Post-Quantum

Cryptography Conference

Scaling Trust: CLM Roadblocks on the Path to Post-Quantum Resilience

Chris Bailey
Chair of the Board of Directors and Executive Council of the PKI Consortium and Board Member of AppViewX

Muralidharan Palanisamy
CSO at AppViewX Inc

Chris Hickman
Chief Security Officer at Keyfactor

George Parsons
Head of PKI Strategy at CyberArk

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

Scaling Trust: Certificate Lifecycle Management (CLM) Roadblocks on the Path to Post-Quantum Resilience

29 October 2025

PKI Consortium

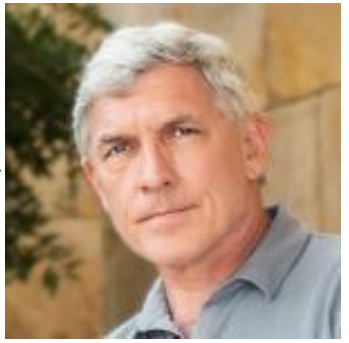
Meet the Panel

Chris Bailey, Moderator – Chair of the Board of Directors and Executive Council of the PKI Consortium and Board Member of AppViewX

Chris Hickman, Panelist – Chief Security Officer of Keyfactor

Muralidharan Palanisamy, Panelist – CSO at AppViewX Inc

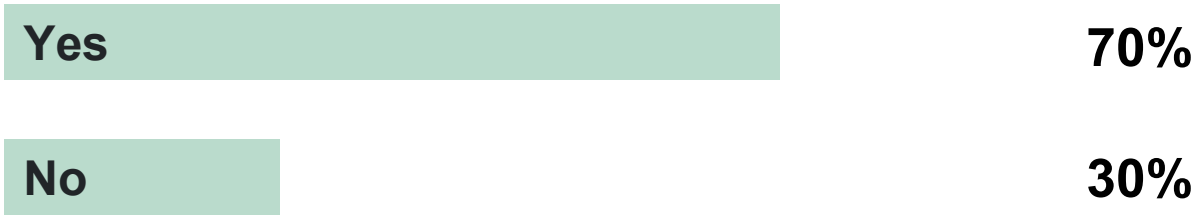
George Parsons, Panelist – Head of PKI Strategy at CyberArk



PKI Consortium

The shift to Post-Quantum Cryptography will be the hardest transition in cybersecurity history.

70% agreed

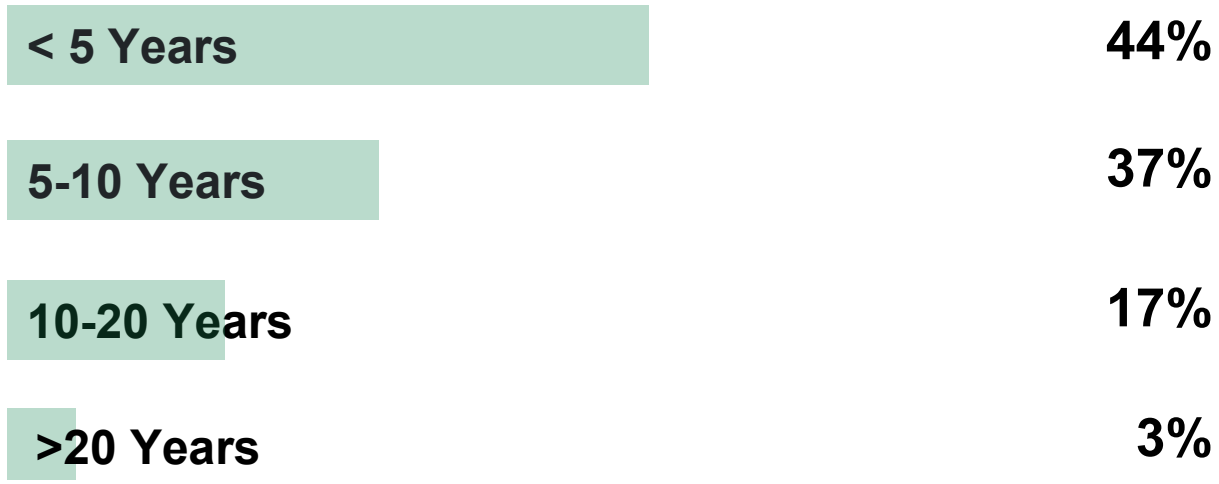


* Almost all larger organization responded - Yes

PKI Consortium

How long will it take before quantum computers can break an RSA-2048 bit key?

Weighted Average = 7.3 Years



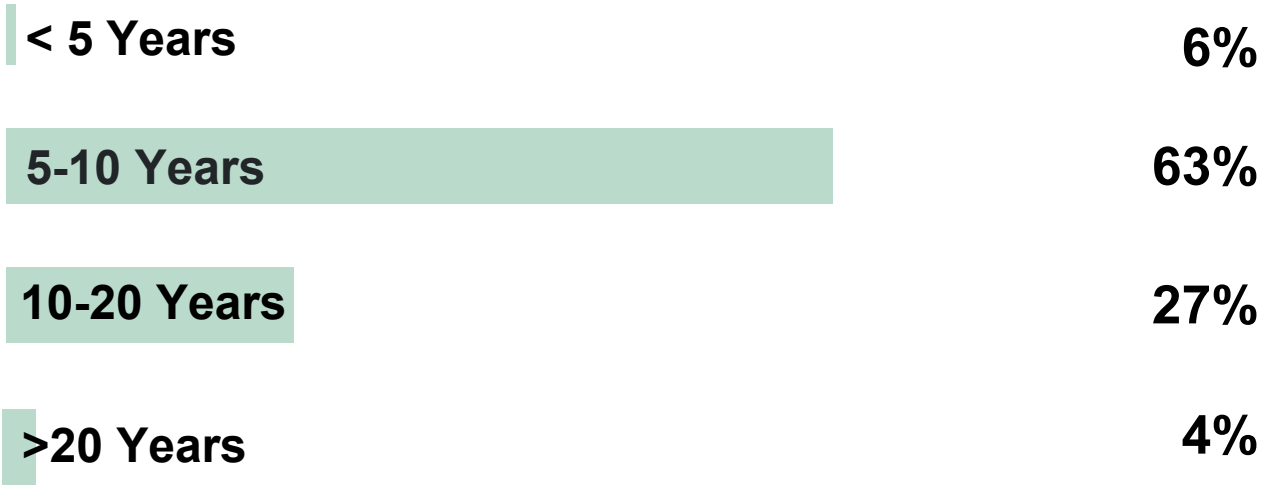
Weighted Average =(2.5*.44)+(7.5*.37)+(15*.17)+(30*.03)

7.3 years = 1.1+2.75+2.55+.9

PKI Consortium

How long will it take large organizations to successfully transition to Post-Quantum Cryptography (PQC)?

Weighted Average = 10.125 Years



Weighted Average =(2.5*.06)+(7.5*.63)+(15*.27)+(30*.04)

10.125 years = 0.15+4.725+4.05+1.2

PKI Consortium

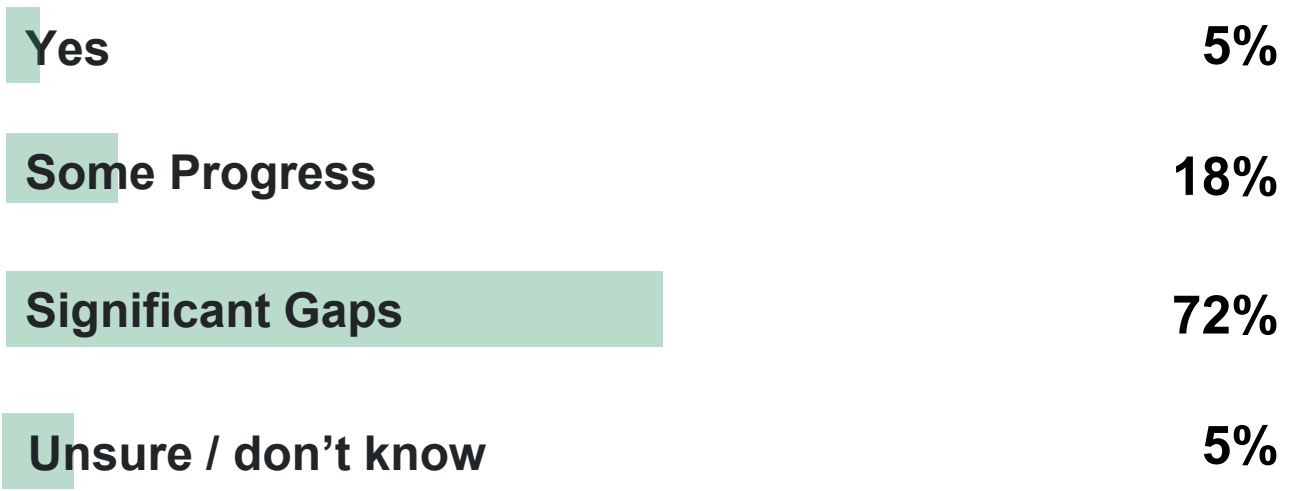
Do we have a problem?

- If RSA-2048 bit is vulnerable in ~ 7.3 years
- It takes organizations ~ 10.125 years to move to PQC
- Is there a problem with a ~ 2.825-year gap?
- What about Harvest Now, Decrypt Later?

PKI Consortium

Do organizations currently have the tools, skills, and budget to safely move to Post-Quantum Cryptography?

72% of organizations see Significant Gaps



PKI Consortium

Question from the Audience?

PKI Consortium

Thank You!

Chris Bailey – Moderator

Chris Hickman – Panelist

Muralidharan Palanisamy – Panelist

George Parsons – Panelist

PKI Consortium

Back up Slides and Directions

Scaling Trust:
Certificate Lifecycle Management (CLM) Roadblocks on the Path to Post-Quantum Resilience

PKI Consortium

Abstract

As enterprises prepare for post-quantum cryptography (PQC), the ability to discover, manage, and transition cryptographic assets at scale has become a mission-critical capability. Certificate Lifecycle Management (CLM) is often seen as the answer, but CLM at enterprise scale is more complex than most anticipate. This panel brings together thought leaders from various CLM vendors and industry experts to unpack the strategic lessons learned and operational friction points that organizations face in aligning CLM systems with quantum-resilient architectures.

PKI Consortium

General Directions

This 30-minute session will be a 20-minute panel with up to 5 mins of audience questions. We will end 5 minutes early so the next speaker can prepare.

Chris Bailey will be the moderator and will be asking the 3 of you (Chris, Murali, and George) questions.

The questions are in a thematic order with some suggested timing of each section.

Because we only have 20 minutes of talking, I will ask a single question to one panelist, someone can jump in after if they have high value to add. I have the list of questions below with how should respond. If you want to add or remove a question, then please give me the suggestion. If you want me to pass the question to someone else, please let me know that too. If you want to also answer the question, please let me know.

PKI Consortium

Welcome and Introductions

Start to Finish in 4 Minutes

Time 0:00

Welcome! Today's panel discussion is titled *"Scaling Trust: CLM Roadblocks on the Path to Post-Quantum Resilience."* In today's panel, we'll explore the challenges enterprises face in scaling Certificate Lifecycle Management (CLM) to prepare for post-quantum cryptography, with industry experts sharing lessons learned and insights on aligning CLM with quantum-resilient architectures.

My name is Chris Bailey, I have over 25 years of experience in PKI and I serve as the board chair of the PKI Consortium and a board member of AppViewX. Today, I am joined by 3 of the most experienced Certificates Lifecycle Management and Public Key Infrastructure talents in the industry. I would like each member to introduce themselves with their Name, Title, organization, and how long they have been in the industry.

Time 1:30
Each Panelist template (45–60s each):
"[Name] and [Title] at [Organization, and how long you have been in the industry.

End Time 4:30 minutes after start

PKI Consortium

Questions, Statement, or Poll Assignments

Question, Statement, or Poll	CB	CH	MP	GP
Opening Welcome – Panelist to introduce themselves	X	X	X	X
Show LinkedIn Poll "The move to PQC will be the hardest transition in Cyber Security history." Show Poll, then Poll Audience, Then ask one panelist why?	X	X		
The Poll was significantly skewed to large organizations believing the answer to be Yes. Can you explain why that might be the case?			X	
Do you think the organizations that said No are underestimating the difficulty of the transition to PQC? Why?				X
How does a Certificate Lifecycle Management Solutions play a significant role in the transition to Post Quantum Cryptography? Can you please explain?		X		
How long will it take before quantum computers can break an RSA-2048 bit key? Show Poll, then ask Audience Members do they generally Agree with the results by a show of hands.	X			
How long will it take large organizations to successfully transition to Post-Quantum Cryptography (PQC)? Show Poll, then ask Audience Members do they generally Agree with the results.	X			
2.825-year gap. Do we have a potential problem? What about Harvest Now and Decrypt Later?	X			
Do you agree in general with these timelines? How exactly can a CLM help accelerate the transition to Post Quantum Cryptography?			X	

PKI Consortium

Questions, Statement, or Poll Assignments

Question, Statement, or Poll	CB	CH	MP	GP
Do organizations have the correct tools, skills and budget to meet these goals today? Show Poll Audience and a show of hands to the audience.	X			
Where are most large enterprises really in PQC readiness, and what's holding them back (budget, skills, vendors, standards)? Please explain				X
What are some common things a large organization can do to help accelerate their PQC migration?		X		
Post Quantum Cryptography is becoming a board level issue for many large organizations. What is the best way to report this information to a board.			X	
What are the KPIs the board should be tracking? Are their any other non board level KPIs organizations should be tracking?				X
In general, who owns CLM day-to-day in very large enterprises? What is the best structure you have seen work for a large organization? The worst? What are the problems with the worst? (Optional: What's one RACI pattern that worked?)		X		
Across industries, what are the top three initiatives enterprises are focusing on right now as they prepare for Post-Quantum Cryptography?			X	
What PQC mistake do you keep seeing in large organizations... Potential Fix?				X

Questions, Statement, or Poll Assignments

Question, Statement, or Poll	CB	CH	MP	GP
Lighting Round – Who wants to take it?	X			
What is the biggest blind spot organizations have with their PQC migration plan? What is the best way to resolve?				
Rollback safety: Describe a tested roll-forward/rollback plan when new algos/profiles fail in a given stack (e.g., Java keystores, legacy ADCs, constrained IoT). What was the canary?				
For large organizations, how do you merge Configuration Management Databases, cloud tags, mesh catalogs, and secrets managers into one inventory, and what's your confidence-scoring recipe?				
Why is Crypto Agility important for Post Quantum Cryptography? How much overlap is there with other problem sets that are adjacent to PQC?				
Audience Questions				
1.				
2.				
3.				

PKI Consortium

Thanks

Tuesday, 29 October 2025

PKI Consortium