Kiteworks

FEATURE BRIEF

Securing Sensitive Data Exchange With TDF

Trusted Data Format: Standards-Based Digital Rights Management for Mission-Critical Operations

The Need to Control Sensitive Data Across Organizational Boundaries

Military operations, intelligence agencies, and government entities face a persistent challenge: securely exchanging classified and sensitive data across dissimilar systems, remote locations, and organizational boundaries. Whether transmitting operational intelligence from deployed sensors to command elements, sharing sensitive government data across agencies, or transferring critical infrastructure data from remote field sites to analysts, organizations need granular control over who accesses their data and under what conditions. Traditional file sharing methods lack the embedded security controls necessary to protect data once it leaves the sender's environment. Organizations require a solution that travels with the data itself, enforcing custom policies, classification levels, and access attributes regardless of where the data moves or which systems process it.

Standards-Based DRM That Travels With Data

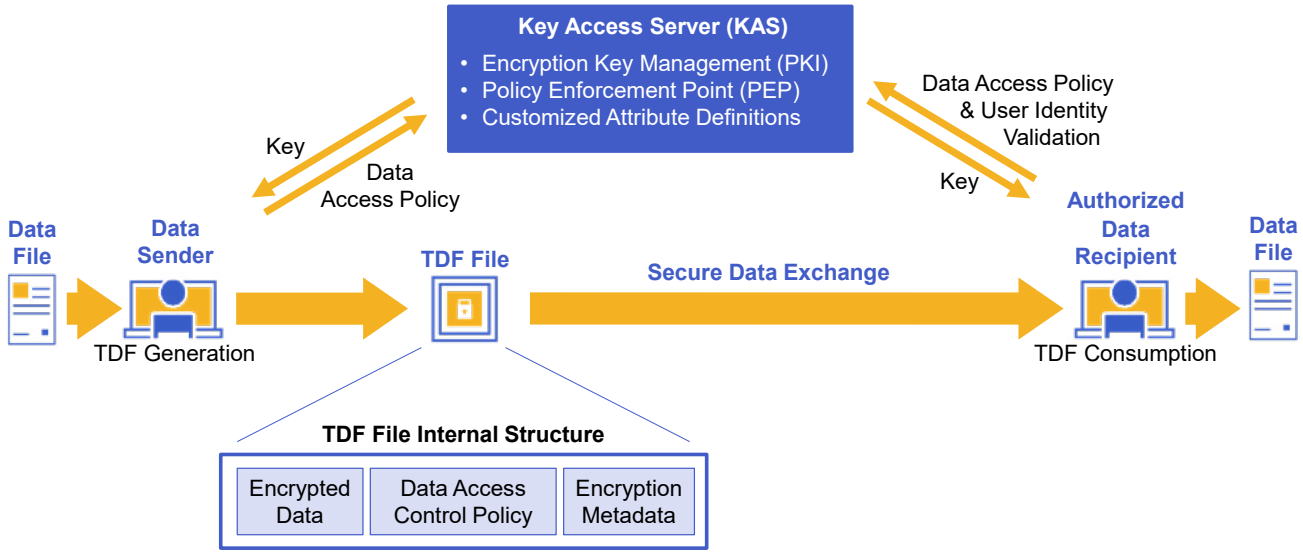

Figure 1: Trusted Data Format (TDF) Diagram.

Kiteworks addresses this challenge through its implementation of the OpenTDF (Open Trusted Data Format) standard, a standards-based digital rights management (DRM) solution integrated into the Kiteworks Private Data Network platform. OpenTDF provides strong, persistent encryption that embeds attribute-based access control (ABAC) policies directly within the data itself. This means a sender can define precisely who accesses their data based on custom attributes such as security clearance level, organizational affiliation, location, or operational role.

For example, intelligence data marked as Top Secret can be restricted to personnel holding appropriate clearances within specific geographic regions and time windows.

The Kiteworks implementation includes the OpenTDF Key Access Service (KAS) and Policy Enforcement Point (PEP), which validate recipient identity and access privileges before granting data access. Because these controls are embedded in the data file rather than relying on perimeter security, the protection persists whether the data crosses organizational boundaries, moves between agencies with different systems, or travels to remote locations with minimal infrastructure. The platform-independent nature of OpenTDF ensures interoperability across diverse technology environments without requiring recipients to use identical systems.

Organizations using Kiteworks gain visibility into data usage through a comprehensive audit log that tracks every access attempt, supporting compliance requirements such as CMMC, FedRAMP, FISMA, and HIPAA. Users access TDF-protected data through the familiar Kiteworks interface alongside standard files, eliminating workflow disruption while maintaining robust security controls.

Mission-Critical Security Across Five Key Sectors

Military: Secure transmission of intelligence and operational data from deployed systems, sensors, and personnel across all theaters to authorized command elements, ensuring only cleared personnel with appropriate need-to-know can access mission-critical information.

Government: Enables secure sharing of sensitive government data across agencies and governments while maintaining strict access controls and supporting compliance with federal security requirements.

Critical Infrastructure: Securely transfers IoT data from sensors and equipment in remote locations such as oil fields, dam sites, and telecommunications equipment to designated analysts and decision-makers at processing centers.

Healthcare: Enables transfers of medical records and research datasets between hospitals, clinics, researchers, insurance companies, and other entities while enforcing HIPAA compliance and preventing data breaches.

Financial Services: Secure sharing of financial transaction data, records, and audit logs between institutions, regulators, and partners with granular control over access and comprehensive audit capabilities.

Data Security That Transcends System Boundaries

The Kiteworks Trusted Data Format delivers the security controls that military, government, and critical infrastructure organizations require when exchanging sensitive data across organizational and system boundaries. By embedding access policies directly in the data and implementing the OpenTDF standard, Kiteworks ensures that sensitive information remains protected regardless of where it travels or which systems handle it.