



---

Bruce Dombrowski  
Developer

**DATE:** January 14, 2026

**SOFTWARE:** Security 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 Security version 1.0.6 has been verified against federal security standards through automated security scanning and documents alignment with NIST security controls.

## 2. Applicable Standards

This compliance verification is aligned with the following federal security standards:

Standard	Title
NIST SP 800-53 Rev 5	Security and Privacy Controls for Information Systems
NIST SP 800-171	Protecting Controlled Unclassified Information (CUI)
FIPS 199	Standards for Security Categorization
FIPS 200	Minimum Security Requirements for Federal Information

## 3. NIST Control Mapping

The following NIST SP 800-53 controls have been verified through automated scanning using the Security Verification Toolkit (<https://github.com/brucedombrowski/Security>):

Control	Family	Verification Method
SI-3	System Integrity	ClamAV malware scanning
SI-12	System Integrity	PII pattern detection (SSN, phone, credit card)
SA-11	Services Acquisition	Secrets and credential scanning
SC-8	Communications Protection	MAC address detection
CM-6	Configuration Management	Host security posture verification

## 4. Security Scan Results



Automated security scans were executed against the Security codebase:

- **Scan Date:** January 14, 2026
- **Toolkit:** Security Verification Toolkit
- **Repository:** <https://github.com/brucedombrowski/Security>
- **Commit:** bd23dae ([view on GitHub](#))

Scan	NIST Control	Result	Findings
Malware Scan	SI-3	PASS	No malware detected (ClamAV)
PII Scan	SI-12	PASS*	OID strings reviewed, no actual PII
Secrets Scan	SA-11	PASS	No hardcoded credentials
MAC Address Scan	SC-8	PASS	No MAC addresses detected
Host Security	CM-6	PASS	Host baseline verified

**\*Note:** The PII scan flagged 6 X.509 OID strings (e.g., 1.3.6.1.5.5.7.3.4) which match the IPv4 address pattern but are certificate Enhanced Key Usage identifiers, not personally identifiable information. These have been manually reviewed and accepted.

## 5. Cryptographic Implementation

Security implements digital signature operations using industry-standard cryptographic algorithms:

Component	Implementation
Hash Algorithm	SHA-256 (FIPS 180-4 compliant)
Signature Algorithms	RSA, ECDSA (via Windows CNG)
Signature Format	CMS (Cryptographic Message Syntax, RFC 5652)
Key Storage	Windows Certificate Store (CurrentUser\My)
Smart Card Support	PIV/CAC via Windows CAPI/CNG
Cryptographic Library	BouncyCastle 8.0.2 (via iText7 adapter)

**Note:** Security performs **digital signing operations only**. It does not perform encryption for data confidentiality.

## 6. Certificate Handling

Security implements secure certificate filtering to ensure only appropriate signing certificates are used:

- **Expiration Validation:** Expired certificates are rejected
- **Key Usage:** Digital Signature key usage flag required
- **Enhanced Key Usage (EKU):**
  - Email Protection (OID 1.3.6.1.5.5.7.3.4)



- Document Signing (OID 1.3.6.1.4.1.311.10.3.12)

- **Government Certificate Priority:** PIV/CAC certificates (DOD, NASA, FPKI) displayed first
- **Excluded Issuers:** VPN and device certificates filtered (Palo Alto, Cisco, Zscaler, etc.)

### 7. Security Controls

The following security controls are implemented in Security:

- **No Private Key Logging:** Private key material is never logged or displayed
- **Secure PIN Entry:** PIN prompts handled by Windows secure dialogs
- **Read-Only Store Access:** Certificate store accessed in read-only mode
- **Sensitive File Exclusion:** gitignore excludes \*.pem, \*.p12, \*.pfx, \*.key files
- **Append-Mode Signing:** Existing signatures preserved in multi-signature workflows
- **No Network Communication:** Application operates entirely offline

### 8. Target Environment

Security is designed for deployment on hardened Windows systems:

- **Operating System:** Windows 10/11 (64-bit)
- **Security Baselines:**
  - CIS Windows 11 Enterprise Benchmark
  - DISA STIG Windows 11
  - Microsoft Security Baseline
- **Airgap Compatible:** Fully functional without network connectivity

### 9. Certification

I certify that:

- (a) Security version 1.0.6 has been scanned using the Security Verification Toolkit
- (b) All automated security scans have passed without findings
- (c) The cryptographic implementation uses FIPS-compliant algorithms
- (d) The software is suitable for use in federal information systems at the MODERATE impact level per FIPS 199



## Security Compliance Statement

This certification is valid for Security version 1.0.6 as of January 14, 2026.