



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY
REFER TO: Joint Interoperability Test Command (JTE)

MEMORANDUM FOR DISTRIBUTION

9 Aug 11

Subject: Special Interoperability Test Certification of the LiteScape Biometric Secure Profile Authentication Reader (SPAR)TM with Firmware Version 3.0 and Secure Profile Management (SPM) Release 4.4

References: (a) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) CJCSI 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008
(c) through (e), see Enclosure 1

1. References (a) and (b) establish the Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification.

2. The LiteScape Biometric SPARTM with Firmware Version 3.0, Net4.0 for Linux 2.4, and SPM Release 4.4 is hereinafter referred to as the System Under Test (SUT). The SUT meets all of its critical interoperability requirements and is certified as interoperable for joint use within the Defense Information System Network (DISN) as an Internet Protocol (IP) Customer Premise Equipment (CPE). The SUT meets the critical interoperability requirements set forth in Reference (c), using test procedures derived from Reference (d). The SUT was tested and certified with the Cisco Media Communications Server (MCS) 7835H2. Since other Cisco MCS Servers also listed on the Unified Capabilities (UC) Approved Product List (APL) or previously listed on the UC APL are functionally identical to the MCS 7835H2, JITC analysis determined the SUT is also interoperability certified for joint use with these other servers. Furthermore, the SUT was tested and certified for joint use only with the Cisco Unified Communication Manager (CUCM) Release 7.1(2). However, JITC analysis determined the SUT is also certified for joint use with any other CUCM or Cisco Call Manager (CCM) Private Branch Exchange and their associated IP end instruments that are listed on the UC APL or have been previously listed on the UC APL. The SUT is certified to support DISN assured services over IP with any Assured Services Local Area Network (ASLAN) certified for use. No other configurations, features, or functions, except those cited within this report, are certified by the JITC. This certification expires upon changes that could affect interoperability, but no later than three years from 19 July 2011; which is the date the DISA Certifying Authority (CA) provided a positive Recommendation for the SUT Information Assurance posture.

3. This finding is based on interoperability testing, DISA adjudication of open test discrepancy reports, review of the vendor’s Letter of Compliance (LoC), and DISA CA recommendation. Interoperability testing was conducted by JITC at the Global Information Grid Network Test Facility, Fort Huachuca, Arizona, from 27 through 29 October 2010. The DISA adjudication of outstanding test discrepancy reports was completed on 24 February 2011. The DISA CA recommended positive approval on 19 July 2011 based on the security testing completed by DISA-led IA test teams and published in a separate report, Reference (e). Enclosure 2 documents the test results and describes the tested network and system configurations.

4. The Functional Requirements used to evaluate the interoperability of the SUT and the interoperability statuses are indicated in Table 1.

Table 1. SUT Functional Requirements and Interoperability Status

Interfaces	Critical	Certified	Functional Requirements	Status	UCR Paragraph																								
IP 100BaseT (IEEE 802.3-2005)	Yes	Yes	MLPP Interaction (R)	Met ¹	5.2.3.2																								
			VoIP System Security (R)	Met ²	5.4																								
			IPv6 (C)	Not Tested ³	5.3.5																								
			VoIP System Service Tagging-End User Devices (R)	Met	5.3.3.3.2																								
<p>NOTES:</p> <p>1 All MLPP call scenarios were successful met with the following minor exception: An incoming higher precedence call placed to the SUT fails to be properly diverted if the user is in the process of logging out of the SUT and then cancels the logout process by pressing the exit button. To eliminate this anomaly from occurring, it is recommended that when logging in or logging out with the SUT, that the user not interface with the SUT until the login or logoff process is complete. When a higher precedence call is placed to the SUT’s respective IP end instrument while the login or logoff is in progress, the calls are properly diverted to the alternate directory number as required by the UCR, paragraph 3.3.</p> <p>2 Security is tested by DISA-led Information Assurance test teams and published in a separate report, Reference (e).</p> <p>3 In accordance with UCR 2008 Change 1 section 5.3.5 Table 5.3.5-1 with exception of IP End Instruments all CPE devices have a conditional requirement for IPv6 capability. This capability is conditional for the SUT and was not tested.</p> <p>LEGEND:</p> <table> <tr> <td>100BaseT</td> <td>100 Mbps (Baseband Operation, Twisted Pair) Ethernet</td> <td>IPv6</td> <td>Internet Protocol version 6</td> </tr> <tr> <td>802.3-2005</td> <td>Local Area Network/metropolitan Area Network Carrier Sense Multiple Access/Collision Detection Access Method</td> <td>MLPP</td> <td>Multi-Level Precedence and Preemption</td> </tr> <tr> <td>CPE</td> <td>Customer Premise Equipment</td> <td>R</td> <td>Required</td> </tr> <tr> <td>DISA</td> <td>Defense Information Systems Agency</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>IEEE</td> <td>Institute of Electrical and Electronics Engineers</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>IP</td> <td>Internet Protocol</td> <td>VoIP</td> <td>Voice over Internet Protocol</td> </tr> </table>						100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	IPv6	Internet Protocol version 6	802.3-2005	Local Area Network/metropolitan Area Network Carrier Sense Multiple Access/Collision Detection Access Method	MLPP	Multi-Level Precedence and Preemption	CPE	Customer Premise Equipment	R	Required	DISA	Defense Information Systems Agency	SUT	System Under Test	IEEE	Institute of Electrical and Electronics Engineers	UCR	Unified Capabilities Requirements	IP	Internet Protocol	VoIP	Voice over Internet Protocol
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	IPv6	Internet Protocol version 6																										
802.3-2005	Local Area Network/metropolitan Area Network Carrier Sense Multiple Access/Collision Detection Access Method	MLPP	Multi-Level Precedence and Preemption																										
CPE	Customer Premise Equipment	R	Required																										
DISA	Defense Information Systems Agency	SUT	System Under Test																										
IEEE	Institute of Electrical and Electronics Engineers	UCR	Unified Capabilities Requirements																										
IP	Internet Protocol	VoIP	Voice over Internet Protocol																										

5. No detailed test report was developed in accordance with the Program Manager’s request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (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>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <https://jit.fhu.disa.mil> (NIPRNet), or <http://199.208.204.226> (SIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly through


JITC Memo, JTE, Special Interoperability Test Certification of the LiteScape Biometric Secure Profile Authentication Reader (SPAR)TM with Firmware Version 3.0 and Secure Profile Management (SPM) Release 4.4

government civilian or uniformed military personnel from the Unified Capabilities Certification Office (UCCO), e-mail: ucco@disa.mil.

6. The JITC point of contact is Mr. Edward Mellon, DSN 879-5159, commercial (520) 538-5159, FAX DSN 879-4347, or e-mail to edward.mellon@disa.mil. The JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The tracking number for the SUT is 1015201.

FOR THE COMMANDER:

2 Enclosures a/s


for BRADLEY A. CLARK
Chief
Battlespace Communications Portfolio

Distribution:

Joint Staff J-6

Joint Interoperability Test Command, Liaison, TE3/JT1

Office of Chief of Naval Operations, CNO N6F2

Headquarters U.S. Air Force, Office of Warfighting Integration & CIO, AF/XCIN (A6N)

Department of the Army, Office of the Secretary of the Army, DA-OSA CIO/G-6 ASA (ALT), SAIS-IOQ

U.S. Marine Corps MARCORSSYSCOM, SIAT, MJI Division I

DOT&E, Net-Centric Systems and Naval Warfare

U.S. Coast Guard, CG-64

Defense Intelligence Agency

National Security Agency, DT

Defense Information Systems Agency, TEMC

Office of Assistant Secretary of Defense (NII)/DOD CIO

U.S. Joint Forces Command, Net-Centric Integration, Communication, and Capabilities Division, J68

Defense Information Systems Agency, GS23

ADDITIONAL REFERENCES

- (c) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008, Change 1," 22 January 2010
- (d) Joint Interoperability Test Command, "Defense Switched Network Generic Switch Test Plan (GSTP), Change 2," 2 October 2006
- (e) Joint Interoperability Test Command, "Information Assurance (IA) Assessment of LiteScape Biometric Secure Profile Authentication Reader (SPAR)TM with Secure Profile Management (SPM) Release 4.4 (Tracking Number 1015201)," 19 July 2011

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. The LiteScape Biometric Secure Profile Authentication Reader (SPAR)[™] with Firmware Version 3.0 and Secure Profile Management (SPM) Release 4.4, is hereinafter referred to as the System Under Test (SUT).

2. PROPONENT. Defense Information Systems Agency (DISA).

3. PROGRAM MANAGER. Mr. Quinten Ancar, NS41, Post Office Box 4502, Arlington, Virginia, 22204-4502, e-mail: quentin.ancar@disa.mil.

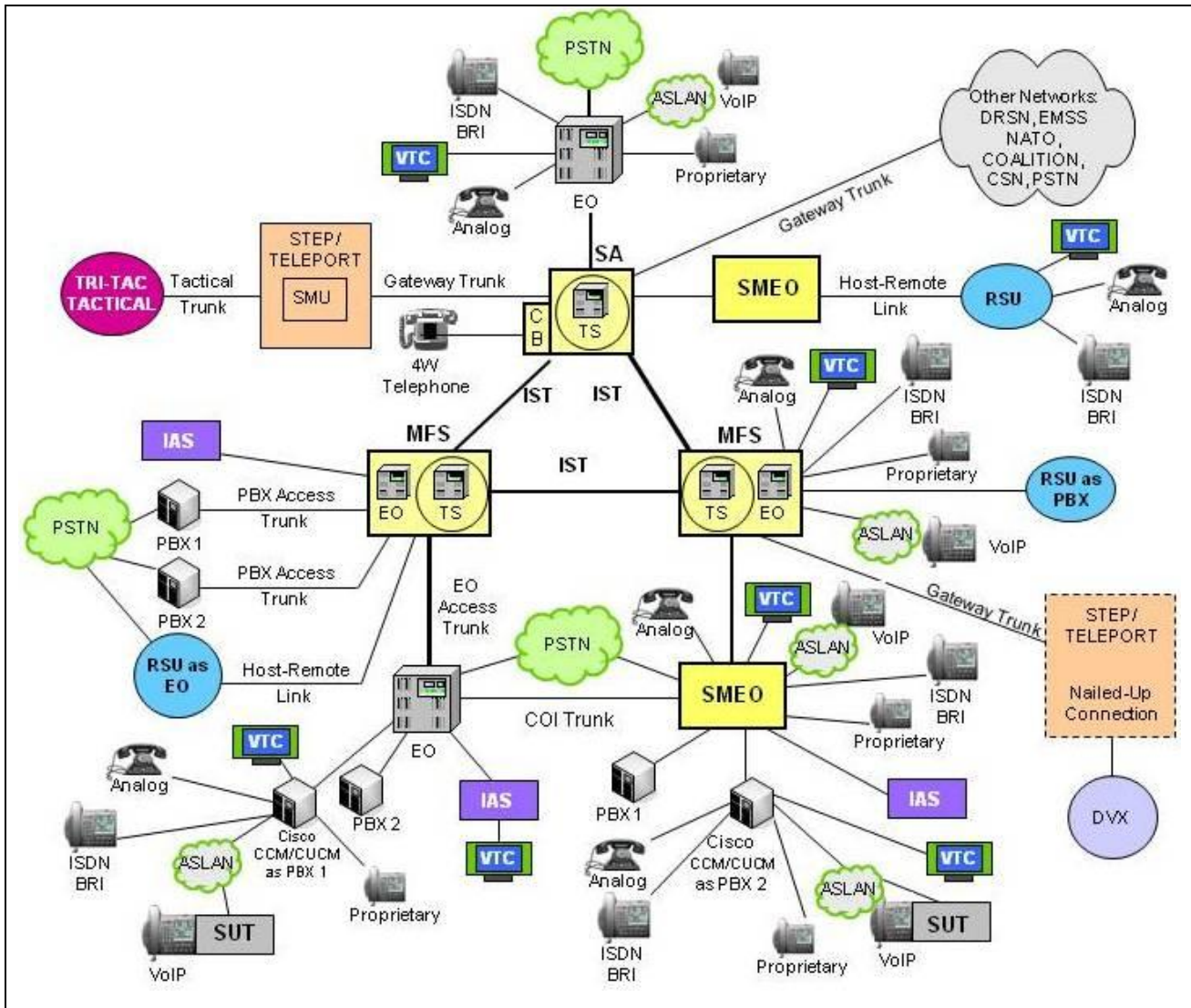
4. TESTER. Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona.

5. SYSTEM UNDER TEST DESCRIPTION. LiteScape SPM is a session-aware, Identity Management Solution (IMS) to securely Authenticate, Authorize and Account (AAA) users “access” to Internet Protocol (IP)-based telephony systems, computer systems, and/or facilities. AAA access is accomplished and based on a configurable, policy-based application SPM which uses encrypted and survivable replicable storage database with secure transport between the SPM application and a hardware device SPAR. AAA is a combination of up to four factor authentication (Magnetic, RFID, Personal Identification Number (PIN) and/or Biometrics).

a. LiteScape IMS interaction with Cisco Unified Communications Manager (CUCM) is based on the Cisco concept of extension mobility and user profiles as a “back-engine” for AAA function. As an example, the default “Profile” for Cisco extension mobility as applied to a telephone is a static, inert configuration defined by organizational policy that also provides no access to IP Directory or Services. “Inert” could be further defined as restrictions in precedence calling, off-net calling, emergency calling only, etc, or any combination created based on policy with-in CUCM. Once the IMS verifies and approves a user’s access, SPM notifies CUCM of a users AAA approval so CUCM can change the inert device profile within extension mobility to the “users” profile with granted rights as defined by policy within CUCM for that individual or job function: This can include, but not be limited to, access to IP Directory and Services.

b. The LiteScape system is managed locally with the SPM software running on two servers running Microsoft Server 2003 SP 2.

6. OPERATIONAL ARCHITECTURE. The Unified Capabilities Requirements (UCR) Defense Switched Network (DSN) architecture in Figure 2-1 depicts the relationship of the SUT to the DSN switches.



LEGEND:

4W	4-Wire	MFS	Multifunction Switch
ASLAN	Assured Services Local Area Network	NATO	North Atlantic Treaty Organization
BRI	Basic Rate Interface	PBX	Private Branch Exchange
CB	Channel Bank	PBX 1	Private Branch Exchange 1
CCM	Cisco CallManager	PBX 2	Private Branch Exchange 2
CUCM	Cisco Unified Communication Manager	PSTN	Public Switched Telephone Network
COI	Community of Interest	RSU	Remote Switching Unit
CSN	Canadian Switch Network	SMEO	Small End Office
DRSN	Defense Red Switch Network	SMU	Switched Multiplex Unit
DSN	Defense Switched Network	STEP	Standardized Tactical Entry Point
DVX	Deployable Voice Exchange	SUT	System Under Test
EMSS	Enhanced Mobile Satellite System	TDM/P	Time Division Multiplex/Packetized
EO	End Office	Tri-Tac	Tri-Service Tactical Communications Program
IAS	Integrated Access Switch	TS	Tandem Switch
IPCC	Internet Protocol Contact Center	VoIP	Voice over Internet Protocol
ISDN	Integrated Services Digital Network	VTC	Video Teleconferencing
IST	Interswitch Trunk		

Figure 2-1. DSN Architecture

7. REQUIRED SYSTEM INTERFACES. Requirements specific to the SUT and interoperability results are listed in Table 2-1. These requirements are derived from the UCR Interface and Functional Requirements (FRs) and verified through JITC testing and review of vendor's LoC.

Table 2-1. SUT FRs and Interoperability Status

Interfaces	Critical	Certified	Functional Requirements	Status	UCR Paragraph																								
IP 100BaseT (IEEE 802.3- 2005)	Yes	Yes	MLPP Interaction (R)	Met ¹	5.3.2.3																								
			VoIP System Security (R)	Met ²	5.4																								
			IPv6 (C)	Not tested ³	5.3.5																								
			VoIP System Service Tagging-End User Devices (R)	Met	5.3.3.2																								
<p>NOTES:</p> <p>1 All MLPP call scenarios were successful met with the following minor exception: An incoming higher precedence call placed to the SUT fails to be properly diverted if the user is in the process of logging out of the SUT and then cancels the logout process by pressing the exit button. To eliminate this anomaly from occurring, it is recommended that when logging in or logging out with the SUT, that the user not interface with the SUT until the login or logoff process is complete. When a higher precedence call is placed to the SUT's respective IP end instrument while the login or logoff is in progress, the calls are properly diverted to the alternate directory number as required by the UCR, paragraph 3.3.</p> <p>2 Security is tested by DISA-led Information Assurance test teams and published in a separate report, Reference (e).</p> <p>3 In accordance with UCR 2008 Change 1 section 5.3.5 Table 5.3.5-1, with the exception of IP End Instruments, all CPE devices have a conditional requirement for IPv6 capability. This capability is conditional for the SUT and was not tested.</p> <p>LEGEND:</p> <table> <tr> <td>100BaseT</td> <td>100 Mbps (Baseband Operation, Twisted Pair) Ethernet</td> <td>IPv6</td> <td>Internet Protocol version 6</td> </tr> <tr> <td>802.3-2005</td> <td>Local Area Network/metropolitan Area Network Carrier Sense Multiple Access/Collision Detection Access Method</td> <td>MLPP</td> <td>Multi-Level Precedence and Preemption</td> </tr> <tr> <td>CPE</td> <td>Customer Premise Equipment</td> <td>R</td> <td>Required</td> </tr> <tr> <td>DISA</td> <td>Defense Information Systems Agency</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>IEEE</td> <td>Institute of Electrical and Electronics Engineers</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>IP</td> <td>Internet Protocol</td> <td>VoIP</td> <td>Voice over Internet Protocol</td> </tr> </table>						100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	IPv6	Internet Protocol version 6	802.3-2005	Local Area Network/metropolitan Area Network Carrier Sense Multiple Access/Collision Detection Access Method	MLPP	Multi-Level Precedence and Preemption	CPE	Customer Premise Equipment	R	Required	DISA	Defense Information Systems Agency	SUT	System Under Test	IEEE	Institute of Electrical and Electronics Engineers	UCR	Unified Capabilities Requirements	IP	Internet Protocol	VoIP	Voice over Internet Protocol
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	IPv6	Internet Protocol version 6																										
802.3-2005	Local Area Network/metropolitan Area Network Carrier Sense Multiple Access/Collision Detection Access Method	MLPP	Multi-Level Precedence and Preemption																										
CPE	Customer Premise Equipment	R	Required																										
DISA	Defense Information Systems Agency	SUT	System Under Test																										
IEEE	Institute of Electrical and Electronics Engineers	UCR	Unified Capabilities Requirements																										
IP	Internet Protocol	VoIP	Voice over Internet Protocol																										

8. TEST NETWORK DESCRIPTION. The SUT was tested at JITC's Global Information Grid Network Test Facility, Fort Huachuca, Arizona, in a manner and configuration similar to that of the DSN operational environment. Testing the system's required functions and features was conducted using the test configuration depicted in Figure 2-2.

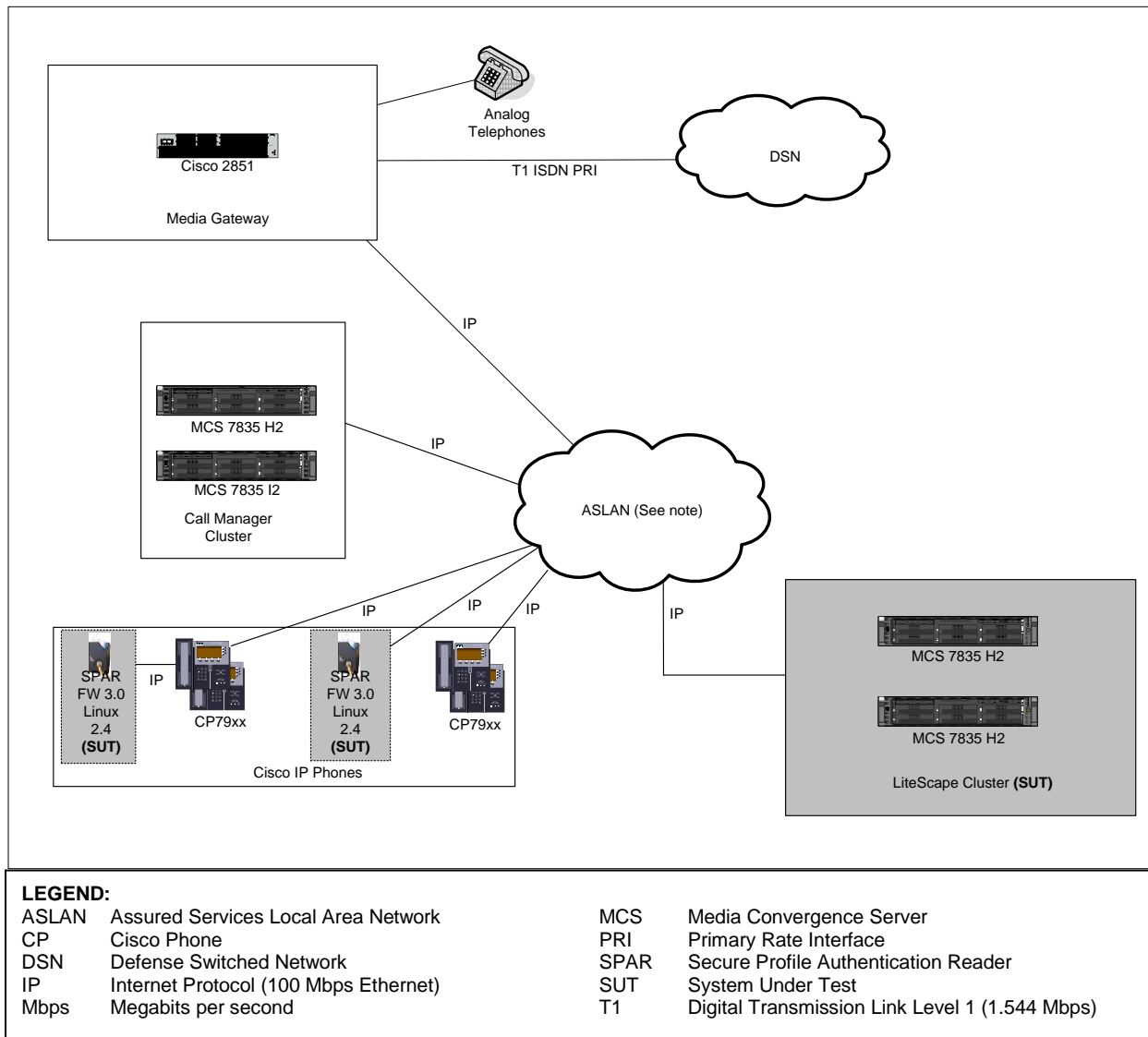


Figure 2-2. SUT Test Diagram

9. TESTED SYSTEM CONFIGURATION. Table 2-2 provides the system configurations, hardware and software components tested with the SUT. The SUT was tested in an operationally realistic environment to determine interoperability with a complement of DSN switches noted in Table 2-2. The DSN switches listed in Table 2-2 depict the tested configuration. The SUT is certified with any CCM or CUCM listed on the UC Approved Products List (APL) that offers the same certified interfaces.

Table 2-2. Tested System Configurations

System Name		Software Release	
Siemens EWSD		Release 19d Patch Set 46	
Avaya CS2100		Avaya CS2100 XA-Core SE09.1 with AS5300 Release 2.0.	
CUCM Version 7.1(2) with IOS Software Release 15.1(1) T			
Component	Release	Sub-components	
Cisco CUCM MCS7835H2, MCS7835I2	7.1(2.30006-6)	N/A	
2851 Integrated Services Router (Gateway)	IOS 15.1(1) T	NM HD 2VE	
		VIC 4FXS/DID	
		VWIC2 2MFT T1/E1	
		EVM HD 8FXS/DID	
		EM HDA 8FXS	
CP-7940G and CP-7960G	Ver: 8.0(4.0) App: P00308010100	NM HDV2 2T1/E1	
		NA	
SUT	Hardware	Software/Firmware	
	Cisco MCS7835H2 <small>(See note)</small>	Windows 2003 Server SP1, IIS 6.0 with ASP.NET, SQL 2005 SP1 Standard, .NET Version 1.1, McAfee 8.0, LiteScape SPM 1.0	
	LiteScape Biometric SPAR™	Firmware version 3.0, Net4.0 for Linux 2.4	
	SPM	Windows Server 2003 SP 2	
		Sun Java 6 JRE	
		Internet Explorer 7	
		IIS 6.0	
		MSXML 6 SP2	
		Oncast v4.40.14	
		McAfee 8.7.0i	
		IE 8/Firefox 2.x, 3.x	
		Microsoft SQL Server 2005 SP2	
		Apache Tomcat 5.5.29	
ActiveClient			
WinRAR archiver			
Tumbleweed Desktop Validator			
Cisco 7940G and 7960G VoIP Phones	P00308010100		
NOTE: The SUT was tested with the Cisco MCS7835H2 and MCS7835I2 servers; however, it is also certified with any CUCM and CCM server that is listed on the UC APL.			

LEGEND:

5ESS	Class 5 Electronic Switching System	EM	Expansion Module	SCCP	Skinny Client Control Protocol
10/100BaseT	10/100 Mbps (Baseband Operation, Twisted Pair) Ethernet	EVM	Extension Voice Module	SP	Service Pack
APL	Approved Products List application	EWSD	Elektronisches Wählsystem Digital	SPAR	Secure Profile Authentication Reader
App	Approved Products List application	Fax	facsimile	SPM	Secure Profile Management
ASP	Active Server Pages	FXS	Foreign Exchange Station	SQL	Structured Query Language
CCM	Cisco CallManager	G	10/100BaseT Ethernet	SR	Service Release
CP	Cisco Phone	GE	Gigabit Ethernet	SUT	System Under Test
CS	Communication Server	HD	High Density	T1	Digital Transmission Link Level 1 (1.544 Mbps)
CUCM	Cisco Unified Communications Manager	HDA	High Density Analog	UC	Unified Capabilities
DI	Drop and Insert	IIS	Internet Information Services	V	Voice
DID	Direct Inward Dialing	IOS	Internetwork Operating System	VE	Voice/Fax Enhanced
DSN	Defense Switched Network	Mbps	Megabits per second	Ver	Version
E1	European Basic Multiplex Rate (2.048 Mbps)	MCS	Media Convergence Server	VIC	Voice Interface Card
		MFT	Multiflex Trunk	VoIP	Voice over Internet Protocol
		MSXML	Microsoft XML Core Services	VWIC	Voice WAN Interface Card
		NM	Network Module	WAN	Wide Area Network
				XML	Extensible Markup Language

10. TEST LIMITATIONS. None.

11. TEST RESULTS

a. Discussion. The SUT can be configured in two configurations as shown in Figure 2-2. The SUT can be directly connected to the Assured Services Local Area Network (ASLAN) or connected to the IP port on the IP end instrument. The following paragraphs depict the testing conduct and results of these two configurations.

(1) Multi-Level Precedence and Preemption (MLPP): In accordance with Section 5.2.3.2 of UCR 2008 Change 1, if the SUT supports MLPP interaction it shall meet it in accordance with Section 5.2.2. When a call is placed to the SUT's respective IP end instrument while the logoff is in progress, the calls can be answered or are properly diverted to the alternate directory number. When a call is placed to the SUT's respective IP end instrument while the logon is in progress, the calls cannot be answered but are properly diverted to the alternate directory number. When the SUT affiliation is completed, MLPP interaction with the SUT's end instrument was accomplished. Various profiles with different authorized precedence levels were configured in the SUT server. Each profile was affiliated with a specific IP end instrument, SPARTM, swipe card, and biometric fingerprint. The SUT associated IP end instruments were configured with a default classmark of ROUTINE precedence with intra switch dialing only. Each SUT swipe card and the biometric reader were tested with its respective IP end instrument to insure that the precedence level and classmark features were automatically updated as assigned in the SUT server. The configured profiles were properly assigned to the respective end instruments. MLPP call scenarios were conducted with the SUT's respective end instruments during affiliation (logging in), after affiliation (logged on), and while logging out. All MLPP call scenarios were successfully met.

(2) Internet Protocol (IPv6): In accordance with UCR 2008 Change 1 with the exception of IP End Instruments all CPE devices have a conditional requirement for IPv6 capability. This capability was not tested and is conditional for the SUT.

(3) Voice over Internet Protocol (VoIP) System Security. In accordance with Section 5.4 of UCR 2008 Change 1, the SUT VoIP security was tested by DISA-led Information Assurance test teams and was published in a separate report.

(4) Differentiated Services Code Point (DSCP). In accordance with the UCR 2008, Change 1, paragraph 5.3.3.3.2, DSCP, the product shall support the plain text DSCP plan, as shown in Table 5.3.3-1, DSCP Assignments, and the DSCP assignment shall be software configurable for the full range (0-63). The SUT DSCP assignments are software configurable for the full range of 0-63, which meets this requirement.

b. Test Summary. The SUT met the interface and functional requirements for an IP CPE and is certified for joint use within the DSN. The SUT meets the critical interoperability requirements set forth in Reference (c), using test procedures derived from Reference (d). The SUT was tested and certified with the Cisco Media Communications Server (MCS) 7835H2. Since other Cisco MCS Servers also listed on the Unified Capabilities (UC) Approved Product List (APL) or previously listed on the UC APL are functionally identical to the MCS 7835H2, JITC analysis determined the SUT is also interoperability certified for joint use with these other servers. Furthermore, the SUT was tested and certified for joint use only with the CUCM Release 7.1(2). However, JITC analysis determined the SUT is also certified for joint use with other CCM Private Branch Exchange and their associated IP end instruments that are listed on the UC APL or have been previously listed on the UC APL. The SUT is certified to support DISN assured services over IP with any ASLAN certified for use.

12. TEST AND ANALYSIS REPORT. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (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>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet), or <http://199.208.204.226> (SIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitic.fhu.disa.mil/tssi>. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly through government civilian or uniformed military personnel from the Unified Capabilities Certification Office (UCCO), e-mail: ucco@disa.mil.