Enabling Zero Trust at the Tactical Edge

Biometrics, Derived Credentials & Post-Quantum Encryption for the Future Fight

DAFITC 2025
Montgomery, AL

Shawn Moorhead, Vice President, Lastwall

Agenda

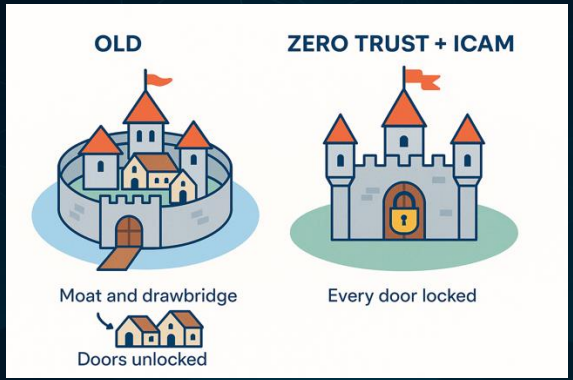
1. **Why ZT & ICAM Matter**
   Context & Background
2. **The Challenge at the Edge**
   Problem & DAF Zero Trust Strategy
3. **Biometrics & Derived Credentials**
   Enabling secure access on mobile devices
4. **Tactical Identity Bridge**
   Maintaining identity in DDIL operations
5. **Quantum-Ready Security**
   Post-Quantum Cryptography & Roadmap
6. **Policy Mandates & Deadlines**
   Compliance drivers for Zero Trust & PQC

Context: Why ZT & ICAM Matter

- **The Modern Battlespace is Digital, Distributed, and Exposed:** Devices like phones and tablets are everywhere, and so are attack surfaces.
- **Adversaries Adapt Quickly:** Lost or captured gear can compromise missions if not locked down.
- **Current State of Play:** Today's solutions are heavy, complex, and logistically taxing.
- **The Shift - Zero Trust and ICAM Lighten the Load:** Reduce physical carry while improving local control, resilience, and security.

Context: Zero Trust & ICAM 101

- **Zero Trust:** No Implicit Trust: “Never trust, always verify”, every user, device, and action must be authenticated continuously.
- **ICAM - Identity, Credential, Access Management:** Defines who you are, how you prove it, and what you’re allowed to do, foundation for access decisions.
- **ZT + ICAM: Integrated Control and Visibility:** Together, they enforce access policies and maintain visibility across users, devices, and services.
- **Tactical Edge - Where Control Gets Hard:** Disconnected, Degraded, Intermittent, and Limited (DDIL) networks demand solutions that work without reach-back.
- **Enterprise vs. Edge, A Reality Gap:** Enterprise assumes constant connectivity and centralized control; the edge demands autonomy and resilience.



Problem: Identity & Access at the Edge

- Perimeter security fails in disconnected operations; every connection must be treated as untrusted.
- Complex login processes (especially in DDIL environments) frustrate users, reduce security, and hinder access to critical data.
- Human Factors & Device Types: Workarounds (shadow IT) and access friction. Mobile devices, laptops, tablets, etc.
- Legacy Systems & Siloed Credentials
- Complex Partner & Coalition Access
- Credential Theft and Identity Compromise

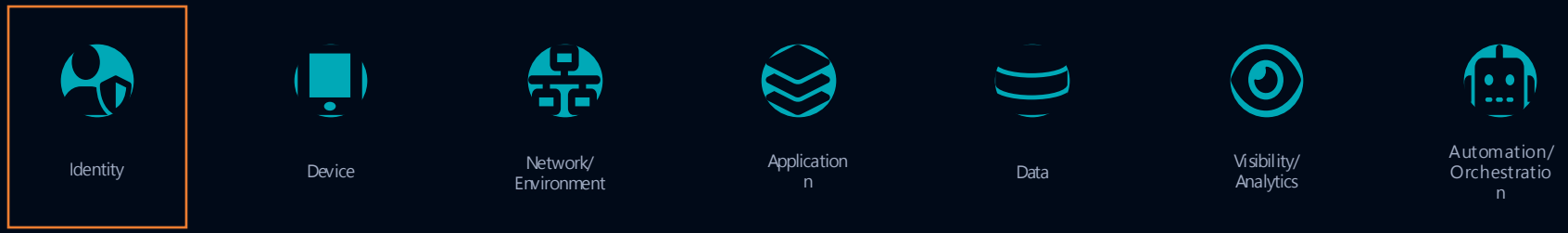
Operators need **local**, rapid, secure, reliable authentication across multiple domains

DOD & DAF Zero Trust Strategy

Shift to data-centric security

Assume all connections are untrusted; continuously verify identity, device & context. Dynamic risk management aligns access policies with mission needs.

Seven Pillars of Zero Trust



DAF Zero Trust: Identity as the Foundation

Identity: Validates users/devices with MFA, biometrics, derived credentials

Device: Ensures endpoints are continuously assessed for posture and trust, including DDIL/contested environments.

Network/Environment: Enforces adaptive access controls, segmentation, and resilience in degraded or coalition scenarios.

Application: Uses policy-based authentication and authorization to protect apps, services, and workloads.

Data: Protects sensitive information with tagging, encryption, and continuous identity-driven access controls.

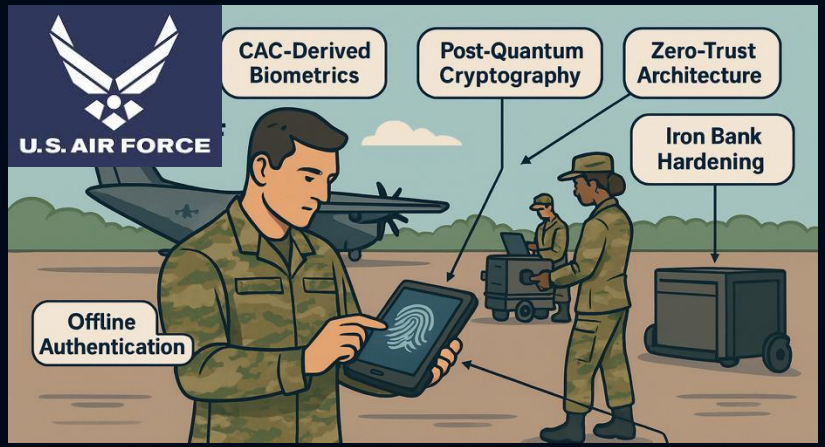
Visibility: Provides continuous monitoring, risk scoring, and User & Entity Behavior Analytics across all layers.

Automation: Dynamically enforces policies and responds to threats in real time with machine-speed actions.

Identity at the Tactical Edge

Disconnected & contested environments demand localized trust decisions to enables dynamic access control for warfighters and coalition partners, even when cloud connectivity is limited.

- **Local, Containerized ICAM for DDIL:** Run full identity services at the edge, no reliance on cloud or enterprise connectivity.
- **Biometrics, Passkeys, MFA Without Cloud:** Enable secure, phishing-resistant access using built-in device factors, even in air-gapped environments.
- **Federation & Cross-Domain Trust:** Support mission partner access with flexible, policy-driven identity bridging across domains and coalitions.
- **Portable Infrastructure, Deploy Anywhere**: Package ICAM in small-form, ruggedized compute, ready for FOBs, vehicles, or disconnected operations.

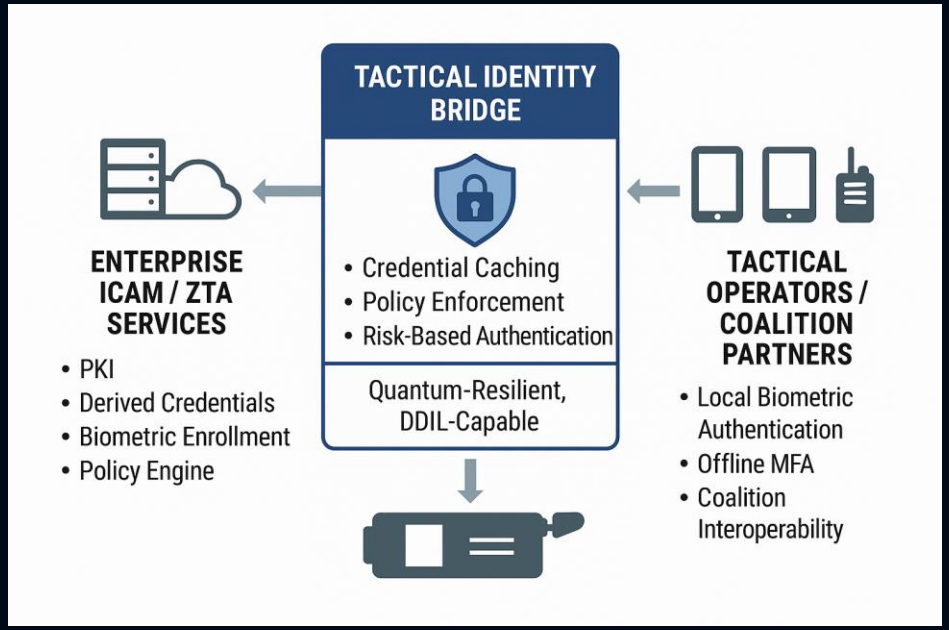


Derived Credentials: Secure Mobile Authentication

- CAC-derived credentials are X.509 certificates and WebAuthn passkeys bound to a user's biometrics and device, delivering FIDO-level phishing resistance.
- Certificates are generated from CAC/PIV smart cards per NIST SP 800-157; issuers include DISA Purebred and others.
- Provision once on desktop, then issue device-bound passkeys with biometric unlock that remain valid for mission length offline in DDIL environments.
- Accelerates Zero Trust adoption by eliminating shared passwords and enabling passwordless MFA across the force.

Tactical Identity Bridge & Implementation

- Provides local identity services when disconnected; maintains local directory of identities & roles.
- Authenticates users via CAC/PIV/Biometric; phishing-resistant MFA.
- Enables provisioning of new users and generation of cryptographic credentials at the edge.
- Synchronises updates with enterprise identity services once connectivity is restored.



Quantum Computing: The Threat

“Post-quantum cryptography is about proactively developing and building capabilities to secure critical information critical information and systems from being compromised through the use of quantum computers… The key is to be The key is to be on this journey today and not wait until the last minute.” — Rob Joyce, Director of NSA Cybersecurity, NSA Cybersecurity, Aug. 21, 2023

“The Department of Defense is already taking precautions against potential future quantum threats by modernizing by modernizing its cryptography, which… in most cases is ‘either obsolete or nearing obsolescence.’ … ‘We’ve got a … ‘We’ve got a very large-scale crypto modernization program… [moving] to… algorithms that… are quantum quantum resistant.’” — David McKeown, DoD Deputy CIO for Cybersecurity, June 9, 2023.

Quantum Computing: Offense & Defense

- "Store Now, Decrypt Later” - Adversaries capture encrypted encrypted data today to decrypt it later when quantum quantum computers break current algorithms
- Q-Day (or Y2Q) refers to the moment a cryptographically relevant quantum computer renders today’s encryption and authentication methods ineffective.
- Post-Quantum cryptography and zero trust identity ensure that even harvested data remains secure in the quantum era.
- Upgrading to quantum-resilient algorithms now protects sensitive mission data far into the future.

Quantum-Ready Security

Finalised PQC standards ready now

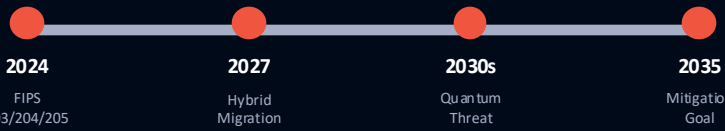
NIST released FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA) in August 2024. Organizations should begin adopting these quantum-resistant algorithms today.

Impending quantum threat

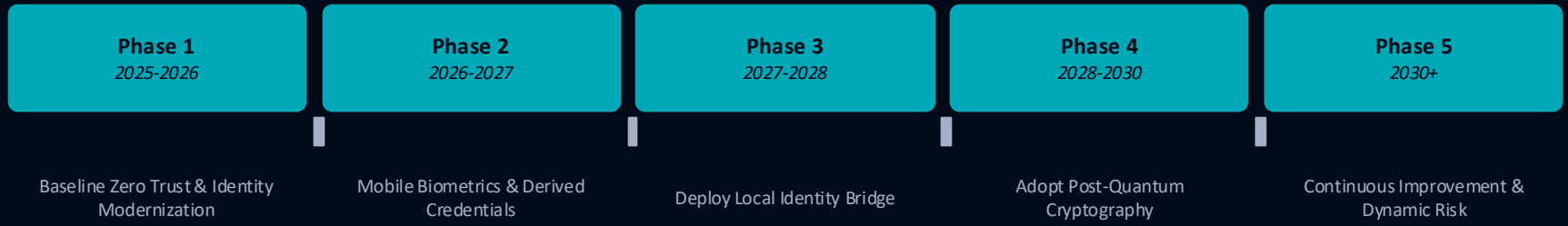
Cryptanalytically relevant quantum computers may arrive in the 2030s, jeopardising today's encryption. The U.S. aims to mitigate quantum risk by 2035 — early migration is essential.

Transition guidance

NIST will select additional algorithms in future sets; do not wait to migrate. Adopt PQC alongside classical algorithms in a hybrid approach and inventory cryptography to plan your transition.



Integration Roadmap



Phased roadmap aligns Zero Trust adoption with tactical requirements and emerging standards.

Policy Mandates: Zero Trust (MFA) and PQC

- DAF Enterprise Zero Trust Roadmap v2.0 (Oct 2024, SAF/CN) – Identity is the first pillar; enables DDIL/tactical operations and underpins every ZT control.
- DoD Zero Trust Strategy & Roadmap (Nov 2022, DoD CIO) – Requires ZT implementation across DoD by FY27, naming ICAM as the foundation.
- OMB M-22-09: Federal Zero Trust Strategy (Jan 2022) – Mandates phishing-resistant MFA and identity-centric access across all federal agencies.
- DoD Zero Trust Reference Architecture v2.0 (2022) – Defines required ZT capabilities and technical controls, with ICAM at the enforcement point.
- NSM-10: Quantum Readiness (May 2022, White House) – Directs national-security systems to transition to quantum-resilient cryptography.
- OMB M-23-02: Migrating to Post-Quantum Cryptography (Nov 2022) – Requires inventory and upgrade of crypto to ensure future mission data security.
- Quantum Computing Cybersecurity Preparedness Act (Dec 2022, Congress/OMB) – OMB to issue PQC migration guidance one year after NIST standards (due Aug 2025) and prioritize PQC acquisition.
- NSA CNSA 2.0 (Sept 2022, NSA) – Sets timeline to adopt post-quantum algorithms: signing & VPNs by 2030, web/cloud services by 2033, and full PQC adoption by 2035.
- EO 14144: Strengthening and Promoting Innovation in Cybersecurity (Jan 2025, White House) – Requires agencies to support TLS 1.3 or successor by Jan 2, 2030 as a step toward PQC readiness.

Sample Use Cases – ACE & Cyber Hunt

ACE Crews on Dispersed Pacific Strips

Problem:
Agile Combat Employment expects Airmen to operate in contested, degraded & operationally-limited settings. When SATCOM is jammed or degraded, CAC log-ins fail and sortie flow slows.

Solution:
Deploy containerized identity platform on a portable node (e.g., a NUC in a Pelican case) to issue device-bound passkeys that remain valid for mission/exercise, with logs syncing automatically when even a thin link re-appears.

Value:
Pilots file flight plans and maintainers pull e-TOs during blackout periods, sustaining rapid sortie tempo and reducing crew exposure on remote airstrips.

Cyber Protection Teams using the Joint Cyber Hunt Kit (JCHK)

Problem:
Host enclaves often block traffic during or after an incident, forcing CPT analysts to rely on shared or local passwords and sacrificing non-repudiation.

Solution:
Issue containerized identity with the JCHK lets analysts authenticate locally via hardware or device-based passkeys, wrap traffic in post-quantum cryptography and buffer signed logs for export once connectivity returns.

Value:
Hunt crews begin work instantly with non-repudiable credentials, reducing dwell time for malware and fulfilling the "SOC-in-a-box" promise.

Sample Use Cases – Cloud & Coalition

Cloud One Developers & Operators

Problem:
SAF/CDN's FY-25 plan calls for improved Cloud One security and user experience, while the Zero-Trust Strategy mandates universal MFA. Dev teams still endure 30–60 second CAC round-trips from remote bases, encouraging insecure work-arounds.

Solution:
Run containerized identity platform as a side-car within the EKS cluster lets users enroll once with CAC and thereafter authenticate via device-bound passkeys entirely inside the Cloud One VPC, yielding sub-100 ms logins.

Value:
Developers recover minutes each push, ops teams close change windows faster, and Cloud One achieves zero-trust security with seamless, post-quantum-resilient user experience.

Coalition Pilots & Intel Cells at Red Flag

Problem:
Red Flag 25-1 showed U.S., RAF and RAAF crews juggling temporary accounts because identity federation lags policy, hampering timely coalition access.

Solution:
Bridges partner SAML 2/OIDC assertions, issues exercise-scoped WebAuthn passkeys on-site, and auto-expire them at ENDEX.

Value:
Allied aircrews log in once, share real-time intel without credential chaos, and Blue forces gain coalition tempo from day one.

[26] [27] [28] [29]

Conclusion & Next Steps

- Adopt a data-centric Zero Trust posture that continuously verifies identity, device and context.
- Embrace CAC-derived biometric passkeys to deliver FIDO-compliant, device-bound credentials that function offline in DDIL environments.
- Deploy local identity bridging to extend Zero Trust to the tactical edge.
- Begin migrating to post-quantum cryptography now to stay ahead of future quantum threats and plan adoption via a phased roadmap.

Questions?

Contact:
shawn.moorhead@lastwall.com