certificate provision remains high. With cloud-based alternatives, the heavy opportunity cost for developers waiting for any initial certificate provision is significantly reduced.

Private certificate authorities also better match service ephemerality. Automating the renewal of short-lived certificates for devices and services lowers security risk. As the classes of devices and services change, private certificate authorities can effectively create different segments, driving an even more dynamic trust model.

Conclusion

Increasingly decentralized architectures are driving the need for greater amounts of centralized trust. As enterprises continue their digital transformation, supporting services and infrastructure should scale to follow the same development, optimized cost models and developer enablement to maximize innovation.

Just as services and devices need to mutually build trust, developer, security and operator personnel need to understand and leverage each other's abilities. Security practitioners should increase their awareness and understanding of developer initiatives. Conversely, developers and operators should better understand what security tools and resources are available. Together, these groups can better build trust and safety in their enterprises' far-reaching services and markets.

Learn more about how you can create private certificates to identify resources and protect data with AWS Private Certificate Authority.

About the author

Justin Lam

Analyst, Information Security

Justin is a research analyst at S&P Global Market Intelligence, leading data security research within the Information Security channel since October 2021. At S&P Global Market Intelligence, Justin leverages his years of industry experience and his unique understanding of both how customers buy and why sellers sell to help investors, practitioners and entrepreneurs understand and contextualize industry trends.

Prior to this role, Justin successfully served and advised numerous startups in information and data security in strategy, sales and partner-development roles. He has built worldwide partnership and sales programs from scratch and has been fortunate enough to earn several "Presidents Club" and "Quota Club" awards. Within these startups, Justin has held both technical and enterprise customer-facing roles, with assignments in engineering, product management, customer success, consulting, prospecting and closing. Justin has been part of five exits, including two IPOs. He has also seen the process evolution of data security adoption.

Justin holds a Bachelor of Science degree from the Tepper School of Business at Carnegie Mellon University.

About S&P Global Market Intelligence

At S&P Global Market Intelligence, we understand the importance of accurate, deep and insightful information. Our team of experts delivers unrivaled insights and leading data and technology solutions, partnering with customers to expand their perspective, operate with confidence, and make decisions with conviction.

S&P Global Market Intelligence is a division of S&P Global (NYSE: SPGI). S&P Global is the world's foremost provider of credit ratings, benchmarks, analytics and workflow solutions in the global capital, commodity and automotive markets. With every one of our offerings, we help many of the world's leading organizations navigate the economic landscape so they can plan for tomorrow, today. For more information, visit www.spglobal.com/marketintelligence.

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html