



How XQ Uniquely Delivers on ACP 240 with Zero Trust Data

With the formal adoption of **Allied Communication Publication (ACP) 240** by FVEY partners and allied nations, data-centric, Zero Trust collaboration is no longer a vision—it is a standard.

ACP 240 relies on the **Zero Trust Data Format (ZTDF)** to enable secure, interoperable, and policy-driven data sharing across coalition environments.

Zero Trust Data Format (ZTDF) is an interoperable data security wrapper.

It seamlessly understands all variations of the TDF metadata standard, allowing organizations to build custom policy enforcement points. ZTDF facilitates secure collaboration and data sharing, enabling files, messages, and documents to be shared across borders and classifications.

It allows organizations to integrate data-centric governance controls into legacy and next-generation applications, ensuring sensitive information remains protected.

ZTDF provides auto-enforcing granular access controls and grants access only to authorized individuals. (virtru.com)

To operationalize ACP 240 in real-world environments, organizations need more than metadata standards—they require platforms that can embed, enforce, and audit policies across complex, multi-domain systems.

XQ is uniquely designed to do exactly that.

Overview of ACP 240

Allied Communication Publication (ACP) 240 is a NATO-standardized metadata framework for data-centric security, designed to enable secure, interoperable sharing of sensitive information across allied partners.

It aligns with Zero Trust principles and supports the use of open standards like Zero Trust Data Format (ZTDF) to protect data at rest, in transit, and in use, regardless of the underlying network or platform.





Key ACP 240 and ZTDF Requirements and Use Cases

Based on the ZTDF standard and XQ's analysis, ACP 240 introduces several critical capabilities:

1. Interoperability Across Allied Domains

- ZTDF enables cross-national data sharing, reconciling classification differences between nations (e.g., U.S. "Top Secret" vs. U.K. "Above Secret").
- Supports federated, distributed, and disconnected deployments for coalition partners.

2. Data-Centric Security (Encryption + Policy Binding)

- Policy and encryption travel with the data object.
- Attribute-Based Access Control (ABAC) ensures decryption only occurs for authorized individuals, considering identity, role, clearance, and environmental factors.

3. Key Management & Disconnected Operations

- Multi-Key Access Server (Multi-KAS) architecture allows each nation to maintain its own keys while securely synchronizing across coalition partners.
- Supports offline or DDIL (Denied, Degraded, Intermittent, Limited) environments, enabling edge or tactical deployment.

4. Zero Trust Identity + Data Pillar Convergence

- Identity and device attributes are embedded into each data object.
- Real-time evaluation enforces continuous Zero Trust validation.

5. Scalability & Open Standards

- ZTDF and TDF family standards are open and extensible.





- Designed for large files, streaming data, and flexible deployment, with full audit and governance capabilities.

How XQ Aligns with and Exceeds ACP 240 and ZTDF Requirements

1. Interoperability Across Allied Domains

- **ZTDF-Native Wrapping:** XQ supports ZTDF-compliant data objects, embedding classification, policy, and metadata for seamless coalition sharing.
- **Policy Translation:** XQ maps different national or alliance classification systems, ensuring consistent policy enforcement across borders.
- **Federated Deployment:** Each nation or command can maintain independent nodes while enforcing shared ACP 240 policies.

2. Data-Centric Security

- **Object-Level Encryption and Policy:** Every file, message, or record is wrapped with encryption and policy metadata that travels with the object.
- **Advanced ABAC:** Real-time policy evaluation based on role, clearance, location, and mission context ensures granular access control.
- **Policy Lifecycle Management:** XQ dynamically updates or revokes access as user attributes change.

3. Key Management & Offline / Disconnected Operations

- **Flexible Key Store:** External or self-hosted key management gives partners full control over cryptographic assets.
- **Offline Capability:** XQ enables secure offline data wrapping and encryption, with safe syncing when connectivity is restored.





- **Resilient Synchronization:** Secure coordination of keys and policies across multiple nodes ensures coalition-wide security.

4. Zero Trust Identity + Data Integration

- **Identity-Driven Access:** Access is contingent on real-time evaluation of user identity, device posture, and context.
- **Continuous Enforcement:** Policies are not static; decryption is only possible when all ABAC conditions are met.
- **Embedded Attributes:** Identity information is bound to each data object, ensuring access control persists even in disconnected environments.

5. Operationalization: SDKs, APIs, and Enforcement

- **Developer Tools:** SDKs and APIs allow integration of ACP 240/ ZTDF compliance into legacy or mission-critical applications.
- **Policy Enforcement Points (PEPs):** Pre-built enforcement points support common use cases like secure messaging, file sharing, and cross-domain transfers.
- **Ecosystem Enablement:** XQ partners with cross-domain solution providers and communications vendors for full coalition interoperability.

6. Audit and Governance

- **Comprehensive Logging:** Every access event, decryption attempt, and attribute evaluation is tracked.
- **Revocation and Control:** Policies can be updated or revoked dynamically, maintaining secure access over time.

7. Scalability & Future-Proofing





- **Standards-First Architecture:** Open-standard TDF/ZTDF support ensures future extensibility.
- **Large File and Streaming Support:** Handles mission-critical workloads of any size.
- **Federated & Distributed Deployment:** Supports multi-node, multi-national coalition environments.

Real-World Use Case: Coalition Edge Operations

Scenario: A multi-national task force must share sensitive intelligence across FVEY nations and NATO allies, including from forward operating bases with limited connectivity.

Challenge:

- Ensure secure sharing across classification boundaries.
- Retain national key sovereignty.
- Enforce policy dynamically across diverse environments.

XQ Solution:

1. Data is wrapped in ZTDF format with classification, policy, and mission-role metadata.
2. Each nation maintains its own key store, supporting sovereign control.
3. Forward units can wrap and encrypt data offline; XQ syncs securely when connectivity is restored.
4. Access is granted dynamically via ABAC evaluation, only for authorized users matching policy attributes.
5. All events are logged, providing full auditability across coalition operations.

Strategic Differentiators for XQ





- **Purpose-Built for ZTDF:** Designed for ACP 240 compliance with native data wrapping, ABAC, and cross-domain support.
- **Coalition Key Sovereignty:** Multi-KAS architecture ensures secure, sovereign key management.
- **Developer-Friendly:** SDKs, APIs, and PEPs accelerate mission application integration.
- **Zero Trust Maturity:** Continuous, object-level enforcement aligns with identity and data pillars of Zero Trust.
- **Audit & Governance:** Full logging and metadata tracking maintain accountability across multi-national operations.

Who Does ACP 240 Apply To?

ACP 240 primarily applies to:

- **NATO member nations and allied partners**, including the Five Eyes (FVEY) countries (United States, United Kingdom, Canada, Australia, and New Zealand).
- **Defense and military organizations** involved in multinational operations, such as coalition forces, carrier strike groups, and command structures.
- **Government agencies and contractors** in the Department of Defense (DoD) and equivalent organizations in allied nations, particularly those handling classified or mission-critical data.
- **Technology providers and integrators** building or deploying ACP 240-compliant systems, including software developers, security platforms (e.g., Virtru's Data Security Platform), and ecosystem partners that embed data protection into applications.

It is increasingly adopted for real-world operations, such as the UK's Operation HIGHMAST, where it facilitated secure data sharing among multiple allied partners during a global carrier strike group deployment.

What Data Does ACP 240 Apply To?

ACP 240 applies to:

- **Classified and sensitive data** shared in coalition environments, including operational intelligence, mission-critical files, emails, and collaboration documents.
- **Protected data requiring audit trails, access controls, and traceability**, such as information crossing command boundaries or involving multiple partners.





- **Any data in Zero Trust architectures**, where continuous validation of users, devices, and access is enforced—enabling flexibility for new partners to join without infrastructure overhauls.

The standard emphasizes metadata-based protections (e.g., policy enforcement points for email, files, and tools) to maintain security while improving agility in dynamic operations. It does not apply to unclassified or public data unless explicitly extended for compliance.

Conclusion

ACP 240, underpinned by ZTDF, establishes a new baseline for secure, interoperable, and policy-driven coalition collaboration. **XQ** is uniquely positioned to operationalize this standard, providing the tools, architecture, and integration capabilities necessary for real-world, mission-critical deployments.

Organizations looking to adopt ACP 240, enable cross-domain sharing, or implement Zero Trust data governance can rely on XQ to deliver scalable, secure, and fully auditable solutions.

Appendix:

ZTDF ACP-240 Ed A is a data-centric security standard that builds on the [Trusted Data Format \(TDF\)](#) to enable secure data sharing between the U.S. and NATO allies. It is an interoperable version of the TDF standard, ratified by the [NATO CCEB](#), that reconciles different classification and naming conventions, making it easier to share sensitive data securely across borders. The standard uses principles like encryption, metadata tagging, and attribute-based access control (ABAC) to protect data directly, not the perimeter around it.

Key features of ZTDF ACP-240 Ed A

- **Interoperability:** ZTDF acts as a bridge between U.S. and NATO standards (like NATO STANAGs 4774, 4778, and 5636). For example, it can automatically map a "Top Secret" tag to a "Above Secret" tag, ensuring proper handling across different frameworks.
- **Data-centric security:** Security is embedded directly into the data itself, not just the network. This means data remains protected no matter where it is, such as across clouds, networks, or countries.





- **Granular access control:** ZTDF uses attribute-based access control (ABAC) to grant access based on dynamic policies and attributes, rather than static, pre-defined groups. This ensures that only authorized individuals can access the data.
- **NATO and Five Eyes adoption:** ZTDF is at the core of ACP 240, a standard adopted by the U.S. Joint Chiefs of Staff, NATO, and the Five Eyes (FVEY) intelligence alliance. It is designed to facilitate secure coalition operations and is aligned with the [Combined Joint All-Domain Command and Control \(CJADC2\)](#) initiative.
- **Secure collaboration:** It enables seamless and secure data sharing and collaboration among allied nations by integrating with existing collaboration applications.
- **Dynamic data management:** The standard allows for the secure management and distribution of encryption keys across different domains.

