Simon Elisha (00:01):

AWS Smart Business Day 2023. Spend half a day with AWS on May 10, 2023 and take your business to the next level. Hear how customers are using AWS to solve their problems and technical challenges, chat with AWS experts, and explore training and certification opportunities for you and your team. Join this robust virtual experience with each session designed to give you information and resources to help you modernize, optimize, and monetize your business. This virtual experience runs from 9:00 a.m. Pacific Daylight Time till 1:00 p.m. Pacific Daylight Time, and you can learn more and register for Smart Business Day 2023 using the link in the show notes.

Speaker 2 (00:38):

Podcast confirmed. Welcome to the official AWS Podcast.

Simon Elisha (00:47):

Hello everyone and welcome back to the AWS Podcast. Simon Elisha with you. Great to have you back. And I'm joined by two very special guests. I'm joined by Todd Cignetti, who is the General Manager of AWS Private CA. Welcome to the podcast, Todd.

Todd Cignetti (00:58):

Hi, Simon. Good to be here.

Simon Elisha (01:00):

Good to have you here. I'm also joined by Param Sharma, who is a Principal Software Engineer on that particular team as well. Welcome to the podcast, Param.

Param Sharma (01:08):

Thank you, Simon. Good to be here.

Simon Elisha (01:10):

Good to have you both here. Now, we are talking about a really interesting topic, and it's a topic that often gets forgotten in the world of IT and infrastructure, et cetera, but it's kind of like connective tissue. But let's start with the start. And Todd, as the general manager of the service, we build services for customers because well over 90% of our roadmap comes from customer feedback. So I'm sure you didn't wake up one morning and go, "I'd really like to build a private certificate authority." There was obviously some form of inspiration from customers that came there. So let's start with the start. Where did the idea come from?

Todd Cignetti (01:51):

Yeah, that's right. So Param and I both worked on the AWS Certificate Manager Service that we launched in 2016. And as we were developing the certificate manager, which does certificate lifecycle management, public certificates for use on AWS, we heard from a lot of customers that they were also struggling with another problem, which was that creating and managing private certificate authorities, which are used to issue certificates that are used within an organization, was also a challenge.

(02:26):

And the knowledge and expertise required to operate a private CA was high. The operating costs, the infrastructure was all time-consuming and complex. And so after we released ACM, we looked at this next challenge that customers were having and looked to solve this, how to create a managed service for our customers for managing private certificate authorities.

Simon Elisha (02:59):

And regular listeners would be very disappointing to me if I didn't use the phrase undifferentiated heavy lifting. But this sounds like well in that particular world. And before we get into the service, maybe, Param, let's do some backgrounding for those who may not be familiar with it because the world of certificates is kind of one of these weird things where it's built into actually pretty much everything we do, in using the internet and connecting systems, et cetera. But it's probably not that well understood. So maybe let's talk a bit about certificates first, and then we'll talk about certificate authorities and private CA. So help us with the explainer.

Param Sharma (03:35):

Sure, Simon. And before I talk about certificates, I have this interesting story to share.

Simon Elisha (03:41):

Please.

Param Sharma (03:41):

So I met Todd eight years ago, more than eight years ago, and our first conversation was we're going to make things simple for our customers and how do we make certificates simple for our customers, certificate management or a private CA management. And since then, the goal has not changed. The goal is still keeping things simple. And you mentioned the word undifferentiated heavy lifting, that's rightly fitting into the mark here. So I just wanted to call you out because I remembered the whole story.

Simon Elisha (04:14):

It starts from the start.

Param Sharma (04:16):

Yep. And to answer your question around certificates, so X.509 certificates, they improve security by identifying resources. And some of them are, for example, host or containers or they can even be used for identity if you want to know what the certificate belonged to or what this public key belonged to.

[NEW_PARAGRAPH]So certificates use applied cryptography and principles for handling keys, which is known as public infrastructure, or we call it PKI in short form. And we think certificates as a gold standard for identifying resources and establishing secure connections because certificates, PKI and TLS are widely supported and established technology. They have been around since the 90s in the days of Netscape and early E-commerce. So despite many predictions that PKI would go away, certificates and TLS are going stronger than ever. And because the need to establish the identity of servers, securing connections is as important as ever.

Simon Elisha (05:21):

So it is that critical plumbing. And as with many pieces of critical plumbing, it's often forgotten. And I know that for myself, I don't think about certificates that often, but much like most problems when you

get to the bottom of them are DNS. Often, you'll hear about sort of catastrophic values that take place from a system's perspective, and it all comes back to a certificate that wasn't renewed. And that's when you realize everything has certificates underneath it, doesn't it? It can't work without it.

Param Sharma (05:49):

Yep. And for example, when you go to amazon.com, you see that padlock icon. So you can click on that, you can see what is the certificate, which is being used for the TLS communication. And that certificate has subject in it. And you will see that the subject has amazon.com. So that tells you that you are connecting to a real amazon.com site. And that certificate is usually issued by a root, and that root is trusted by your browser or your operating system. So that's how public certificates work.

(06:21):

Private certificates on the other hand, they are similar to public certificates, but they are for establishing secure connections within a private network. And the other thing is private certificates are used in a similar way, but they are used with the endpoints and resources within an organization instead of public resources on the internet.

(06:41):

The other key difference that as applications and IT infrastructure evolve and grow to span on-prem, our cloud service meshes microservices and multi-cloud applications. These secure connections have to be created automatically for every connection. And then the private search form the basis for all of these secure connections for the internal endpoints, meshes and applications. And we are seeing that this usage is even expanding to IoT devices, identity certificates, and few more areas and applications.

Simon Elisha (07:13):

So the delineation between I guess the public CA and the private CA is interesting, and clearly it's become even more important. And Todd, recently, AWS Private CA became its own service outside of what existed for AWS Certificate Manager. Help us understand what drove that and how customer needs, I guess, really dictated that.

Todd Cignetti (07:36):

Yeah, so we basically rebranded AWS Private Certificate authority, so it is now classified as its own service. And what drove that was really customers being confused about the difference between AWS Certificate Manager and Private CA.

(07:56):

When we launched, we launched Private CA as a feature of AWS Certificate Manager because at the time our thinking was these are closely related to certificates and for customers, they're going to look at ACM and then they're going to go into private CA and consider using private ca. But what we found was that there were a lot of customers that just want a managed certificate authority, and they may use AWS Private Ca by itself without using the certificate lifecycle management capabilities of AWS Certificate Manager.

(08:34):

So there was a lot of confusion. Customers weren't aware that they could use just private ca or just ACM. Now, it just so happens they work well together. If you need to use private certificates on AWS and manage the lifecycle, that's a great use case where you want ACM to manage lifecycle, private CA to

operate the certificate authority. But there are also lots of cases where you just want managed certificate authority.

(09:02):

And so by rebranding the service to be AWS Private CA, we found a lot of customers have since found the service. In fact, a couple weeks after we rebranded, a big customer came to us and said, "Hey, this is a great new service. We saw that you launched. It is just what we were looking for. We looked for this three years ago and we didn't find it. So we built one ourselves."

Simon Elisha (09:27):

You're like, "We kind of had that, but it's okay."

Todd Cignetti (09:30):

Yeah. Clearly, our rebranding was necessary. So they were very happy to find us. They got to get rid of a CA that they had built themselves and they're on a much better path now with the AWS Private CA.

Simon Elisha (09:46):

So then thinking about, I guess what a CA does and how that might evolve over time, it's easy to simplify and go, "Well, you're just generating certificates. How hard could it be?" AS with the answer of most things in it, way more complicated than we thought. What are some of the capabilities that you guys have worked on over the years for customers to help make it easier to integrate this into the world that they live in?

Param Sharma (10:09):

Sure. So I guess the biggest one I have seen is creating CA hierarchies. So a CA hierarchy is usually you have a root ca on the top, which is parent CA, and then you have subordinate CAs, and then you have issuing CAs. So you can go many level down in the CA hierarchy. So that's one of the big features that Private CA offers in terms of creating those hierarchies.

(10:34):

And there are a few more. For example, you can customize certificates to all your needs. You can create your custom extension. So every certificate has a structure to it. So you can add standard key usage, subject [inaudible 00:10:47], bunch of extensions like that. So Private CA, it does allow adding standard extensions as well as adding custom extensions, which might be specific to a organization's need.

Simon Elisha (11:01):

So you mentioned earlier as well that there were a lot of system-to-system interactions. Is this something that, for example, IoT and other types of requirements fit into?

Param Sharma (11:11):

Yes, absolutely. So we have seen requirements for IoT devices, such as there is a new standard called Matter where there is a need to issue certificates which identify devices with custom extensions in it. And it has a custom object identifiers that go into the certificate. So that's one of the requirements that we are seeing on the device world side where customers want to customize the certificates that they can issue. And Private CA does give the capability of customizing these certificates with key usage, extended key usage, which may be pertaining to the devices or even subjects which may have a device ID in it. So that's another way to issue private certificates that work with devices.

Simon Elisha (11:56):

And so there's lots of, I guess, iteration that goes on in a service like this. And Todd, I know the team's been working on things like Kubernetes plugins and API Passthrough and Tag-On Create. What are some of the things you've really seen customers resonate with in terms of some of the things that have evolved over the years?

Todd Cignetti (12:13):

Well, that's one truism for working with PKI and certificates is that the standard is very, as Param said, it's old. It's been around since the mid-90s, and there's a lot of flexibility and a lot of different use cases for how certificates are being used. So this ability to customize is something we've really spent a lot of time on and giving customers a lot of different options for what they can include in their certificates, whether it be custom extensions or ways to issue that give control to the certificate authority administrator and less control to the requester of the certificate. So that customization.

(12:55):

Some other aspects that we've seen evolve over time are things like we launched with CRLs, which are certificate revocation lists, as a way to keep track of which certificates have been revoked. So it's an important part of the PKI process is to have a mechanism for revoking certificates, basically saying this certificate was issued, it was good, it's no longer good.

(13:22):

But another mechanism for doing that is called OCSP, Online Certificate Status Protocol. And that's a dynamic back-and-forth protocol that happens at the time the certificate is being used. And so we added a very scalable infrastructure that we operate on behalf of customers who have private CAs to take care of the problem of operating that OCSP responder.

Simon Elisha (13:46):

That's amazing. So there's some really interesting scaling opportunities there. Now, there's also something that happened recently in another service that relates to this one too, which is Identity and Access Manager introduced IAM Roles Anywhere. And that lets customers obtain temporary security credentials in IAM for things like servers, containers, and applications that run outside of AWS. Now, to use this, you must use X.509 certificates issued by a certificate authority. Do you know of a certificate authority that customers might want to use for this particular capability? Is this where this can fit in?

Param Sharma (14:19):

Exactly. So IAM Roles Anywhere provides the benefit of using the same IAM policies and IAM roles that you can use with AWS applications to access other AWS resources. And in order to use IAM Roles Anywhere, you must use X.509 certificates that's issued by your certificate authority. And now, that certificate authority could be a AWS Private CA resource where you offload the management of the CA using the AWS Private CA service. And like any other AWS service, Private CA provides integration with SDK cloud formation. You can use CLI. You can automate the creation of CAs and even the management of CA and revocation infrastructure that Todd just mentioned. So all of these come together in kind of like a ecosystem.

Simon Elisha (15:07):

And Param, you get to speak a lot with customers directly. And I think one of the best things about customers is hearing what they ask for and what some of their questions are. Give us a flavor for some of the things that they're asking for and the questions you hear quite often.

Param Sharma (15:21):

So one of the first question usually that we hear is how can I move my PKI hierarchy to cloud? And it has two parts. So for example, if you want to move your root CA to cloud, that's one option where you go to Private CA, you create a root CA, and then you design your subordinate CA hierarchy. And then you can have IAM controls on top of it, which IAM role can issue certificate, which IAM role can manage the CA, and which IAM role is allowed to generate audit reports off of that private CA. So that's one way.

(15:55):

The second way is you can move your PKI infrastructure slowly over to the cloud. So you can create a subordinate CA, for example, let's say in AWS Private CA, and you can chain that to an existing root which may or may not exist inside PCA. So that gives you the capability to slowly move over your workload from your on-prem into the cloud. And once you have that subordinate CA created, you can even look into moving your root into cloud based on your organizational need where you can slowly do trust or rotation. That's one way.

(16:28):

The other common question that I have heard is how do I design my CA hierarchy that scales for long-term PKI needs? And there is a reason behind it because a well-designed CA hierarchy offers lot of benefits. For example, you can have a division of administrative tasks for better load balancing and security. There is a granular security control which is appropriate to each CA. So you can say that subordinate CA one can only issue certificates for my hr.amazon.com. Let's say you're using a name constraint to control that. And your subordinate CA two can only issue certificates for IT. You can similarly do that for dev and prod environment. So there are various ways you can make those security controls which are appropriate to each CA.

[NEW_PARAGRAPH]And then you can have a use of CA with a limited revocable trust for daily operations. And then you can define your validity periods and certificate past limits to see that how big your CA hierarchy can be. So you can say, "My organization only allows three-level hierarchy. I don't want to go bigger than that because that would extend my chain of trust."

Simon Elisha (17:38):

Interesting. So there's lots of complexity that comes up, but I guess lots of common answers. I know that a lot of customers have been using Kubernetes and Containers for their applications, and that brings its own challenges of scale. What have you seen in terms of some of the integration that's been needed there?

Param Sharma (17:57):

Sure. So AWS Private CA supports an open source plugin for cert-manager that offers a certificate authority solution for Kubernetes Containers. Cert-manager is a widely adopted solution for certificate management in Kubernetes itself. And customers who are using cert-manager for application certificate management can use the Kubernetes connector, the AWS Private CA Kubernetes connector for issuing certificates.

(18:22):

So one of the biggest benefit here is the certificate authorities are managed through HSMs. So the key use itself happens in HSM rather than the standard CA, which lives in the memory when you use cert-manager. So those are the biggest things we have seen in terms of customers who especially have regulatory requirements for controlling access to and auditing their CA operation can use the solution to improve the auditability and support compliance as per their company needs.

Simon Elisha (18:52):

Nice. And Todd, earlier on I touched on the fact that security certificates do expire and sometimes people get caught out by that. But sometimes you want that. And I understand you recently launched an additional operating mode for AWS Private CA, which is called short-lived certificates. Where do they fit in?

Todd Cignetti (19:11):

Yeah, so there are a number of cases where customers want to limit the lifetime of certificates. It's often used as an alternative to revocation. So if you have a certificate that lasts a year and something happens where you think maybe the private key was lost or released, you have to revoke that certificate because of the long lifetime. If you have nine months remaining, it's not acceptable to have that key floating around for nine months. Whereas with short-lived certificate mode, the length of the certificates issued by a CA in that mode is seven days.

(19:49):

And so it depends definitely on your security policy and your tolerance, but a lot of customers are finding seven-day certificates with the automated mechanism for renewing them and keeping them updated allows them to worry more about the renewal process and less about the need to revoke certificates.

Simon Elisha (20:12):

Yeah, it makes more sense to rather than have to go back and pull things out. You just know it expires in a very reasonable timeframe.

Todd Cignetti (20:20):

Yeah. You just rely on the expiration to take care of...

Simon Elisha (20:24):

Built-in revocation in a way. Yeah.

Todd Cignetti (20:26):

Built-in revocation. That's right. And so there's use cases like logging into workspaces or AppStream where a credential, a certificate is issued intended to last the lifetime of the login experience. And so it just naturally the best thing to do is to have it expire relatively quickly. But there's a number of cases like that that it's preferable to expire certificates on a short-lived basis.

Simon Elisha (20:55):

Nice. Interesting. Now, let's put our forward-looking glasses on if we can. Yeah. Quantum computing is obviously on the horizon, but it's still a few years away. But people are starting to think about, well, if quantum computing comes into fruition, it essentially could render a lot of existing cryptographic

algorithms easy to solve for. So where's the thinking in this space? And I guess, Todd, this is probably one of those things that you've had to really look over the horizon around what would it mean for our customers and for folks who use that service. What can you tell us about that?

Todd Cignetti (21:30):

That's right. AWS is very involved in setting the standards for post-quantum cryptography. We have had a few, or two algorithms that have been in consideration for post-quantum asymmetric crypto. We have positioned how we feel and what we recommend to customers. That advice is evolving over time as these standards develop.

(21:56):

From a private CA perspective, we are very much in the position of we're going to adopt the standards as they come. We have dependencies. We use hardware security modules for operating on the private keys for private CAs. And so the standards have to evolve so that the hardware security modules support these algorithms and then we can pick them up. But we're closely following the standards and we'll be adopting as the standards evolve. We have a link we'll share on AWS positions.

Simon Elisha (22:28):

Yeah, we'll put that in the show notes. Yeah, absolutely. And I guess that's part of the nature of using a service like this is it means you've got folks who are thinking about this and looking at it and building it in as standards evolve rather than sort of wake up one day and go, "Oh my goodness, we're in trouble here. We need to retrofit," which is that's what we want to be in a position to help our customers.

(22:49):

Now, we touched on earlier on, Param, around the concept of the new standards around the IT world. I know that's a big thing in terms of what's next for private CA. And you touched on Matter. What else are you seeing in this domain that folks should be aware of?

Param Sharma (23:09):

I think the big ones are that I heard. So for example, how do you run ceremonies in cloud? That's one interesting question that I have heard over and over again. So it's an interesting paradigm because you have the option to automate and remove the manual processes out of it, but you still have the capability to do operations like, one IAM role has the capability to enable CA, another one can only issue certificate. So you're sort of doing a Quorum control mechanism. So that might be interesting in terms of how CAs are operated, which are complying to Matter and other standards, or even industries or companies who are interested in much better control and auditing over their certificate authorities. They can, for example, use audit reports in Private CA to look at what kind of certs have been issued.

(24:01):

And you already talked about the short-lived CA, which is another interesting one because now you don't have to worry about revocation, because that's another thing that we keep on talking about, that how CRLs operate or how OCSP operate.

Simon Elisha (24:13):

And Todd, what about the concept of zero trust? That seems to be something related to a lot of security work as well.

Todd Cignetti (24:20):

Yeah, that's one of the trends. This trend has been happening for five years. It's under different names, but the idea of having a central protected set of resources kind of gone away over time, and now it's very distributed. And certificates definitely play a big role in that. As we move architectures and think about distributed applications and microservices that connect across a mesh, certificates really underlie the security of making zero trust and service meshes and microservices because they're at the heart of establishing secure connections between all of these endpoints.

(25:01):

And so since we started Private CA in 2018, we've been evolving and looking for ways to help customers solve this underlying security problem that they have. And it's just getting bigger and bigger. As we go from a central protected set of infrastructure to a very distributed set, these meshes are getting bigger and more complicated. And so having certificates at every endpoint becomes really a checkbox for security. And to make that happen, you need a solid, secure infrastructure for issuing those certificates. And that's what AWS Private CA is.

Simon Elisha (25:38):

Sounds like the future is rich and growing. Todd, thanks so much for coming on the podcast today.

Todd Cignetti (25:44):

Thank you very much. It's good to be here, Simon.

Simon Elisha (25:46):

And Param, thank you so much for joining us and sharing what you're seeing out there as well.

Param Sharma (25:50):

Thank you.

Simon Elisha (25:52):

And there are links in the show notes to all the information we spoke about. And as always, we do love to get your feedback. Awspodcast@amazon.com is the place to do it. And until next time, keep on building.