



DEFENSE INFORMATION SYSTEMS AGENCY
JOINT INTEROPERABILITY TEST COMMAND
P.O. BOX 12798
FORT HUACHUCA, ARIZONA 85670-2798

Mr. Paul Townsend
CoreStreet, Ltd.
One Alewife Center, Suite 200
Cambridge, MA 02140

13 Jun 08

Dear Mr. Townsend:

The Joint Interoperability Test Command (JITC) completed Department of Defense (DoD) Public Key Infrastructure (PKI) testing of CoreStreet, Ltd.'s Responder Appliance 2400D, version 3.0.1 build 2.

The JITC certifies that the Online Certificate Status Protocol (OCSP) Responder, CoreStreet, Ltd.'s Responder Appliance 2400D, version 3.0.1 build 2, complies with the applicable requirements defined in "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol, Request for Comments 2560," June 1999, to the extent detailed in the enclosed "Compliance Testing Summary." Table 1 shows certification requirements for all OCSP Responders and the test results for CoreStreet, Ltd.'s Responder Appliance 2400D, version 3.0.1 build 2.

CoreStreet, Ltd.'s Responder Appliance 2400D, version 3.0.1 build 2 supports all mandatory requirements and some non-mandatory requirements.

Table 1. Test Results

OCSP REQUIREMENT	MANDATORY	RESULT
Unsigned OCSP Requests	YES	PASSED
Signed OCSP Requests	YES	PASSED
Multiple Certificate Status Requests	YES	PASSED
Signed OCSP Responses	YES	PASSED
OCSP Response Extensions		
Nonce	NO	NOT SUPPORTED
CRL Reference	NO	NOT SUPPORTED
Acceptable Response Type	NO	PASSED
Archive Cutoff	NO	NOT SUPPORTED

Table 1. Test Results (continued)

OCSP REQUIREMENT	MANDATORY	RESULT
Retrieving Large CRLs		
Retrieve 2-MB CRL	YES	PASSED
Retrieve 4-MB CRL	YES	PASSED
Retrieve 8-MB CRL	YES	PASSED
Verifying Communications Protocol from OCSP Responder to OCSP Client		
Accept OCSP requests using HTTP	YES	PASSED
Accept OCSP requests using HTTPS	YES	PASSED
Verifying Communications Protocol from OCSP Responder to DoD Class 3 PKI		
Retrieve CRL using HTTP	YES	PASSED
Retrieve CRL using HTTPS	NO	PASSED
Retrieve CRL using LDAP	YES	PASSED
Retrieve CRL using LDAPS	NO	NOT SUPPORTED
LEGEND:		
CRL	Certificate Revocation List	LDAPS
DoD	Department of Defense	MB
HTTP	Hypertext Transfer Protocol	OCSP
HTTPS	HTTP, Secure, over SSL	PKI
LDAP	Lightweight Directory Access Protocol	SSL
		LDAP over SSL
		Megabyte
		Online Certificate Status Protocol
		Public Key Infrastructure
		Secure Sockets Layer

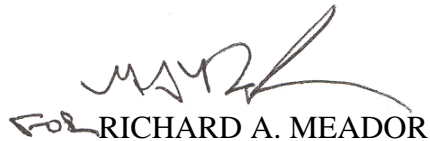
The JITC conducted the test at its Fort Huachuca, AZ, Public Key Enabled Application Testing Laboratory from 19 through 21 February 2008 using the JITC "Department of Defense Online Certificate Status Protocol Responder Interoperability Master Test Plan," version 1.0, July 2003. Testing did not include an evaluation of interoperability between OCSP Responders, or between OCSP Responders and OCSP clients other than the one used in the test.

The JITC distributes testing information via the JITC Electronic Report Distribution system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) E-mail. More comprehensive testing 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> Secret Internet Protocol Router Network.

The JITC also provides information about OCSP Responder testing, which is accessible via the JITC PKI public web site at <http://jitc.fhu.disa.mil/pki>.

The JITC point of contact is Mr. Michael Kutch, DSN 879-5265, commercial (520) 538-5265, or E-mail: Michael.Kutch@disa.mil.

Sincerely,


RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

1 Enclosure:
Compliance Testing Summary

Copy to:
National Security Agency, Public Key Infrastructure Program Management Office,
ATTN: Ms. Debra Grempler, 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