PKI Insights

Monitor your critical PKI assets giving insights on its health, posture & performance

360º PKI Monitoring & Posture

CA

Get 24x7 health checks for your CAs ensuring critical PKI services are always available & secure.

SSL End Point

Stay ahead of certificate expirations and misconfigurations with proactive SSL endpoint monitoring.

HSM

Protect the backbone of your cryptographic infrastructure with dedicated HSM monitoring.

Criticality of PKI Health & Posture

Public Key Infrastructure (PKI) sits at the core of digital trust securing identities, communications, and transactions. Yet, PKI can only be relied upon if it is both healthy and well-postured.

PKI Health ensures that core components like **Microsoft CAs**, **Microsoft Cloud PKI**, **SSL endpoints** and **HSMs** are available responsive, and error-free. Without continuous health monitoring, organizations risk service outages, failed authentications, or expired certificates that can disrupt business operations.

PKI Posture reflects the broader security readiness of the environment covering policy compliance, key management practices, certificate lifecycle governance, and configuration integrity. A weak posture may leave room for internal misuse, non-compliance penalties, or exploitation by attackers, even if the infrastructure looks "healthy" in the moment.

PKI Health & Posture in One View

PKI Insights brings together the best of operational monitoring and strategic risk management.

On the health side, it continuously monitors Microsoft CAs / ADCS, Microsoft Cloud PKI, SSL endpoints and HSMs to ensure services are running smoothly, certificates are renewed on time, and potential failures are detected before they cause downtime.

On the posture side, it provides visibility into configuration gaps, policy compliance, and certificate lifecycle risks that could weaken digital trust.

PKI Insights strengthens compliance with Zero Trust, NIST, ISO 27001, and PCI DSS by continuously monitoring CAs, certificates, and HSMs.

Together, PKI health and posture form the foundation of resilient digital trust. Monitoring both in tandem ensures not only uptime today but also security and compliance for tomorrow.

Why ADCS, MS Cloud PKI, SSL Endpoints, and HSMs Must Be Monitored

Microsoft Active Directory Certificate Services (ADCS), SSL/TLS endpoints, MS Cloud PKI and Hardware Security Modules (HSMs) together collectively manage identities, secure communications and protect cryptographic keys that enable business operations. However, these critical components are often poorly monitored, leaving organizations exposed to risks that can compromise confidentiality, integrity and availability.

ADCS is deeply integrated with Active Directory, a compromise here can cascade into domain-wide trust breaches, making it most sensitive assets in the IT landscape.

SSL/TLS endpoints must be continuously tracked to prevent expired, misconfigured, or weak certificates, which can lead to outages, man-in-the-middle attacks, or compliance violations.

HSMs secure the most sensitive cryptographic material. Without visibility into access attempts, operational health, or key usage, even minor misconfigurations can lead to key compromise.

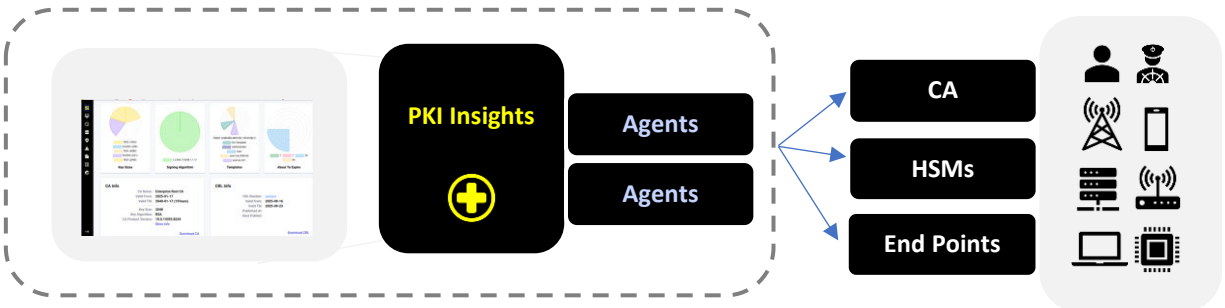
PKI Insights Coverage

Governance and Best Practices: Empower your PKI teams to **review, audit** and **optimize** ADCS operations against industry standards such as **NIST, ISO, WebTrust, PCI, HIPAA, NAESB and NIS2** ensuring that configurations & policies align with compliance.

Offline and Secure Deployment: PKI Insights runs entirely on-premise, requiring no Internet connection making it ideal for regulated or air-gapped environments where data sovereignty and security isolation are mandatory.

Operational Resilience: Improve uptime, availability, and recoverability of your PKI and HSM infrastructure through continuous health checks misconfiguration detection, and early warning alerts ensuring your trust infrastructure remains secure and audit-ready.

Centralized Visibility: Gain real-time insights across all Certificate Authorities templates and issued certificates. PKI Insights transforms fragmented data into clear dashboards and actionable intelligence reducing investigation time and improving control.



PKI Insights - Core Features

Get 360° PKI Health & Posture

Get an overall health of your ADCS PKI, Microsoft Cloud PKI, SSL end Points & HSM by:

- Detecting anomalies
- Accessing data for all CAs from one dashboard
- Filtering data via searchable portal
- Get stats on certs, failures, templates, up time
- Follows CA/B Forum guidelines for SSL certs

Detection of ADCS/Microsoft CA Exploits

PKI Insights helps prevent real-world ADCS attacks by detecting risky conditions linked to **SpecterOps ESC misconfigurations** and exposure to **PetitPotam** NTLM relay attacks.

By flagging these weaknesses early PKI Insights enables administrators to remediate issues before they lead to privilege escalation or domain compromise strengthening both PKI health and security posture.

Analyse Trends

Get stats & insights on multiple PKI areas:

- Alerts, Failed calls
- Failed Calls
- Certificate Expiry, CA Up/Down time
- Certificates issuance (valid, expired)
- Certificate Templates, Revocation
- About to Expire Certificates
- Key Length, Signing Algorithm
- Certificate issuance trends

Proactive Alerts

Get alerts on failures such as:

- CA server / HSM status & health changes
- Template updates & Issuance of High valued certs
- Certificate issued from unpublished templates
- Long lifespans & not following template configs
- Published CRL matching with current issued CRL
- Suspicious certificate issuance
- About to expire certs
- OCSP & CDP uptime & OCSP whitelisting
- Get Daily Summary Reports

HSM Monitoring

PKI Insights keeps a close watch on your Hardware Security Modules (HSMs) the foundation of your cryptographic security. It provides active visibility into the current health and operational status of each HSM ensuring keys remain protected and available when needed. If an HSM becomes unresponsive or fails to operate as expected, PKI Insights immediately raises alerts, allowing administrators to take swift action and prevent service disruptions.

Performs 200+ Certificate Checks

PKI Insight detects a range of X.509 certificate issues covering:

- Signing, Public Key Algorithm & Lengths
- Certs expiry beyond acceptable limits
- Failures coming while issuing certificate
- Detects deviance from RFC 5280

Secure Access & Simple Administration

Authentication is done over SSL/TLS Client authentication giving the most powerful, password less authentication. Supports all major browsers.

Helps administrators to improve ADCS health rating by allowing them to revoke certificate without having to login to the CA.

Cryptographic Agility

PKI Insights supports diverse cryptographic requirements such as:

- RSA (2048, 4096, 8192)
- ECDSA (192, 224, 256, 320, 384, 512)
- SHA1, SHA-256, 384 and 512
- Dilithium (PQC)

Fault Tolerant

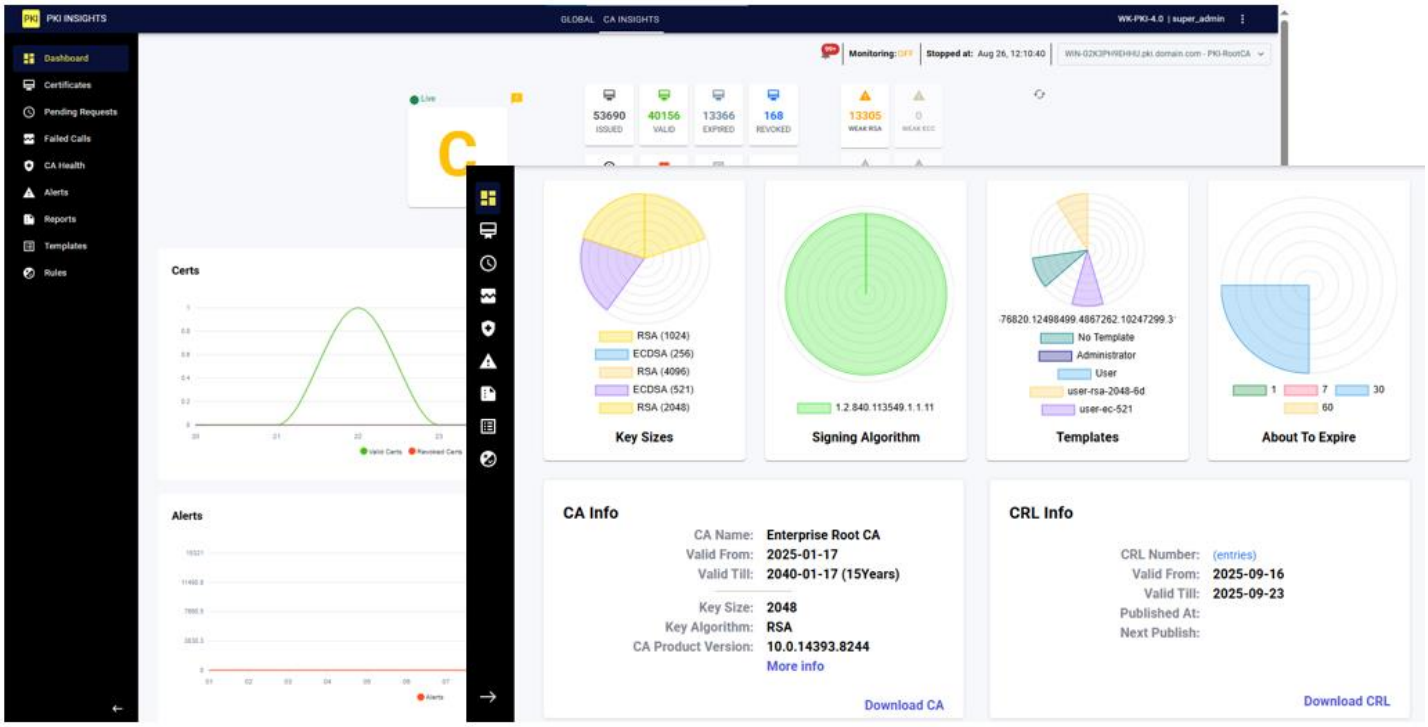
PKI Insights can be run in fault tolerant mode, minimizing latency enabling high throughput. Admin can setup multiple Agents as well for monitoring.

Serve Multiple CAs & PKIs

A single deployment of PKI Insights can handle multiple Certification Authorities / HSMs & end points making it easy to handle from a single portal.

Summary

Algorithms / Protocols	Supported OS / Languages / H/W
• RSA (2048/3072/4096/8192) • ECDSA (NIST_P, SECP (K1, R1), BRAINPOOL (R1, T1) – 160, 192, 224, 256, 384, 521) • RFC 5280, X.500, SMTP • X.509 Certificate & CRLs • Dilithium (Post Quantum Cryptography)	• All flavors of Windows Server • Languages including English, French, Spanish, Chinese, Croatian. • 4 GB RAM, 2 vCPU (2.3 GHz), 10 GB Hard disk



[Contact us](#) **today** to see how PKI Insights provides a complete inventory of your certificate landscape in less than **60 minutes**.

Codegic is a security provider specializing in innovative PKI & Digital signatures products & services. Codegic delivers easy to use PKI products for areas like PKI, Document Signing, Timestamping, PKI Monitoring, Digital Certificates issuance & more. We utilise all the latest technologies to help companies & enterprises solve complex security issues that always emerge during their digital evolution journey.

USA | UAE | PK

Facilitating Digital Trust by providing World-Class PKI & Digital Signature Solutions

Email: info@codegic.com

Learn more at https://www.codegic.com/