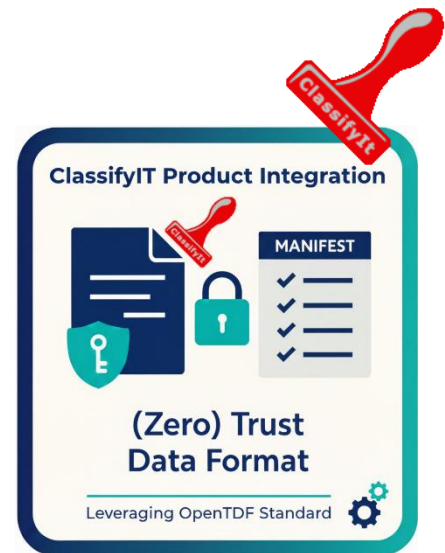


01 January 2026

## ClassifyIt: Driving Persistent Data Security

### **Enforcing Zero Trust Through OpenTDF & ZTDF Integration**

ClassifyIt is evolving from classification and labeling into a core engine for cryptographically enforced data protection. By integrating OpenTDF (Zero Trust Data Format), ClassifyIt brings persistent, policy-bound security directly into the data layer.



### **Why OpenTDF & ZTDF?**

Traditional perimeter security fails once data leaves the system. OpenTDF and ZTDF solve this by embedding protection directly into the file itself—independent of storage, transport, or location:

- **Interoperability:** No vendor lock-in
- **Access policies:** Rules stay embedded in the file
- **Cryptographic protection:** Security is tied to the data
- **Zero-Trust enforcement:** Embedded directly into the file

### **Security-First Implementation**

The implementation in ClassifyIt follows modern, high-assurance cryptographic standards from day one:

- **ECDH** (Elliptic Curve Diffie-Hellman) - Secure key exchange with strong forward secrecy
- **AES-256-GCM** - Authenticated encryption for confidentiality and integrity
- **Per-object Data Encryption Keys** (DEK) - Never reused, never exposed
- **Zero Trust by design** - No implicit trust in users, systems, or networks
- **(later) Policy-controlled key release** - Keys are only released after ABAC policy evaluation, with a Key Management System
- **(current) Local Elliptic Curve Certificate support** - exchange through standard PEM files

### **What This Enables**

- Persistent protection of documents and data
- Cryptographically enforced access control
- Interoperability with OpenTDF-compliant ecosystems
- Alignment with Zero Trust architectures (ZTNA / ABAC)
- A future-proof foundation for regulated and classified environments

### **Status**

**Active implementation in progress.** The focus is correctness, interoperability, and cryptographic robustness—before features and UI polish.