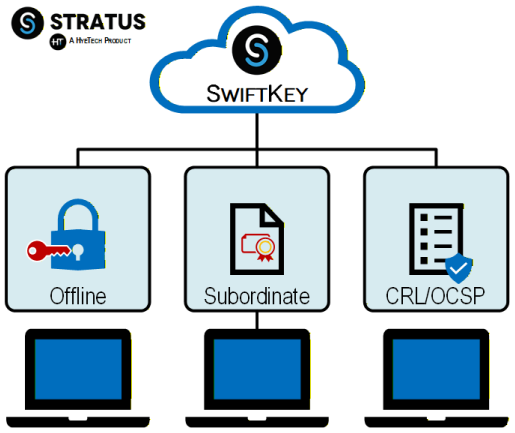
SwiftKey - Hosted PKI

Hye Tech Network & Security Solutions LLC

Modern Trust Without the Complexity

HyeTech's Hosted PKI (SwiftKey) removes the maintenance and risk that comes with running your own ADCS environment. It provides stronger security, higher reliability, and global availability, all with predictable cost and no internal overhead.

Hosted PKI vs ADCS at a Glance



ADCS	Hosted PKI
Complex to maintain	Fully managed
Local availability risks	Cloud distribution
Sensitive to CRL failures	High reliability
Staff-dependent	Expertise included
Outdated crypto risk	Modern algorithms
802.1X instability	Stable and consistent

Why SwiftKey Is the Better Choice

Stronger trust that lasts

No expired chains. No broken CRLs. No forgotten renewals. Hosted PKI preserves trust year after year.

Built for modern security

Supports Zero Trust, device identity, cloud workloads, IoT onboarding, DevOps signing, and short-lived certificates.

Secure by design

Backed by FIPS-compliant HSMs, strict governance, and continuous cryptographic modernization.

Perfect for 802.1X networks

Reliable certificates for wired and wireless authentication. No outages caused by local CRL failures. Fewer device lockouts.

Modern revocation strategy

Uses OCSP stapling and short-lived certificates where appropriate, with full OCSP and CRL support for enterprise environments that require it.

Lower and predictable cost

Eliminates hardware, servers, backups, and specialized staffing.

SwiftKey - Hosted PKI

Hye Tech Network & Security Solutions LLC - Whitepaper

Simplifying Complexity | Modernizing Service Delivery | Accelerating Performance

Benefits of SwiftKey vs Self-Managed ADCS

HyeTech's Hosted PKI solution, SwiftKey, provides a significant advantage when compared with traditional self-managed Microsoft Active Directory Certificate Services. Hosted PKI solutions, simplify operations, preserve long-term trust, reduce organizational risk, and support modern identity and networking requirements. The following sections outline the complete set of benefits.

Modern IT Services Challenge

1. Reduced Operational Overhead

Self-hosted PKI environments require servers, HSMs, CRL distribution points, AIA locations, database backups, and multi-tier CA hierarchies. They also require continuous patching, monitoring, lifecycle planning, and specialized engineering expertise. A hosted PKI removes this burden and replaces it with a fully managed, provider-secured platform.

---

2. High Availability and Global Scalability

Hosted PKI platforms deliver resilient multi-region availability, globally distributed CRL endpoints, and modern OCSP stapling support when applicable. They also maintain redundancy and uptime guarantees that individual organizations rarely achieve with on-premises ADCS.

---

3. Security and Compliance Alignment

Hosted PKI solutions provide FIPS-compliant HSM key protection, controlled key ceremonies, enforced policy governance, and modern cryptographic algorithms such as RSA-3072, RSA-4096, and ECC. They align with frameworks such as NIST 800-53, CJIS, PCI-DSS, and ISO 27001. Achieving equivalent standards internally is costly and difficult.

4. Faster Deployment and Modern Integration Support

Hosted PKI enables rapid onboarding through cloud-native APIs, SDKs, and automated issuance workflows. ADCS typically involves complex template tuning, cross-forest trust configuration, CRL publication management, and manual chaining tasks.

5. Lower Total Cost of Ownership

Self-managed PKI requires hardware, HSMs, disaster recovery infrastructure, backups, monitoring tools, and dedicated engineering labor. Hosted PKI replaces these expenses with predictable subscription pricing and eliminates most operational overhead.

6. Modern Use Case Enablement

Hosted PKI supports modern requirements that stretch ADCS beyond its intended design. Examples include:

- Zero Trust device identity
- IoT identity and attestation
- Kubernetes workload identity
- Automated DevOps signing pipelines
- Short-lived certificates for enhanced security
- API and service identity
- Multi-cloud workload protection

ADCS can be extended to support some of these cases, but only with significant customization and ongoing maintenance.

7. Long-Term Trust Preservation

Maintaining PKI trust over ten to twenty years is one of the hardest security challenges. Trust degradation happens silently when organizations fail to maintain cryptographic standards, chain publishing, CA renewals, and template hygiene. A hosted PKI ensures all lifecycle tasks are managed correctly and on schedule.

8. Removal of Hidden Maintenance and Governance Debt

Most self-managed PKI deployments accumulate silent technical debt. Common problems include:

- Stale CRLs
- Broken AIA paths
- Expired or unmonitored intermediate certificates
- Deprecated cryptographic algorithms
- Overly permissive certificate templates
- Untracked private key sprawl
- Inconsistent issuance policies

Hosted PKI solutions eliminate these risks by continuously governing, updating, and validating all chain components.

9. Protection from Institutional Knowledge Loss

PKI knowledge often resides with one or two individuals. When they leave the organization, the PKI becomes risky to operate or modify. Hosted PKI eliminates personnel dependency by transferring institutional knowledge and operational continuity to a dedicated provider team.

10. Continuous Cryptographic Modernization

Cryptographic standards evolve rapidly. RSA-1024 and SHA-1 were once accepted but are now considered insecure. Post-quantum preparation is now underway. A hosted PKI automatically keeps algorithms and policies aligned with current security requirements without forcing organizations into disruptive migration projects.

11. Professional Incident Response

When a private key is compromised, a certificate is mis-issued, or a chain issue arises, rapid expert intervention is essential. Hosted PKI providers maintain structured response playbooks that cover revocation, chain reconstruction, key rollover, and rapid certificate replacement.

12. OCSP Positioning in Modern PKI

Modern best practices avoid traditional client-side OCSP lookups because they create availability issues and privacy concerns. The industry now prefers:

- OCSP stapling for TLS servers
- Short-lived certificates that reduce the need for real-time status checks
- Robust CRLs for private networks and device identity systems

Hosted PKI supports these modern methods while still maintaining OCSP services for environments that rely on them.

13. Enhanced Support for 802.1X (Wired and Wireless)

Enterprise-grade reliability for EAP-TLS

802.1X deployments depend on consistent certificate issuance, stable status checking, and accurate chain validation. Hosted PKI improves these deployments through:

- Cloud-distributed CRLs that remain reachable during outages
- Predictable templates for user and device certificates
- Automated renewal processes to prevent expired certificate lockouts

- Strong identity assurance with enforced key protection
- Reduced risk of misconfigured or outdated template settings

Stronger security for wired and wireless access control

Hosted PKI enhances EAP-TLS by providing:

- Reliable revocation information for network access control decisions
- Stronger machine identity for both corporate and guest onboarding
- Better alignment with modern wireless controllers and NAC systems

This improves security and reduces help desk incidents caused by certificate issues.

14. Comparison Table

Feature	ADCS Self-Managed	SwiftKey Hosted PKI
Root CA Governance	Manual and error prone	Provider-managed governance
Subordinate CA Lifecycle	High maintenance load	Fully managed lifecycle
CRL Availability	Local and fragile	Global and resilient
OCSP Behavior	Live lookups required	Stapling, short-lived certs, and modern patterns
Crypto Modernization	Requires migration events	Continuous modernization
Trust Integrity Over Time	High risk of drift	Consistently preserved
Template Hygiene	Manual and inconsistent	Enforced best practices
Incident Response	Variable by staff	Expert-guided procedures
Compliance Alignment	Internal burden	Provider-managed
Knowledge Retention	Risky	Guaranteed continuity
802.1X Stability	Susceptible to outages	Reliable and predictable
Cost	Hardware plus labor	Predictable subscription

15. Closing Summary

A Hosted PKI provides a secure, scalable, and long-term solution that eliminates the operational challenges found in self-managed ADCS environments. It delivers stronger trust preservation, better support for 802.1X, modern cryptographic readiness, and a cleaner alignment with current PKI best practices such as OCSP stapling and short-lived certificates. Hosted PKI reduces risk, improves reliability, and provides a future-ready foundation for both traditional and cloud-first identity architectures.