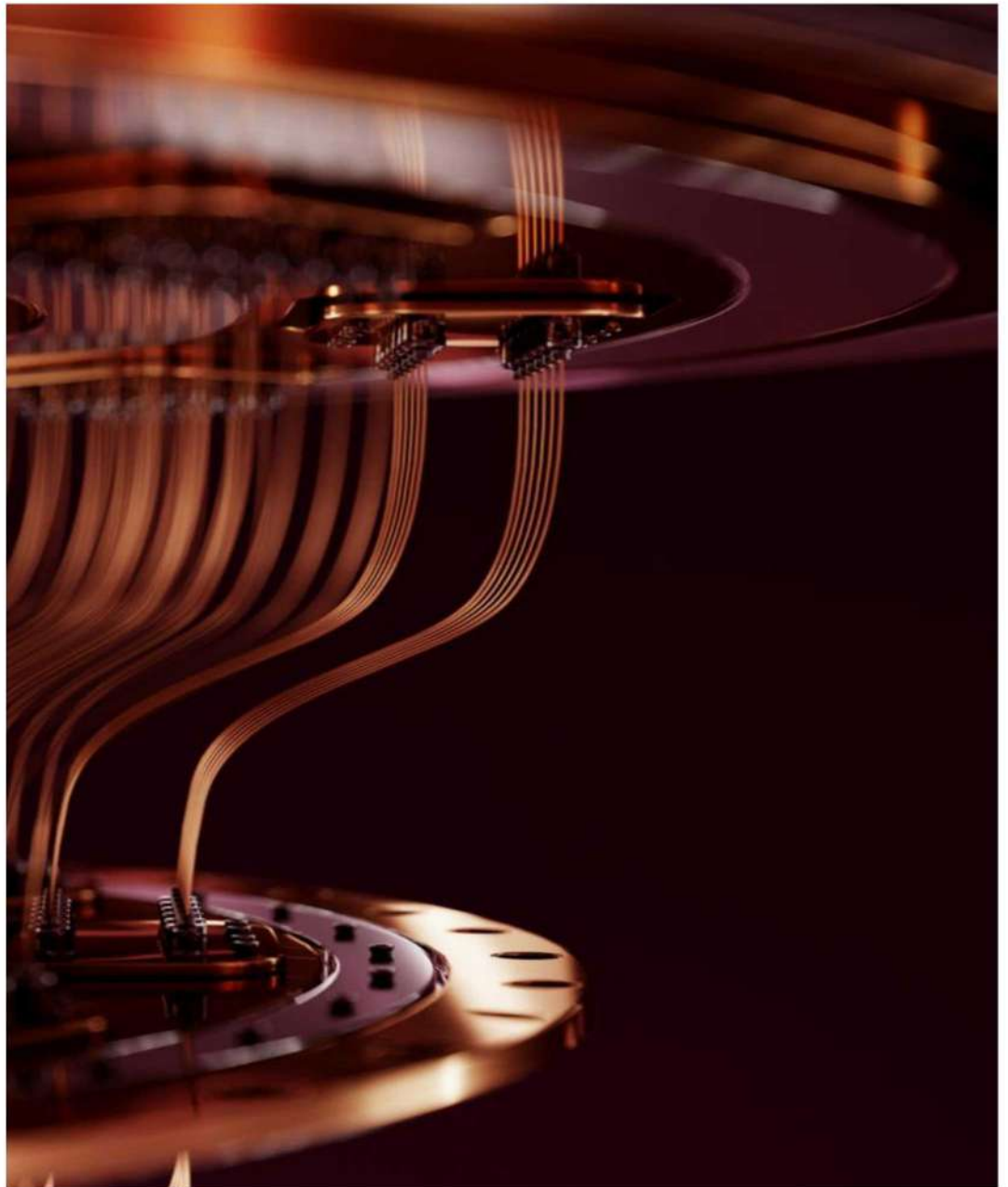


QUANTUM READY PKI

Discover. Assess. Prioritize. Transform.



The Quantum Threat is becoming **real**

Why CISOs and Technology Leaders are Prioritizing PQC Readiness Today

Today's encrypted data will not be safe tomorrow

Quantum computing poses a major threat to current cryptographic systems such as RSA, ECC, and DH, which are secure against classical attacks but vulnerable to quantum ones. Preparing for post-quantum cryptography (PQC) is essential to safeguard systems and applications in the coming decades. Experts also warn of the '**Harvest Now, Decrypt Later (HNDL)**' risk, where encrypted data intercepted today could be harvested and decrypted once quantum computers mature. To ensure long-term confidentiality - especially for governments and organizations managing sensitive citizen data - adopting quantum-resistant cryptography is the only effective path forward.



The Nexus Zero-Disruption PQC Transition Methodology



Crypto-Agility

When the ecosystem is fully mature, orchestrate the transition to Pure PQC across thousands of endpoints with minimal operational disruption

3



The Safe Transition, hybridization

Target your critical assets first. Deploy **Hybrid Certificates** to ensure legacy continuity while securing data against quantum harvesting.

2



The Crypto-Inventory

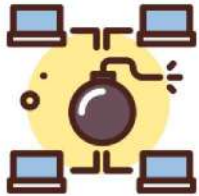
You cannot migrate what you cannot see. Build an accurate **inventory** of every certificate, key, and algorithm hiding in your infrastructure.

- PQC Readiness Score **58/100**
- Protected Workflows **21%**
- RSA/ECC Assets **48,376**
- Long-Life Workflows **245**

1

Why Organizations Choose Nexus for Their PQC Journey

Pure PQC (The "Big Bang")



1 Key / 1 PQC Signature.

High risk of breaking legacy applications, outdated browsers, and constrained IoT devices.

Hybrid (Catalyst) Certificates



2 Keys / 2 Signatures

Zero Disruption. Backward compatible with legacy systems, while instantly protecting against “**Harvest-Now, Decrypt-Later**” attacks.

Composite Certificates



Combined public keys.

Complex standardization, but less flexible than the Hybrid approach. No backward compatibility

PQC support in Certificate Manager

Supported PQC Algorithms

- Encryption: FIPS 203 (ML-KEM or CRYSTALS-Kyber)
- Digital Signing: FIPS 204 (ML-DSA or CRYSTALS-Dilithium) and FIPS 205 (SLH-DSA or SPHINCS+)
- Future-ready: Roadmap support for emerging standards such as FIPS 206 (FN-DSA or Falcon)

Hybridization

- Composite Certificates for dual classical + PQC trust
- Hybrid (Catalyst) Certificates for phased migration

Nexus Certificate Manager

HSM support

- PKCS#11 v3.2 support
- Validated with leading HSM platforms (Thales, Entrust, Utimaco, Eviden, etc)

Quantum-Safe Operations

- Common Criteria EAL4+ certified platform
- Quantum-safe internal communications and OCSP validation

Our Customers



POS Digicert

d-trust.



Certifying Authorities



Central bank of the Philippines

YES BANK

Yes bank - India



Central bank of Oman

BANQUE DE FRANCE
EUROSISTÈME

Central bank of France



Bangladesh Bank

Financial Services



Government of India
Ministry of Communications & Information Technology,
Department of Electronics and Information Technology
Controller Of Certifying Authorities
Controller of Certifying Authorities
(CCA) - India



Ministry of Finance - Thailand

ICT Authority

ICT Authority Kenya



MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER

Ministry of the Interior (France)

Government/ Public

vodafone



etisalat and

Jio

Safaricom

Telecom



الشركة السعودية للكهرباء
Saudi Electricity Company



Energa

e-on

Energy & Utilities

TVS



Electrolux

SIEMENS



Volkswagen

Danfoss

Manufacturing

Let's discuss trusted identities!

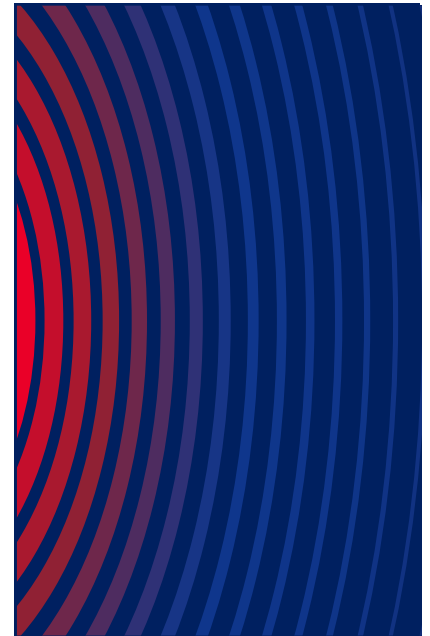
Contact us : nexus.marketing@ingroupe.com



Discover how Nexus solutions are being implemented and used by organizations around the world

Scan the QR code to know more





We secure society by enabling **trusted identities**

Trusted and secure identities made easy - for Workforce, Workplace devices and IoT. One platform, built on PKI, to issue, manage and automate identity across people and things.

COMPANY OVERVIEW

An innovative, fast-growing identity & security company

Nexus secures society by enabling trusted identities for people and things. Our customers are mainly large organizations in industry, finance, telecom, public sector and defense. Nexus is part of the French IN Groupe, which delivers state-of-the-art identity solutions and secure digital services for governments and companies worldwide



Common Criteria
EAL4+



ISO 27001



RL/SE Certified



TISAX

What's in it for you



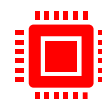
Workforce

Trusted identities for employees, contractors and visitors — issued, used and retired from one platform.



Workplace devices

Certificate-based identities for laptops, printers, network gear and every connected endpoint.

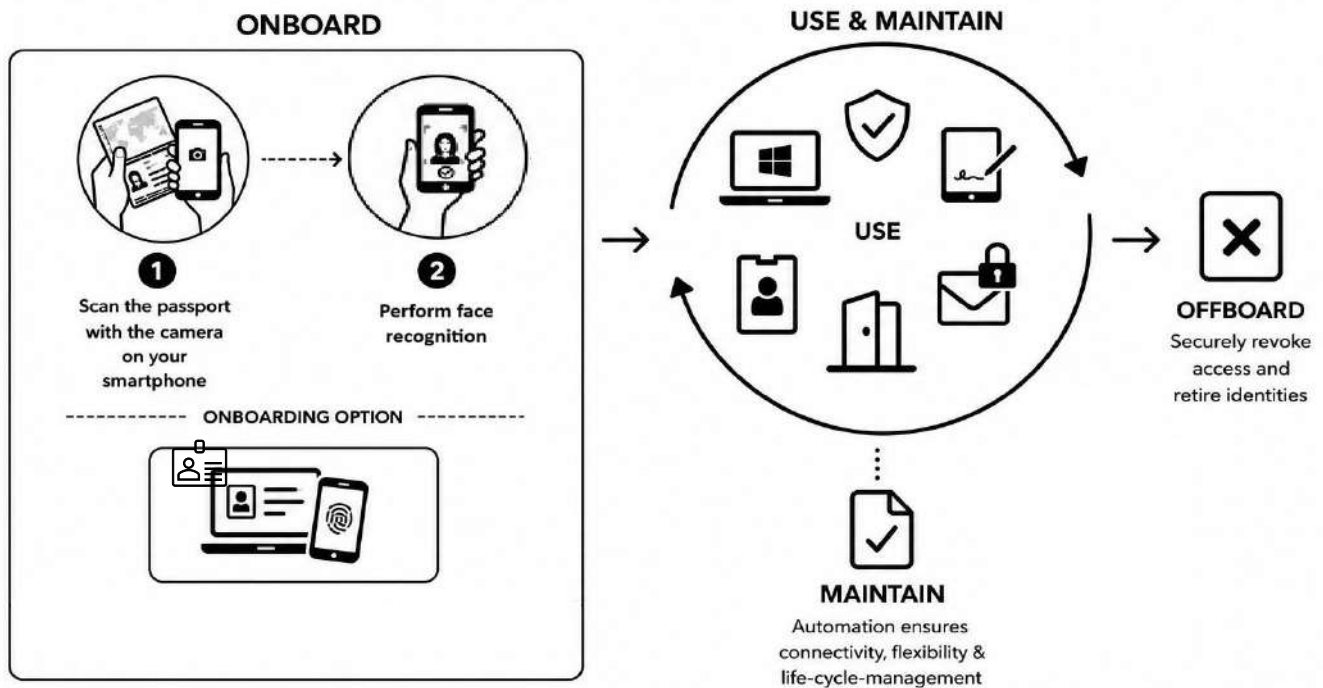


Internet of Things

PKI-based security scaling from small deployments to hundreds of millions of devices.

Enabling trusted identities for the Workforce

Digital transformation and Zero Trust concepts require issuance and management of trusted identities to mitigate risk, ensure regulatory compliance, and restrict access based on business needs. Nexus Smart ID manages the identities of employees, contractors and visitors in one central system - easily integrated into existing corporate directories.



Smart ID for the workforce - the platform with many choices



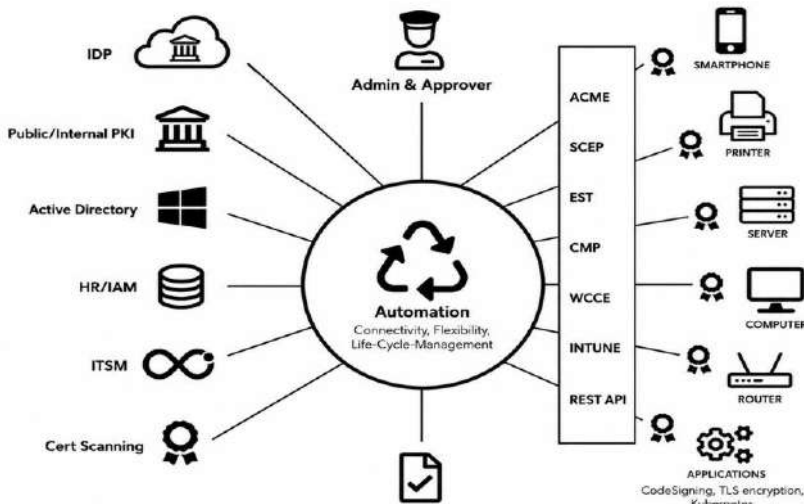
- Strong authentication
- Physical access control
- Visual identification
- Digital signing
- Encryption & privacy
- Email encryption
- Data integrity
- Remote access
- Smart cards
- Virtual smart cards
- Mobile identities
- Full audit trail

Why organizations choose Smart ID

- ✓ Ensure compliance with regulations
- ✓ Simplify on- and offboarding
- ✓ Integrate with standard systems
- ✓ Deploy in the way that suits you
- ✓ Improve everyday usability
- ✓ Trace actions & audit with ease

Enable trusted identities for Workplace devices

Simplify and automate the full lifecycle management of your workplace device identities, by taking advantage of ready-to-use workflows, automation and self-service functionality. Manage trusted identities from external CAs in the same platform where you manage your own PKI.



Workplace Security Benefits

- ✓ Certificate Lifecycle Management (CLM)
- ✓ Crypto-agility
- ✓ Network Trust
- ✓ Asset Visibility
- ✓ Device Authentication
- ✓ Zero Touch Provisioning
- ✓ Certificate Renewal

Enable trust for the Internet Of Things Certificate-based identity, end to end

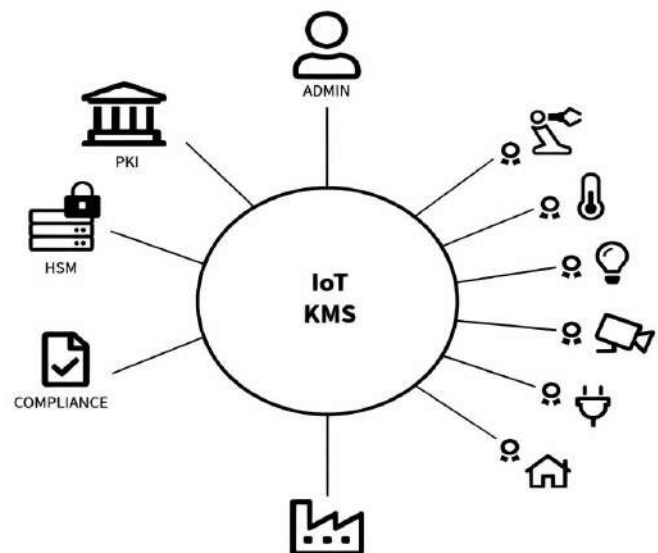
End-to-end cryptographic key lifecycle control, built for utility-scale smart metering. Nexus IoT KMS secures millions of meters with HSM-backed trust, compliance, and automation.

The IoT PKI platform issues certificate-based, cryptographically secure and unforgeable identities that enable:

Strong authentication: Certificate-based authentication ensures that only authorized users, devices or servers can connect to a network or application. Revocation of certificates instantly blocks access in case of compromise or emergency.

Encryption and Privacy: Certificates enable encrypted communication between devices and services for secure transmission of data over TLS.

Integrity: Digitally signed messages based on certificates can be used to prove the origin of data, and to detect manipulation of data. Signed firmware enables secure software updates.



Strong authentication and encryption safeguard high-risk, high-value infrastructure from internal & external threats



Encryption protects data privacy and integrity within complex, third-party dependent IoT networks



Interoperable security solution that can be adapted for millions of devices with varied and complex use-cases



Scalable and future-proof security solution that can be adapted to evolving technology and newer use-cases

Our Customers



POS Digicert

d-trust.



**Certifying
Authorities**



Central bank of the Philippines

YES BANK

Yes bank - India



Central bank of Oman



Central bank of France



Bangladesh Bank

**Financial
Services**



Government of India
Ministry of Communications & Information Technology,
Department of Electronics and Information Technology
Controller Of Certifying Authorities

Controller of Certifying Authorities
(CCA) - India



Ministry of Finance - Thailand



ICT Authority Kenya



Ministry of the Interior (France)

**Government/
Public**



Telecom



**Energy &
Utilities**



Volkswagen



Manufacturing

Let's discuss trusted identities!

Contact us : nexus.marketing@ingroupe.com



Discover how Nexus solutions are being implemented and used by
organizations around the world

Scan the QR code to know more

