



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, version 5.1.5.

The JITC certifies that the Online Certificate Status Protocol (OCSP) Responder, CoreStreet Ltd.'s Responder, version 5.1.5, 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, version 5.1.5.

CoreStreet Ltd.'s Responder, version 5.1.5 supports all mandatory requirements and some non-mandatory requirements.

Table 1. Test Results

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

Table 1. Test Results (continued)

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

The JITC conducted the test at its Fort Huachuca, AZ, Public Key-Enabled Application Testing Laboratory from 6 February through 5 March 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,


FOR 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, Maryland 20755
Defense Information Systems Agency, API, ATTN: Ms. Trish Janssen, 5275 Leesburg Pike,
NE32 Room #3W08-3A, Falls Church, Virginia 22041