



B² Cryptography: **A Symmetric, Hardware-Bound** **Authentication Architecture**

GoldKey Alliance
Technical White Paper

March 2026

ABSTRACT

This white paper describes B² Cryptography, the authentication framework underlying the GoldKey Alliance identity platform. B² replaces the structural assumptions of Public Key Infrastructure — certificate authorities, asymmetric key pairs, and computational hardness conjectures — with a symmetric-only, hardware-bound architecture where every security property is demonstrable rather than assumed.

This document is intended for security architects and technical evaluators assessing B² for integration into enterprise, education, healthcare, and regulated environments. It covers the architecture's design rationale, its cryptographic primitives and their composition, a comparative threat model analysis against PKI-based authentication, and the offline authentication model for disconnected environments.

Executive Summary for CISOs

B² Cryptography is the authentication foundation of the GoldKey Alliance identity platform. It eliminates the architectural categories of risk that dominate PKI-based authentication — and with them, the operational cost of managing that risk.

What changes:

- **No certificate infrastructure.** There are no certificates to issue, renew, monitor, or revoke. No CA hierarchy to defend. No CRL distribution or OCSP availability to maintain. The entire certificate lifecycle — and the attack surface it creates — is eliminated.
- **No asymmetric cryptography.** B² uses AES-256 symmetric encryption exclusively. This removes the quantum computing threat without a PQC migration, without algorithm transitions, and without hybrid deployment phases. There is no "harvest now, decrypt later" exposure.
- **Hardware-bound credentials.** The long-term authentication secret exists only inside tamper-resistant hardware (the authenticator and the Alliance HSM). It cannot be exfiltrated through software compromise, network interception, or phishing. Credential theft requires physical possession of the hardware.
- **Immediate cryptographic revocation.** Revocation destroys the key binding at the HSM. It takes effect immediately — not after CRL propagation, not after OCSP lookup, not after a database flag is checked. A revoked authenticator cannot complete any authentication event.

- **Phishing resistance by construction.** Authentication proves possession of a hardware device, not knowledge of a secret. There is no password, no OTP, and no software token to intercept.

Risk posture impact:

Risk Category	PKI Status	B ² Status
CA compromise / certificate mis-issuance	Active, ongoing risk	Eliminated (no CA, no certificates)
Quantum computing threat to authentication	Requires PQC migration	Not applicable (no asymmetric crypto)
Credential phishing	Mitigated by training and tooling	Structurally prevented
Revocation latency	Hours to days (CRL) or availability-dependent (OCSP)	Immediate
Certificate lifecycle failures (expiration outages)	Active operational risk	Eliminated
Post-quantum migration complexity	Multi-year program, ongoing	Not required

Governance model: The GoldKey Alliance is a 501(c)(3) not-for-profit, member-funded, with no commercial incentive to monetize user data. Board members hold voting seats and set strategic direction. The Alliance operates as a trusted third party whose legal structure and member oversight provide the trust foundation that a centralized symmetric architecture requires.

Deployment model: Subscribers integrate via the Subscriber Integration Interface. The Alliance handles authentication; the subscriber retains full control over authorization. Offline authentication is supported through onsite HSM infrastructure for environments without continuous connectivity. Both NFC card and USB token form factors provide identical cryptographic assurance.

Bottom line: B² reduces the authentication threat model to hardware compromise and physical theft — attack vectors that are orders of magnitude more constrained than the network-based, software-exploitable attack surfaces that PKI-based systems require organizations to manage today. It is deployed now, not on a roadmap.

TABLE OF CONTENTS

1. Introduction	4
2. The Structural Problem with PKI-Based Authentication	5
3. B ² Architecture Overview	7
4. Factory Entanglement and the Hardware Root of Trust	10
5. Session Key Derivation and Session Isolation	12
7. Revocation Model	15
8. Threat Model Comparison: B ² vs. PKI	16
9. Offline Authentication Architecture	19
10. Encryption Key Management	20
11. Conclusion	23
12. Glossary	24

1. Introduction

Authentication on the internet has been dominated for decades by a single architectural paradigm: Public Key Infrastructure. PKI was an elegant solution to the key distribution problem of the 1990s — it enabled two parties who had never communicated to establish a secure channel by trusting a common third party. But key distribution and identity assurance are fundamentally different problems, and the security properties that make PKI adequate for the former are insufficient for the latter.

B² Cryptography was developed to address this gap. Rather than layering identity assurance on top of PKI's trust model, B² starts from a different set of primitives: AES-256 symmetric encryption, hardware-bound key material, and a centralized trust anchor in the GoldKey Alliance Hardware Security Module (HSM) infrastructure. The result is an authentication system with a dramatically reduced attack surface, no dependence on computational hardness conjectures, and quantum resistance as an inherent property rather than a migration target.

The GoldKey Alliance operates as a 501(c)(3) not-for-profit organization — a member-funded trusted third party with no commercial incentive to monetize user data or weaken security guarantees. This

governance model is not incidental to the cryptographic architecture; it is a prerequisite. A symmetric authentication system requires a trustworthy central authority, and the Alliance's legal structure, member oversight, and mission alignment provide that foundation.

Audience and Scope

This white paper is written for security architects and technical evaluators — the people responsible for assessing whether an authentication technology meets their organization's security requirements, threat model, and operational constraints. It assumes familiarity with PKI concepts, symmetric and asymmetric cryptography, and standard identity frameworks (NIST 800-63, FIDO2/WebAuthn).

An Executive Summary for CISOs precedes the technical body for readers who need the risk posture and operational impact without the architectural detail.

Throughout this document, subscriber refers to any organization that integrates GoldKey authentication into its own systems and services — universities, enterprises, healthcare providers, financial institutions, or any entity whose users authenticate via GoldKey credentials. Subscribers contract with the Alliance for identity and authentication services but retain full control over their own authorization policies. The term is used consistently regardless of the subscriber's membership tier or deployment model.

2. The Structural Problem with PKI-Based Authentication

Transitive Trust and the CA Compromise Surface

PKI authentication depends on a chain of transitive trust. A relying party trusts a root Certificate Authority, which trusts one or more subordinate CAs, which issued a certificate to an endpoint. Every link in that chain is a point of compromise — and the historical record demonstrates that these are not theoretical concerns.

Real-world CA failures include:

- **DigiNotar (2011):** A root CA was fully compromised, allowing attackers to issue fraudulent certificates for Google, Microsoft, and other high-value domains. The incident enabled state-sponsored surveillance of Iranian users. The CA was subsequently delisted from all major trust stores, but the fraudulent certificates had been in active use for weeks.

- **Symantec/Thawte (2015–2017):** Google's investigation revealed systematic mis-issuance of certificates, including unauthorized test certificates for live domains. The resulting distrust of Symantec's CA infrastructure — at the time the world's largest — required a multi-year transition affecting millions of certificates.
- **Let's Encrypt domain validation (ongoing):** Automated domain validation via HTTP-01 and DNS-01 challenges is routinely exploited through BGP hijacking, DNS spoofing, and cloud infrastructure misconfigurations to obtain valid certificates for domains the attacker does not control.

These are not implementation bugs in otherwise sound systems. They are structural consequences of an architecture that separates the credential from the entity it represents. The certificate is a signed assertion about an entity, issued by a third party whose own security is outside the relying party's control. The entity's identity is inferred from the certificate, not proven by possession.

The Computational Hardness Conjecture

The deeper problem is mathematical. PKI authentication rests on asymmetric cryptography — RSA, ECC, and their successors — whose security is a computational hardness conjecture. The RSA problem (factoring the product of two large primes) and the ECDLP (elliptic curve discrete logarithm problem) are believed to be computationally infeasible on classical hardware at current key sizes. But "believed to be infeasible" is not a proof, and the history of cryptanalysis provides no guarantee that these problems will remain hard.

Shor's algorithm already demonstrates that they do not survive the transition to quantum computation. A sufficiently capable quantum computer can factor RSA moduli and solve the ECDLP in polynomial time, rendering the entire security foundation of PKI-based authentication invalid.

The industry response — post-quantum cryptography (PQC) — replaces one set of hardness conjectures with another. NIST's selected PQC algorithms (ML-KEM, ML-DSA, SLH-DSA) are based on lattice problems and hash functions that are believed to resist quantum attack, but these beliefs are newer and less battle-tested than the conjectures they replace. The PQC transition also introduces significant operational complexity: larger key sizes, different performance profiles, hybrid deployment periods, and the risk of "harvest now, decrypt later" attacks during migration windows.

Certificate Lifecycle as Operational Burden

PKI imposes a certificate lifecycle that creates its own attack surface and operational cost:

- **Issuance** requires validation — often automated and imperfect (see domain validation attacks above).

- **Renewal** must occur before expiration; failures cause outages. Certificate expiration has caused high-profile incidents at organizations ranging from Equifax (contributing to the delayed detection of their 2017 breach) to Microsoft Azure and Spotify.
- **Revocation** depends on CRL distribution or OCSP responder availability. CRL propagation delays create windows where revoked certificates remain trusted. OCSP introduces an online dependency and a privacy concern (the relying party reveals which certificates it is validating to the OCSP responder). OCSP stapling mitigates the privacy issue but transfers the availability burden to the certificate holder.

Each of these lifecycle stages represents both an operational cost and a potential failure mode. Organizations managing thousands or millions of certificates invest substantial resources in certificate lifecycle management — and failures in that management are a recurring source of both security incidents and service outages.

3. B² Architecture Overview

B² Cryptography eliminates the architectural elements that create the vulnerabilities described above. The system uses the following primitives and design principles:

Cryptographic Primitives

Component	Specification
Encryption algorithm	AES-256 (symmetric only)
Key storage	Hardware-bound; keys never leave the hardware security boundary
Session key entropy	Quantum Random Number Generator (QRNG)
Session key derivation	HMAC-SHA-256
HSM standard	FIPS 140-2 Level 2
Authenticator form factors	NFC card, USB token

What B² Does Not Include

The following elements, standard in PKI-based authentication systems, are absent by design:

- **No asymmetric key pairs.** There is no RSA, ECC, or post-quantum asymmetric algorithm anywhere in the system. Authentication does not depend on computational hardness conjectures.

- **No certificates.** There are no X.509 certificates, no certificate chains, and no certificate lifecycle to manage.
- **No Certificate Authorities.** There is no CA hierarchy, no root of trust delegation, and no transitive trust chain. Trust is direct — between the authenticator hardware and the Alliance HSM.
- **No PKI infrastructure.** There is no CRL distribution, no OCSP, no certificate transparency logs, and no certificate pinning. These mechanisms do not exist because the attack classes they mitigate do not exist in a symmetric architecture.

Trust Model

B² replaces PKI's distributed, transitive trust model with a centralized, direct trust model. The GoldKey Alliance HSM infrastructure is the sole trust anchor. Every authenticator is cryptographically bound to the Alliance HSM at time of manufacture, and every authentication event is verified — directly or through a delegated onsite HSM — against that binding.

This model requires trust in the Alliance as a central authority. That trust is grounded in:

- **Legal structure:** The Alliance is a 501(c)(3) not-for-profit corporation, member-funded, with no commercial incentive to compromise user security or privacy.
- **Member governance:** Board members (the highest membership tier) hold voting seats on the Board of Directors and set the Alliance's strategic direction, budget priorities, and governance policies.
- **Operational transparency:** The Alliance's security architecture, operational practices, and compliance posture are subject to member oversight.

For organizations accustomed to the CA model, this is a different trust relationship — but it is a simpler and more auditable one. Instead of trusting a chain of CAs (each with its own security posture, jurisdiction, and business incentives), the relying party trusts a single, auditable, mission-aligned entity.

Ecosystem Compatibility

GoldKey authenticators natively support FIDO2, and B² authentication operates in the browser over the WebAuthn API. Organizations adopting B² are not abandoning the FIDO2 ecosystem — they are building on it. Existing FIDO2-compatible infrastructure, including browsers, operating systems, and relying party libraries, works with GoldKey authenticators without modification.

What B² adds beyond FIDO2 is architectural: a symmetric cryptographic foundation that is inherently quantum-resistant, a portable Universal ID that persists across organizations rather than scoping credentials per relying party, and a centralized revocation model that takes effect immediately rather than depending on per-service implementation.

Standards Alignment

The architecture described in this paper aligns with the following standards and frameworks:

- **NIST SP 800-63B (Authentication and Lifecycle Management):** GoldKey hardware authenticators meet the requirements for the highest Authenticator Assurance Level (AAL3), providing phishing-resistant, hardware-bound authentication with verifier impersonation resistance.
- **FIPS 140-2 Level 2:** GoldKey authenticators are designed to FIPS 140-2 Level 2 requirements, providing tamper-evidence and role-based authentication for the cryptographic module.
- **NIST SP 800-63A (Identity Proofing):** The Universal ID lifecycle supports identity proofing at multiple assurance levels, with a progressive trust model that allows identity assurance to increase over time as additional verification factors are added.

4. Factory Entanglement and the Hardware Root of Trust

The Entanglement Process

Every GoldKey authenticator — whether NFC card or USB token — is cryptographically bound to the Alliance HSM at time of manufacture through a process called factory entanglement. This process establishes a shared long-term secret, K , that exists only in two places: inside the authenticator's tamper-resistant hardware boundary and inside the Alliance HSM.

Key properties of factory entanglement:

- **K is generated within the hardware boundary** using entropy from the Alliance's Quantum Random Number Generator (QRNG). It is not imported, transmitted, or derived from externally supplied material.
- **K never leaves either hardware boundary.** It is not exported, backed up to software, or transmitted over any channel — including the manufacturing network.
- **K is never used directly in any authentication session.** It serves exclusively as the root from which per-session keys are derived.
- **The binding is unique and permanent.** Each authenticator is bound to exactly one K , and each K is bound to exactly one authenticator. The binding cannot be transferred, cloned, or re-established.

What Factory Entanglement Eliminates

The factory entanglement model eliminates the key distribution problem entirely. In PKI, the fundamental challenge is establishing that a given public key belongs to a given entity — the problem that certificates, CAs, and the entire trust chain exist to solve. In B^2 , there is no key to distribute. The shared secret is established at manufacture and never moves. Authentication proves possession of hardware that contains the secret, not possession of a credential that can be copied, forwarded, or intercepted.

This has direct implications for several attack classes:

- **Credential theft without physical access is impossible.** The secret is hardware-bound. Unlike a private key stored in a software keystore, a session token in a cookie, or a password in a database, K cannot be exfiltrated through software vulnerabilities, memory dumps, or network interception.

- **Credential cloning is prevented by hardware.** The tamper-resistant boundary of the authenticator prevents extraction of K. Cloning would require physical compromise of the hardware — a fundamentally different (and vastly more constrained) attack than network-based credential theft.
- **Man-in-the-middle attacks against the credential are structurally prevented.** There is no certificate to intercept, no public key to substitute, and no handshake to downgrade. The authentication is between the authenticator and the HSM, using a shared secret that was never transmitted.

Authenticator Form Factors

GoldKey authenticators are available in two form factors:

- **NFC card:** Contactless authentication via NFC-enabled readers. Suitable for physical access control, mobile authentication, and environments where a card form factor is operationally preferred.
- **USB token:** Direct USB connection for workstation authentication. Suitable for desktop and laptop environments where USB is the primary interface.

Both form factors implement B² Cryptography identically. Cryptographic properties — key length, derivation method, session security, revocation behavior — do not vary by form factor, issuance path, or subscriber branding. A subscriber that issues NFC cards to its users and USB tokens to its administrators is providing the same cryptographic assurance to both populations.

Universal ID and the Identity Layer

Each authenticator is associated with a **Universal ID** — a persistent, Alliance-managed identity that survives authenticator replacement, revocation, and recovery. The Universal ID is the identity anchor; the authenticator is a cryptographic proof of that identity.

A user may — and is encouraged to — hold multiple authenticators bound to the same Universal ID. For example, an NFC card for building access and a USB token for workstation authentication. Each authenticator has its own independently generated K; revoking one does not affect the others. This provides both redundancy and operational flexibility.

This separation is also significant for recovery: when an authenticator is lost, stolen, or damaged, the user's identity is not lost. A replacement authenticator is bound to the same Universal ID through a fresh factory entanglement event, with new key material that is cryptographically

independent of the revoked authenticator's key material. Prior session keys derived from the old K cannot be derived from the new K, and vice versa. The user's identity continues; the compromised credential is cryptographically destroyed.

5. Session Key Derivation and Session Isolation

Per-Session Key Generation

Each authentication event derives a fresh session key from K using **HMAC-SHA-256**. The derivation incorporates entropy sourced from the Alliance's **Quantum Random Number Generator (QRNG)**, ensuring that each session key is unique and non-repeatable.

The QRNG produces entropy from quantum mechanical processes — physical phenomena whose randomness is guaranteed by the laws of physics, not by the computational difficulty of predicting a deterministic algorithm's output. This distinguishes QRNG entropy from pseudorandom number generators (PRNGs), which are ultimately deterministic and whose output can be predicted if the internal state is known.

The session key derivation process ensures that:

- Each session uses a unique key that has never been used before and will never be used again.
- The session key is derived from K but does not expose K. Compromise of a session key does not allow an attacker to derive K or any other session key.
- K is never used directly in any cryptographic operation visible to the network or to either endpoint's software stack.

Authentication Flow

At a high level, a B² authentication event proceeds as follows:

1. The user presents their GoldKey authenticator (NFC card or USB token) to the subscriber's system.
2. The Alliance HSM (or delegated onsite HSM in offline deployments) issues a challenge incorporating fresh QRNG entropy.
3. The authenticator derives a session key from K and the challenge using HMAC-SHA-256.

4. The authenticator returns a response based on the derived session key.
5. The Alliance HSM independently derives the same session key from its copy of K and the challenge, and verifies the response.

The shared long-term secret K is never transmitted, exposed to software, or used directly in the exchange. The QRNG entropy ensures that each challenge — and therefore each derived session key — is unique and non-repeatable.

Session Isolation Properties

B² provides **session isolation** — the property that compromise of any individual session key does not expose K or any other session key. The KDF is one-way: from K and QRNG entropy to session key, with no feasible reverse path. An attacker who obtains one session key gains no advantage in deriving any other session key or the long-term secret.

The security of past sessions depends on the secrecy of K. Because K is hardware-bound and non-exportable — it exists only inside the authenticator's tamper-resistant boundary and inside the Alliance HSM — the attack path to K requires physical compromise of hardware, not network-based exfiltration. This is a fundamentally different and more constrained threat than the software key compromise scenarios that most authentication systems must defend against.

If K is suspected of compromise, revocation and replacement issue a new K with fresh key material that shares no mathematical relationship with the old one. Past and future sessions are cryptographically independent.

6. Quantum Resistance as a Native Property

Why B² Is Not a Post-Quantum Migration

B² Cryptography is quantum-resistant not because it was hardened against quantum attacks, but because its architecture contains no cryptographic structures that quantum algorithms can exploit.

Shor's algorithm threatens cryptosystems based on:

- Integer factorization (RSA)
- Discrete logarithms over finite fields (DSA, DH)
- Elliptic curve discrete logarithms (ECDSA, ECDH)

B² contains none of these. There is no integer factorization problem to exploit, no discrete logarithm to solve, and no elliptic curve operation to invert.

Grover's algorithm provides a quadratic speedup for brute-force search, which halves the effective security level of symmetric ciphers. AES-256 under Grover's attack provides 128 bits of security — equivalent to AES-128 on classical hardware. This remains well beyond computational feasibility by any current or projected estimate of quantum computing capability.

Implications for Post-Quantum Planning

For organizations currently evaluating or executing post-quantum migration plans, B² presents a fundamentally different proposition:

- **No algorithm migration required.** The cryptographic algorithms deployed in GoldKey authenticators today are the same algorithms that will be deployed after NIST PQC standards are fully adopted. There is no transition period, no hybrid deployment phase, and no risk of "harvest now, decrypt later" attacks during migration.
- **No key size changes.** PQC algorithms typically require significantly larger key sizes than their classical counterparts (ML-KEM-768 public keys are 1,184 bytes vs. 32 bytes for X25519). B² key sizes are unchanged because the underlying algorithm is unchanged.
- **No performance regression.** AES-256 is hardware-accelerated on virtually all modern processors (via AES-NI and equivalent instructions). PQC algorithms have different and generally less favorable performance profiles, particularly for key generation and encapsulation.
- **No dependency on evolving standards.** The NIST PQC standardization process is ongoing, with algorithm selections subject to potential future revision as cryptanalysis matures. B² has no dependency on this process because it does not use the algorithm class that PQC is designed to replace.

This is not a claim of superiority over PQC — it is a claim of irrelevance. PQC solves the problem of securing asymmetric cryptography against quantum attack. B² does not use asymmetric cryptography. The two approaches address different architectural choices.

7. Revocation Model

Immediate Cryptographic Revocation

When an authenticator must be revoked — due to loss, theft, compromise, or administrative action — revocation in B² is a cryptographic operation, not a record update.

The Alliance HSM destroys or quarantines the key binding associated with the revoked authenticator. Once this operation completes, the authenticator is permanently unable to complete an authentication event. There is no grace period, no propagation delay, and no dependency on an external distribution mechanism.

Contrast with PKI revocation:

Property	PKI (CRL/OCSP)	B ² Cryptographic Revocation
Revocation latency	Hours to days (CRL publication cycle) or real-time (OCSP) with availability dependency	Immediate upon HSM operation
Propagation	Requires distribution to all relying parties	No distribution required for online authentication; offline sites apply revocations upon synchronization (see Section 9)
Offline verification	Cached CRLs may be stale; OCSP requires connectivity	Revocation is enforced at the HSM; see Section 9 for offline model
Availability dependency	OCSP responder must be reachable; soft-fail policies allow bypass	No external dependency; revocation is a state change at the HSM
Reversibility	Certificate can be un-revoked in some implementations	Revocation is permanent; recovery issues a new credential with new key material

Revocation and Replacement

Revocation and credential replacement are operationally decoupled. When an authenticator is revoked:

1. The key binding at the Alliance HSM is destroyed.
2. The authenticator ceases to function for all online authentication events immediately. At offline sites, revocation takes effect upon synchronization (see Section 9).

3. A replacement authenticator is issued and bound to the user's Universal ID through a new factory entanglement event with fresh key material.
4. The replacement authenticator's key material is cryptographically independent of the revoked authenticator's key material. Prior session keys cannot be derived from the new K, and the new K cannot be derived from the old K.

This independence property is significant for compliance and incident response. If an authenticator is revoked due to suspected compromise, the replacement credential provides no information about prior sessions, and an attacker who possessed the compromised authenticator gains no advantage against the replacement.

8. Threat Model Comparison: B² vs. PKI

The following table compares the attack surfaces of a standard PKI-based authentication deployment against B² Cryptography. For each attack class, it identifies whether the attack is applicable, and if so, what mitigation or structural prevention exists.

8.1 Credential and Key Material Attacks

Attack	PKI Exposure	B ² Exposure
Private key exfiltration	Private keys stored in software keystores (PKCS#12, PEM files) can be exfiltrated via file access, memory dump, or side-channel attack. HSM-backed keys mitigate this but are not universal.	K never leaves the hardware boundary. Software-based exfiltration is structurally impossible.
Credential cloning	Software-based credentials can be copied. Even hardware-backed keys (e.g., TPM-bound certificates) may be cloneable via firmware vulnerabilities.	Hardware tamper resistance prevents K extraction. Cloning requires physical hardware compromise.
Credential reuse from exfiltrated key material	A compromised or exfiltrated private key can be used to authenticate from any location indefinitely, until the certificate is revoked and the revocation propagates.	Per-session keys derived from QRNG entropy are single-use. The long-term secret K never leaves the hardware, so there is no extractable credential to reuse.
Harvest now, decrypt later	Encrypted sessions using RSA or static DH key exchange can be recorded and decrypted when quantum computers are available.	No asymmetric key exchange to harvest. Session keys are derived from a symmetric secret that is never transmitted.

8.2 Infrastructure Attacks

Attack	PKI Exposure	B ² Exposure
CA compromise	An attacker who compromises a CA can issue arbitrary certificates for any domain or identity. Impact is global (all relying parties that trust the CA).	No CA exists. There is no entity whose compromise would allow issuance of arbitrary credentials.
Certificate mis-issuance	Automated domain validation (HTTP-01, DNS-01) is exploitable through BGP hijacking, DNS spoofing, and cloud infrastructure misconfiguration.	No certificates are issued. Authentication is bound to physical hardware, not domain ownership.
MITM via certificate substitution	An attacker with a fraudulently obtained or mis-issued certificate can intercept and decrypt traffic. Certificate pinning mitigates this but is fragile and widely deprecated.	No certificate to substitute. Authentication is between hardware and HSM using a shared secret that was never transmitted.
OCSP/CRL bypass	Soft-fail OCSP policies (the default in most browsers) allow revoked certificates to pass validation when the OCSP responder is unreachable.	No OCSP or CRL mechanism exists. Revocation is a cryptographic state change at the HSM.

8.3 Quantum Computing Attacks

Attack	PKI Exposure	B ² Exposure
Shor's algorithm (factoring/ECDLP)	Breaks RSA, DSA, ECDSA, DH, and ECDH. Renders all currently deployed asymmetric cryptography insecure.	Not applicable. No asymmetric cryptography is present in the system.
Grover's algorithm (symmetric brute force)	Halves effective symmetric key length. AES-128 reduced to 64-bit security; AES-256 reduced to 128-bit security.	AES-256 reduced to 128-bit effective security. 128 bits remains computationally infeasible.

8.4 Centralized Trust and the Alliance HSM

B² concentrates key material in the Alliance HSM infrastructure. This is a deliberate architectural choice — and it means the Alliance HSM is a high-value target. An attacker who compromised the HSM infrastructure would have access to the long-term secrets of all authenticators bound to it.

This concentration of trust is not unique to B². PKI-based authentication distributes the same class of trust dependency across a longer chain — root CAs, subordinate CAs, hardware security modules at each CA, the hardware manufacturers who built them, and the registration authorities

who validate certificate requests. Each link in that chain has its own security posture, its own operational controls, its own jurisdiction, and its own business incentives. A compromise at any point in the chain can issue fraudulent credentials that all downstream relying parties will accept.

B² consolidates these trust dependencies into a single entity: the GoldKey Alliance. The result is a smaller trust surface with fewer points of failure:

Property	PKI Trust Chain	B ² Trust Model
Trust anchors	Multiple CAs, each independently operated	Single Alliance HSM infrastructure
Compromise blast radius per entity	Varies by CA — root CA compromise is global	Alliance HSM compromise affects all authenticators
Number of entities requiring trust	Root CAs + subordinate CAs + registration authorities + hardware vendors	GoldKey Alliance + authenticator hardware manufacturer
Auditability	Each CA audited independently, if at all	Single entity to audit
Governance alignment	Commercial CAs operate for profit; incentives may diverge from relying party interests	501(c)(3) not-for-profit, member-governed, mission-aligned

The centralized model does not eliminate the need for trust — it reduces the number of entities that must be trusted, and places that trust in an organization whose legal structure, governance model, and operational transparency are designed to warrant it.

8.5 Operational and Lifecycle Attacks

Attack	PKI Exposure	B ² Exposure
Certificate expiration causing outage	Expired certificates cause authentication and service failures. Certificate lifecycle management at scale is a significant operational burden.	No certificates; no expiration. Authenticator validity is a function of the key binding state at the HSM.
Revocation latency exploitation	Revoked certificates remain trusted until CRL propagation completes or OCSP is checked. Attackers can exploit this window.	Revocation is immediate. The key binding is destroyed at the HSM; the authenticator ceases to function.
Phishing for credentials	Users can be tricked into entering passwords or approving fraudulent certificate prompts.	Authentication requires physical possession of the hardware authenticator. Phishing cannot obtain the hardware or the secret it contains.
Authenticator enumeration	Timing differences in authentication responses can reveal whether accounts exist.	Constant-time recovery and authentication interfaces reveal no information about authenticator state through timing or differential responses.

9. Offline Authentication Architecture

The standard B² authentication model verifies every event against the Alliance HSM in real time. For environments where internet connectivity is intermittent or prohibited — manufacturing clean rooms, field operations, secure facilities, building access systems — B² supports an onsite HSM model that extends the same cryptographic trust properties to disconnected environments.

Onsite HSM and Local Entanglement

An onsite HSM deployed at a subscriber's premises can form its own entanglement with authenticators that have been presented at the site. When an authenticator is first presented during an online period, the Alliance HSM brokers a new entanglement between the authenticator and the onsite HSM — establishing a shared secret between the two that is independent of the authenticator's original factory entanglement with the Alliance HSM. The onsite HSM can then verify the authenticator directly through a challenge-response protocol using this local entanglement and entropy from the onsite HSM's own random source.

The security properties of local authentication — per-session key derivation, session isolation, and hardware-bound key material — are the same as centralized authentication. The entropy source depends on the onsite HSM's hardware; the quality of the random source is a function of the subscriber's HSM selection. The trust anchor difference is that authentication is verified against the onsite HSM rather than the Alliance HSM.

Enrollment Constraint

An authenticator must be presented at the site during an online period before it can authenticate offline. The first presentation triggers the Alliance-brokered entanglement between the authenticator and the onsite HSM. This prevents an attacker from introducing unknown credentials into a facility while it is disconnected.

Authenticators that have never been presented at a given site cannot authenticate there while offline — even if they are valid Alliance credentials.

Validity Windows

A configurable validity window limits how long offline authentication remains valid. Authenticators that have not been verified against the Alliance HSM within the validity window will not authenticate locally, even against a valid local entanglement. This bounds the exposure window for compromised credentials in disconnected environments.

Synchronization and Revocation

Upon reconnection, the synchronization sequence enforces a strict ordering:

1. Download and apply all pending revocations, destroying the local entanglement for any revoked authenticators.
2. Verify local entanglement state against Alliance HSM state.
3. Resume normal authentication operations.

Revocations are applied before any new authentications are accepted. An authenticator revoked at the Alliance while a site was disconnected is blocked the moment connectivity is restored — before any further authentication events are processed.

10. Encryption Key Management

The preceding sections describe B² as an authentication architecture. The same entanglement mechanism also provides a foundation for encryption key management — allowing authenticators and local HSMs to share encryption keys without the asymmetric cryptography that conventional key management depends on.

The Key Distribution Problem in Conventional Encryption

Encryption key management in PKI-based systems relies on asymmetric cryptography to solve the key distribution problem. A sender encrypts a symmetric data key with the recipient's public key (RSA key transport) or negotiates a shared secret through a key exchange protocol (ECDH). The symmetric key then encrypts the data. The security of the data ultimately depends on the security of the asymmetric key exchange — and inherits all of the vulnerabilities described in Section 2: computational hardness conjectures, quantum susceptibility, and certificate-based trust chains.

B² solves this problem through the same mechanism used for offline authentication: the Alliance HSM brokers a direct entanglement between the endpoints that need to share keys.

Entanglement-Based Key Sharing

Two authenticators — or an authenticator and a local HSM — can establish a direct entanglement through the Alliance HSM. This follows the same pattern described in Section 9 for offline authentication: the Alliance HSM brokers the entanglement during an online period, establishing a shared secret between the two endpoints that is independent of either endpoint's factory entanglement with the Alliance HSM.

Once established, the entanglement provides a symmetric channel for saving and sharing encryption keys between the entangled endpoints. No asymmetric key exchange is involved at any point — the shared secret was established through the Alliance HSM broker, and keys are protected by AES-256 encryption over that shared secret.

The properties of entanglement-based key sharing:

- No asymmetric cryptography. Key sharing uses the entangled symmetric secret. No RSA, ECC, or post-quantum asymmetric algorithm is involved in key distribution.
- Quantum-resistant. Keys are protected by AES-256 over the entangled secret. There is no asymmetric key exchange to harvest or decrypt later.
- Hardware-bound. The entangled secret exists only within the hardware boundaries of the two endpoints. Key sharing operations occur within the tamper-resistant environment.
- Revocable. When an authenticator is revoked, its entanglements — both the factory entanglement with the Alliance HSM and any direct entanglements with other authenticators or local HSMs — are destroyed. The revoked authenticator can no longer participate in key sharing.
- Independent per entanglement. Each entanglement between two endpoints has its own shared secret. Compromise of one entanglement does not expose any other.

Contrast with PKI-Based Key Management

Property	PKI Key Management	B ² Key Management
Key distribution mechanism	Asymmetric encryption (RSA) or key agreement (ECDH)	Direct entanglement between endpoints, brokered by Alliance HSM
Quantum vulnerability	Key exchange is vulnerable to Shor's algorithm; "harvest now, decrypt later" applies	No asymmetric key exchange; keys protected by AES-256 over entangled secret
Certificate dependency	Recipient's public key must be certified; CA compromise enables key interception	No certificates; key sharing is between entangled hardware endpoints
Key escrow and recovery	Complex; often requires separate escrow infrastructure	Alliance HSM can broker new entanglements for key recovery to replacement authenticators

Scope and Boundaries

B² encryption key management is an extension of the authentication architecture, not a replacement for a subscriber's full encryption infrastructure. The subscriber retains responsibility for how shared keys are used, applied to data, and rotated according to its own policies. B² provides the key sharing channel and the assurance that it was established without asymmetric cryptography and without exposure outside the hardware trust boundary.

11. Conclusion

B² Cryptography represents a fundamental architectural departure from PKI-based authentication. By eliminating asymmetric cryptography, certificate authorities, and the transitive trust model, it removes entire categories of attack surface rather than mitigating them through additional layers of complexity.

The architecture's core properties — symmetric-only construction using AES-256, hardware-bound key material that never leaves the security boundary, per-session key derivation with QRNG entropy providing session isolation, and quantum resistance as an inherent property rather than a migration target — address the structural weaknesses of PKI at the design level, not the implementation level.

For security architects evaluating authentication infrastructure, the practical implications are: elimination of the certificate lifecycle and its associated attack surfaces, immediate cryptographic revocation without CRL/OCSP dependencies, phishing resistance through hardware-bound credentials, and offline authentication capability without trust degradation. The threat model contracts to hardware compromise and physical theft — attack vectors that are orders of magnitude more constrained than the network-exploitable surfaces that PKI-based systems require organizations to defend.

The Alliance welcomes independent review of B² Cryptography's security properties. Detailed protocol specifications and security documentation are available to Alliance members; researchers interested in formal analysis are invited to contact the Alliance directly.

12. Glossary

Term	Definition
Alliance HSM	The GoldKey Alliance's Hardware Security Module infrastructure — the central trust anchor for all B ² authentication operations.
AES-256	Advanced Encryption Standard with a 256-bit key. The sole encryption algorithm used in B ² Cryptography.
Factory entanglement	GoldKey Alliance terminology for the process by which a GoldKey authenticator is cryptographically bound to the Alliance HSM at time of manufacture, establishing the shared long-term secret K. Not related to quantum entanglement.
Session isolation	The property that compromise of any individual session key does not expose the long-term secret K or any other session key. Each session key is derived one-way from K and unique QRNG entropy.
K	The long-term shared secret established during factory entanglement. Exists only within the authenticator hardware and the Alliance HSM. Never transmitted or used directly in sessions.
QRNG	Quantum Random Number Generator — produces entropy from quantum mechanical processes for session key derivation.
Subscriber	Any organization that integrates GoldKey authentication into its systems and services. Subscribers contract with the Alliance for identity and authentication services but retain full control over their own authorization policies.
Universal ID	A persistent, Alliance-managed identity that survives authenticator replacement, revocation, and recovery. The identity anchor to which authenticators are bound.
Onsite HSM	A Hardware Security Module deployed at a subscriber's premises to support offline authentication through local entanglement records.

Published by the GoldKey Alliance. For technical inquiries, contact the Alliance through the member portal or at the address listed on goldkey.com.