Short-Lived Certificates Are Approaching: Prepare for 47-Day SSL/TLS Certificates

Lim Huck Hai, Managing Partner - Consulting, Baker Tilly

5 Aug 2025

bakertilly

Introduction

The CA/Browser voted to officially shorten the lifetime of TLS certificates down to 47 days.

Apple, Google, Microsoft and Mozilla all voted YES

Shortening will be done through phases with the final goal of reaching 47 days by 15 March 2029.

Involvement in PKI since 90s

From left to right: Lim Huck Hai, Partner In-Charge of IRM for Malaysia; Stuart Campbell, Partner In-Charge of IRM Practice for US, Dato Ab Halim, PIC of Assurance for Malaysia, Kevin Coleman, IRM Partner, Stratton Sclavos, VeriSign CEO, Tan Sri Dato' Dr Othman Yeop Abdullah, Executive Chairman, MDC, Sarina Karim, CEO, MSC Venture Corporation, Redza Rafiq Abdul Razak, Manager, MDC, Quentin Gallivan, Executive VP, VeriSign at Verisign Inc. at Mountain View, California.

MSC Trustgate.com Sdn Bhd,

a licensed Certification Authority and an Affiliate of

VeriSign Trust Network

by Lim Huck Hai

KPMG IRM has charted another significant milestone in its Secure Electronic Commerce practice after being awarded a large contract to setup the second licensed Certification Authority (CA) for MSC Trustgate.com Sdn Bhd (formerly known as MSC Cybersign International Sdn Bhd). MSC Trustgate.com (or Trustgate) is a subsidiary of Multimedia Development Corporation ("MDC"), a government-backed corporation entrusted to manage and catalyse the development of Malaysia's high-tech Multimedia Super Corridor.

Our win in this public tender (competing against more than 10 local and international players, including Big 5s) was attributed to its extensive knowledge and experience in implementing CA both locally and internationally. Led by Dato' Halim Mohyiddin, Lim Huck Hai and Kevin Coleman and supported by around 20 IRM consultants, this prestigious turn-key project enables MSC Trustgate.com to issue legally binding digital certificates. Digital certificates allow the parties in an Internet-based transaction to verify each other's identity, making the transaction more secure.

Continued on page 3

KPMG worked with a number of technology partners including VeriSign, CISCO and Sun Microsystems in delivering a PKI solution to Trustgate. VeriSign, being the prime partner and a shareholder of Trustgate, is a world-class Public Key Infrastructure (PKI) solution provider as well as a leading public CA operator that is well respected for its market share of the PKI playing field. Both KPMG and VeriSign have leveraged on the collective knowledge and real world experience in defining a PKI framework and architecture, and in implementing a public PKI solution.

From left to right: : Sarina Karim, Kevin Coleman, Tan Sri Dato' Dr Othman Yeop Abdullah, Dato' Ab Halim, Lim Huck Hai during the contract signing in VeriSign Head Office at Mountain View, California

https://www.linkedin.com/in/huckhai-lim-847234a

Malaysian Communications And Multimedia Commission (MCMC) | Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) - List of Qualified Auditors

- FCA (ICAEW), CFE, CISA, CRISC, CISM, CGEIT, FCPA (CPA Aust), CA (Mal), CPA (Mal), CMIIA, ISO27001 Lead Auditor, ISO37001 Snr Lead Implementer, PECB Certified Trainer
- Bachelor of Economics (Accounting & Computer Science), Monash University, Australia
- Graduate Diploma in Business Law, Staffordshire University, UK
- President, ACFE – Malaysia Chapter, Member, ICAEW Tech Faculty Board

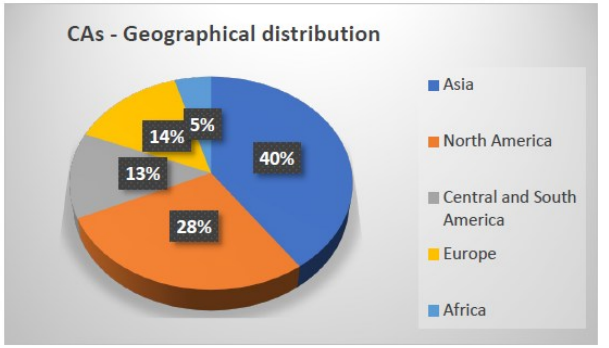
"Securing **E-Commerce Through PKI "** Seminar

KPMG IRM and MSC Trustgate.com Sdn Bhd jointly organized a public seminar entitled "Securing E-Commerce Through PKI" on 23rd June 2000 at Sheraton Imperial Hotel, Kuala Lumpur. The speakers were Lim Huck Hai (IRM Partner of KPMG Malaysia), Kevin Coleman (IRM Partner of KPMG San Francisco) and En Badrul Hisham Mahari (CEO of MSC Trustgate.com Sdn Bhd).

Badrul presented to the audience the role, importance, liability allocation and regulation of a Certification Authority ("CA") in the context of our Malaysian Digital Signature Act 1997. While Kevin discussed the latest developments in security standards and techniques for online transaction such as Secure Electronic Transaction (SET), Identrus and Wireless Application Protocol (WAP), Huck Hai shared from his wealth of experience on Web Assurance Service. Together with the demonstration through the display of a secured WebTrust seal, Huck Hai, presented on how this assurance can be provided by an independent and objective public accountant. This seminar was well accepted by the audience, mostly senior executives from the banking sector and capital market sectors.

By Lim Huck Hai

A Trustworthy CA…



WebTrust was developed jointly by the AICPA and CICA in 1997 to increase consumer confidence with the internet/ecommerce.

- Version 1.0 Baseline assurance service developed in 2000
- 2002 became part of trusted Microsoft Root Program
- March 2006 WebTrust became an integral part of the CA/Browser Forum and was included in triannual in-person events and committees.

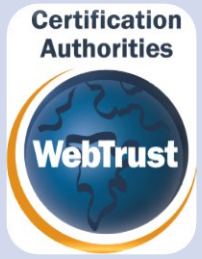
Once all the browsers became part of the CA/B Forum, WebTrust requirements were incorporated into all trusted root programs.

Today, the ownership of the WebTrust program and licensing sits with CPA Canada.

The WebTrust Task Force (WTTF) was created to support CPA Canada's WebTrust for Certification Authorities Program.

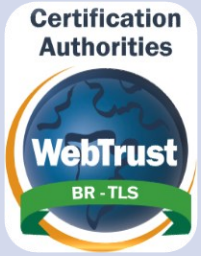
CPA Canada runs the WTTF with a team of global practitioners who provide advice.

WebTrust Seals



WebTrust for Certification Authority (WTCA)

seal for digital certificates for secure online transactions and communications



BR TLS

Cryptographic protocols used to secure communication over the internet

Network Security

CA site has implemented appropriate measures to safeguard its network and protect sensitive information from security threats

Code Signing

Process of digitally signing software or code to verify its authenticity and integrity. Seal demonstrates commitment to security and trustworthiness in the CS process

Extended Validation

Process used to authenticate and verify the identity of a website owner before issues an SSL certificate

Secure/ Multipurpose Internet Mail Extensions (S/MIME)

Protocol for securing email messages using encryption and digital signatures

Registration Authority

RA responsible for verifying the identity of certificate applicants and processing certificate requests before they are issued by the CA

Mark Certificate

Digital certificate that allows organizations and individuals to display a trademarked logo in the list view of recipients' email inboxes next to the sender field

Qualified Seal

New seal(s) created by CPA Canada after consultation with WTTF and Browsers. Rolled out in 2023

CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

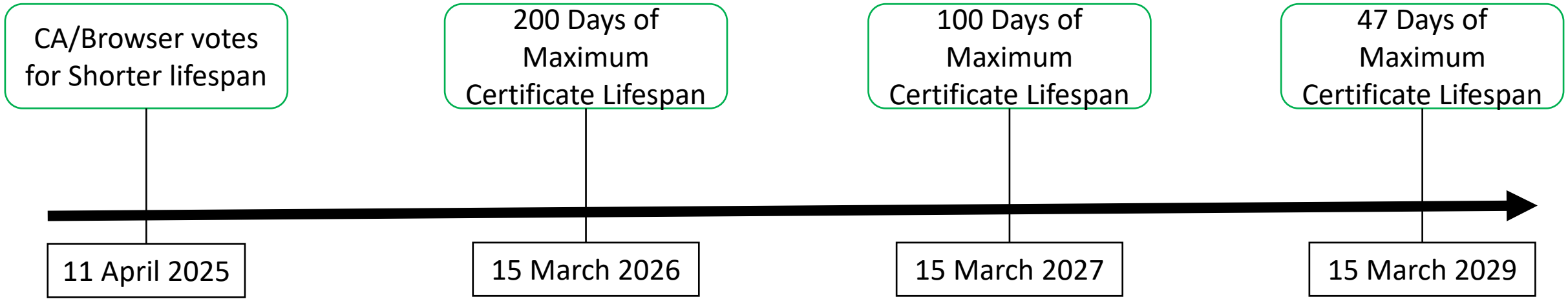
LATEST TLS Baseline Version 2.9

Principle 1: TLS Baseline Requirements Business Practices Disclosure	Principle 2: TLS Service Integrity	Principle 3: CA Environmental Security
• TLS Certificate Public Disclosure • TLS Certificate practice, policies and procedures • CP/CPS • Public Access to CP/CPS • CA DNS Records • Repository Access	• Key Generation Ceremonies • Certificate Content and Profile • Subscriber and Subordinate CA Private Keys • Certificate Issuance by Root CA • Certificate Revocation and Status Checking • Employees and Third Parties • Data Records • Audit	• Security Program • Risk Assessment • Security Plan • Business Continuity Plan • Certificate Management Process • Physical and Logical Access • System Development and Maintenance • System Access • Personnel Practices • Audit Logs • Private Key Protection

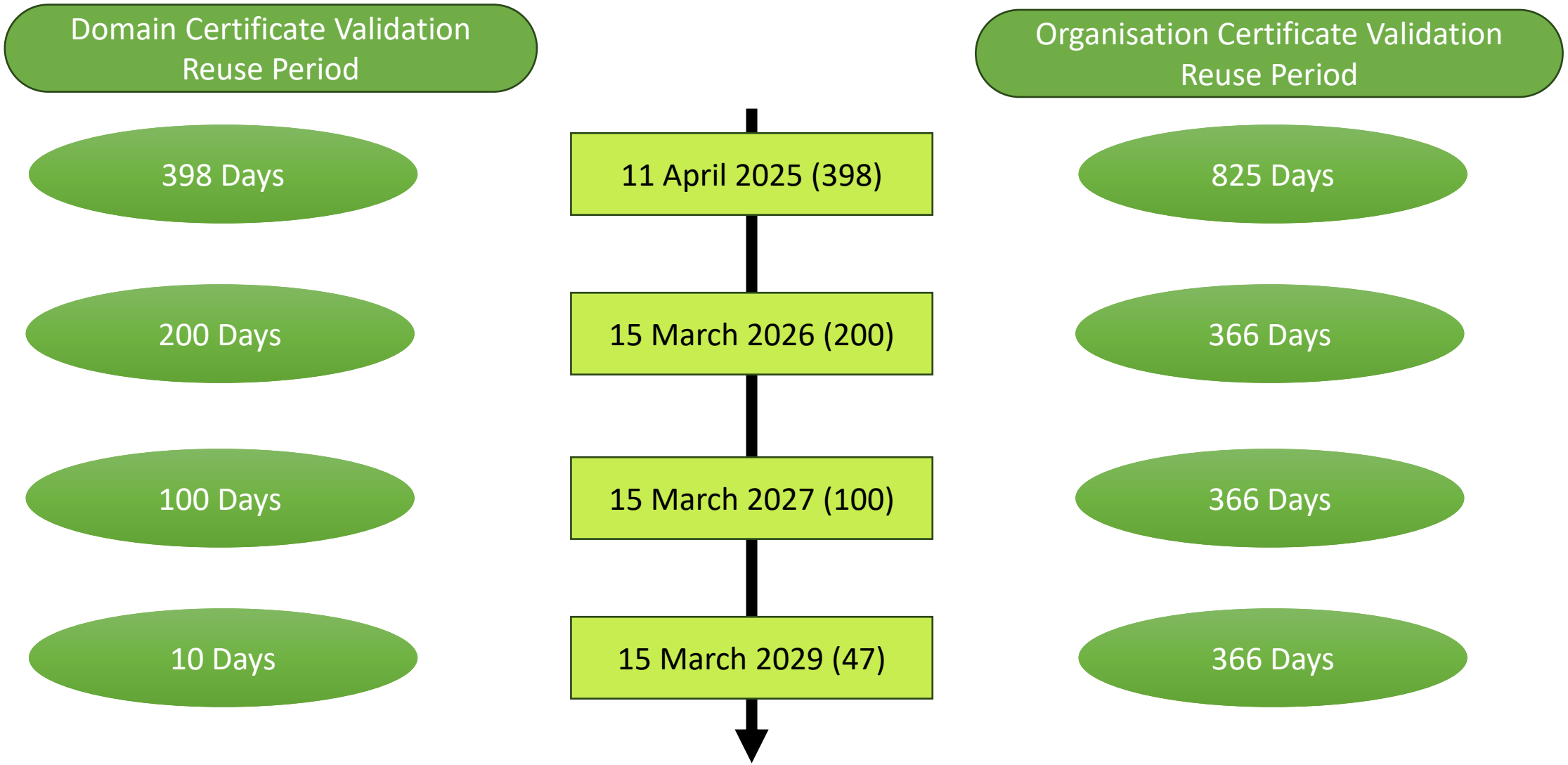
LATEST EV TLS Version 2.0.1

Principle 1: Extended Validation TLS Business Practices Disclosure	Principle 2: Extended Validation TLS Service Integrity
• EV TLS Certificate practices, policies, and procedures disclosure • Revocation Guidelines • Reporting Mechanisms • CP/CPS Public Access	• Key Generation Ceremonies • EV TLS subscriber and certificate content profile • EV TLS certificate request requirements • Information Verification Requirements • Certificate Revocation and Status Checking • Employees and Third Parties • Data Records • Audit and Legal

The Shortening Timeline



The Shortening Timeline



Why Shortening?

Major browsers and industry bodies are enforcing these changes to improve security

Enhanced Security: Short-lived certificates reduce the time window for exploiting compromised keys

Better Hygiene: Frequent renewals eliminate forgotten or stale certificates

Limiting Outdated Cryptographic Standards: Short lifespans prevent long-term reliance on obsolete or vulnerable ciphers

Modern Security Alignment: Supports zero trust and continuous validation principles

Preparations – Automated Issuance

As industry mandates reduce certificate lifespans, IT teams face a significant increase in manual workload - up to 6x more certificate renewals annually.

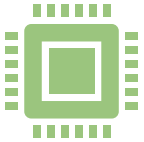
An effective certificate automation platform is key to relieve IT teams of this burden and reduce the risk of outages.

Automated Certificate Management Environment (ACME) is a popular protocol for automating certificate renewals that is supported by many server technologies.

What is Certificate Automation?

Automates the Full Certificate Lifecycle:
From **Certificate Signing Request (CSR)** generation to **issuance**, **installation**, **renewal**, and **revocation**—automation streamlines every step without manual intervention.

Scalable Management Across Environments:
Designed to handle **hundreds to thousands** of certificates across cloud, on-premises, and hybrid environments efficiently.



Minimizes Human Error & Expiry Risks:
Automated monitoring and renewal reduce the chances of **service disruptions** due to expired certificates.

Centralized Control & Visibility:
Gain full visibility into your certificate landscape with a **centralized dashboard**, enabling better compliance and security oversight.

Supports Modern Protocols & Integration:
Leverages industry protocols like **ACME**, **EST (Enrolment over Secure Transport)**, and **REST APIs** for seamless integration into DevOps pipelines and enterprise infrastructure.

Why Automation Matters

Shorter Certificate Lifespans = More Frequent Renewals	• Industry shifts require organizations to renew certificates more frequently, multiplying operational workload.
Manual Processes Are Error-Prone and Costly	• Human-managed renewals often lead to missed expirations, resulting in service outages, compliance violations, and brand damage. These risks scale rapidly in larger environments.
Automation Prevents Downtime and Security Gaps	• By automatically renewing and installing certificates, organizations ensure uninterrupted service availability, minimized administrative effort, and reduced security exposure.
Improved Operational Efficiency	• Automation frees up IT teams to focus on strategic initiatives rather than repetitive certificate tasks. It also ensures policy enforcement, standardized configurations, and audit-readiness.

The cost of Certificate Mismanagement

- **Downtime from expired certificates**
  Forgotten or missed renewals can lead to outages in applications, websites, or services.
- **Revocation**
  Revoked certificates can result in service disruptions, emergency fixes, and damage to business credibility—costing time, money, and trust.
- **Misissuance**
  Occurs when a Certificate Authority (CA) improperly issues a certificate, leading to response delays, financial penalties, and loss of customer trust in data protection

Preparing for the Post-Quantum Cryptography (PQC) Era

Quantum Threat is Real	Quantum computers will eventually break RSA and ECC algorithms used in today's PKI.
NIST Standardization Underway	Algorithms like CRYSTALS-Kyber and Dilithium are being selected as quantum-safe standards.
Why Act Now	Organizations must prepare for crypto-agility to transition to quantum-safe algorithms when mandated.
Certificate Automation Enables PQC Readiness	Automates rollout of new certs using quantum-safe algorithms across large infrastructures.

Why become Crypto-Agile?

Post-Quantum Readiness

- Crypto-agile systems can be upgraded to stronger or quantum-resistant algorithms without significant re-architecture.

Regulatory and Compliance Changes

- Crypto-agility ensures continued compliance with minimal business disruption.

Incident Response

- Crypto-agility enables quick key rotation or algorithm change, reducing exposure time and limiting damage.

Vendor Interoperability

- Crypto-agile systems can easily adapt to different standards and requirements across global supply chains and partners.

Improved Risk Management

- Crypto-agility helps with resilience planning to reduce long-term security and operational risk.

Comprehensive Certificate Lifecycle Management

- Crypto-agility helps deliver enterprise certificate lifecycle automation.

Summary

TLS Certificate Lifetimes and of CA-validated information are shrinking down to **47 days** in phases by 2029

Automated Certificate Management is essential to ensure uptime, compliance, and scalability in increasingly dynamic environments.

Organizations must build crypto-agility today to ensure smooth migration to quantum-safe cryptography **(PQC)**

The Quantum Threat

• Background

- At a time when the world is grappling with cybersecurity issues daily, the arrival of Quantum computers presents a unique challenges. Quantum computers are based on the nature of quantum entanglement and superposition rather than the on/off states of switches (i.e. bits) in Classical computers. This unique attribute means that Quantum computers will render today's cryptographic technologies obsolete.
- Since cryptography formed the security bedrock of all digital activities today, day-to-day functions such as financial transactions, digital identification as used in ID cards and passports, data protection, blockchain transactions, etc., would be significantly impacted: because the cryptographic algorithms would become unsafe overnight.

• Quantum Supremacy

- The race to "quantum supremacy" has compressed the development timeframe of Quantum computers. The availability of Quantum computing capability in the Cloud also means that this technology will be widely accessible when it becomes available, for both legitimate purposes and by bad actors. While there are still uncertainties over when this "Q-Day" will arrive, breakthroughs in Quantum research reported in 2024 suggest that this transformational technology is fast becoming a reality. Technology advancement aside, hackers are already adopting a "grab and wait" strategy by stealing the data now and decrypting once they can get hold of the cracking tools. These developments inevitably complicate the Quantum Threat.

- *…… the transition to post-quantum encryption algorithms is as much dependent on the development of such algorithms as it is on their adoption. While the former is already ongoing, planning for the latter remains in its infancy.* ***We must prepare for it now to protect the confidentiality of data that already exists today and remains sensitive in the future****.*

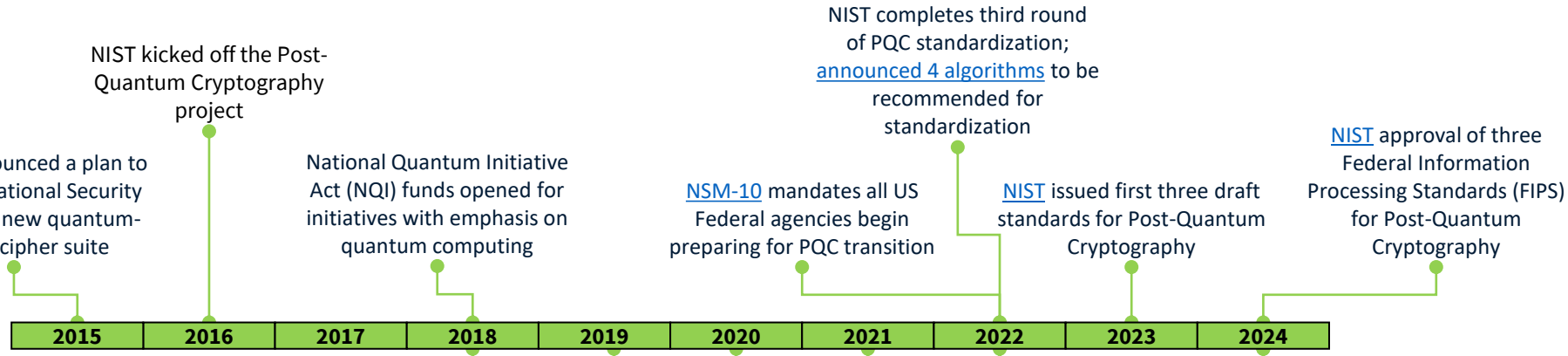
- *Alejandro Mayorkas*

Secretary of United States Homeland Security

Response to the Quantum Threat

1994
Shor's Algorithm Published

1996
Grover's Algorithm Published



2022: GSMA formed the Post-Quantum Telco Network Taskforce to help define policy, regulation and operator business processes for the telecommunications industry

2024: Banco Santander announced development of a Cryptography Bill of Materials to dissect and understand the components of their software, providing valuable insight into their vulnerability to quantum attack.

2024: HSBC announced participation in commercial quantum-secured metro network, connecting two UK sites using Quantum Key Distribution (QKD)

2024: Apple announced introduction of post-quantum cryptographic protocol PQ3 to enable quantum-secure messaging

2024: Google announced adoption of quantum-resistant encryption for Chrome for safe web browsing

Quantum Economic Development Consortium formed as a US based collaboration of academia, government, and industry stakeholders

NIST published whitepaper "Getting Ready for Post-Quantum Cryptography"

UK National Cybers Security Centre published whitepaper on mitigating threat to cryptography from development in Quantum Computing

Singapore to build National Quantum-Safe Network that provides robust cybersecurity for critical infrastructure

US Department of Homeland Security published roadmap on transition to post-quantum cryptography

EU encourages Member States to develop a comprehensive strategy for the adoption of Post-Quantum Cryptography

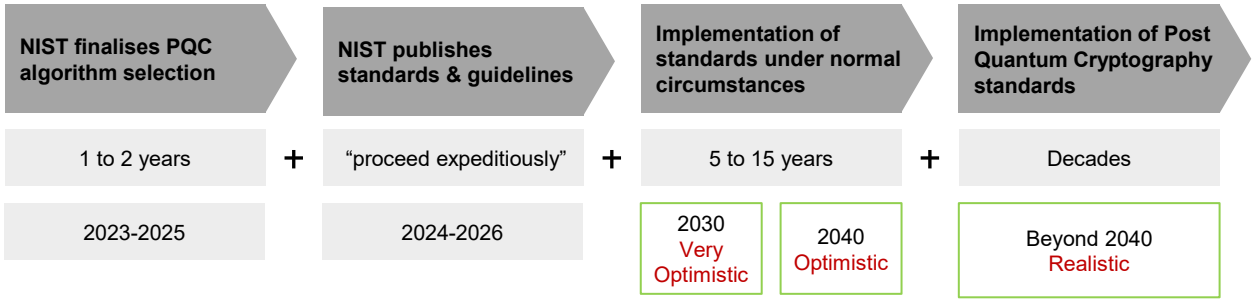
Monetary Authority of Singapore published advisory on addressing cybersecurity risks associated with Quantum computing

Governments and Industries have taken steps to secure critical infrastructure against the Quantum Risk

Need for a Robust Business Plan

Initial studies and research by leading institutions indicate that significant time would be needed for the adoption and transition to quantum-safe cryptographic protocols, even if standards are available by 2025. Rapid transition to new information security technologies, tools and methodologies is unrealistic given the extent of global systems connectivity in many sectors, such as financial services, civil aviation, telecommunication, etc. Significant infrastructural, cultural and procedural change will be needed, as well as funding for such initiatives. Transformation on this scale takes time, as indicated by NIST's own projections illustrated below.

Given the technical and operational complexities, the length of time needed, and the extent of coordination on both National and global level, it is essential for Malaysia to develop a robust business plan to support the migration to a quantum-safe technology infrastructure for both public and private sector participants.



> *…… Algorithm selection is expected to be completed in the next year or two, and work on standards and implementation guidelines will proceed expeditiously …* ***in the best case, 5 to 15 or more years will elapse*** *… before a full implementation of those standards is completed. Unfortunately, the implementation of post-quantum public-key standards is likely to be more problematic … it may be decades before the community replaces most of the vulnerable public-key systems currently in use …*

source: NIST's 28 April 2021 publication, Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms

Proposed Business Plan: Strategic **Success Factors**

The success of the PQC transition process will be dependent on many interconnected factors. The following strategic factors are key to ensuring a successful outcome:

Critical Infrastructure

Priority given to ensuring government and critical infrastructure systems are upgraded to support PQC.

Pilot Projects Selection

Selection and launch pilot projects to test and refine PQC implementations in real-world scenarios, targeting key industry participants.

International Collaboration

Engage in international collaborations to share knowledge, resources, and best practices in PQC.

Participation in Global Forums

Actively participation in global forums and initiatives focused on quantum computing and PQC.

Monitoring and Evaluation

Establish a framework for continuous monitoring and evaluation of PQC implementations throughout the transition period.

Feedback and Update

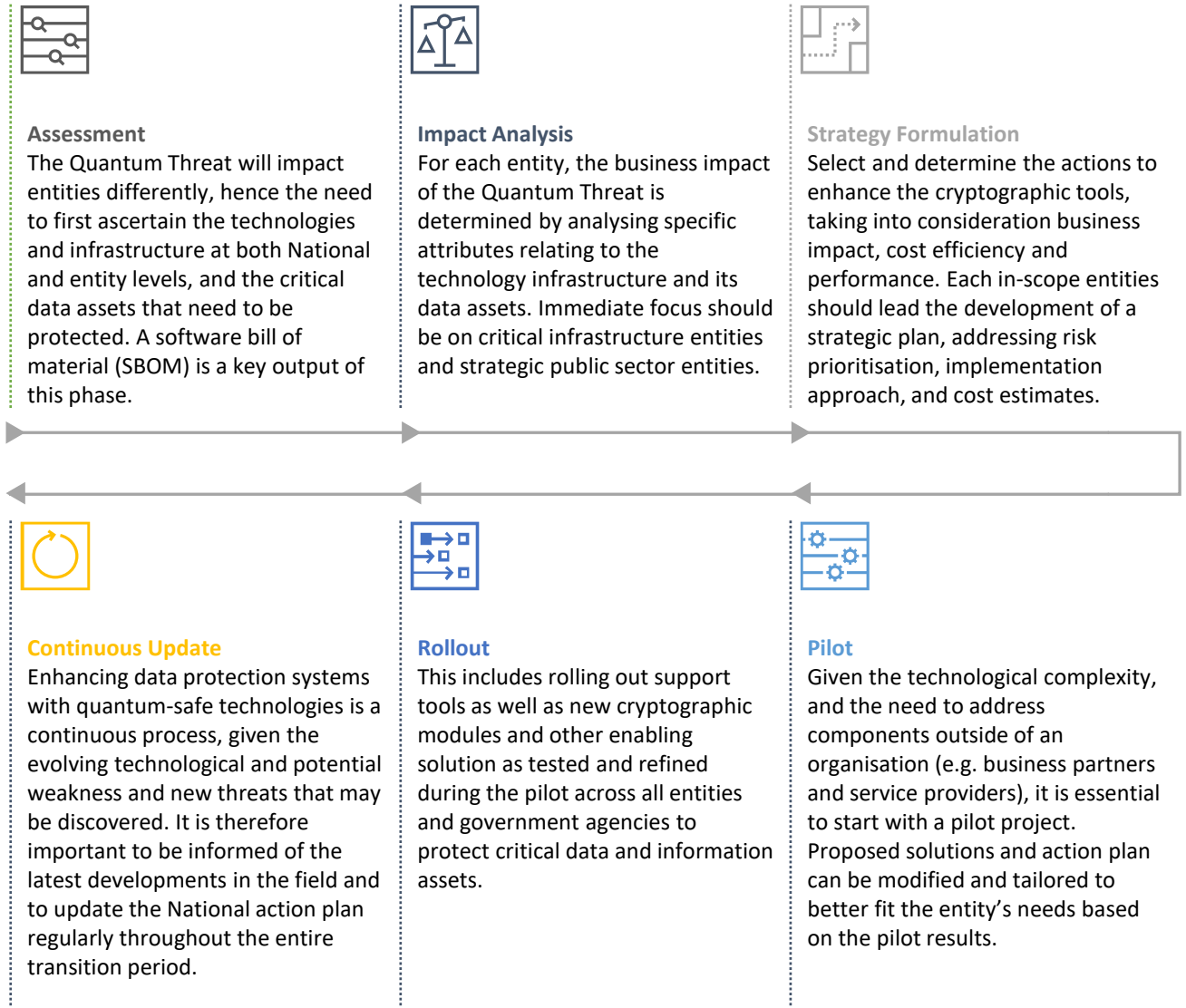
Create mechanisms for feedback and improvement to ensure the effectiveness of PQC strategies.

Cryptographic Agility by Design

Enable organisations to respond to vulnerabilities or risks as these are discovered, including efficient transition to alternative cryptographic schemes

By incorporating these strategic elements into the business plan, Malaysia can proactively address the challenges posed by PQC and ensure the security and resilience of its digital infrastructure.

Phased PQC Transition Process



The complexity of today's technology infrastructure, both at a National level and at entity level, requires a robust and well-planned transition approach. The key objectives are to:

- Identify and create an inventory of all applications, IT (Information Technology) equipment and OT (Operational Technology) equipment within an entity's environment that uses public key cryptography;
- Determine the value of all data within their environment that is currently protected by public key cryptography;
- Create a transition plan for the use of PQC algorithms within an entity's environment, including the testing and adoption of new PQC algorithms as well as the decommissioning of legacy cryptographic algorithms; cryptographic agility should also be considered in the overall design;
- Discuss anticipated PQC requirements with vendors and/or those involved in post-quantum cryptographic research and standards development;
- Educate relevant areas of organisations on the eventual transition to the use of PQC algorithms and provide any necessary training.

Technology aside, the entire transition process will be a lengthy one spanning multiple years, involving a large number of stakeholders, including government agencies, industry regulators, commercial entities, as well as domestic and overseas partners, especially for sectors such as financial services, telecommunication, etc., with extensive global connectivity. A robust **Program Management Office** is critical to the success of the PQC transition process.

Our Offices

BAKER TILLY LHH

Sunway Nexis, C-10-07 and D-13A-06
1, Jalan PJU5/1, Kota Damansara,
47810 Petaling Jaya, Selangor
Malaysia

T:+603 6145 0889
F: +603 6158 9923
M: +60126209868
E: hlim@bakertillyconsulting.com.my

Kuala Lumpur Office

Baker Tilly Tower
Level 10 Tower 1 Avenue 5
Bangsar South City
59200 KualaLumpur
FederalTerritory of KualaLumpur

T:+603 2297 1000
F: +603 2282 9980

www.bakertilly.my

Penang

9-2, 9th Floor, Wisma Penang Garden 42,
Jalan Sultan Ahmad Shah
10050 Georgetown
Penang

T: +604 2279258
F:+604 227 5258

Johor Bahru

38-02, Jalan Sri Pelangi 4 Taman
Pelangi
80400 Johor Bahru Johor

T: +607 332 6925 / 6926
F: +607 3326988

Kota Kinabalu

1-3-1A, 3rdFloor
Block B, Kolam Centre Phase IIJalan
Lintas, Luyang
88300 Kota Kinabalu Sabah

T: +6088233 791
F:+6088 249 691

Batu Pahat

33, Jalan Penjaja 3, Ground Floor
Kim's Park Business Centre 83000 Batu
Pahat
Johor

T: +607 4315403
F:+607 431 4840

Seremban

Level 2, Wisma Sim Du
37, Jalan Dato' Bandar Tunggal 70000
Seremban
Negeri Sembilan

T: +606 762 2518 / 763 8936
F: +606 763 6950

Labuan

1st Floor, U0509
Lazenda Commercial Centre Phase 11,
Jalan Tun Mustapha 87000 Labuan Federal
Territory of Labuan

T: +608 744 0800