Transformativ IP
Software Development & Implementation for Regulatory Compliance & Quantum Security

SMART-InfoSecur® and SMART-SecurKey®

Post-Quantum Cryptographic (PQC) Architecture

A Technical Blueprint for CTOs and Security Decision-Makers

Table of Contents **Page**

1. Understanding the Threat Landscape 2
2. Why Simply Swapping Algorithms Fails 3
3. The SMART-SecurKey™ Architecture: Dynamic Key Generation 4
4. The SMART-InfoSecur™ Architecture: Self-Enforcing Data 5
5. How SMART-InfoSecur and SMART-SecurKey Work Together 7
6. Practical Deployment: Two Implementation Paths 7
7. Strategic Applications and Use Cases 9
8. Implementation Roadmap: Your Path to PQC Readiness 10
9. The Value Proposition for Technical Leaders 11
10. Conclusion: Building Architectural Resilience 13
11. Appendix: Key Technical Terms 14

Executive Summary

Here's the bottom line: The transition to post-quantum cryptography (PQC) isn't just about swapping algorithms. It's about fundamentally rethinking how we protect data in a world where AI accelerates attacks today and quantum computers will decrypt our secrets tomorrow.

The SMART-InfoSecur and SMART-SecurKey architecture from Transformative IP addresses this dual threat with an approach that goes beyond mathematics to solve the structural problems that make traditional encryption vulnerable. This isn't incremental improvement—it's an architectural rethinking of how cryptographic security works.

What Makes This Different:

- **No static keys to steal** – Keys are generated dynamically and exist only during transactions
- **No central vault to compromise** – Eliminates the single point of failure that makes traditional systems vulnerable
- **Authorization travels with data** – Security policies are cryptographically fused with encrypted content
- **Simple deployment for legacy systems** – Protects critical infrastructure without code changes or downtime

- **Instant access revocation** – Updates take effect immediately without re-encrypting terabytes of data

This report will walk you through exactly how this architecture works, why it delivers superior protection against both current and future threats, and how your organization can implement it with minimal disruption to existing operations.

1. Understanding the Threat Landscape

Before diving into solutions, let's establish a clear picture of what we're defending against. The challenge facing enterprise security isn't a single threat—it's a convergent attack model where two distinct technologies work in devastating combinations.

The Dual-Threat Reality

AI: The Present-Day Harvester

Artificial intelligence isn't just automating old attack methods—it's changing the fundamental economics of cybercrime. AI engines excel at three critical attack capabilities:

- **Pattern matching at scale** – AI scans distributed systems to find weak implementations, version mismatches, and unpatched protocols faster than human security teams can remediate
- **Adaptive credential attacks** – Massive, real-time learning systems that evolve their approach based on what works
- **Attack vector prediction** – Mapping lateral movements through complex cloud, IoT, and ICS environments to identify paths to high-value data

Think of AI as creating the breach infrastructure. It's harvesting encrypted data at unprecedented scale right now, creating massive stockpiles of currently unreadable information.

Quantum: The Future Decryptor

Quantum computing has moved from theoretical to operational reality. Over 12 major commercial manufacturers—including IBM, Google, Amazon Braket, and Microsoft Azure Quantum—are actively producing quantum machines with cloud access. Recent milestones like Google's self-correcting Willow chip and Caltech's 6,100-qubit array signal that the engineering challenges are being overcome faster than predicted.

The impact is straightforward: Shor's algorithm running on a sufficiently powerful quantum computer can break RSA and ECC encryption, reducing decryption time from 'the lifetime of the universe' to minutes or seconds. The expert consensus puts widespread quantum decryption capability—Q-day—at 2 to 3 years away, possibly sooner.

The Harvest Now, Decrypt Later Strategy

This convergence enables the 'Harvest Now, Decrypt Later' (HNDL) attack vector. Sophisticated threat actors—particularly nation-states—are actively exfiltrating and stockpiling encrypted data with no intention of breaking it today. They're hoarding intellectual property, classified communications, financial records, and sensitive personal information with complete confidence that quantum computers will soon make it all transparent.

The clock is already running. Any data created today with a lifespan longer than 2-3 years is already vulnerable to future exposure. This isn't a distant problem—it's an immediate risk to long-term data security.

2. Why Simply Swapping Algorithms Fails

The natural response to quantum threats is to replace vulnerable algorithms like RSA and ECC with NIST-approved post-quantum alternatives. While this seems logical, it's dangerously insufficient. The problem isn't just the mathematics—it's the entire architecture of how we manage keys and enforce access control.

Four Critical Architectural Failures

1. Key Management Centralization

Traditional systems—even those upgraded with PQC algorithms—rely on centralized key vaults like Key Management Services (KMS) or Hardware Security Modules (HSM). This creates a massive single point of failure. The vault becomes a high-value target for sophisticated attacks and insider threats. One successful compromise grants access to vast amounts of sensitive data. The fundamental problem: you can't protect something that exists as a target.

2. Static, Long-Term Keys

Conventional cryptographic systems generate keys once and use them to protect data for months or years. This creates an enormous attack surface over time. A single successful breach of one static key renders all harvested data protected by it vulnerable to future decryption. This makes the static key the absolute lynchpin of the HNDL strategy—attackers only need one successful strike to unlock years of stockpiled data.

3. Implementation Overhead

Retrofitting new PQC algorithms into legacy 'brownfield' environments presents immense practical challenges. Critical infrastructure in operational technology (OT), industrial control systems (ICS), and mainframes cannot tolerate significant downtime or costly re-engineering. Additionally, many lattice-based PQC algorithms introduce data bloat—larger keys and ciphertext—which strains bandwidth and increases latency, making

them unsuitable for real-time and resource-constrained systems.

4. The Access Control Gap

Standard encryption ensures secrecy but doesn't enforce authorization. We've traditionally relied on external Access Control Lists (ACLs) managed at the application or network layer. This creates a critical vulnerability: security rules don't travel with data. If an attacker bypasses the network perimeter or an insider exfiltrates an encrypted file, the external ACLs become useless. The data is left protected only by an algorithm whose key the attacker is now free to pursue.

These failures demonstrate that a new algorithm alone is insufficient. What's required is a fundamentally different architectural approach.

3. The SMART-SecurKey™ Architecture: Dynamic Key Generation

SMART-SecurKey represents a paradigm shift in cryptographic key management. Instead of storing keys, it generates them dynamically and ephemerally based on verified user attributes. This fundamental change eliminates the key-at-rest vulnerability that makes traditional systems susceptible to HNDL attacks.

How It Works: Attribute-Based Key Derivation

The technical mechanism is elegant and powerful. Here's the process:

- **User requests access** – A user attempts to decrypt an encrypted data object • **Attributes are verified** – The system pulls verified attributes from a trusted policy engine (unique ID, clearance level, location, time of day, or zero-trust policy token) • **Key is generated on-the-fly** – These verified attributes, along with secret seeds and public parameters associated with the data, are fed into a robust Key Derivation Function (KDF)
- **Key exists only for the transaction** – The KDF deterministically generates a unique, session-specific decryption key that exists only for the duration of the transaction and is never stored

The Strategic Impact

This approach delivers three critical security advantages:

No Target for Attackers

Because keys are ephemeral and never stored, there's no static, long-term key for adversaries to target. The HNDL strategy loses its value proposition—there's no key asset to find or steal. Even if attackers successfully harvest encrypted data, they can't decrypt it because the keys they need will never exist in any vault, file, or memory location they can compromise.

Eliminates Single Point of Failure

Traditional key vaults—whether KMS, HSM, or other centralized repositories—create a single point of catastrophic failure. SMART-SecurKey eliminates this architectural vulnerability entirely. There's no centralized vault to protect, no master keys to guard, no catastrophic compromise scenario where one successful attack exposes everything.

AI-Resistant Design

AI-driven attacks excel at finding patterns and exploiting predictable structures. SMART-SecurKey denies AI its preferred shortcuts because keys are generated dynamically with no predictable static patterns to learn from or exploit. The system removes the primary targets for structural analysis attacks, hardening defenses against the rapid reconnaissance capabilities of modern AI.

Understanding the Trade-Off

Dynamic key generation carries a marginal computational cost compared to retrieving a pre-computed key from storage. However, this is an architecturally sound trade-off. The upfront computational cost is negligible compared to the catastrophic risk of key vault compromise. Modern processors handle KDF operations efficiently, and the security benefits far outweigh the minimal performance impact.

4. The SMART-InfoSecur™ Architecture: Self-Enforcing Data

While SMART-SecurKey solves the key management problem, SMART-InfoSecur addresses the access control gap. It does this through a simple but powerful innovation: embedding authorization policies directly into encrypted data payloads.

Creating Self-Enforcing Crypto Objects

SMART-InfoSecur cryptographically fuses the Access Control List (ACL) with the encrypted data itself. This creates a 'self-enforcing crypto object' where the data and the rules governing its access are inseparably bound together in a structured authenticated encryption format.

Traditional systems separate encryption from authorization. The encrypted file exists independently from the ACL that controls who can access it. This separation creates vulnerability—if an attacker bypasses the perimeter or an insider copies the file, the ACL no longer applies. The data loses its protective context.

SMART-InfoSecur eliminates this vulnerability by making the authorization intrinsic to the data itself. The security policies travel with the data, no matter where it's copied, stored, or transmitted.

Three Game-Changing Capabilities

1. Provenance Maintenance

Because access rules are inseparable from the data, security policies remain intact and enforced regardless of where data is stored, moved, or copied. The data protects itself. An attacker who exfiltrates an encrypted file doesn't just need to break the encryption—they also need to satisfy the embedded authorization requirements, which are verified against a trusted policy engine they cannot control.

2. Rapid Response Capability

This is perhaps the most operationally significant benefit. Access can be instantly revoked without costly and time-consuming bulk re-encryption. When an employee is terminated, a clearance is compromised, or a security incident occurs, administrators simply update the policy definition in the central Zero Trust Architecture (ZTA) engine.

At the user's very next decryption attempt, their new attributes will fail to satisfy the policy's requirements. The KDF will no longer generate the correct decryption key. Access is immediately denied, even for data that was encrypted months or years ago. No re-encryption required. No massive data processing jobs. No operational disruption. This capability transforms incident response from a multi-day crisis into a simple policy update.

3. Single-Copy Data Storage

Traditional systems handling multi-level classified data require separate, isolated storage systems for each classification level—Top Secret on one system, Secret on another, Confidential on a third, Unclassified on a fourth. This creates massive infrastructure complexity, compliance burdens, and operational overhead.

SMART-InfoSecur enables multi-level classification data to be stored in a single file on a standard unclassified system. The embedded ACL acts as the gatekeeper, ensuring users can only decrypt the specific portions they're authorized to see based on their verified clearance attributes. This dramatically simplifies infrastructure, reduces storage costs, minimizes compliance complexity, and reduces insider risk for storage administrators who no longer need access to the classified content itself.

5. How SMART-InfoSecur and SMART-SecurKey Work Together

The power of this architecture comes from the tight integration of these two components. They create a layered defense where each component addresses a specific vulnerability that algorithm-only PQC solutions leave exposed.

The Complete Protection Cycle

When a user attempts to access protected data, here's what happens:

- **Authentication and attribute verification** – The system verifies the user's identity and pulls their current attributes from the trusted policy engine

- **Policy evaluation** – The embedded ACL in the data object is evaluated against the user's verified attributes
- **Dynamic key generation** – If the user's attributes satisfy the policy requirements, SMART-SecurKey generates a session-specific decryption key using the KDF • **Data decryption** – The ephemeral key decrypts only the portions of the data the user is authorized to access

• **Key disposal** – The key is immediately discarded after use, never stored or cached

Defense in Depth

This integrated approach creates multiple independent security barriers. Consider what an attacker would need to accomplish to compromise data:

- Break quantum-resistant encryption algorithms (mathematically infeasible with current and near-future technology)
- Find and steal keys that don't exist in any permanent form
- Overcome AI-resistant architecture that denies pattern-based attacks • Satisfy embedded authorization requirements verified against a trusted policy engine they cannot control

Even if one layer is somehow compromised, the other layers remain intact. This is genuine defense in depth, not security theater.

6. Practical Deployment: Two Implementation Paths

Architecture is only valuable if it can be implemented in real-world environments. The Transformative IP solution provides two distinct deployment methods designed for different scenarios and organizational requirements.

Method 1: SDK Integration for Greenfield Applications

This method represents the deep integration path for new applications and systems under active development. Developers embed the SMART-InfoSecur and SMART-SecurKey libraries directly into application code using a provided Software Development Kit (SDK).

Primary Advantages:

- **Maximum granularity** – Encrypt individual database fields, specific microservice communications, or particular API endpoints
- **Fine-grained control** – Apply unique ACLs to different data elements based on their sensitivity and business requirements
- **Tight integration** – Align cryptographic operations closely with business logic and application workflows

Trade-Offs:

This approach requires dedicated development time, rigorous testing, and changes to

application codebase. It's the ideal long-term strategy for new systems where security can be designed from the ground up, but it's not suitable for protecting legacy systems that cannot be modified.

Method 2: Transport Layer Protection for Legacy Systems

This is the 'quick win' deployment method designed specifically for achieving immediate quantum resistance for legacy assets where code changes are impractical or impossible.

The mechanism is elegant: deploy an independent gateway or proxy that transparently PQC-encrypts the entire data stream before it enters the existing network or VPN. The legacy application remains completely unaware of the cryptographic layer operating beneath it.

Critical Benefits:

- **Zero application changes** – The existing application code requires no modifications whatsoever
- **No downtime** – Implementation doesn't require taking systems offline • **No re-engineering** – Protects brittle OT/ICS environments, mainframes, and critical systems without touching their core logic
- **Immediate protection** – Provides instant quantum and AI resistance for legacy assets

This creates a powerful 'security by architectural overlay' approach. It's particularly valuable for protecting operational technology (OT) and industrial control systems (ICS) that cannot tolerate modification or risk, as well as mainframes and other critical infrastructure that must continue operating without disruption.

Choosing the Right Method

The choice between methods depends on your specific circumstances:

- **Use Method 1 when:** Building new applications, have development resources available, need fine-grained field-level encryption, want deep integration with business logic
- **Use Method 2 when:** Protecting legacy systems, code changes are impractical, downtime is unacceptable, need immediate protection, working with OT/ICS environments

Many organizations use both methods—Method 2 for immediate protection of critical legacy assets, and Method 1 for strategic integration into new development projects.

7. Strategic Applications and Use Cases

The combination of dynamic keying, embedded authorization, and quantum-resistant algorithms enables this architecture to solve specific high-value security challenges across diverse industries and digital ecosystems.

Multi-Level Data Storage

Organizations handling classified or sensitive data at multiple levels can consolidate storage infrastructure. Store Top Secret, Secret, Confidential, and Unclassified data in a single file on standard unclassified infrastructure. The embedded ACL ensures users only decrypt portions
matching their verified clearance level. This reduces insider risk by separating storage administration from security policy, simplifies compliance, and dramatically reduces infrastructure costs.

CI/CD Pipeline Security

Secure communication paths between each stage of distributed software development pipelines. Maintain integrity of machine learning models with hash protection. Provide code obfuscation to protect valuable intellectual property from being stolen at any point during the build process. This is particularly critical as software supply chain attacks become increasingly sophisticated.

IoT and Edge Computing

Lightweight dynamic keying is ideal for resource-constrained devices like drones, sensors, and edge computing nodes. Support secure over-the-air (OTA) rekeying without requiring physical access—a critical capability for devices operating in physically insecure locations or remote deployments. The ephemeral key approach also reduces memory and storage requirements on edge devices.

Database Field-Level Encryption

Enable granular encryption down to individual database fields. Protect specific sensitive data—medical records, salary figures, social security numbers—from being accessed even by authorized database administrators who have no need-to-know. This dramatically reduces insider threat risk while maintaining database functionality and performance.

Supply Chain Security

Embed encryption and ACLs directly into Bills of Materials (SBOM/HBOM/AISBOM). Ensure verifiable provenance and integrity across the entire supply chain, as only authorized entities can decrypt and certify the contents of component manifests. This addresses growing concerns about software and hardware supply chain integrity.

8. Implementation Roadmap: Your Path to PQC Readiness

The transition to post-quantum cryptography doesn't require a complete infrastructure overhaul. The recommended approach, aligned with CISA guidance, follows a pragmatic three-step process.

Step 1: Inventory Your Cryptographic Assets

Begin with a comprehensive cryptographic asset inventory. The goal is to identify your most sensitive, long-lifespan data—the 'crown jewels' that require immediate protection from HNDL attacks.

Key Questions to Answer:

- What data has a lifespan longer than 3 years?
- Which datasets would cause the most damage if compromised?
- Where are your current cryptographic implementations?
- Which systems cannot tolerate modification or downtime?

This inventory phase typically takes 2-4 weeks for most organizations and provides essential visibility into where quantum threats pose the greatest risk.

Step 2: Secure Legacy Systems First

Deploy Method 2 (Transport Layer Protection) to achieve immediate risk mitigation on your most critical and difficult-to-change brownfield systems. This provides an instant layer of defense without operational disruption.

Priority Targets:

- Operational technology (OT) and industrial control systems (ICS)
- Mainframes and legacy databases
- Critical infrastructure that cannot be taken offline
- Systems with long-lived data and brittle codebases

This phase can typically be completed in 4-8 weeks per system, providing immediate quantum protection while buying time for strategic planning.

Step 3: Integrate with New Development

Use the protection gained from Step 2 to strategically plan Method 1 (SDK Integration) for future greenfield applications and services. This allows you to build deep, granular security and fine-grained ACL control into new systems from the ground up.

Integration Opportunities:

- New microservices and cloud-native applications
- Database modernization projects
- API development and service mesh implementations
- Data pipeline and analytics infrastructure

This phased approach balances immediate risk mitigation with strategic, long-term security architecture improvements.

9. The Value Proposition for Technical Leaders

For technical decision-makers, this translates to more than security—it offers operational efficiency, risk reduction, and infrastructure future-proofing.

Peace of Mind Through Layered Defense

The architecture delivers genuine peace of mind because it doesn't rely on a single point of security. Even if attackers successfully harvest encrypted data, they face multiple independent barriers:

- They can't decrypt it (quantum-resistant algorithms)
- They can't find keys (none are stored)
- They can't brute-force it (AI-resistant architecture)
- They can't access what they're not authorized for (embedded ACLs)

This is defense in depth that actually works, not security theater.

Operational Efficiency Gains

Simplified Infrastructure

Single-copy data storage eliminates the need for separate storage systems for each classification level. This reduces hardware costs, simplifies administration, and minimizes compliance complexity.

Instant Access Revocation

Rapid Response Capability transforms incident response from a multi-day crisis involving massive re-encryption jobs into a simple policy update. When an employee is terminated or a clearance is revoked, access to all protected data is instantly denied at the next decryption attempt—no re-encryption, no bulk operations, no downtime.

Reduced Insider Threat

Storage administrators no longer need access to the classified content they're managing. Database administrators can maintain database infrastructure without being able to read sensitive fields. This separation of duties dramatically reduces insider threat risk.

Risk Reduction

Eliminates Catastrophic Compromise Scenarios

Traditional systems have single points of catastrophic failure—the key vault, the HSM, the KMS. One successful attack can expose vast amounts of data. This architecture eliminates those single points of failure entirely.

HNDL Attack Mitigation

By eliminating static keys, the architecture removes the primary value proposition of Harvest Now, Decrypt Later attacks. Even if adversaries successfully exfiltrate encrypted data today, they cannot decrypt it tomorrow because the keys they need will never exist in any form they can compromise.

Future-Proof Protection

The architecture is designed to evolve. As new quantum-resistant algorithms are developed and standardized, they can be integrated without changing the fundamental architecture. You're not locked into today's algorithms—you're building on a resilient architectural foundation.

Simple, Quick Implementation

Perhaps most importantly for busy technical leaders, implementation doesn't require a complete infrastructure overhaul:

• **Legacy systems:** Protected immediately with no code changes using Method 2 • **New systems:** Deep integration via SDK when resources are available • **Phased approach:** Protect critical assets first, expand strategically • **No disruption:** Production systems continue operating during implementation

10. Conclusion: Building Architectural Resilience

The transition to post-quantum cryptography represents a fundamental shift in how we think about data security. It's not just about upgrading algorithms—it's about building resilient architectures that can withstand both current AI-driven attacks and future quantum decryption capabilities.

The SMART-InfoSecur and SMART-SecurKey architecture delivers this resilience through a holistic approach that addresses the entire security stack:

• **Quantum-resistant algorithms** protect against future decryption
• **Dynamic key management** eliminates the stored key as a target
• **Embedded authorization** ensures security policies travel with data
• **AI-attack resistance** denies pattern-based exploitation
• **Flexible deployment** accommodates both legacy and new systems • **Legacy compatibility** protects critical infrastructure without re-engineering

This isn't a collection of features—it's a system of interlocking defenses where each layer

is designed to nullify a specific attack vector that traditional PQC swaps leave exposed.

The Path Forward

For technical leaders charting their organization's path through the post-quantum transition, the implementation plan is straightforward:

- **Inventory:** Identify your crown jewels—the data that requires immediate protection
- **Secure Legacy:** Deploy Transport Layer Protection for immediate risk mitigation • **Integrate Strategically:** Build deep security into new systems as resources allow

The clock is running. Data being created today with a lifespan longer than 2-3 years is already vulnerable to future quantum decryption. The organizations that act now to implement genuine architectural resilience will be the ones that maintain their competitive advantage and protect their stakeholders' trust.

The question isn't whether to transition to post-quantum cryptography—it's whether you'll do it with a solution that actually addresses the full scope of the threat, or one that merely swaps algorithms and leaves the fundamental vulnerabilities intact.

The SMART-InfoSecur and SMART-SecurKey architecture provides a clear path to genuine security in the post-quantum era. The technology is ready. The implementation path is clear. The time to act is now.

Appendix: Key Technical Terms

ACL (Access Control List)

A list of permissions defining who can access specific data or resources. In SMART-InfoSecur, ACLs are cryptographically embedded within the encrypted data itself.

Attribute-Based Key Derivation

A method of generating cryptographic keys dynamically based on verified user attributes (ID, clearance level, policy tokens) rather than storing static keys.

Ephemeral Key

A cryptographic key that exists only for the duration of a single transaction or session and is never stored permanently.

HNDL (Harvest Now, Decrypt Later)

An attack strategy where adversaries exfiltrate and stockpile encrypted data with the intention of decrypting it once quantum computers become available.

HSM (Hardware Security Module)

A physical device used to manage and store cryptographic keys. Traditional HSMs create single points of failure that SMART-SecurKey eliminates.

KDF (Key Derivation Function)

A cryptographic function that generates keys from input parameters. SMART-SecurKey uses KDFs to create session-specific keys from user attributes.

KMS (Key Management Service)

A centralized service for managing cryptographic keys. Traditional KMS architectures create single points of failure.

PQC (Post-Quantum Cryptography)

Cryptographic algorithms designed to be secure against attacks from both classical and quantum computers.

Q-day

The anticipated date when quantum computers become powerful enough to break current encryption standards at scale. Expert consensus estimates 2-3 years.

Self-Enforcing Crypto Object

A data structure where authorization policies are cryptographically bound to the encrypted data, ensuring access control travels with the data.

Shor's Algorithm

A quantum algorithm that can efficiently solve the mathematical problems underlying RSA and ECC encryption, rendering them insecure.

Zero Trust Architecture (ZTA)

A security framework that eliminates implicit trust and continuously verifies all users and devices. SMART-InfoSecur integrates with ZTA engines for attribute verification.