

AIR FORCE DODIIS INFRASTRUCTURE

(AFDI)

2.0 REQUIREMENTS MATRIX

DOCUMENT VERSION 1.0

01 SEPTEMBER 2000

Table of Contents

1.0	System Functions	3
1.3	Web Interface Function	3
1.6	Deadman Function	3
1.8	Database Access and Functionality	3
1.10	Availability	4
2.0	User Functions and Utilities	4
2.4	Secure Email Function	4
3.0	System Administration	4
3.1	Printing	4
3.8	Disk Space Function	4
3.9	Performance Management Function	5
3.13	Network Services Function	5
3.19	Peripherals Function	5
3.26	Alert Messages Function	5
3.27	Segmentation Function	6
4.0	Security Management	6
4.1	Security Administration Function	6
4.2	Accountability	6
4.4	Logging and Security Audit Function	6
4.5	Security and Confidentiality Requirements	7
4.7	Trusted Facility Management (TFM) Function	7
4.12	Public Key Infrastructure Functions	7
4.13	DAC Checker Function	8
4.14	User Access Function	9
4.15	Login Function	9
4.16	System Access (LOGIN) Authentication Function	9
4.17	Password Operation Function	10
4.18	Data Security Function	10
4.19	Object Reuse Function	10
4.20	Data Confidentiality	11
5.0	Account Management	11
5.1	Account Creation Function	11

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.x	Doc	Para.
1.0 System Functions						
1.3.1 AFDI shall provide a Web interface for infrastructure services.			X		CSE	
1.3.2 AFDI shall provide the capability to detect when the AFDI baseline (kernel, patches and/or segments) has been modified.			X		ADMSRS	3.2.1.71
1.6 Deadman Function This function shall:						
1.6.3.1 Per user(s)			X		DCOITM	3.2.5.12.3.1
1.6.3.2 Per Workstation(s)	X				DCOITM	3.2.5.12.3.2
1.6.3.3 Per groups(s)			X		DCOITM	3.2.5.12.3.3
1.6.3.4 Per administrative domain(s)			X		DCOITM	3.2.5.12.3.4
1.6.3.5 Per entire system			X		DCOITM	3.2.5.12.3.5
1.8 Database Access and Functionality						
1.8.1 AFDI Security Service functions must operate with the following software:						
1.8.1.1 Relational Data Base Management Systems (RDBMSs):						
1.8.1.1.1 Sybase			X		NMSRS	
1.8.1.1.2 Oracle			X		NMSRS	
1.8.1.1.3 Informix			X		NMSRS	
1.8.2 AFDI DBMSs shall provide the capability to audit user access to databases for the following security relevant events: Attempts to change access control permissions, Attempts to create, copy, sanitize, purge, or execute databases			X		DCOITM	3.2.18.1
1.8.3 AFDI shall provide the capability to interface with AFDI DBMS(s) to create, modify, and delete database access control permissions (e.g., grant permissions) at the following levels: Table, View, Row or record, Field or element.			X		DCOITM	3.2.18.2
1.8.4 AFDI shall provide the capability to interface with AFDI DBMS(s) to define access control permissions for the following: User(s), Profile, Workstation.			X		DCOITM	3.2.18.3
1.8.5 AFDI DBMS(s) shall provide the capability to label (security) database information at the following levels of abstraction: Database, Data row or record			X			3.2.18.5
1.8.6 Security services functions must operate in a distributed computing environment and/or client server environment.			X		ADMSRS	3.3.11

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.x	Doc	Para.
1.10 Availability						DCOITM 3.2.4
1.10.12 The primary default capability for notifying the trusted user that a system service or resource has failed is a message to the console of a system where the trusted user is logged in.				X	DCOITM	3.2.4.1.5.1
2.0 User Functions and Utilities						
2.4 Secure Email Function AFDI shall provide a secure e-mail capability for selected users to:						
2.4.1 Share sensitive information.				X	DCOITM	3.2.21.1
2.4.2 Encrypt sensitive e-mail traffic.				X	DCOITM	3.2.21.2
2.4.3 Digitally sign their e-mail transactions.				X	DCOITM	3.2.21.3
2.4.4 Authenticate the sender of e-mail traffic.				X	DCOITM	3.2.21.4
2.4.5 Manage public keys for use with e-mail.				X	DCOITM	3.2.21.5
2.4.6 Manage private keys for use with e-mail.				X	DCOITM	3.2.21.6
2.4.7 Include attachments to their e-mail traffic.				X	DCOITM	3.2.21.7
2.4.8 Encrypt attachments in e-mail traffic.				X	DCOITM	3.2.21.8
2.4.9 Digitally sign attachments in e-mail traffic.				X	DCOITM	3.2.21.9
2.4.10 Send secure e-mail to multiple recipients.				X	DCOITM	3.2.21.10
2.4.11 Overwrite e-mail messages marked for deletion.				X	DCOITM	3.2.21.11
2.4.12 Validate the integrity of e-mail received.				X	DCOITM	3.2.21.12
2.4.13 Share sensitive information				X	DCOITM	3.2.21.13
3.0 System Administration						
3.1 Printing						
3.1.1 AFDI shall provide the capability to centrally monitor and control print queues in a heterogeneous environment and perform the following administration tasks:	X				ADMSRS	3.2.1.40
3.1.1.5 Prioritize print jobs in the print queue.				X	ADMSRS	3.2.1.40
3.1.1.6 Move print jobs between print queues.				X	ADMSRS	3.2.1.40
3.8 Disk Space Function						
3.8.1 AFDI shall check the availability of space on each of its disks at regular intervals. If the used space on a disk exceeds a default limit of 85%, or other limit as set by a trusted user, an audit event shall be triggered. In the event of a trigger a notification shall be generated to the designated users, and a predetermined system action shall be performed. System actions may be one or more of the following:				X		

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.x	Doc	Para.
3.8.3.1 System shut down				X		
3.8.3.2 Abort current space demanding tasks				X		
3.8.3.3 Archive and purge inactive files				X		
3.8.3.4 Perform compression on inactive files				X		
3.8.4 AFDI shall provide the capability to control disk resources and perform the following administration tasks:			X		ADMSRS	3.2.1.49
3.8.4.1 Allocate user disk space including setting quotas.			X		ADMSRS	3.2.1.49
3.8.4.2 Modify disk partitions.			X		ADMSRS	3.2.1.49
3.8.4.3 Mount file systems.			X		ADMSRS	3.2.1.49
3.8.4.4 Unmount file systems.			X		ADMSRS	3.2.1.49
3.8.4.5 Determine disk space usage.			X		ADMSRS	3.2.1.49
3.8.4.6 Determine disk space availability.			X		ADMSRS	3.2.1.49
3.8.4.7 Create file systems.			X		ADMSRS	3.2.1.49
3.8.4.8 Modify file systems.			X		ADMSRS	3.2.1.49
3.8.4.9 Create file system tables.			X		ADMSRS	3.2.1.49
3.8.4.10 Modify file system tables.			X		ADMSRS	3.2.1.49
3.8.4.11 Export file system tables.			X		ADMSRS	3.2.1.49
3.9 Performance Management Function						
3.9.4 AFDI shall provide the capability to generate a notification and a log entry when CPU utilization exceeds a specified threshold for a specified period of time.				X	ADMSRS	3.2.3.24
3.13 Network Services Function						
3.13.5 AFDI shall provide the capability to display user's active profiles				X		
3.13.6 AFDI shall provide the capability to display inactive profiles				X		
3.19 Peripherals Function						
AFDI shall provide the capability to monitor and control peripherals within the administrative domain such as:						
3.19.1 CDROMS			X		ADMSRS	3.2.1.52
3.19.3 Tape drives			X		ADMSRS	3.2.1.52
3.19.4 AFDI shall provide the capability to allocate access to peripherals.			X		ADMSRS	3.2.1.52a
3.26 Alert Messages Function						
The following conditions shall cause an alert to be transmitted to selected users:						
3.26.1 Detection of malicious code on hard drives or removable media				X		
3.26.2 Detection of malicious code in incoming data streams				X		

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.x	Doc	Para.
3.26.3 Data storage nearing critical capacity on a hard drive or removable medium				X		
3.26.4 A user ID is locked				X		
3.26.5 Dead man capability activates				X		
3.26.6 Audit data has reached the current limit of available storage capacity				X	DCOITM	3.2.2.15
3.26.7 Audit process(s) has failed				X	DCOITM	3.2.3.1.4
3.26.8 Failure of a AFDI system service				X	DCOITM	3.2.4.1.1
3.26.9 Time to perform audit archive ??				X	DCOITM	3.2.3.1.5.4
3.26.10 Alerts shall take the form of:						
3.26.10.1 Visible message on the workstation screen				X	DCOITM	3.2.13.4.3.1
3.26..10.2 Audible alarm				X	DCOITM	3.2.13.4.3.2
3.27 Segmentation Function						
3.27.1 AFDI shall provide the capability for Point and Click/Drag and Drop Segmentation			X			
3.27.2 AFDI shall provide the capability to perform Configuration Definition Modeling			X			
3.27.3 AFDI shall provide the capability for Segment enhancements			X			
3.27.4 AFDI shall provide a web based interface for the segmentation process			X			
3.27.5 AFDI shall provide the capability for Segment testing			X			
4.0 Security Management						
4.1 Security Administration Function						
4.1.1.9 Sort log files.				X	ADMSRS	3.2.1.54
4.1.1.10 Query log files.				X	ADMSRS	3.2.1.54
4.1.1.11 Save log files to other files.				X	ADMSRS	3.2.1.54
4.2 Accountability						
4.2.9 AFDI shall provide the capability to check for unexpected file system corruption or security breaches using Cyclic Redundancy Checks (CRCs) and changes to a file's inode attributes.	Solaris			NT	ADMSRS	3.2.4.1.11
4.2.10 AFDI shall provide the capability to measure intrusion detection by reporting changes to a file's RSA MD5 encryption signature.				X	ADMSRS	3.2.4.1.11
4.4 Logging and Security Audit Function						
4.4.5.4 Increase storage capacity for audit data				X	DCOITM	3.2.3.1.3.1.4

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.x	Doc	Para.
4.4.6 Provide an interface for configuring which trusted user shall receive notifications when the audit data has reached the threshold n percent of available storage capacity.				X	DCOITM	3.2.3.1.3.1.3 .1
4.4.14 AFDI shall provide the capability to archive and selectively retrieve audit data				X	DCOITM	3.2.3.1.5
4.4.15 AFDI shall provide the capability to automatically archive audit data when the audit data reaches a configurable threshold of percent of available storage capacity.				X	DCOITM	3.2.3.1.5.1
4.4.16 AFDI shall provide the capability for a trusted user to configure the threshold of n percent upon which audit data shall be automatically archived.				X	DCOITM	3.2.3.1.5.2
4.4.17 The default threshold shall be 70 percent.				X	DCOITM	3.2.3.1.5.2.1
4.4.21 Provide a GUI for a trusted user to configure the time, represented as every n hours.				X	DCOITM	3.2.3.1.5.4.1
4.4.22 The default threshold n shall be every 168 hours.				X	DCOITM	3.2.3.1.5.4.2
4.4.39 For events that introduce an object into a user's address space, and for object deletion events, AFDI audit record shall identify the name of the object.				X	DCOITM	3.2.3.7
4.4.44 Provide the capability to generate reports based on fields in event records or Boolean combinations of those fields.				X	DCOITM	3.2.3.11.1
4.4.47 AFDI shall provide the capability for trusted users to generate reports of audit data that has been collected based on fields in event records or Boolean combinations of those fields, or based on ranges of system date and time that audit records were collected.				X	DCOITM	3.2.3.11
4.5 Security and Confidentiality Requirements						
4.5.1 AFDI shall provide for the management of the network, system and security mechanisms and be comprised of a set of management application entities and a management communications protocol stack.				X	ADMSRS	3.3.7
4.7 Trusted Facility Management (TFM) Function						
4.7.36 AFDI shall provide the following capabilities for a trusted user (e.g., security officer) for managing the audit log(s):					DCOITM	
4.7.36.7 Sort				X	DCOITM	3.2.16.7.1
4.12 Public Key Infrastructure Functions						
AFDI shall provide the capability to:						

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.x	Doc	Para.
4.12.1 Request creation of X.509 certificates in accordance with PKCS #10.				X	DCOITM	3.2.20.1
4.12.2 Receive and store X.509 certificates.				X	DCOITM	3.2.20.2
4.12.3 Request certificate revocation lists (CRL).				X	DCOITM	3.2.20.3
4.12.4 Request third-party X.509 certificates.				X	DCOITM	3.2.20.4
4.12.5 Validate third-party X.509 certificates. Validation of third-party certificates shall include the following:				X	DCOITM	3.2.20.5
4.12.5.1 Verifying the certificate of the certifying authority of the certificate				X	DCOITM	3.2.20.5.1
4.12.5.2 Verifying the certificate chain (i.e., checking the validity dates and signature of the certificate issuer for the original certificate, the issuer's certificate, etc., until a trusted authority is reached)				X	DCOITM	3.2.20.5.2
4.12.5.3 Verifying that the certificate nor anything on the certificate chain is on the CRL				X	DCOITM	3.2.20.5.3
4.12.5.4 Verifying that the validity period of the certificate has not expired				X	DCOITM	3.2.20.5.4
4.12.5.5 Verifying that the certificate is being used for its intended purpose.				X	DCOITM	3.2.20..5
4.12.6 AFDI shall provide the capability to create and verify digital signatures. The digital signatures supported by AFDI shall meet the following standards:				X	DCOITM	3.2.19
4.12.6.1 The Digital Signature Standard (DSS) as specified in FIPS Publication 186				X	DCOITM	3.2.19.2.1
4.12.6.2 Rivest, Shamir,, and Adleman (RSA) public key cryptography system as specified in Public Key Cryptography Standards (PKCS) #1				X	DCOITM	3.2.19.2.2
4.12.7 AFDI shall provide the capability to generate public/private keys for both the RSA and DSS.				X	DCOITM	3.2.20
4.12.8 AFDI shall provide the capability to export private keys in accordance with PKCS#12				X	DCOITM	3.2.19.4
4.12.9 AFDI shall provide the capability for the recipient of an information transaction to determine proof of the origin and originator of the data (e.g., using digital IDs).				X	DCOITM	3.2.14.1
4.12.10 AFDI shall provide the capability for the sender of an information transaction to determine proof of delivery (e.g., using digital IDs).				X	DCOITM	3.2.14.2
4.13 DAC Checker Function This function shall provide the ability to:						

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.x	Doc	Para.
4.13.18 AFDI shall provide the capability to control access of mobile code (e.g., Java applets, ActiveX controls) to objects.			X		DCOITM	3.2.5.13
4.13.19 AFDI shall provide a secure X-display that controls access to X resources by individual. AFDI shall provide the capability to control access to resources based on the following:				X	DCOITM	3.2.5.14
4.13.19.1 Means of access	Solaris			NT	DCOITM	3.2.5.15.1
4.13.19.2 Port (i.e., network protocol) of entry		Solaris		NT	DCOITM	3.2.5.15.2
4.13.19.5 Calendar date range (i.e., 15 June 1997 to 14 June 1998)	Solaris			NT	DCOITM	3.2.5.15.5
4.13.21 AFDI shall provide the interface for configuration of screen-lock capabilities by a trusted user (e.g., system administrator).			X		DCOITM	3.2.5.16.4
4.14 User Access Function The User Access Function shall:						
4.14.10 Provide procedures and documentation for disk cloning			X		CSE	
4.14.11 Provide procedures and documentation for automated installs of the AFDI product			X		CSE	
4.15 Login Function						
4.15.9 AFDI shall provide the capability for strong user authentication (i.e., using cryptographically protected authentication or one-time passwords).				X	DCOITM	3.2.1.4.4
4.15.10 AFDI shall provide a trusted user the capability to enable or disable display of last successful login date and time and the number of unsuccessful login attempts.				X	DCOITM	3.2.1.4.5.1
4.16 System Access (LOGIN) Authentication Function						
4.16.2 AFDI shall provide the capability for users, the security officer, and the system to generate passwords.				X	DCOITM	3.2.1.4.1.1
4.16.5 AFDI shall prevent unauthorized disclosure of passwords during transmission across a network.				X	DCOITM	3.2.1.5.1
4.16.16 Provide a non-forgable, non-replayable distributed authentication mechanism that supports both unilateral (client-to-server) or mutual (client-to-server and server-to-client) authentication.				X	DCOITM	3.2.1.7
4.16.17 Provide a single sign-on capability that permits access to resources (e.g., applications and information) in a distributed system for which the user is authorized without the user being required to re-authenticate at each host where the resources reside.				X	DCOITM	3.2.1.8

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.x	Doc	Para.
4.16.18 Provide the capability to restrict the time period for which a user may be permitted to use single sign-on to access resources to n minutes where n is configurable by a trusted user.				X	DCOITM	3.2.1.8.1
4.16.19 After n minutes the user shall be required to re-authenticate to access remote resources.				X	DCOITM	3.2.1.8.1.1
4.16.20 The default time period n for which a user may be permitted to use single sign-on shall be 480 minutes.				X	DCOITM	3.2.1.8.1.2
4.16.21 Support single sign-on using hardware tokens (e.g., smart card, FORTEZZA card as an authentication mechanism during the user's initial login.				X	DCOITM	3.2.1.8.2
4.16.22 Support single sign-on using X.509 v3 certificates as an authentication mechanism during the user's initial login.				X	DCOITM	3.2.1.8.3
4.16.23 Provide the capability to configure user-based access control for use in a single sign-on implementation, where a single user could be granted access to all or a specific subset of available resources,				X	DCOITM	3.2.1.8.4
4.17 Password Operation Function						
4.17.4 The system shall be able generate passwords				X	DCOITM	3.2.1.4.1.1
4.17.13 When changing the password, AFDI shall prohibit the reuse of the current password and n passwords used prior to the current password where n is defined by a trusted user.	NT		Solaris		DCOITM	3.2.1.4.1.3
4.18 Data Security Function						
4.18.1 AFDI shall provide the capability for the recipient of an information transaction to determine proof of the origin and originator of the data (e.g., using digital IDs).				X	DCOITM	3.2.14.1
4.18.2 AFDI shall provide the capability for the sender of an information transaction to determine proof of delivery (e.g., using digital IDs).				X	DCOITM	3.2.14.2
4.19 Object Reuse Function						
4.19.1 AFDI shall ensure that no information, including encrypted representations of information, produced by a prior subject's actions is made available to any subject that obtains access to an object that has been released back to AFDI.				X	DCOITM	3.2.10.1
4.19.2 AFDI shall ensure that all authorizations to information contained within a storage object have been revoked prior to initial assignment, allocation, or reallocation to a subject from AFDI's pool of unused storage objects				X	DCOITM	3.2.10.2

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.x	Doc	Para.
4.20 Data Confidentiality						
4.20.1 AFDI shall provide accessible cryptographic application programming interfaces for use by applications to selectively encrypt and decrypt data and files.				X	DCOITM	3.2.11.1
4.20.2 The AFDI shall provide a set of assured APIs capable of accommodating both Type I and Type II Security Services, which can be configured with different security policies.				X	Security SRS	3.2.11.1.1
4.20.3 AFDI shall provide the capability for end-to-end encryption services for user sessions.				X	DCOITM	3.2.11.2
4.20.4 AFDI shall provide end-to-end encryption using a unique private key for each user.				X	DCOITM	3.2.11.2.1
4.20.5 AFDI shall protect the confidentiality and integrity of user private keys.				X	DCOITM	3.2.11.2.2
4.20.6 AFDI shall provide the capability for a user to transport his or her private key from one user platform to another user platform.				X	DCOITM	3.2.11.2.3
4.20.7 AFDI shall provide the capability for key recovery.				X	DCOITM	3.2.11.3
4.20.8 AFDI shall provide an Internet Protocol Security (IPSEC) encryption capability as defined in the Internet Protocol, Version 6 (Ipv6) Specification (Deering, 1997).				X	DCOITM	3.2.11.4
4.20.9 AFDI shall provide an administrative interface that allows a security officer to manage the IPSEC Security Policy Database (SPD) as defined in the <i>Security Architecture for the Internet Protocol</i> (Kent, 1998).				X	DCOITM	3.2.11.4.1
5.0 Account Management						
5.1 Account Creation Function						
5.1.1 AFDI shall provide the capability for centralized user account <i>creation</i> in a heterogeneous environment with the capability to define the following user parameters:	X				ADMSRS	3.2.1.19
5.1.1.4 Automatic password generation in accordance with the Security SRS				X	ADMSRS	3.2.1.19
5.1.1.8 Default profile			X		ADMSRS	3.2.1.19
5.1.2 The user account creation mechanism shall provide an API or equivalent mechanism that shall support the execution of additional tasks during user account creation as required by AFDI and its segments. These tasks may include adding users to the DBMS, Profile Database and creating the user's home directory.	Solaris			NT	ADMSRS	3.2.1.20

Air Force DoDIIS Infrastructure (AFDI) Requirement	Release				Requirement	
	1.0	1.1	2.0	2.x	Doc	Para.
5.1.3 AFDI shall create users such that it shall support single sign-on of the user in accordance with the Security SRS.				X	ADMSRS	3.2.1.21
5.1.4 AFDI shall provide a single sign-on capability to support transparent, distributed login for all users in accordance with the Security SRS.				X	ADMSRS	3.2.1.22
5.1.6 If the user's home directory file server is modified, the account modification mechanism shall create a new home directory on that server.			X		ADMSRS	3.2.1.23
5.1.8 The user account deletion mechanism shall be extensible such that it shall support the execution of additional tasks during user account deletion as required by AFDI and its segments. These tasks may include deleting users from the DBMS, Profile Database and deleting the user's home directory.	Solaris			NT	ADMSRS	3.2.1.25