



Bruce Dombrowski
Developer

DATE: January 15, 2026

SOFTWARE: PdfSigner v1.0.6

REPOSITORY: <https://github.com/brucedombrowski/PdfSigner>

SUBJECT: Security Compliance Verification and NIST Control Alignment

1. Purpose

This Security Compliance Statement certifies that PdfSigner version 1.0.6 has been verified against federal security standards and documents alignment with NIST security controls.

2. Applicable Standards

This software has been evaluated for compliance with:

Standard	Title
NIST SP 800-53 Rev 5	Security and Privacy Controls for Information Systems
NIST SP 800-171	Protecting CUI in Nonfederal Systems and Organizations
FIPS 199	Standards for Security Categorization of Federal Information
FIPS 200	Minimum Security Requirements for Federal Information Systems

3. NIST Control Mapping

The following NIST SP 800-53 controls have been verified through automated scanning:

Control	Description	Implementation
SI-3	Malicious Code Protection	ClamAV malware scanning with signature database
SI-12	Information Management	PII pattern detection (SSN, phone, IP, credit card)
SA-11	Developer Testing and Evaluation	Secrets and credential scanning
SC-8	Transmission Confidentiality	MAC address and network identifier detection
CM-6	Configuration Settings	Host OS security posture verification
CM-8	System Component Inventory	CUI-marked host inventory collection



4. Security Scan Attestation

Automated security scans were executed using the Security Verification Toolkit:

- **Toolkit Repository:** <https://github.com/brucedombrowski/Security>
- **Scan Date:** January 15, 2026
- **Scan Results:** All automated checks passed

Scans performed include malware detection, PII pattern matching, secrets detection, and MAC address identification. Detailed scan artifacts are maintained in the project's `.scans/` directory.

5. Cryptographic Implementation

PdfSigner implements digital signature operations using industry-standard cryptographic libraries:

Component	Implementation
Hash Algorithm	SHA-256 (FIPS 180-4)
Signature Algorithms	RSA, ECDSA
Signature Format	CMS (Cryptographic Message Syntax, RFC 5652)
Key Storage	Windows Certificate Store (CAPI/CNG)
Smart Card Support	PIV/CAC via PKCS#11

6. Certificate Handling

The software implements secure certificate selection and handling:

- **EKU Requirements:** Certificates filtered by Extended Key Usage (Email Protection, Document Signing)
- **Government Prioritization:** DOD, NASA, and FPKI certificates prioritized in selection
- **X.509 OID Filtering:** Source code uses OIDs to filter certificates by purpose (e.g., 1.3.6.1.5.5.7.3.4 for Email Protection)
- **Read-Only Access:** Certificate store accessed in read-only mode

7. Security Controls

The following security controls are implemented in the software:

- **No Private Key Logging:** Private key material is never written to logs or output
- **Secure PIN Entry:** PIN prompts handled via Windows secure dialog (no application access)
- **Certificate Store Protection:** Read-only certificate store access prevents modification



- **Sensitive File Exclusions:** `.gitignore` excludes `*.pfx`, `*.p12`, `*.key`, and other sensitive file types

8. CUI Handling

Host inventory data generated during security verification is marked as Controlled Unclassified Information (CUI) per:

- **Authority:** 32 CFR Part 2002
- **Category:** CTI (Controlled Technical Information)
- **Safeguarding:** Per NIST SP 800-171

CUI-marked data includes MAC addresses, serial numbers, and system inventory. Handle according to organizational security policies.

9. Certification

I certify that:

- PdfSigner version 1.0.6 has been scanned using the Security Verification Toolkit
- All automated security checks have passed
- The software implements the security controls documented herein
- This statement is accurate and complete to the best of my knowledge