Security Summit

Milano 17-18-19 marzo 2026

Sessione

Cripto-agilità e Post-Quantum:

come evolvere la PKI senza perdere controllo

Simone Griffini | Enterprise Account Manager DigiCert
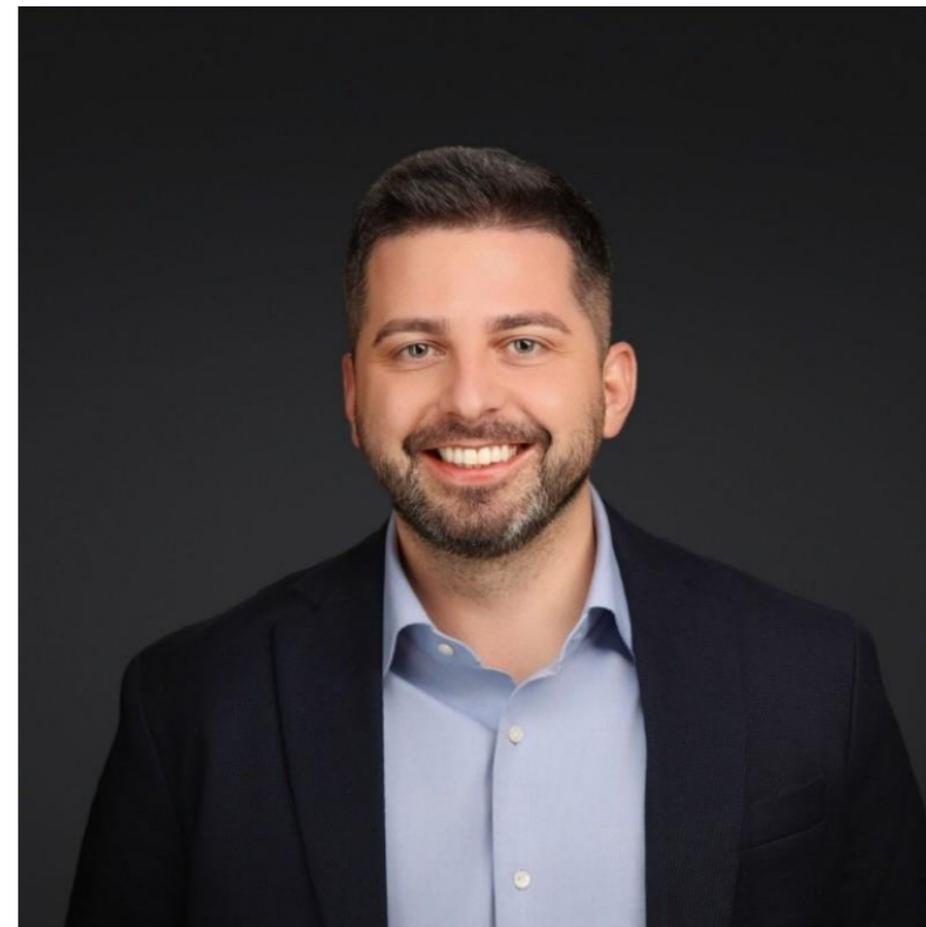
Simone Griffini

Enterprise Account Manager DigiCert per l'Italia

Contatti:

E: Simone.griffini@digicert.com

M +39 331 354 1620 - +44 7533731405

Agenda:

1. Introduzione: DigiCert

2. Iniziative CA/B Forum

3. Riduzione del ciclo di vita dei certificati SSL e dei domini

4. X9 per il settore finanziario

5. Sviluppi della crittografia post-quantum e l'IA

VB VentureBeat

Machine identities outnumber humans 82 to 1 and legacy IAM can't keep up

Dec 30 • By Louis Columbus

BetaNews

Enterprises face increasing challenges with certificate management

Oct 7 • By Ian Barker

BI Business Insider

Google, Microsoft, and others are racing to crack open quantum computing. Here's how their breakthroughs stack up.

Mar 9, 2025 • By Hugh Langley, Riddhi Kanetkar & Katherine Tangalakis-Lippert

siliconANGLE [the voice of enterprise and emerging tech]

TECHFORWARD AWARDS   CLOUD   AI   SECURITY   INFRA   BLOCKCHAIN   BIG DATA   EMERGING TECH

Anthropic reveals first reported 'AI-orchestrated cyber espionage' campaign using Claude

BY DUNCAN RILEY

Riduzione dei certificati digitali e validità di domini

March 15, 2026

March 15, 2027

March 15, 2029

Max validity:
200 days

Max data reuse:
200 days

Max validity:
100 days

Max data reuse:
100 days

Max validity:
47 days

Max data reuse:
10 days
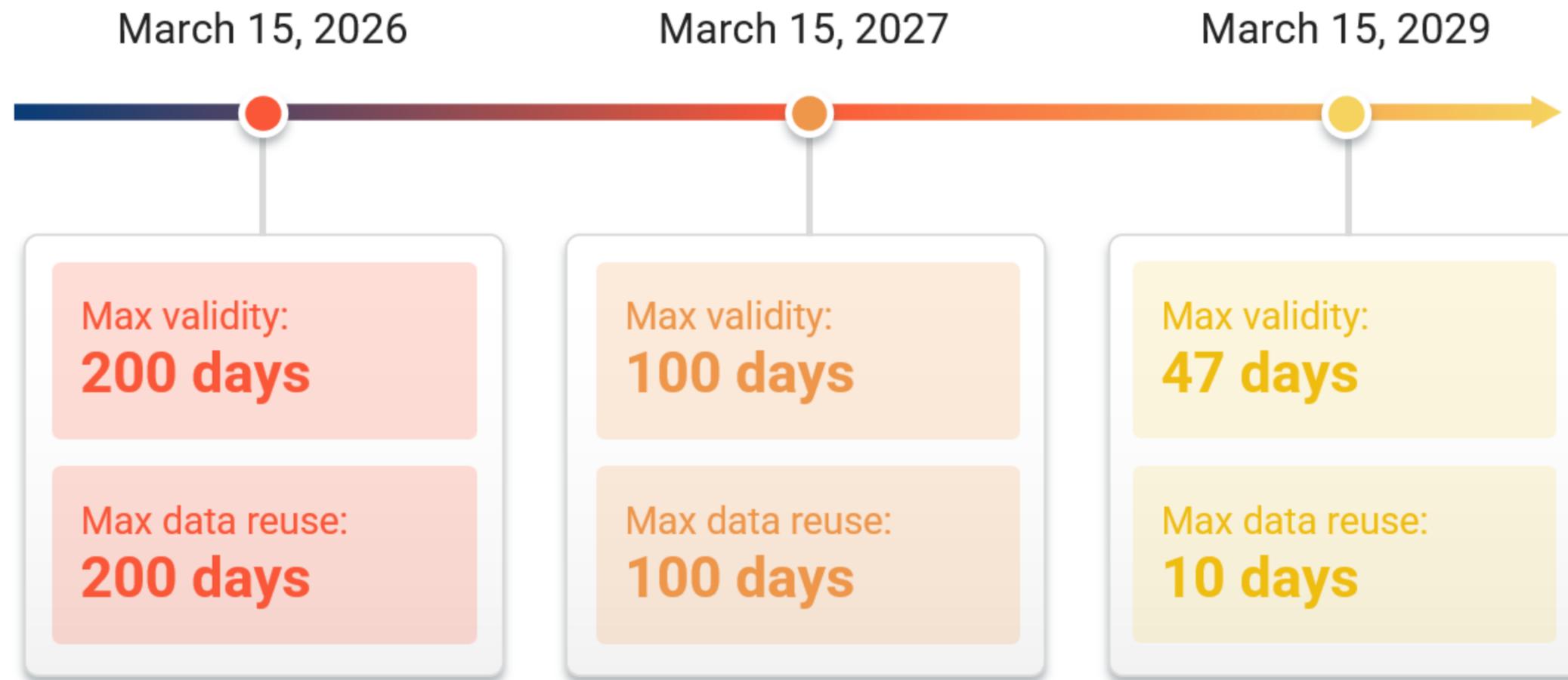
8X more certificates, **40X** more validations will be needed

Massive increase in operational cost, even more outages

Urgent need for PKI Modernization and AUTOMATION

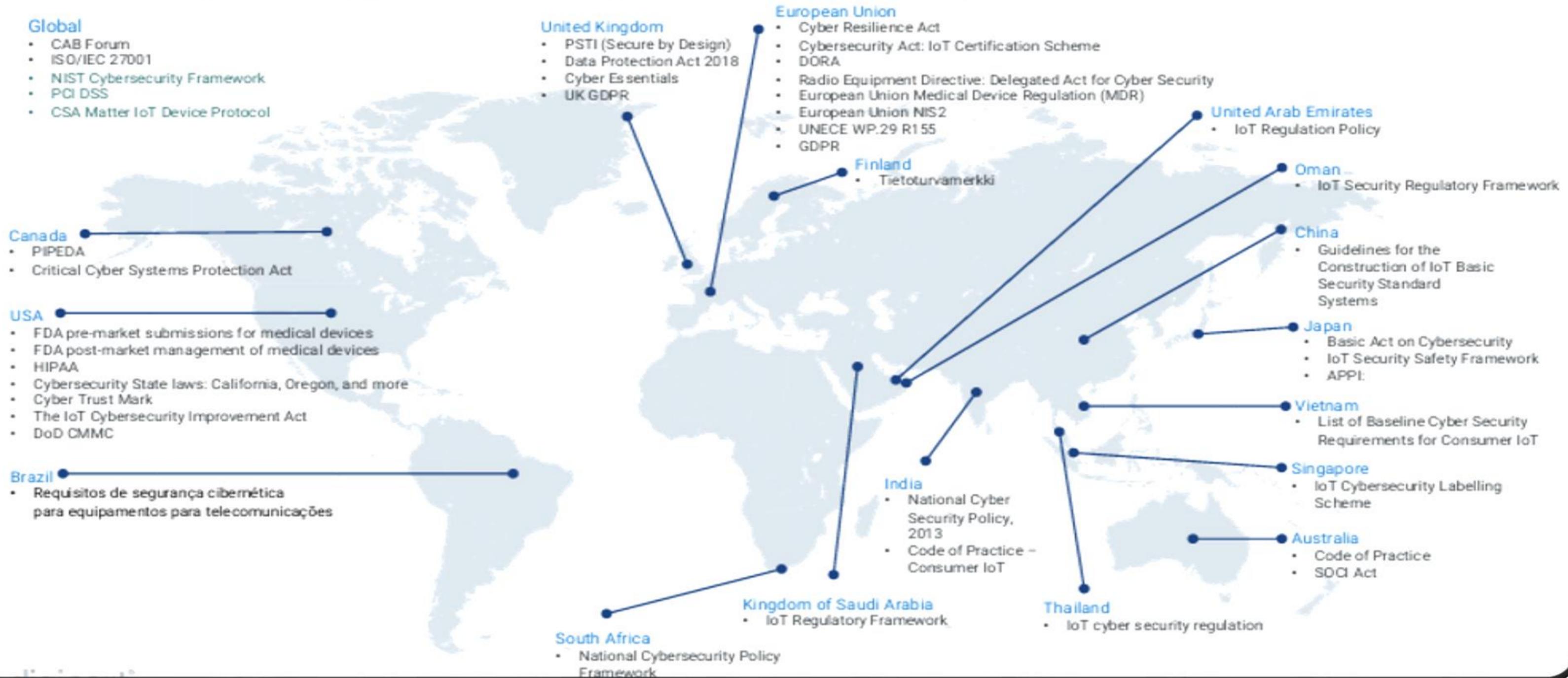# Motivazioni per la riduzione dei certificati SSL/TLS a 47 giorni

Web PKI Challenges

- Evolving standards

- Compromised certificates can live long lives

- Stringent revocation requirements

Automation is imperative

- Humans can't keep up with such lifetimes

- Frequent outages are unacceptable

- Available standards for automation (ACME ARI)

A complex global regulatory map

Global
- CAB Forum
- ISO/IEC 27001
- NIST Cybersecurity Framework
- PCI DSS
- CSA Matter IoT Device Protocol

United Kingdom
- PSTI (Secure by Design)
- Data Protection Act 2018
- Cyber Essentials
- UK GDPR

European Union
- Cyber Resilience Act
- Cybersecurity Act: IoT Certification Scheme
- DORA
- Radio Equipment Directive: Delegated Act for Cyber Security
- European Union Medical Device Regulation (MDR)
- European Union NIS2
- UNECE WP.29 R155
- GDPR

Finland
- Tietoturvamerkki

United Arab Emirates
- IoT Regulation Policy

Oman
- IoT Security Regulatory Framework

Canada
- PIPEDA
- Critical Cyber Systems Protection Act

China
- Guidelines for the Construction of IoT Basic Security Standard Systems

USA
- FDA pre-market submissions for medical devices
- FDA post-market management of medical devices
- HIPAA
- Cybersecurity State laws: California, Oregon, and more
- Cyber Trust Mark
- The IoT Cybersecurity Improvement Act
- DoD CMMC

Japan
- Basic Act on Cybersecurity
- IoT Security Safety Framework
- APPI

Vietnam
- List of Baseline Cyber Security Requirements for Consumer IoT

Brazil
- Requisitos de segurança cibernética para equipamentos para telecomunicações

India
- National Cyber Security Policy, 2013
- Code of Practice – Consumer IoT

Singapore
- IoT Cybersecurity Labelling Scheme

Australia
- Code of Practice
- SOCI Act

Kingdom of Saudi Arabia
- IoT Regulatory Framework

Thailand
- IoT cyber security regulation

South Africa
- National Cybersecurity Policy Framework

Altre iniziative del CAB forum e dei browser

S/MIME

Code Signing

mTLS Certificates Maggio 2026

Mandatory CAA checking

Support for PQC Algorithms

PQC

Code Signing

Adoption of secure cloud signing services

- Shorten validity from 39 months to 460 days. (March 1, 2026)

Chrome is moving to reject TLS certificates configured for client authentication

What Is ASC X9?

Leader in Worldwide Standards for the Financial Services Industry

Mission: To create and maintain US and International standards that improve payments and securities transactions, protect data and facilitate information exchange.

Accredited by ANSI with around 100 member companies
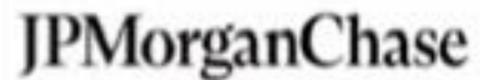
X9 PKI Background

Why create X9 PKI?

- CA/Browser Forum trends incompatible with financial services needs

- Lack of interoperability between disparate Private PKIs

- Around 30 PKI use cases for financial services identified

- No governing body for Financial PKI

- Post-Quantum Cryptography (PQC) readiness and crypto-agility

Financial Industry needed a governing body to manage Financial PKI

- WebTrust for CA auditing standard provides a framework

- Auditing and reporting on CA's control environments and compliance

- Certificate Practice Statement (CPS)

Rischi del Quantum Computing e AI

Innovazioni del Quantum Computing
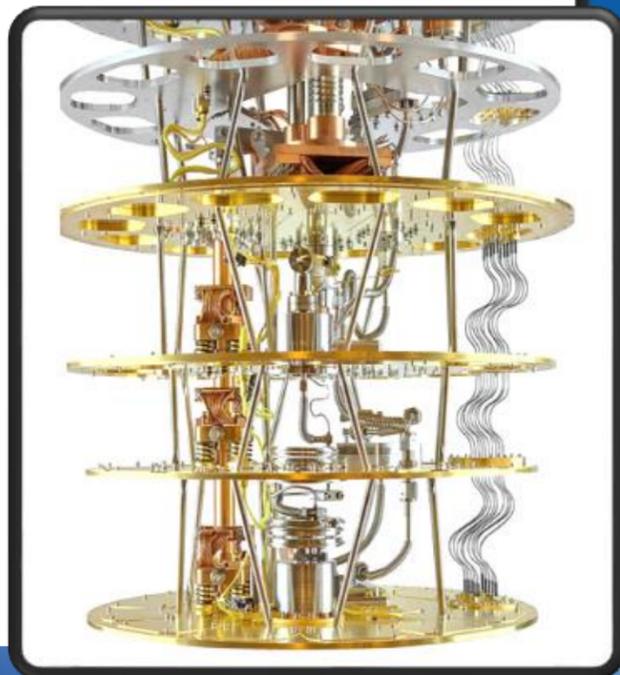
Rischi del Quantum Computing

Stolen Now, Cracked Later

Cyber Warfare

Global Digital Meltdowns

Financial Market Chaos

PKI Complexity Rising Rapidly in Enterprises

Cloud Workloads

aws
ORACLE
A

Servers & Infrastructure

Users & Agents

PKI

Web Presence

Devices

100X
Machine to User Identities

Certificate Management is Becoming More Complex

53%
Organizations lack sufficient PKI staff

256K
Average certificates per organization

AI Agents Will Be Everywhere

Sfide e rischi dei certificati digitali scaduti

MSN

Google starts rolling out fix for Chromecasts after five-day outage

Good news for annoyed Chromecast owners whose devices haven't been working this week: Google is rolling out a fix for affected devices.

1 week ago

CIO

ServiceNow certificate error disrupts operations for hundreds of organizations

The expired MID Server Roo G2 SSL certificate caused connectivity failures across multiple services, including Orchestration, Discovery...

Sep 24, 2024

www.thestack.technology

Expired Certificate crashed $6 trillion Bank of England system

Network configuration, CA and SWIFT issues, and certificate expiration blamed for a series of RTGS outage sthe past year.

Sep 30, 2024

Data Center Knowledge

Windows Azure Cloud Crashed by Expired SSL Certificate

Microsoft suffered a major outage for its Azure storage cloud and other online services after an SSL certificate expired.

May 30, 2024

Clusit

SECURITY SUMMIT

ASTREA

Strategia per una Crittografia post-quantica sicura

Transizione al post quantum computing
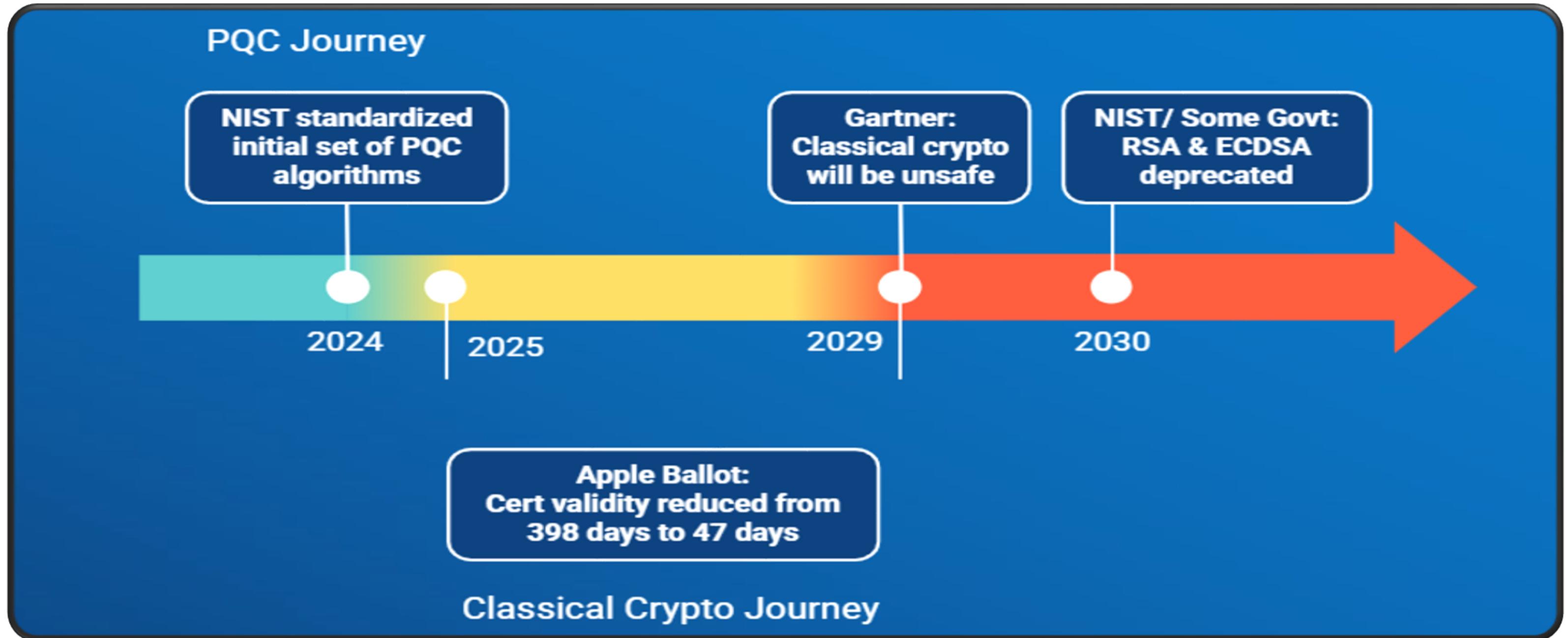
Da dove iniziare per una transizione sicura al PQC?
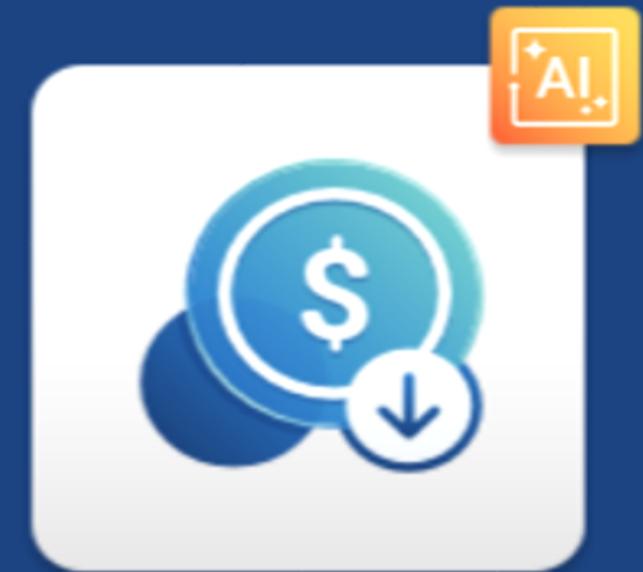
The Intelligent Trust Platform
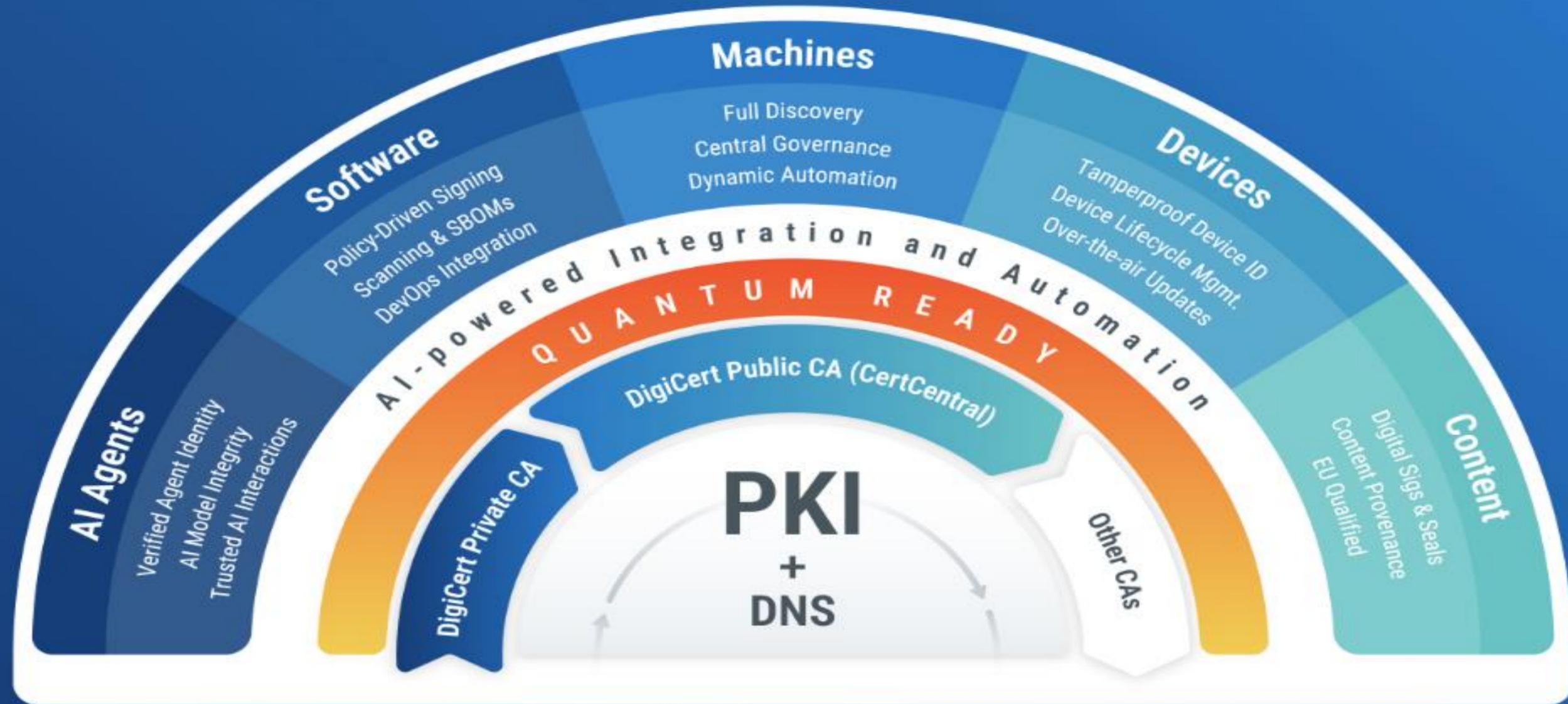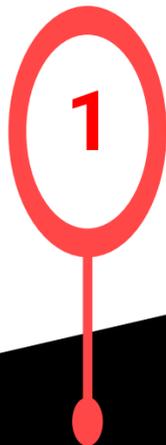
digicert® ONE

Crypto agility model, dove vi trovate?

Comincia da

- **Discover** crypto assets – certificates, SBOM, CBOM...

- **Create test plan & tools - test issuance with DigiCert One Labs**
  - **https://www.digicert.com/digicert-labs**

- **Design for Automation**

1
- Limited visibility
- Manual Processes
- Compliance Failures
- Security Risks
- Outages & Downtime

2 **Visibility**
- Full visibility
- Security Insights
- Alerting & Reporting
- Audit Trails

Control

3
- *Automated renewals*
- *Policy Enforcement*
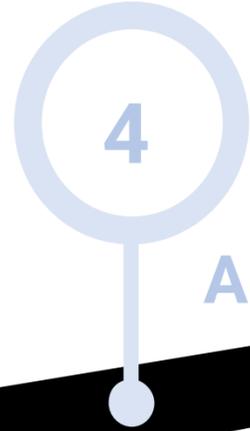- *Self-service Portals*
- *Policies & Best Practices*

4 **Automation**
- Eliminate Outages
- Zero Touch provisioning
- Advanced RBAC
- Seamless Cloud & DevOps integrations
- Reduce need for PKI expertise

Crypto-Agile **5**
- **Rapid Response to threats/incidents**
- **Reduced TTR**
- **Compliant**
- **PQC Ready**
- **Apple-47 day Read**
- **CA & Endpoint Ready**

Vi aspettiamo al nostro booth!!!

Contatti:

E: Simone.griffini@digicert.com

M +39 331 354 1620 - +44 7533731405

Q&A

Contatti:

simone.griffini@digicert.com

Venite a trovarci al nostro Stand!