



DEFENSE INFORMATION SYSTEMS AGENCY
JOINT INTEROPERABILITY TEST COMMAND
2001 BRAINARD ROAD
FORT HUACHUCA, ARIZONA 85613-7051

IN REPLY

REFER TO: Networks, Transmission, and
Intelligence Division (JTE)

24 Oct 02

Information Security Corporation
ATTN: Mr. Jonathan Schulze-Hewett
1141 Lake Cook Road, Suite D
Deerfield, IL 60015-9461

Dear Mr. Schulze-Hewett:

The Joint Interoperability Test Command (JITC) completed Department of Defense (DOD) Public Key Infrastructure (PKI) certification compliance testing of Information Security Corporation's SecretAgent 5.6.0

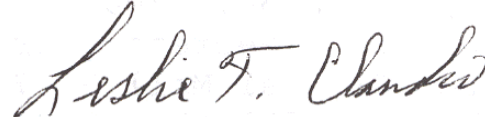
JITC certifies the Public Key-Enabled application, SecretAgent 5.6.0, meets the applicable requirements of the "Department of Defense Class 3 Public Key Infrastructure Public Key-Enabled Application Requirements, Version 1.0," 13 July 2000, to the extent detailed in the enclosed summary, "Certification Compliance Testing Summary."

JITC conducted the test at its PKI laboratory on Fort Huachuca, Arizona, using the JITC test plan "Department of Defense Public Key Infrastructure Interoperability Master Test Plan, Version 1.2." The test purpose was to determine the extent SecretAgent 5.6.0 interoperates with the DOD PKI.

JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system - using unclassified (NIPRNET) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/.gov users on the NIPRNET at: <https://stp.fhu.disa.mil/>. Related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at: <http://jit.fhu.disa.mil> (NIPRNET) or <http://199.208.204.125> (SIPRNET).

The JITC point of contact is Ms. Cammie Webster, DSN 879-5485, commercial (520) 538-5485, or e-mail websterc@fhu.disa.mil.

Sincerely,



LESLIE F. CLAUDIO
Chief
Networks, Transmission and
Intelligence Division

1 Enclosure:
Certification Compliance
Testing Summary

Copy to:

Department of Defense, Public Key Infrastructure Program
Management Office, ATTN: Mr. Marvin Jennings, 9800 Savage Road,
Fort Meade, MD 20755

Defense Information Systems Agency, API, ATTN: Ms. Betsy
Appleby, 5275 Leesburg Pike, Room 2W-16-6A, Falls Church, VA
22041

CERTIFICATION COMPLIANCE TESTING SUMMARY

1. **CANDIDATE.** Information Security Corporation's SecretAgent 5.6.0
2. **TESTER.** Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona.
3. **APPLICATION UNDER TEST DESCRIPTION.** Information Security Corporation's SecretAgent 5.6.0 is a file encryption and digital signature utility. Automatically installed macros allow users to sign and/or encrypt Microsoft (MS) Office documents or e-mail message bodies and attachments within Outlook, GroupWise, and Netscape. Messaging application interface support allows secure e-mail to be sent directly within SecretAgent. A graphical user interface tool based on MS Windows explorer allows users to sign and encrypt files or folders. SecretAgent provides integration with MS Cryptography Application Interface (CAPI) databases so the same certificates can be used with Internet Explorer, Outlook, and other CAPI-based applications.
4. **PURPOSE.** To determine the extent Information Security Corporation's SecretAgent interoperates with the Department of Defense (DOD) Public Key Infrastructure (PKI).
5. **TEST DESCRIPTION.** The test exercised the capability of SecretAgent to use DOD PKI software certificates issued from the JITC PKI Test Certificate Authority (CA) servers. JITC introduced valid, revoked, and expired certificates to determine the extent SecretAgent complies with DOD procedures. Testing determined the capability of SecretAgent to properly use software certificates issued by DOD PKI and determined the accuracy of the methods SecretAgent uses to communicate with the DOD PKI. The test did not address the security assurance methods, procedures, and algorithms that SecretAgent uses to secure data.

6. TEST NETWORK CONFIGURATION. The test did not require any special test equipment. Figure 1 shows the SecretAgent test network.

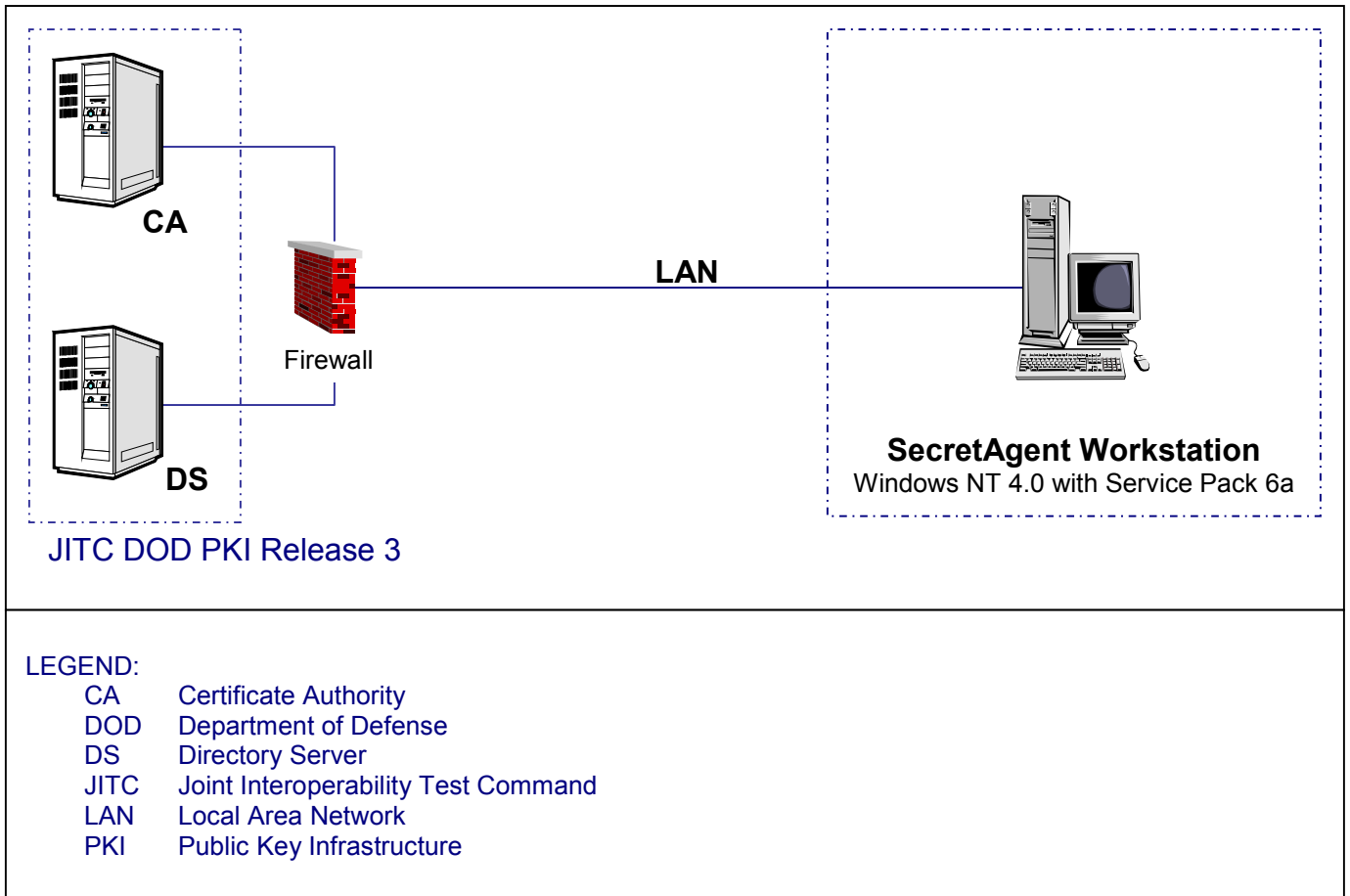


Figure 1. SecretAgent 5.6.0 Test Network

7. WORKSTATION CONFIGURATION. Table 1 shows the workstation configuration information for all tests.

Table 1. Workstation Configuration

Specifications	SecretAgent 5.6.0 Workstation
Hardware	Micron Client Pro 800 Megahertz (MHz) Processor 256 Megabyte (MB) Random Access Memory (RAM)
Operating System	MS Windows NT 4.0 Server, with Service Pack (SP) 6a
Software	Information Security Corporation's SecretAgent 5.6.0 Information Security Corporation's Certificate Explorer 2.6.0.68 MS Internet Explorer 5.5 with SP 2 MS Office 2000
Communications Link	Unclassified but Sensitive Internet Protocol Router Network (NIPRNET)
Certificates Used	National Institute of Standards and Technology (NIST) Level 1 and Level 2 Path Processing Suite of Test Certificates. JITC-issued certificates: Valid, expired, and revoked test software test certificates

8. TEST LIMITATIONS. None.

9. TEST RESULTS. Information Security Corporation's SecretAgent 5.6.0 is certified as compliant with "Department of Defense (DOD) Class 3 Public Key Infrastructure (PKI) Public Key-Enabled Application Requirements, Version 1.0," 13 July 2000. SecretAgent 5.6.0 accomplished the following:

- Retrieved DOD PKI certificates.
- Imported DOD PKI public and private encryption keys contained in DOD PKI identity certificates.
- Provided for the addition and deletion of DOD PKI trust points.
- Used the Lightweight Directory Access Protocol (LDAP) to communicate with the DOD PKI.
- Resolved the status of certificates.
- Processed and developed a path of certificates and Certificate Revocation Lists (CRLs) that related a given end-entity to a trust point using path processing.
- Was configured for use with the DOD PKI.
- Included a user's manual that provided adequate instruction on proper and secure use of the application. SecretAgent manuals included configuration instructions to operate with the DOD PKI.

Specific test findings are in tables in Appendix A.

APPENDIX A

SPECIFIC TEST FINDINGS

<u>Table #</u>	<u>Table Title</u>
A-1	Retrieving Certificates
A-2	Importing Keys and Certificates
A-3	Storing Trust Points
A-4	Verifying Communication Protocols
A-5	Checking Certificate Status
A-6	Path Development and Processing
A-7	Application Configuration
A-8	Application Documentation

Table A-1. Retrieving Certificates

EVENT	PROCEDURE	OBSERVATION	RESULTS
1.1	Sign test document using User1 certificate and send document to User2.	Signed document with User1 certificate and sent document to User2.	PASS
1.2	Login as User2 and validate User1 certificate.	Logged in as User2 and validated User1 certificate.	PASS

Table A-2. Importing Keys and Certificates

EVENT	PROCEDURE	OBSERVATION	RESULTS
2.1	Load certificates for use by SecretAgent.	Loaded certificates.	PASS
2.2	Sign test document using User1 identity certificate and send document to User2.	Signed a test document using User1 identity certificate.	PASS
2.3	Login as User2 and validate User1 identity certificate.	Logged in as User2 and validated User1 identity certificate.	PASS

Table A-3. Storing Trust Points

EVENT	PROCEDURE	OBSERVATION	RESULTS
3.1	Add trust for JITC root and intermediate CA certificate into the trust point list.	Added the JITC root and intermediate CA certificate into SecretAgent's Certificate Explorer.	PASS
3.2	Sign test documents using JITC-issued certificates.	Signed test documents using JITC-issued certificates.	PASS
3.3	Remove trust for JITC root and intermediate CA certificates from the trust point list.	Removed the JITC root and intermediate CA certificate from SecretAgent's Certificate Explorer.	PASS
3.4	Sign test documents with the trust removed for JITC-issued certificates.	Unable to sign test documents with the trust removed for JITC-issued certificates.	PASS

Table A-4. Verifying Communication Protocols

EVENT	PROCEDURE	OBSERVATION	RESULTS
4.1	Signed test document using User1 certificate and send document to User2.	Signed document with User1 certificate and sent document to User2.	PASS
4.2	Login as User2 and validate User1 certificate to verify proper use of LDAP by SecretAgent.	Logged in as User2 and validated User1 certificate.	PASS

Table A-5. Checking Certificate Status

EVENT	PROCEDURE	OBSERVATION	RESULTS
5.1	Verify the signature on each Certificate Revocation List (CRL) in the certification path using the same public key used to sign certificates.	Signatures verified.	PASS
5.2	Verify that the issuer name in the certificate matches the issuer name in the CRL.	Issuer name matched.	PASS
5.3	Attempt to reject the path if any certificate in the certificate path has been revoked.	Path rejected.	PASS

Table A-5. Checking Certificate Status (continued)

EVENT	PROCEDURE	OBSERVATION	RESULTS
5.4	Ensure SecretAgent rejects the path if any certificate in the certificate path had been revoked regardless of whether or not there were unrecognized critical <i>crlEntryExtensions</i> present in the CRL.	Path rejected.	PASS
5.5	Ensure SecretAgent detects an invalid CRL if the <i>nextUpdate</i> time in the certificate is earlier than the current time.	Invalid CRL detected.	PASS
5.6	Ensure SecretAgent detects a CRL that does not contain the <i>deltaCRLIndicator</i> extension.	Issuing <i>deltaCRLIndicator</i> extension not present.	PASS

Table A-6. Path Development and Processing

EVENT	PROCEDURE	OBSERVATION	RESULTS
6.1	Verify digital signatures on each certificate in the certification path using the superior public key.	Digital signatures verified.	PASS
6.2	Verify the <i>notBefore</i> time of each certificate in the certification path is earlier than the current time.	<i>notBefore</i> time earlier.	PASS
6.3	Verify the <i>notAfter</i> time of each certificate in the certification path is later than the current time.	<i>notAfter</i> time later.	PASS
6.4	Verify that names chain correctly.	Names chain correctly.	PASS
6.5	Ensure SecretAgent rejects the certificate path when unable to retrieve revocation data.	Certificate path rejected.	PASS
6.6	Ensure SecretAgent rejects the certificate path if any certificate in the certificate path has been revoked.	Certificate path rejected.	PASS
6.7	Verify the <i>basicConstraints</i> extension is present in every intermediate certificate in the certification path.	<i>basicConstraints</i> extension present.	PASS
6.8	Verify every intermediate certificate in the certificate path has the <i>basicConstraints</i> extension present and the <i>cA</i> component set to <i>true</i> .	<i>basicConstraints</i> present/ <i>cA</i> present and the <i>cA</i> component set to <i>true</i> .	PASS

Table A-6. Path Development and Processing (continued)

EVENT	PROCEDURE	OBSERVATION	RESULTS
6.9	Verify the certificate has the <i>cA</i> component of the <i>basicConstraints</i> extension present and set to <i>true</i> when it encounters an intermediate certificate in the certificate path. The certificate should have the <i>keyUsage</i> extension present and marked critical with the <i>keyCertSign</i> bit set to <i>true</i> .	<i>basicConstraints</i> present/ <i>cA</i> present and the <i>keyCertSign</i> bit set to <i>true</i> .	PASS
6.10	Verify every intermediate certificate in the certificate path (that has the key usage extension present) has the <i>keyCertSign</i> bit set to <i>true</i> .	<i>keyCertSign</i> bit set to <i>true</i> .	PASS
6.11	Verify every intermediate certificate in the certificate path containing the public key of a CRL signer (that has the <i>keyUsage</i> extensions present) has the <i>cRLSign</i> bit set to <i>true</i> .	<i>keyUsage</i> extensions present and the <i>cRLSign</i> bit set to <i>true</i> .	PASS

Table A-7. Application Configuration

EVENT	PROCEDURE	OBSERVATION	RESULTS
7.1	Inspect SecretAgent documentation and system configuration to verify its capability of being configured to operate with the DOD PKI.	SecretAgent User's Guide covers the procedures to configure SecretAgent to operate with the DOD PKI.	PASS
7.2	Verify SecretAgent documentation identifies the operating conditions required of its operating environment.	SecretAgent User's Guide identifies the operating conditions of the operating environment.	PASS
7.3	Verify SecretAgent identifies all necessary conditions and dependencies for it to securely perform its functions.	SecretAgent uses DOD PKI issued PKI certificates in the Public Key Cryptography Standards #12 format.	PASS

Table A-7. Application Configuration (continued)

7.4	Verify SecretAgent has the capability to be configured for secure operation in its intended environments.	SecretAgent operates while trusting the DOD Root only.	PASS
7.5	Verify SecretAgent provides automated features to satisfy minimum DOD requirements. If not, verify SecretAgent procedures are well documented and easily followed.	SecretAgent provides automated features. SecretAgent's procedures are well documented and easily followed in the User's Guide.	PASS
7.6	Verify SecretAgent is capable of being configured to operate with only DOD PKI trust points.	Ensured SecretAgent uses its Certificate Explorer utility to operate with only DOD PKI trust points.	PASS

Table A-8. Application Documentation

EVENT	PROCEDURE	OBSERVATION	RESULTS
8.1	Verify instructions cover installing DOD PKI trust points.	SecretAgent User's Guide (page 90) explains how to load the trust anchors into SecretAgent's Certificate Explorer.	PASS
8.2	Verify instructions cover removing non-DOD PKI trust points.	SecretAgent User's Guide (page 107) explains how to remove the trust anchors from SecretAgent's Certificate Explorer.	PASS
8.3	Verify instructions cover requesting and obtaining certificates or importing keys and certificates.	SecretAgent User's Guide (page 94, 97, and 100) provides instructions for requesting and importing keys and certificates.	PASS
8.4	Verify instructions cover installing Uniform Resource Indicators for DOD PKI Services, such as obtaining certificates for other entities and performing status checking.	SecretAgent User's Guide (page 79 and page 119) explains how to remove the trust anchors from SecretAgent's Certificate Explorer.	PASS