digicert®

CERTIFICATE LIFE CYCLE MANAGEMENT: TRENDS TO WATCH IN 2025

DigiCert's Dean Coclin on Need for Automation to Keep Pace with Change

ISMG
INFORMATION SECURITY
MEDIA GROUP

DEAN COCLIN

Senior Director, Digital Trust Specialist, DigiCert

Coclin is Senior Director of Digital Trust at DigiCert. He brings more than 35 years of business development and product management experience in software, security and telecommunications to the company. In his role at DigiCert, he is responsible for representing the company in industry consortia and providing PKI expertise to customers and partners. Coclin is the former chair of the CA/Browser Forum and currently chairs the Code Signing Working Group of the Forum. He also chairs the ASC X9 PKI Study Group, developing next-generation PKI standards for the finance industry.

Revocation events, decreasing certificate lifetimes, new trends in software trust - 2024 was a busy year for certificate life cycle management. And 2025 looks just as frenetic, says DigiCert's Dean Coclin, who shares insights on trends to watch and automation solutions to investigate in the New Year.

In this video interview with Information Security Media Group, Coclin also discussed:

- The current state of certificate life cycle management;
- The possible impact of discussions to shorten certificate lifetimes;
- Changes to code signing certificates and their impacts.

"The old days of putting calendar reminders in Outlook and sending alerts to your cell phone won't work anymore with these short certificate lifetimes."

STATE OF CERTIFICATE MANAGEMENT

TOM FIELD: As we wrap up 2024, how would you describe the state of certificate life cycle management?

DEAN COCLIN: The state is improving. We've gone a long way from where we were a few years ago, not only in terms of vendor products, but also from the way organizations are adopting certificate life cycle management. There is a need to adopt certificate life cycle management because of ongoing factors in the industry like shortening certificate lifetimes and quantum computers.

UNDERSTANDING REVOCATION EVENTS

FIELD: What are the effects of revocation events?

COCLIN: For organizations using publicly trusted certificates - which are governed by the CA/Browser Forum guidelines - revocations can happen. Whether the issue may be minor - including a spelling mistake - or major - such as a threat to the ecosystem, a cryptographic change or something similar - a revocation event will affect some customers at some point in their life cycle. There's a short window - anything from 24 hours to five days - when certificates have to be revoked. In that case, unless you have a certificate life cycle management tool, it will be impossible to try to meet those deadlines within the timeline scheduled by the CA/Browser Forum. So revocation is something that organizations have to be aware of, have to be cognizant of and have to be prepared for.

CERTIFICATE LIFETIME CHANGES

FIELD: What about the ongoing discussions on decreasing certificate lifetimes?

COCLIN: Chrome has been talking about reducing certificate lifetimes from their current one-year term down to 90 days. Apple has now come up with a proposal to reduce them to 45 days by 2027. These dramatic shifts in the way certificates are issued and managed mean that the only way to manage those is going to be with a certificate life cycle management tool. The old days of putting calendar reminders in your Outlook and sending alerts to your cell phone is not going to work anymore with these short certificate lifetimes.

SOFTWARE TRUST EVOLUTION

FIELD: What's the impact of software trust and code signing certificates?

COCLIN: Code signing is when you digitally sign a code so that the person receiving the code knows that no one has tampered with it. It is also done to make sure that you're telling people who developed this code and who signed that code. Currently, code signing certificates are good for a maximum of a three-year lifetime, but there is a proposal to reduce those to a one-year lifetime.

That's not going to affect the code validity because all code is timestamped and the timestamp is what applications rely on. But it could affect the ability of developers to use those certificates. All of those certificates have to be on tokens or hardware security modules, so having to replace those every year could become burdensome. That's why we recommend that developers use a software signing service such as Software Trust Manager from DigiCert. The certificates are stored in the cloud, you don't have to worry about when they expire, that's all done for you by the service. When you're ready to sign that code, you can upload the code to the service or upload a hash to the service and that is returned to you fully signed.

QUANTUM COMPUTING CHALLENGE

FIELD: Is quantum computing arriving sooner than expected?

COCLIN: It is. This is a big buzzword that's been going on for quite a few years, but people are saying, "Oh, I don't need to worry about that. That's something maybe in 2030 or 2035." But in reality, you do have to start worrying about it now. There are a couple of attacks that you need to be aware of. One is called "harvest now and decrypt later." This is where attackers could be storing and siphoning data from your network and taking that data and storing it and saying, "When a quantum computer is developed that can decrypt this, I'll have all this data that I can decrypt."

Some data that you're using or passing through encrypted today may not need to live that long. It could be data that temporarily needs to be encrypted. For example, credit card data, credit cards expire after a few years, so in 10 years, those credit card numbers will be useless. But there could be other data such as corporate secrets and patents that you don't want people to know about the details of.

What we're recommending to folks now is that they start getting educated about quantum cryptography and quantum-safe cryptography. NIST has come up with a bunch of algorithms that they say are quantum-safe. Organizations need to determine where they use cryptography. Prioritize those assets - what are the ones that need to be encrypted for the long term and should not be threatened by quantum computers? Then figure out exactly what your plan is going to be to safeguard those assets going forward. Moving to some of these quantum-safe algorithms could be the right time to do that, but we certainly encourage you to get advice from experts, and we here at DigiCert have the capability to help you through that process.

THE NEED FOR AUTOMATION

FIELD: What would you say is the overall message about automation and certificate life cycle management?

COCLIN: Most people manage a lot of certificates that may not be in that one department but may be scattered all over the world in different departments. A certificate outage would be a major event. It could be an income loss event. Think about a website that does online transactions - it doesn't have to be Target or Amazon, it could be a smaller organization, but they depend on their website being up. If a certificate expires, that means nobody can get to your website. If a certificate is revoked, nobody can get to your website. When they can't get to your website, they can't make purchases. When they can't make purchases, your CFO is going to notice that.

Get a hold of things, get certificate life cycle management and get comfortable with it. If you don't have it, start talking to folks that can help you automate.

One of the things we hear about why people are not moving to certificate life cycle management is they say some of their systems are legacy and cannot adapt to that. Have a new discussion with vendors about that because there have been a lot of updates and changes in APIs that can help legacy systems automate. This is the time to start looking at it before your website goes down.

ENTERPRISE CHALLENGES

FIELD: You work with organizations across various sectors. Where do you see enterprises struggling the most to respond to these trends?

COCLIN: We're hearing a lot from organizations that have government regulations. Think about financial institutions or even government entities that are not allowed to make changes to their infrastructure because of a lockdown period. Someone says, "The certificate is going to be revoked in the next five days." And they say, "Five days, I can't even get into the infrastructure in five days, never mind getting approval for doing that."

Having automation that can do that automatically helps in that situation. Some people might argue they still need approval, but it's a matter of convincing them that automation is the way to go and that approval is not necessary there.

We are seeing challenges from those types of organizations. But when it impacts your bottom line, those are the ones that are really going to be affected the most.

THE DIGICERT APPROACH

FIELD: How is DigiCert guiding customers through these trends?

COCLIN: From a certificate life cycle perspective, we're making everyone aware in real time about what's going on and the discussions going on in the CA/Browser Forum. I'm the incoming chair of the CA/Browser Forum starting in a couple of weeks. We also have a great team of individuals who have been long-time industry experts who chair various committees including the validation subcommittee in the secure mail working group, and also another group within the forum.

These folks are stalwarts in the industry, and we try to get that knowledge and get it right out to our customers so they know what's happening in terms of things like revocation or decreased certificate lifetime, which are the hot topics right now. Code signing is also a very hot topic, and quantum computing rounds out the list of hot topics. We try to inform our customers and then meet one-on-one because many customers want more details. We've had continuing calls to have meetings with our

"Organizations need to look at where cryptography is used in their organization, prioritize those assets and figure out exactly what their plan is going to be to safeguard those assets going forward."

experts, and that's an area we will continue to address going forward with all of our customers and partners.

LOOKING AHEAD TO 2025

FIELD: Beyond the trends we've discussed, are there any other trends we should watch for as we go into 2025?

COCLIN: AI is something that everyone is talking about. It hasn't been really a topic in the CA/Browser Forum except in one area when we validate identities. In many cases, we have to do validation of driver's licenses, passports and sometimes a face-to-face video call. With the advent of AI, a lot of those things can be easily spoofed. Even a face-to-face video call can be faked, and even your body movements and your speech can be very convincingly faked.

That's an area that I think we as the CA/Browser Forum and as certificate authorities have to pay extra close attention to in 2025 and beyond as AI continues to improve. A few years ago, it was not very easy to fake identities. That has changed dramatically over the last few years. I saw an article today about fake driver's licenses and a fraudster was showing how they can duplicate the hologram and the barcode on the license and make it look authentic.

That's scary not just for certificate authorities, but anywhere you use those IDs - banks, airlines, et cetera. This could be a very scary thing, and this causes everyone to be extremely vigilant when examining these documents.

digicert®

From patients to payers, from data to devices, digital trust is a must.

Learn how DigiCert can secure every corner of the financial services ecosystem.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to cybersecurity, information technology, artificial intelligence and operational technology. Each of our 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment, OT security, AI and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY CyberEd.io

CIO.inc DeviceSecurity.io PaymentSecurity.io FraudToday.io

CYBER THEORY CyberEdBoard Xtra mile LIFECYCLE MARKETING GREYHEAD

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io