



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

IN REPLY

REFER TO: Networks and Transport Division (JTE)

10 January 2005

Tumbleweed Communications Corporation
Mr. John Hines
Director, Software Engineering
700 Saginaw Drive
Redwood City, CA 94063

Dear Mr. Hines:

The Joint Interoperability Test Command (JITC) has completed Department of Defense (DOD) Public Key Infrastructure (PKI) testing of Tumbleweed Valicert Enterprise Validation Authority (EVA) 4.7.3.

JITC certifies that the Online Certificate Status Protocol (OCSP) Responder, Tumbleweed Valicert EVA 4.7.3, 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 Tumbleweed Valicert EVA 4.7.3.

Tumbleweed Valicert EVA 4.7.3 supports all mandatory requirements and some non-mandatory requirements.

Table 1. Tumbleweed Valicert EVA 4.7.3 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	PASSED
CRL Reference	NO	NOT SUPPORTED
Acceptable Response Type	NO	PASSED
Archive Cutoff	NO	NOT SUPPORTED

Table 1. Tumbleweed Valicert EVA 4.7.3 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	PASSED	
LEGEND			
CRL	Certificate Revocation List	LDAPS	LDAP over SSL
DOD	Department of Defense	MB	Megabyte
HTTP	Hypertext Transfer Protocol	OCSP	Online Certificate Status Protocol
HTTPS	HTTP Secure	PKI	Public Key Infrastructure
LDAP	Lightweight Directory Access Protocol	SSL	Secure Sockets Layer

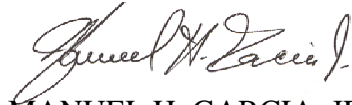
JITC conducted the test at its Fort Huachuca, AZ, Public Key Enabled (PKE) Application Testing Laboratory from 7 through 10 December 2004 using the JITC "Department of Defense Online Certificate Status Protocol Responder Interoperability Master Test Plan," version 1.0, July 2003. Testing did not include an evaluation of interoperability between OCSP Responders or between OCSP Responders and OCSP clients other than the one used in the test.

JITC distributes testing information via the JITC Electronic Report Distribution (ERD) 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.

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. Mark Lehtimaki, DSN 879-0487, commercial (520) 538-0487, or e-mail lehtimam@fhu.disa.mil.

Sincerely,



MANUEL H. GARCIA, JR.
Acting Chief
Networks and Transport Division

1 Enclosure a/s

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