



National Aeronautics and
Space Administration

NOT MEASUREMENT
SENSITIVE

NASA-STD-2804M
Effective August 11, 2009

MINIMUM INTEROPERABILITY SOFTWARE SUITE

NASA TECHNICAL STANDARD

FOREWORD

This standard is approved for use by NASA Headquarters and all NASA Centers and is intended to provide a common framework for consistent practices across NASA programs.

The material covered in this standard is governed and approved by the NASA Information Technology Management Board. Its purpose is to define the baseline software suite necessary to support interoperability both between NASA end user computers and within the NASA operating environment. The standard establishes Client Reference Configurations, Operating System Standards, and Compliance Dates for computers running Microsoft Windows, Apple Mac OS, and various Linux and UNIX operating systems. Adherence to this standard ensures compliance with federal requirements for desktop computers, laptops, and other end user devices.

Requests for information, corrections, or additions to this standard should be directed to the John H. Glenn Research Center at Lewis Field (GRC), Emerging Technology and Desktop Standards Group, MS 142-5, Cleveland, OH, 44135 or to desktop-standards@lists.nasa.gov. Requests for general information concerning standards should be sent to NASA Technical Standards Program Office, ED41, MSFC, AL, 35812 (telephone 256-544-2448). This and other NASA standards may be viewed and downloaded, free of charge, from the NASA Standards web page: <http://standards.nasa.gov/>.

/signature on file/

Bobby German
Chief Information Officer (Acting)

This Page Left Blank Intentionally

Table of Contents

1	SCOPE	1
1.1	Purpose	1
1.2	Applicability	1
1.3	Waivers	1
2	ACRONYMS AND DEFINITIONS.....	1
2.1	Acronyms	1
2.2	Definitions.....	2
2.2.1	<i>Desktop Computer</i>	2
2.2.2	<i>Support for Basic Interoperability</i>	2
3	DETAILED REQUIREMENTS	2
3.1	Architectural Compliance Requirements.....	2
3.2	Agency Security Configuration Standards	3
3.3	Client Reference Configurations.....	3
3.3.1	<i>Client Reference Configuration for Windows XP</i>	4
3.3.2	<i>Client Reference Configuration for Mac OS X</i>	6
3.3.3	<i>Client Reference Configuration for Linux</i>	8
3.4	Additional Client Reference Configuration Guidance	10
3.4.1	<i>Office Automation Applications</i>	10
3.4.2	<i>Electronic Messaging</i>	10
3.4.3	<i>Web browser</i>	11
3.4.4	<i>PatchLink</i>	11
3.4.5	<i>Data at Rest (DAR) Encryption</i>	11
3.4.6	<i>Smart Card Middleware</i>	11
3.5	Operating System Standards, Timelines, and Compliance Dates.....	12
3.5.1	<i>Microsoft Windows XP</i>	12
3.5.2	<i>Microsoft Windows Vista</i>	12
3.5.3	<i>Microsoft Windows 64-bit</i>	12
3.5.4	<i>Microsoft Windows 7</i>	12
3.5.5	<i>Mac OS</i>	12
3.5.6	<i>Linux/x86 and x86-64</i>	13
3.5.7	<i>Other UNIX</i>	13
3.6	Electronic forms	14
3.7	Additional X.509 root certificates.....	14
3.8	Operating System Configuration Requirements	15
3.9	Section 508 Compliance Requirements.....	15
3.10	FIPS 140-2 Compliance Requirements	16
3.11	Energy Management.....	16
3.11.1	<i>Computers</i>	16
3.11.2	<i>Printers</i>	17
3.12	Virtualization	17
4	ADDITIONAL SOFTWARE TABLES	17
4.1	Table of Optional Software	17
4.2	Table of Agency Required Software	18
5	REVIEW AND REPORTING REQUIREMENTS	18
5.1	Interoperability Maintenance Reporting	18
5.2	Interoperability Reporting	18
5.3	Basic Interoperability Standards Maintenance	18

6 DURATION 19
6.1 Duration..... 19

7 SUPPORTING DOCUMENTS 19
7.1 Supporting Documents..... 19

1 SCOPE

1.1 Purpose

This standard defines the baseline software suite necessary to support interoperability both between NASA end user computers and within the NASA operating environment. The standard establishes Client Reference Configurations, Operating System Standards, and Compliance Dates for computers running Microsoft Windows, Apple Mac OS, and various Linux and UNIX operating systems. Adherence to this standard ensures compliance with federal requirements for desktop computers, laptops, and other end user devices.

1.2 Applicability

Center CIO's will ensure that all NASA employees at their respective centers have access to an interoperable workstation that is equipped with a minimum software suite that meets the standards listed in Section 3 below.

The Client Reference Configuration (CRC) establishes required functionality and required products necessary to meet that functionality. Future procurements intended to address this functionality are restricted to the products defined in the CRC. Existing licenses for other products may not be renewed. Products will be added, replaced, or removed as appropriate to address agency interoperability requirements.

1.3 Waivers

The waiver process set forth in NPR 2800.1, paragraph 2.2.4, applies to this standard. The Emerging Technology and Desktop Standards group, in cooperation with the Office of the Chief Information Officer, will evaluate and process waivers as appropriate.

2 ACRONYMS AND DEFINITIONS

2.1 Acronyms

<u>CA</u>	Certificate Authority
<u>CIO</u>	Chief Information Officer
<u>CIS</u>	Center for Internet Security
<u>CRC</u>	Client Reference Configuration
<u>DAR</u>	Data at Rest (encryption)
<u>DSI</u>	Desktop Smartcard Integration
<u>ETADS</u>	Emerging Technology and Desktop Standards
<u>FDCC</u>	Federal Desktop Core Configurations
<u>FISMA</u>	Federal Information Security Management Act
<u>HTML</u>	HyperText Markup Language
<u>ICA</u>	Independent Computing Architecture
<u>IMAP</u>	Internet Message Access Protocol
<u>MIME</u>	Multipurpose Internet Mail Extension
<u>NEF</u>	NASA Electronic Forms
<u>NIST</u>	National Institute of Standards and Technology
<u>NOCA</u>	NASA Operational Certificate Authority
<u>NOMAD</u>	NASA Operational Messaging and Directory Service
<u>OMB</u>	Office of Management and Budget
<u>PDF</u>	Portable Document Format

<u>PKI</u>	Public Key Infrastructure
<u>SCAP</u>	Security Content Automation Protocol
<u>SMTP</u>	Simple Mail Transport Protocol
<u>SSL</u>	Secure Sockets Layer
<u>TLS</u>	Transport Layer Security

2.2 Definitions

2.2.1 Desktop Computer

The term desktop computer is used generically to refer to traditional desktop systems as well as laptop computers, notebooks, tablets, engineering workstations, and similar platforms that are utilized to provide basic interoperability.

2.2.2 Support for Basic Interoperability

Systems supporting basic interoperability are defined as desktop computers used to exchange information electronically by end users that require any of the functionality listed in the Client Reference Configuration (Office Automation, Electronic Messaging, Web Browsing, etc. See section 3.3 Client Reference Configurations).

3 DETAILED REQUIREMENTS

3.1 Architectural Compliance Requirements

NASA has baselined and approved the NASA Integrated Information Technology Architecture¹. The architecture is predicated on:

- The selection of standards for a broad and cost-effective infrastructure using commercial off-the-shelf and well-supported open source products to the greatest extent practical
- Interoperability both within and external to NASA
- Flexibility for future growth
- Consistency with generally accepted consensus standards as much as feasible.
- Among these objectives, ensuring interoperability is one of NASA's most critical issues related to information technology.

In many cases, it is in NASA's best interest to specify commercial products as standards for an interoperable implementation of a particular set of related and integrated functions. The products themselves often include additional functionality or proprietary extensions not specified by this standard. While these products can be used to create higher-level interoperability solutions, these solutions may not be recognized within the context of the NASA interoperability environment and may be deprecated without warning by future revisions to this standard. Users of this standard are advised to apply appropriate caution when implementing proprietary or non-standard extensions, features and functions that go beyond the explicitly stated standard functionality.

¹ NASA-STD-2814A, *NASA Integrated Information Technology Architecture—Technical Framework*

3.2 Agency Security Configuration Standards

The annual NASA Chief Information Officer Agency Security Standards letter establishes Agency FISMA compliance goals and reporting requirements for NASA systems, through the use of Agency Configuration Settings.

Compliance with the Agency Security Configuration Standards requires deployment of Federal Desktop Core Configurations (FDCC) settings to all NASA Microsoft Windows XP, Vista, and Windows 7 systems. Compliance for all systems for which FDCC security settings are not available requires the deployment of Center for Internet Security (CIS) Benchmarks.

3.3 Client Reference Configurations.

To address application, data, and infrastructure interoperability, and ensure compliance with federally mandated desktop computer configuration settings, the software functionality, applications, interface standards, configuration settings, versions, and deployment settings established by this standard are definitive.

Client Reference Configurations (CRC) are included for each operating system, with specific version and required configurations listed as appropriate. Interface standards are included to guide service providers and system integrators.

The Client Reference Configurations define the baseline upon which desktop service providers can define common enterprise images for all interoperable desktops computers. All IT initiatives funded or endorsed by the NASA OCIO account for systems that conform to the Client Reference Configurations. Application service providers and software developers can use the reference configurations to assist with integration and acceptance testing.

The NASA Emerging Technology and Desktop Standards group is working to ensure interoperability at the highest possible revision of products included in the Client Reference Configurations. Applications that meet these interface standards while providing improved end user experience, mitigating security risks, reducing support costs, or offering other tangible improvements may be submitted to desktop-standards@lists.nasa.gov for consideration in future revisions to these standards.

3.3.1 Client Reference Configuration for Windows XP

Client Reference Configuration for Windows XP					
Functionality	Application	Interface Standard	Required Settings	Version	Effective Date
Operating System	Windows XP Professional		FDCC ²	Service Pack 3	September 30, 2008
	Windows XP Professional X64 Edition		FDCC ²	Service Pack 2	April 1, 2009
Firewall	Windows Firewall		FDCC ²	XP/SP3	September 30, 2008
Smartcard authentication	ActivIdentity ActivClient	ActivIdentity Proprietary	HDI specified settings ³	6.1.x	October 1, 2009
Data at Rest , Full Disk Encryption	McAfee Endpoint Encryption		Configured to use central policy and key escrow service	5.x	April 1, 2009
Content Encryption	McAfee Endpoint Encryption			5.x	April 1, 2009
PKI	Entrust ESP	Entrust Proprietary	NASA PKI Team specified settings	8.0.x	November 1, 2008
Trusted CA Certificates	See Section 3.6	X.509			June 24, 2008
Anti-virus	Symantec Antivirus		Enterprise update server	10.1.X	June 24, 2008
Anti-Malware	Symantec Antivirus		Enterprise update server	10.1.X	June 24, 2008
Patch Reporting	PatchLink (Update)	Lumension Proprietary	Configured according to local Patchlink server requirements	6.4.x	June 30, 2008
Web Browser	Mozilla Firefox	W3C and industry standards, including the following: HTML 4.01 XHTML 1.0 CSS 2 (Cascading Style Sheets) ECMAScript (JavaScript) capability to run Java 2 applets, SSL version 2 and 3, TLS 1.0	Configured with CA certificates specified in Section 3.6	3.0.x	October 1, 2008
	Microsoft Internet Explorer		FDCC settings, CA certificates specified in Section 3.6	7.0.x	June, 2009
Office Automation	Microsoft Office (Professional Edition with Outlook)			2007 SP2	April 1, 2009
Word Processing	Microsoft Word	Office Open XML file format	Configure to use Office Open XML file format by default	2007 SP2	April 1, 2009
Spreadsheet	Microsoft Excel	Office Open XML file format	Configure to use Office Open XML file format by default	2007 SP2	April 1, 2009
Presentation	Microsoft PowerPoint	Microsoft Powerpoint 97-Office Open XML file format	Configure to use Office Open XML file formats by default	2007 SP2	April 1, 2009
Electronic Mail	Microsoft Outlook	NASA-STD-28015, IMAP4, SMTP, IMAP over SSL/TLS, MAPI over HTTPS	Configured for access to NOMAD	2007 SP2	April 1, 2009

² Check http://etads.nasa.gov/ASCS/ASCS_index.shtml for current configurations

³ See Section 3.4.6 for additional information.

Client Reference Configuration for Windows XP					
Functionality	Application	Interface Standard	Required Settings	Version	Effective Date
Calendaring	Microsoft Outlook as implemented by NOMAD	iCalendar (RFC 2445) ⁴		2007 SP2	April 1, 2009
Instant Messaging	Windows Messenger	SIP	Enterprise LCS Settings as implemented by NOMAD	5.1.x	June 24, 2008
	Pidgin	XMPP	NASA Jabber Service	2.5.x	June , 2009
PDF Viewer	Adobe Acrobat Reader	PDF File		9.1.x	June, 2009
Java	Java run-time environment			Java 6	October 1, 2008
Audio/video player	Apple QuickTime Player	Various Multimedia	Default for Quicktime formats	7.6.x	June 24, 2008
	Adobe Flash Player	Flash SWF		10.0.x	June 24, 2008
	Microsoft Windows Media Player	Windows Media Files	Default for all supported formats	11.0.x	June 24, 2008
	Real Player Enterprise	Real Streaming Media	Enterprise Version Only	11.x	June 24, 2008
	SilverLight	Various Multimedia		2.0.x	July, 2009
	Apple iTunes	Various Multimedia		8.2.x	July, 2009
Access to centrally served Windows applications	Citrix ICA Client	Citrix ICA ProtocolXenApp Plugin		11.0.x	June 24, 2009
Electronic Forms	FileNet Desktop e-Forms	See Section 3.5	NASA Distribution Center	4.2	June 24, 2008

⁴ This standard provides limited interoperability

3.3.2 Client Reference Configuration for Mac OS X

Client Reference Configuration for Mac OS X					
Functionality	Application	Interface Standards	Required Settings	Version	Effective Date
Operating System	Mac OS X		CIS Benchmarks	10.5.x	April 1, 2009
Firewall	Apple Firewall		Allow essential services Enable firewall logging Enable Stealth Mode ⁵		April 1, 2009
Smartcard authentication	ActivIdentity ActivClient	ActivIdentity proprietary	HDI specified settings ⁶	3.1	October 1, 2009
PKI	Entrust Entelligence			7.2	June 24, 2008
Trusted CA Certificates	See Section 3.6	X.509			June 24, 2008
Anti-virus	Symantec Antivirus Enterprise			10.2.x	December 2008
Anti-Malware	Symantec Antivirus Enterprise			10.2.x	December 2008
Data at Rest Encryption	McAfee Endpoint Encryption		Configured to use central policy and key escrow service	Not Available	Not Available
Web Browser	Mozilla Firefox	W3C and industry standards, including the following: HTML 4.01 XHTML 1.0 CSS 2 (Cascading Style Sheets) ECMAscript (JavaScript) capability to run Java 2 applets, SSL version 2 and 3, TLS 1.0		3.0.x	October 1, 2008
	Apple Safari			4.0.x	July 2009
Java	Java run-time environment			Java 6	October 1, 2008
Office Automation	Microsoft Office for Mac			2008	April 1, 2009
Word Processing	Microsoft Word	Office Open XML file format	Configure to use Office Open XML file format by default	2008	April 1, 2009
Spreadsheet	Microsoft Excel	Office Open XML file format	Configure to use Office Open XML file format by default	2008	April 1, 2009
Presentation	Microsoft PowerPoint	Office Open XML file format	Configure to use Office Open XML file formats by default	2008	April 1, 2009
Electronic Mail	Microsoft Entourage	NASA-STD-28015, IMAP4, SMTP, IMAP over SSL/TLS	Configured for access to NOMAD	2008	April 1, 2009

⁵ Vendor terminology for these settings

⁶ See Section 3.4.6 for additional information.

Client Reference Configuration for Mac OS X					
Functionality	Application	Interface Standards	Required Settings	Version	Effective Date
	Apple Mail		Integration with NOMAD limited to email only	Current Mac OS X	June 24, 2008
Calendaring	Microsoft Entourage as implemented by NOMAD	iCalendar (RFC 2445) ⁷	Configured for access to NOMAD	2008	April 1, 2009
Instant Messaging	Microsoft Messenger	SIP	Enterprise LCS Settings as specified by NOMAD	6.0.x	June 24, 2008
	Apple iChat	XMPP	NASA Jabber Service settings	Bundled	June 24, 2008
Patch Reporting	PatchLink (Update)	Lumension proprietary	Configuration for Server info	6.4.x	June 30, 2008
Audio/video player	Apple QuickTime Player	Various Multimedia	Default for all supported formats	7.6.x	June 24, 2008
	Adobe Flash Player	Flash SWF		10.0.x	June 24, 2008
	Telestream Flip4Mac WMV	Windows Media Files	Default for Windows Media	2..2.x	June 24, 2008
	RealPlayer	Real Streaming Media		10.x	June 24, 2008
	Silverlight	Various Multimedia		2.0.x	July, 2009
	Apple iTunes	Various Multimedia		8.2.x	July, 2009
PDF Viewer	Adobe Acrobat Reader			9.1.x	June 24, 2008
	Apple Preview			4.1	June, 2009
Access to centrally served Windows applications	Citrix ICA Client	Citrix ICA Protocol		10.00.x	June 24, 2008
Electronic Forms	FileNet Desktop e-Forms	See Section 3.5	NASA Distribution Center	4.2	June 24, 2008

⁷ This standard provides limited interoperability

3.3.3 Client Reference Configuration for Linux

Client Reference Configuration for Linux					
Functionality	Application	Interface Standards	Required Settings	Version	Effective Date
Operating System	Red Hat Enterprise Linux Desktop with Workstation option		CIS Benchmarks	5.3 or later	June 24, 2008
	SuSE Linux Enterprise Desktop		CIS Benchmarks	11.0 or later	June 24, 2008
Firewall	Bundled		Control inbound and outbound connections enabled by default	Bundled	June 24, 2008
Smartcard authentication	ActivIdentity ActivClient	ActivIdentity Proprietary	HDI specified ⁸	Not Available	Not Available
PKI	Entrust			Not Available	Not Available
Trusted CA Certificates	See Section 3.6	X.509			June 24, 2008
Anti-Virus	F-Prot Anti-Virus			6.0.x	June 24, 2008
Anti-Malware	F-Prot Anti-Virus			6.0.x	June 24, 2008
Data at Rest Encryption	McAfee Endpoint Encryption		Configured to use central policy and key escrow service	Not Available	Not Available
Patch Reporting	PatchLink (Update)	Lumension Proprietary	Configuration for Server info	6.4.x	June 30, 2008
Web Browser	Mozilla Firefox	W3C and industry standards, including the following: HTML 4.01 XHTML 1.0, CSS 2 (Cascading Style Sheets) ECMAscript (JavaScript) capability to run Java 2 applets, SSL version 2 and 3 supporting the requirements of NASA-STD-2820, <i>Encryption and Digital Signature Standards</i> .		3.0.x	October 1, 2008
Office Automation	OpenOffice	Office Open XML file format		3.0.x	June 2009
Word Processing	OpenOffice Writer	Office Open XML file format	Configure to use Office Open XML file format by default	3.0.x	June, 2009
Spreadsheet	OpenOffice Calc	Office Open XML file format	Configure to use Office Open XML file format by default	3.0.x	June, 2009
Presentation	OpenOffice Impress	Office Open XML file format	Configure to use Office Open XML file format by default	3.0.x	June, 2009
Electronic Mail	Thunderbird	NASA-STD-28015, IMAP4, SMTP, IMAP over SSL/TLS	Configured for access to NOMAD	2.0.x	June 24, 2008

⁸ See Section 3.4.6 for additional information.

Client Reference Configuration for Linux					
Functionality	Application	Interface Standards	Required Settings	Version	Effective Date
Calendaring	NOMAD Outlook Web Access	iCalendar (RFC 2445) ⁹ , HTTPS	Web Browser	2.x	June 24, 2008
Instant Messaging	Not Available	SIP	Enterprise LCS Settings as specified by NOMAD		
	Pidgin	XMPP	NASA Jabber Service settings	2.4.x	June 24, 2008
Java	Java run-time environment			Java 6	June 24, 2008
Audio/video player	Mplayer	Multimedia	Default for supported formats	1.0	June 24, 2008
	Adobe Flash Player			10.0.x	June 24, 2008
	RealPlayer	Real Streaming Media		11.x	June 24, 2008
PDF Viewer	Adobe Acrobat Reader			9.1.x	June 24, 2008
Access to centrally served Windows applications	Citrix ICA Client	Citrix ICA		10.0.x	June 24, 2008
Electronic Forms	FileNet Desktop E-Forms			Not implemented at NASA	

⁹ This standard provides limited interoperability

3.4 Additional Client Reference Configuration Guidance

3.4.1 Office Automation Applications

The default file format for Microsoft Office 2007(SP2), Microsoft Office 2008 for Mac, and OpenOffice on Linux systems is the ISO Standard Office Open XML formats.

Microsoft Office 2007 (SP2) Standard Edition (or better) is required on all interoperable Microsoft Windows systems. Microsoft Office (SP2) is approved for immediate deployment. SP2 is primarily a roll up of existing security enhancements and hotfixes. As of April 2009, all interoperable Microsoft Windows systems were required to run Office 2007.

Microsoft Office 2008 for Mac (Standard Edition) is required on all interoperable Mac OS X systems. As of April 2009, all interoperable Mac OS X systems were required to run Office 2008. Note: Office 2008 discontinues support Visual Basic for Applications.

OpenOffice is approved for deployment and use on all Linux platforms and supports the standard Office Open XML file formats. Documents created with Microsoft Office do not always render perfectly in OpenOffice, and vice versa.

3.4.2 Electronic Messaging

NASA has implemented an enterprise-wide electronic messaging service known as NOMAD. This service provides integrated email, calendaring, scheduling, contact management, and instant messaging. All interoperable desktops are required to be configured to access this environment.

Note that while NOMAD is based upon open standards and can support stand-alone email clients that adhere to the defined interface standards of the Client Reference Configurations, utilizing such clients limit end user interoperability, may not be supported by NOMAD, and may result in future inability to participate in the enterprise messaging environment.

Supported Messaging Clients

Windows:	Microsoft Outlook
Mac OS X:	Microsoft Entourage and Apple Mail
Linux:	Mozilla Thunderbird

Apple Mail does not support the NOMAD calendar and scheduling environment and should only be utilized when such integration is not required. NOMAD recommends the use of Microsoft Entourage, which provides full integration and will receive priority engineering support.

Additional clients which conform to the interface standards may be used as point solutions where interoperability might otherwise not be available.

The selection of mail clients will continue to promote secure access to commercial and partner email services in support of extra-Agency (non-NOMAD) collaborative activities.

3.4.3 Web browser

Internet Explorer 7 for Windows was approved for deployment on NASA desktops in July 2007 (NASA-STD-2804K). IE7 remains a NASA standard browser and should continue to be installed on interoperable Windows systems. To prepare for compliance with FDCC settings, by November 2008 all interoperable Windows systems were required to be running IE 7.

Internet Explorer 8 was released in March 2009, and is currently undergoing evaluation and interoperability testing. A deployment timeline will be established as testing nears completion.

Firefox 3.0.x remains the standard for Windows, Macintosh and Linux systems. Firefox 3.5 was released in June 2009, and is currently undergoing evaluation and interoperability testing. A deployment timeline will be established as testing nears completion. Deployment must be completed by January 2010 after which time Mozilla will cease to support Firefox 3.0

Safari 4.0.x is the standard for all interoperable Macintosh systems. Safari 4.0.x is approved for immediate deployment. Apple released Safari 4.0.x to address security vulnerabilities present in Safari 3.0.x. The use of Safari on Windows is not supported.

3.4.4 PatchLink

For current information on the Patchlink Agent, including specific version levels, please refer to the Agency Security Update Service (ASUS) web site at <https://patches.ksc.nasa.gov/>

Patchlink 6.4 contains a SCAP-validated FDCC reporting module and should be installed on all systems.

3.4.5 Data at Rest (DAR) Encryption

NASA has purchased a suite of software from McAfee (previously Safeboot) to provide encryption for data at rest. This software is compliant with federally mandated requirements for encryption of sensitive data on mobile devices (including laptops and removable media). Licenses will be made available to all NASA employees and onsite contractors. All laptops, all desktops with PII or other similarly sensitive data, and all new and refreshed computers are required to implement this encryption technology. McAfee is currently developing a solution for the Macintosh platform with a projected release of Q4. After the product is released it will be evaluated for interoperability and a deployment timeline developed. For more information see <http://etads.nasa.gov/DAR/>

3.4.6 Smart Card Middleware

The Emerging Technology and Desktop Standards Group will work with the relevant teams to identify software required for smart card use and authentication on as many operating systems as possible.

Note that the components identified in Client Reference Configuration will make NASA systems "smart card ready". However, Centers will still be required to implement appropriate Agency infrastructure to actually enable smart card authentication. Additional details about smart card

middleware, such as specific versions and information on additional platform support, will be provided as they become available. See <http://etads.nasa.gov/DSI/> for status.

3.5 Operating System Standards, Timelines, and Compliance Dates

3.5.1 Microsoft Windows XP

Windows XP Professional SP3 remains the standard version of Windows for the agency interoperable computing environment.

Windows XP Home Edition and Windows XP Media Center Edition shall not be deployed.

All Windows XP systems must be compliant with FDCC configuration.

Windows XP should be removed from all NASA systems by January 2013.

3.5.2 Microsoft Windows Vista

The decision to deploy Microsoft Windows Vista has been rescinded. New installations of Vista should be constrained to systems, which require that specific operating system due to software or driver issues. Existing Vista deployments will continue to be supported until Windows 7 has been approved for deployment. All Vista deployments must be compliant with FDCC configuration settings.

Vista should be removed from all NASA systems by January 2013.

3.5.3 Microsoft Windows 64-bit

Windows XP Professional x 64 Edition is specified as the standard version of Windows 64 bit for the agency interoperable computing environment and may be deployed where necessary, subject to the Windows XP Client Reference Configuration.

3.5.4 Microsoft Windows 7

Microsoft has announced that Windows 7 will be released in October 2009. After Windows 7 becomes commercially available, and has been thoroughly tested for use in NASA a migration schedule will be developed to migrate from Windows XP to Windows 7. It is anticipated Windows 7 will be approved for deployment in the March 2010 timeframe. Windows 7 will be required by January 2013.

3.5.5 Mac OS

Mac OS X 10.5 is the currently supported operating system on all interoperable Macintosh systems. Older versions should be removed from the environment. As always, the operating system must be kept up-to-date with vendor patches. At the time of this writing, Mac OS X 10.5.7 is the current maintenance release.

General deployment of Mac OS X 10.5 is currently approved. Mac systems, which currently require 10.5, are the Mac Pro -8 core, MacBook, MacBook Pro and MacBook Air. Mac OS X 10.6 is scheduled to release in September 2009.

3.5.6 Linux/x86 and x86-64

UNIX and Linux systems with no interoperability requirement do not need to comply with the interoperability requirements in this standard. Such systems would include special-purpose computers such as name servers, compute servers, data acquisition systems, special software development workstations, or other components of the overall computing infrastructure.

Several product standards are not available for any Linux or UNIX system. In order to comply with this standard, interoperable desktops must have some way to access these products. It is recommended to use the Citrix ICA client to connect to a Microsoft Windows application server.

Two Linux distributions are supported for use on interoperable desktops:

Red Hat Enterprise Linux Desktop 5 with Workstation option:

<https://www.redhat.com/rhel/desktop/>

SuSE Linux Enterprise Desktop 11

<http://www.novell.com/products/desktop/>

3.5.7 Other UNIX

The following UNIX systems are supported in the NASA interoperable computing environment. Generally, both the current version and prior version of the operating system are acceptable. However, the older version of the operating system must continue to be supported by the vendor, and like all systems, must be kept current with security patches.

3.5.7.1 Sun Solaris/SPARC, x86, and x86-64

Solaris is at version 10. Information about supported Solaris releases may be found at:

<http://www.sun.com/software/solaris/faqs/general.jsp#releases>

3.5.7.2 IBM AIX/POWER

AIX 5L 5.2 and 5.3 are current. AIX versions are described at:

<http://www-1.ibm.com/servers/aix/os/index.html>

3.5.7.3 HP HP-UX/PA-RISC

HP-UX 11i v2 is current. The HP-UX 11i web page is at:

<http://www.hp.com/products1/unix/operating/index.html>

3.6 Electronic forms

Agency requirements for a forms product include the ability to provide access to all NASA employees requiring access to forms (including filler operation across all NASA standard desktop platforms), the capability to enhance NASA business processes through intelligent functionality, ease of use, and an array of functional and operational capabilities.

Since an open application program interface standard for data interchange among forms products has not yet been adopted or approved by any acknowledged standards body, a product-level selection was warranted. After an evaluation of commercial products, FileNet Desktop eForms was found to comply with all key requirements. Other products which meet the requirements and interoperate with the FileNet product may be used via the waiver process.

Agency-level forms used for data collection with an official assigned number must be FileNet forms. Center unique versions of these agency forms should not be created or used.

NASA has purchased an Agency agreement for the use of FileNet Desktop eForms to allow all NASA centers, recognized partners, qualified contractors/service providers, and the general public the use of the product to complete forms when doing business with NASA. This includes center-specific forms, as well as other forms needed in the process of doing business.

Agency forms and software downloads are available through the NASA Electronic Forms (NEF) website <http://nef.nasa.gov>. The NEF website is the central repository for all forms used within NASA (NASA Forms, Standard Forms, Optional Forms, Center-specific forms, etc.), and is available to all internal users and external partners. For the purpose of form distribution an Agency distribution center profile has been created to allow access to Agency forms. All forms users should have the NEF distribution center profile, in addition to all of the profiles established for access to center-specific, and contractor maintained form collections. These profiles are maintained and distributed through the NEF website.

3.7 Additional X.509 root certificates

There are normally multiple local trusted Certificate Authority (CA) certificate stores in addition to those supplied by the operating system vendor: including, but not limited to, Java, Mozilla Thunderbird, and Mozilla Firefox.

On Windows XP and Mac OS (and on other systems where it is feasible to do so), the following X.509 root certificates must be installed as trusted roots in the local certificate stores:

- NASA Data Center Certificate Authority
- NASA Legacy Certificate Authority
- NASA Operational Certificate Authority (NOCA) from <http://newlondon.arc.nasa.gov>
- Federal Bridge Certificate Authority
- U.S. Treasury roots from <http://newlondon.arc.nasa.gov>

3.8 Operating System Configuration Requirements

The Federal Information Security Management Act (FISMA) requires all Federal agencies to utilize a consistent set of operating system and application configuration guidelines.

The National Institute of Standards (NIST) Security Content Automation Program (SCAP) has, with Microsoft collaboration, produced a set of security configurations for desktop Microsoft Windows XP and Vista systems. These configurations are known as the Federal Desktop Core Configurations. The Office of Management and Budget (OMB) has mandated that Federal Agencies use the FDCC settings without alteration, and that all future contractual IT support and procurements certify that they will operate with the mandated settings, in the following memoranda:

M-07-11 Implementation of Commonly Accepted Security Configurations for Windows Operating Systems

M-07-18 Ensuring New Acquisitions Include Common Security Configurations

Operating systems for which FDCC settings are not currently available will continue to use the CIS Benchmarks. Agency-wide guidance is provided in the NASA CIO letter, Center for Internet Security (CIS) Consensus Benchmarks, dated September 2, 2004 in which Centers are directed to use the Center for Internet Security's (CIS) Consensus Benchmarks. Technical guidance regarding specific levels of CIS Benchmarks for NASA systems is available at:

<http://etads.nasa.gov/ASCS>

3.9 Section 508 Compliance Requirements

Software products procured after June 21, 2001 must be in conformance with Section 508 of the Rehabilitation Act. Complete information and guidance on addressing Section 508 requirements is available at:

<http://www.section508.nasa.gov>

When developing and testing software, users are reminded to use the recommended tools for evaluation:

Function	Windows	Mac OS X	Linux
Screen Reading Software	JAWS	VoiceOver	
	Window Eyes		
Desktop Automated Tool	HiSoftware ACCVerify	Deque Ramp	
PDF Documents	Adobe Acrobat	Adobe Acrobat	
	NetCentric Technologies CommonLook Plug-in for Acrobat		

The NASA Emerging Technologies and Desktop Standards team has evaluated vendor-supplied Voluntary Product Accessibility Template (VPATs) for Windows XP, Windows Vista, Mac OS X Tiger, Office 2003, Office 2004, Office 2007, and Firefox 2, and believes that they satisfy the Section 508 requirements to an acceptable degree.

3.10 FIPS 140-2 Compliance Requirements

NASA will adhere to the guidelines and recommendations of the National Institute of Standards and Technology as required by the Federal Information Security Management Act, particularly as they apply to computer security and encryption technology for desktop hardware and software. More specifically, NASA will comply with Federal Information Processing Standards (FIPS) 140-1 and 140-2 as applicable, validated encryption modules become available.

NASA application developers and service providers are reminded that whenever cryptographic-based security systems are used to protect sensitive information in computer systems, the cryptographic modules utilized must be FIPS 140-2 compliant as validated by NIST¹⁰. A current list of validated products can be found at:

<http://csrc.nist.gov/cryptval/>

The following products mentioned in NASA-STD-2804 have been validated by a NIST-accredited testing laboratory and may be appropriate to protect sensitive information with cryptography under specific conditions:

Product	Validation Module	Certification	Comments
Microsoft Internet Explorer	KERNEL MODE CRYPTOGRAPHIC MODULE FOR WINDOWS XP	# <u>997</u>	Single User Mode, FIPS 140-1
Microsoft Outlook	OUTLOOK CRYPTOGRAPHIC PROVIDER	# <u>110</u>	Single User Mode, FIPS 140-1, S/MIME
Entrust PKI Software	ENTRUST ENTELLIGENCE KERNEL MODE CRYPTOGRAPHIC MODULE	# <u>1043</u>	Single User Mode, FIPS 140-2
F-Secure SSH	F-Secure® Cryptographic Library™ for Windows	# <u>437</u>	FIPS 140-2, When operated in FIPS Mode, Single User Mode.
OpenSSL	OPENSSL FIPS OBJECT MODULE (1.2)	# <u>1051</u>	
Citrix ICA Client for Windows	KERNEL MODE CRYPTOGRAPHIC MODULE FOR WINDOWS XP	Not Validated	Uses MS Windows FIPS Crypto Module
McAfee Endpoint Encryption for PCs Client	DIFFIE-HELLMAN	# <u>506</u>	FIPS 140-2, When operated in FIPS Mode
Mozilla	NETWORK SECURITY SERVICES (NSS)	# <u>815</u>	FIPS 140-2, When operated in FIPS Mode
Entrust PKI Software	L VERSION 8.0	# <u>797</u>	FIPS 140-2, When operated in FIPS Mode

3.11 Energy Management

In order to comply with Executive Order 13423, printers, laptops and desktop systems must be configured to use energy-saving settings.

3.11.1 Computers

Requirements:

- Displays shall be set to sleep after 15 minutes of idle time

¹⁰ [Federal Information Processing Standards Publication 140-2](#), Security Requirements for Cryptographic Modules

- Systems shall go to sleep after 60 minutes of idle time

Wake-on-LAN functionality may be useful for administrators to wake the systems in order to perform maintenance.

Generally, the level of sleep should be as effective as possible at saving power, given the constraints of the environment. The S3 power savings mode (keep memory contents intact, and listen for a wake signal) is suitable in most circumstances.

Servers and other special-purpose systems are exempted from this requirement.

3.11.2 Printers

Where possible, duplex printing should be utilized. Networked printer drivers should be configured to utilize duplex printing by default.

3.12 Virtualization

Virtualization technology lets you run multiple operating systems on a single physical computer. If a desktop virtualization product is required for interoperability the recommended solution (VMWare) must be used. See Table of Optional Software

4 ADDITIONAL SOFTWARE TABLES

4.1 Table of Optional Software

The following table contains optional useful functionality that is not required for interoperability. These software applications and utilities can be made available to end users upon request or distributed with standard enterprise images to support interoperability. Where practical, it is recommended that these tools be used rather than similar tools that address the same function. This table often identifies software that will eventually be included in the Client Reference Configurations.

Function	Windows	Mac OS X	Linux
3279 client	QWS3270	tn3270	tn3270
ssh client	F-Secure SSH	bundled	bundled or OpenSSH
sftp client	FileZilla	Fetch	bundled or OpenSSH
Advance file archive extractor/creator	WinZip 12	bundled	bundled
Real A/V Player	RealPlayer 11	RealPlayer 11	RealPlayer 11
Remote access to Windows systems	MS Remote Desktop Connection	MS Remote Desktop Connection	bundled
X window system server	Exceed	Apple X11	bundled
PostScript previewer	Ghostscript	bundled	bundled
PDF creator	Adobe Acrobat, Pro	Adobe Acrobat Pro	Scribus
PDF writer/converter	PrimoPDF, MS Office 2007 PDF plug-ins	bundled	bundled
Project Management	MS Project 2007	OmniPlan	Intellisys Project Desktop
Virtualization	VMWare Workstation	VMWare Fusion	VMWare Workstation

4.2 Table of Agency Required Software

The following table summarizes software that must be installed on all Agency desktop systems, regardless of their interoperability requirements.

This software is included in the Client Reference Configuration.

Function	Windows	Mac OS X	Linux	Unix
FISMA compliance	FDCC	CIS Benchmarks	CIS Benchmarks	CIS Benchmarks
Patch reporting	Patchlink	Patchlink	Patchlink	Patchlink
Anti-Virus	Symantec Anti-Virus Enterprise Edition	Symantec Anti-Virus Enterprise Edition	F-Prot Anti-virus	F-Prot Anti-virus
Data-at-Rest Encryption	McAfee Endpoint Encryption	McAfee Endpoint Encryption ¹¹	McAfee Endpoint Encryption ¹¹	McAfee Endpoint Encryption ¹¹
HSPD12	ActivClient	ActivClient	ActivClient	ActivClient

5 REVIEW AND REPORTING REQUIREMENTS

5.1 Interoperability Maintenance Reporting

Upon request, Center CIO's will provide the NASA CIO with a summary report, outlining the status of minimum interoperability access for each NASA employee.

5.2 Interoperability Reporting

Each Center CIO will utilize the Agency selected processes and tools, both manual and automated, to report on an annual basis to the NASA CIO the hardware and software configuration of all workstations at their respective Centers. This data will contain sufficient information to ascertain if the workstation supports NASA employees or is Government-furnished equipment to a contractor, whether the equipment is required to be interoperable, and a description of the hardware architecture/environment. The report will specify the number of NASA employees that do not have access to interoperable workstations.

5.3 Basic Interoperability Standards Maintenance

This standard, and its companion, NASA-STD-2805 Minimum Hardware Configurations, are maintained on behalf of the NASA CIO by the Emerging Technology and Desktop Standards group. Together, these standards define the software, hardware, and configurations necessary to ensure basic interoperability within the NASA information technology computing infrastructure.

This standard will be reviewed and updated on an as-required basis, not to exceed 12-month intervals. Participation in the revision process is open to all NASA employees. Details on how to be alerted of changes to the standards and/or comment on proposed updates can be found at:

¹¹ Pending vendor availability

<http://desktop-standards.nasa.gov>

This site also maintains interim guidance, position papers, software and hardware reviews, recommendations and other documentation intended to promote standardized basic interoperability.

6 DURATION

6.1 Duration

This standard will remain in effect until canceled or modified by the NASA CIO.

7 SUPPORTING DOCUMENTS

7.1 Supporting Documents

Supporting documents and additional information related to this standard may be found at:

<http://desktop-standards.nasa.gov>