

DAR ENCRYPTION TECHNICAL & FUNCTIONAL REQUIREMENTS FOR DoD and other FEDERAL AGENCIES					
Requirement Number	Product Category		Technical & Functional Requirements	Category Rankings	Instructions to Offerors - Vendors please follow instructions and respond to each technical requirement with a response in the appropriate section below (you may delete the instructions and replace with proposed response), reference an attachment, or state 'No Response'. When referencing attachments, use the same Requirement Numbers in the same order as the Technical & Functional Requirements in this document, or provide a table of cross references.
	FDE	FES			
<p><b>ACQUISITION CATEGORY RANKINGS - CRITICAL (C)</b> - the capability MUST be met in order for a proposal to be successful. Products that do not meet each and every CRITICAL requirement will not be deemed acceptable. <b>IMPORTANT (I)</b> - the capability is important so additional points will be assigned for products providing these capabilities. <b>DESIRED (D)</b> - the capability is desired so additional points will be assigned for products providing these capabilities but at a lower importance factor than for the Important criteria. <b>PRODUCT CATEGORY - FULL DISK ENCRYPTION (FDE)</b> - also referred to as whole disk encryption, is a form of encryption (software or hardware) which encrypts every bit of data that is placed and stored on a disk. <b>FILE ENCRYPTION SYSTEM (FES)</b> - is a form of disk encryption where individual files or directories are encrypted by the file system itself, allowing users to specify which files or folders require encryption and files and/or folders are encrypted and decrypted as necessary. <b>FDE/FES</b> - refers to an integrated full disk encryption and file encryption system. <b>REMOVABLE STORAGE MEDIA (RSM)</b> - refers to cartridge and disc-based removable and portable storage media devices which can be used to easily move data between computers. Examples of removable media include, but are not limited to, floppy disks, compact discs, USB flash drives, external hard drives and other flash memory cards/drives that contain non-volatile memory.*</p>					
<b>CERTIFICATION AND STANDARDS</b>					
1	X	X	The cryptographic module used in the product offered must be NIST FIPS 140-2 compliant.	CRITICAL	<b>Meets Requirement.</b> The Credant Cryptographic Kernel is FIPS 140-2 Level 1 Validated. This validation was performed in the US by a government-approved laboratory and the certificate from NIST is located at: <a href="http://csrc.nist.gov/cryptval/140-1/140crt/140crt452.pdf">http://csrc.nist.gov/cryptval/140-1/140crt/140crt452.pdf</a> Credant's FIPS Validated Cryptographic Kernel (CCK) is the core cryptography library and common across all CMG software components. The CCK provides the encryption algorithms for the Credant Security Services (CSS) library which is also common across all CMG software components. CSS adds key management and higher level APIs which enable all other Credant modules to utilize the cryptographic functions provided by the CCK. CSS does not provide any cryptographic algorithms itself but instead relies upon the FIPS-Validated CCK algorithm to perform all operations. Additionally, the CCK always runs in "FIPS mode". There is never a time that CCK runs in a non-validated mode. Finally, when the Credant software is built, the CCK is never re-built but the version which was FIPS-validated is pulled from a secure storage location within the code repository and linked into the software.
2	X	X	Product shall be NIAP certified	IMPORTANT	<b>CREDANT is currently being evaluated to Common Criteria Certified at EAL 3. Credant is listed on the "in evaluation" web site for Common Criteria: <a href="http://www.niap-cc-evs.org/cc-scheme/in_evaluation.cfm">http://www.niap-cc-evs.org/cc-scheme/in_evaluation.cfm</a> with an anticipated completion date of August 2007. Because there was no available protection profile for DAR encryption, Credant developed a security target which is being used in the CCEVAL process. Documentation of security target is confidential however the document can be made available upon request to government agencies as well as to third-parties pursuant to a Non Disclosure Agreement.</b>
3	X	X	Product shall be compliant with American Disabilities Act Section 508.	IMPORTANT	<b>Meets Requirement.</b> Product meets Section 508 compliance requirements by integrating the client with standard windows alert functionality - which in turn interfaces with industry standard contrast, color, and human interface devices. See Attachment 1 to Annex A. Credant addresses Section 508 compliance on their website at <a href="http://www.credant.com/content/section/10/132/">http://www.credant.com/content/section/10/132/</a>
4	X	X	Product shall be in the NIAP certification process	DESIRABLE	<b>Meets Requirement.</b> CREDANT is currently being evaluated to Common Criteria Certified at EAL 3. Credant is listed on the "in evaluation" web site for Common Criteria: <a href="http://www.niap-cc-evs.org/cc-scheme/in_evaluation.cfm">http://www.niap-cc-evs.org/cc-scheme/in_evaluation.cfm</a> with an anticipated completion date of August 2007. Because there was no available protection profile for DAR encryption, Credant developed a security target which is being used in the CCEVAL process. Documentation of security target is confidential however the document can be made available upon request to government agencies as well as to third-parties pursuant to a Non Disclosure Agreement.
<b>ENCRYPTION</b>					
5	X	X	The product provides Full Disk Encryption (FDE), File/Folder Encryption System (FES), or Integrated FDE and FES.	CRITICAL	<b>Meets Requirement.</b> The Credant Product is FES. Credant encrypts designated Files, Folders, file extensions/types, Any Data coming out of a designated executable (regardless of format/type/extension), Swap Files, Temp Files, Registry Files, Password Hash, All Removable Storage Drives automatically based on Administrator defined Policy per group or individual. Additionally, Credant has an on-demand self-extracting password-based encryption component for user-controlled security above and beyond administrator defined policies. There are no pre-boot requirements, Credant has proven interoperability with Smart Cards, including CAC and PIV, which can encrypt the Credant Synchronous encryption key with their own Authentication (Asynchronous/Challenge-Response). Credant is an Intelligent Encryption System that avoids unnecessary encryption of system files that do not contain sensitive information - this optimizes the encryption time and resources to the key sensitive areas of the hard drive as specified by internal policy according to recommendations of OMB 06-16. Files are not reduced or increased significantly during the process.
6		X	The product provides a capability to automatically encrypt data that is transferred to removable storage media, for example, CD/DVD, USB pin-drives, tapes, external hard drives, etc., without user intervention or circumvention	CRITICAL	<b>Meets Requirement.</b> Administrators have the power to set "auto-encrypt" for all USB drives, all Floppy's, a Large number of PDA's and the most popular CD/DVD applications (available Summer 2007). Administrators have the flexibility to control all these media formats in a way that is transparent to the end user and avoids circumvention through encryption and strong security policies. The following Devices are supported USB: All Attached Storage, including Thumb Drives, iPod's, Camera's, external drives, etc. PDA's: SmartPhones (see OS Compatibility section for complete list) CD/DVD: Nero and Roxio controls available Summer of 2007 Additionally, with minimal user interaction, Credant can secure documents for Tapes Storage, Email, FTP, CD/DVD, or shared drives.

DAR ENCRYPTION TECHNICAL & FUNCTIONAL REQUIREMENTS FOR DoD and other FEDERAL AGENCIES					
Requirement Number	Product Category		Technical & Functional Requirements	Category Rankings	Instructions to Offerors - Vendors please follow instructions and respond to each technical requirement with a response in the appropriate section below (you may delete the instructions and replace with proposed response), reference an attachment, or state 'No Response'. When referencing attachments, use the same Requirement Numbers in the same order as the Technical & Functional Requirements in this document, or provide a table of cross references.
	FDE	FES			
7	X		Product must be capable of using the user's PKI encryption certificate within the DoD CAC or PIV II compliant Smartcard to protect the full volume encryption key	CRITICAL	<b>EXCEEDS REQUIREMENT.</b> For all encryption processes including removable storage devices Credant encrypts the data using the User Roaming encryption key which is protected by CAC/PIV. Credant uses the Mobile Guardian self-extracting encryption process which is password based (Administrator defines password strength) for easier interoperability with exchanging Files to non-Credant Enabled and non-Managed External Systems as outlined requirement #13.
8		X	Product must be capable of using the user's PKI encryption certificate contained in the DoD CAC or PIV II compliant Smartcard to encrypt the file that contains the system generated file/folder encryption key	CRITICAL	<b>EXCEEDS REQUIREMENT.</b> For all encryption processes including removable storage devices Credant encrypts the data using the User Roaming encryption key which is protected by CAC/PIV. Credant uses the Mobile Guardian self-extracting encryption process which is password based (Administrator defines password strength) for easier interoperability with exchanging Files to non-Credant Enabled and non-Managed External Systems as outlined requirement #13.
9	X	X	The product's process for encryption and decryption of data is configurable to be transparent to user	IMPORTANT	<b>Meets Requirement.</b> All of the encryption policies implemented by the administrator are transparent and requires no interaction from the end users. Every time the system connects to the network there is an audit process that reports the proper (or otherwise) functions of the encryption agent as well as any attempt to tamper with the device. Credant also receives any new administrator policies at this time. End users cannot circumvent the encryption process. Any tampering with the Credant application could only disable the user's ability to decrypt their data.

DAR ENCRYPTION TECHNICAL & FUNCTIONAL REQUIREMENTS FOR DoD and other FEDERAL AGENCIES					
Requirement Number	Product Category		Technical & Functional Requirements	Category Rankings	Instructions to Offerors - Vendors please follow instructions and respond to each technical requirement with a response in the appropriate section below (you may delete the instructions and replace with proposed response), reference an attachment, or state 'No Response'. When referencing attachments, use the same Requirement Numbers in the same order as the Technical & Functional Requirements in this document, or provide a table of cross references.
	FDE	FES			
10	X	X	Products shall provide an option to use only FIPS 180-2 compliant algorithms for hashing and signing	IMPORTANT	<u>Meets Requirement.</u> Credant's implementation of the SHA-1 and HMAC-SHA-1 algorithms are FIPS validated.
11	X	X	Product uses an approved random number generator specified in FIPS 140-2 Annex C for key generation	IMPORTANT	<u>Meets Requirement.</u> CREDANT is FIPS 140-2 Validated. RNG-39 (Cert. #88) is the algorithm used by Credant to perform encryption and is FIPS approved.
12	X	X	The product must allow data from an encrypted source to be decrypted to allow transfer of data unencrypted to another destination	IMPORTANT	<u>Meets Requirement.</u> Credant is transparent to the end user. Administrators can set a policy to automatically decrypt data moved to some devices (like USB fobs) for specific users or groups. Decryption is done transparently when a user moves data to a server or attaches an encrypted file to an email. If the administrator has not allowed the user to decrypt data, the user cannot circumvent the process (refer to technical requirement #6).
13	X	X	The product supports distribution of encrypted data to trusted or business partners for data exchange using authenticated self extraction	IMPORTANT	<u>Meets Requirement.</u> If allowed by the administrator, the Credant Mobile Guardian tool "Credant2go" is a user-oriented encryption process for securing data that needs to pass beyond the protected walls of the Credant system. Users can encrypt a file or folder with a password or codeword protected self-extracting archive that can then be shared out-of-band with the recipient of the file, either verbally, via written letter, or some other reference or code which the sender and the recipient understand, but is oblique to a potential hacker/cracker.
14	X	X	If product offers optional encryption algorithms to be used for encryption, the product allows encryption algorithm selection by an administrator	IMPORTANT	<u>Meets Requirement.</u> Credant is centrally managed and the administrator has complete control over the encryption policies. Specifically, choosing the algorithm is done via a drop down list in the administrator interface.
15	X	X	If product is an integrated FDE and FES solution, the product provides FDE and FES under a single product management console	IMPORTANT	<u>Meets Requirement.</u> Credant has many features beyond a typical FES (Such as Temp. Swap, Registry, and Application Data security) but it is not a Full Disk Encryption due to usability/interoperability requirements. Administrators can set encryption policies for all their devices (Windows, Pocket PC, Symbian Palm, removable media, etc) and all users or groups through the Credant web interface.
16	X	X	If the product offers optional encryption algorithms to be used for encryption, the product should have the capability for the administrator to deactivate or 'grey out' undesirable or unauthorized options.	DESIRABLE	<u>Meets Requirement.</u> Credant is centrally managed and the administrator has complete control over the encryption policies. Specifically, choosing the algorithm is done via a drop down list in the administrator interface.
17		X	Product is capable of file compression and encryption in a single step by the user	DESIRABLE	<u>EXCEED REQUIREMENT.</u> Credant is transparent to the end-user and any compression software used does not require any additional steps by the user to complete compression and encryption. Encryption is automatic, based on selections made on the administrator's console.
AUTHENTICATION					
18	X		Product provides boot authentication	CRITICAL	<u>Meets Requirement.</u> Credant provides Full Disk Encryption with pre-boot authentication. Drive Manager requires no portion of the disk to be unencrypted except for the boot sector and includes a pre-boot operating system that is based on a Linux Kernel, which itself is fully encrypted, containing all drivers required for hardware support including network (as required for OCSP), authentication methods (including Biometrics), foreign Language Keyboards, Tablet computer visual keyboards, Bluetooth CAC readers or other required hardware.
19	X		Product must support use of DoD CAC or PIV II compliant Smartcard for boot authentication with no modification of card required	CRITICAL	<u>Meets Requirement.</u> Credant provides Full Disk Encryption with pre-boot authentication using the PKI encryption certificate for the unlocking of the Volume Encryption key. The encrypted key is stored in an encrypted form in a random position on the encrypted disk. The user must present the physical certificate through either a CAC or PIV II compliant mechanism in order to decrypt the volume key. At no point does Credant modify any smartcards, CAC or PIV II cards -strictly read only.
20	X		Product must support use of DoD CAC or PIV II compliant Smartcard on a Government approved token for boot authentication	CRITICAL	<u>Meets Requirement.</u> Credant's pre-boot authentication supports numerous means of authentication, including physical certificate through either a CAC or PIV II compliant mechanism. In addition, DataArmor also provides network connectivity capabilities at a pre-boot fully encrypted state. This will allow live calls between tokens/smartcards and remote authentication authorities. DataArmor supports Gemplus, Axalto, Schlumberger, Oberthur, Gemalto, RSA and Alladin tokens.
21	X		Product shall allow the administrators to set a configurable limit for pre-boot logon attempts and invokes lockout for failed logon attempts after exceeding the limit	CRITICAL	<u>Meets Requirement.</u> Credant enforces the centrally configured policy settings set on the PolicyServer which includes the ability to set password History, Password retention, Password complexity requirements, failed logon attempts with configuration remediation actions ranging from time out, device lock out, forced remote authentication (challenge/response requiring administrator intervention) and/or device erasure, that can be centrally configured on a group or enterprise level.

DAR ENCRYPTION TECHNICAL & FUNCTIONAL REQUIREMENTS FOR DoD and other FEDERAL AGENCIES					
Requirement Number	Product Category		Technical & Functional Requirements	Category Rankings	Instructions to Offerors - Vendors please follow instructions and respond to each technical requirement with a response in the appropriate section below (you may delete the instructions and replace with proposed response), reference an attachment, or state 'No Response'. When referencing attachments, use the same Requirement Numbers in the same order as the Technical & Functional Requirements in this document, or provide a table of cross references.
	FDE	FES			
22	X		Product supports password based pre-boot authentication	IMPORTANT	<u>Meets Requirement.</u> Credant's management console allows for full password rule definitions and enforcement on administrators on a per group basis. Mobile Armor policies can be defined for a set limit of consecutive failed login attempts & then lock the account, as well as password length, # of consecutive characters, case sensitivity, whether it can or can't contain the username within it, forced number of alpha characters, forced number of numeric characters, forced number of special characters, history retention, and forced password change after X amount of days.
<b>ADMINISTRATION &amp; CONFIGURATION</b>					
23	X		The product allows multiple users of the same laptop or device to use their individual DoD CAC or PIV II compliant Smartcard for boot authentication	CRITICAL	<u>Meets Requirement.</u> Drive Manager allows for multiple users to authenticate by means of their CAC card, or multiple CAC cards for a single user. Unlimited multiple users can also authenticate to the same laptop using their registered authorized CAC or PIV II credentials. All access is defined and maintained through policies from the Policy Server. Multiple users who need to share the same device must be members of the same group within the Policy Server.

DAR ENCRYPTION TECHNICAL & FUNCTIONAL REQUIREMENTS FOR DoD and other FEDERAL AGENCIES					
Requirement Number	Product Category		Technical & Functional Requirements	Category Rankings	Instructions to Offerors - Vendors please follow instructions and respond to each technical requirement with a response in the appropriate section below (you may delete the instructions and replace with proposed response), reference an attachment, or state 'No Response'. When referencing attachments, use the same Requirement Numbers in the same order as the Technical & Functional Requirements in this document, or provide a table of cross references.
	FDE	FES			
24	X		The product shall have the capability to allow administrators to update user's credentials when issued a new DoD CAC, PIV II compliant Smartcard, or token	CRITICAL	<b>Meets Requirement.</b> Drive Manager allows for credentials to be reassigned to users either locally or remotely. Re-issuance of a new credential and presentation for re-registration can be forced from the central management Policy Server. The administrator must issue a one-time password for the user with the new CAC which allows him to associate that new CAC with his account.
25	X		Product shall have the capability to allow administrators to provide remote assistance to users who are locked out	CRITICAL	<b>Meets Requirement.</b> Policy Server provides multiple methods for administrators to remotely reset lost passwords including password reset through e-mail, Questions and Answers, or remote authentication. Methods are fully selectable by policy and are selectable on both the enterprise and group level. If it has been configured by the administrator, the user can select self help prior to getting locked out. This will use a question and answer approach (questions configured by administrator) for the user to reset a password. The user could also simply choose remote authentication prior to getting locked out to reset the password after successfully doing a challenge/reply with an administrator with access to the Policy Server. When a user exceeds the failed login limit, policy defines how the client machine should respond: timed lockout, remote authentication, or erasure. The timed lockout reboots the device and restarts the failed login count after a configurable delay. Remote authentication requires assistance from an administrator who has access to the Policy Server. The last choice, erasure of the device encryption key, may be appropriate where risk of loss is exceptionally high. Should the device become erased and later recovered, the only way to recover data on it is to use the Drive Manager Utility
26	X	X	Product shall have the capability to allow administrators to configure the product for decryption and uninstall of encryption product by a system administrator only	CRITICAL	<b>Meets Requirement.</b> Configurations on the client are all policy driven within the Policy Server. It provides 3 methods of un-installation. Each method requires administrator credentials to enable the functionality. The 3 methods are [1] Drive Manager bootable utility CD, [2] built-in client based recovery console, and [3] windows based "Add and Remove Programs" interface. Again, all 3 methods must have administrative authority through secured credential sign-in to initiate.
27	X	X	Product shall prohibit vendor's ability to access, modify, or decrypt data	CRITICAL	<b>Meets Requirement.</b> The customer organization creates and manages all keys that encrypt or decrypt data. There are no back-doors or Master Keys to the system for CREDANT to potentially gain access to sensitive, encrypted data.
28	X	X	Product does not interfere with imaging of hard drive after encryption product is installed	CRITICAL	<b>Meets Requirement.</b> CREDANT does not interfere with existing administration processes such as hard drive imaging, restoration, recovery, erasure or patching. Credant can be installed on the default image and the user will receive their encryption key and encryption policy when they first login to the network.
29	X	X	Product does not interfere with Restoration/Recovery of encrypted data from backup media	CRITICAL	<b>Meets Requirement.</b> CREDANT does not interfere with existing administration processes such as restoration or recovery of data from backup media, whether encrypted or not. Credant can be installed on the default image and the user will receive their encryption key and encryption policy when they first login to the network.
30	X	X	Product does not interfere with full disk data erasure tools	CRITICAL	<b>Meets Requirement.</b> CREDANT does not interfere with existing administration processes to include full disk erasure tools.
31	X	X	The product is capable of secure escrow and recovery of the symmetric encryption key	CRITICAL	<b>Meets Requirement.</b> Keys are generated on the Enterprise Credant Server prior to deployment to the mobile device, therefore escrow keys are kept at the enterprise level. Access to data cannot be lost because of a lost encryption key. Encryption is only performed after the key is created and backed up on the server.
32	X	X	The product shall implement NIST SP 800-53, Control IA-5	CRITICAL	<b>Meets Requirement.</b> Credant relies on the over-arching password controls for CAC and PIV and leverages those through interoperability with these multi-factor authentication technologies that supersede simple passwords.
33	X		If the product requires modification of the Master Boot Record, it shall be validated by the pre-boot environment	CRITICAL	<b>Meets Requirement.</b> The Master Boot Record is over-written at sector 0 with the Drive Manager boot record. A copy of the original MBR is stored in the Drive Manager encrypted data store. Once successful authentication occurs, the Drive Manager boot record calls the original Master Boot Record for access into the native operating system.
34	X	X	The product's encryption/decryption process must occur without loss or corruption of data or content modification	CRITICAL	<b>Meets Requirement.</b> During the initial scan at installation time, Credant uses a two stage encryption process. It creates and validates a cipher text version of existing data prior to deleting and overwriting the original value. During the original scan corruption cannot occur. Subsequently, data is encrypted in-stream as it is written to the media. The only corruption possible is one that would occur during an abnormal hardware write operation, and is not caused by Credant. File metadata such as dat and timestamps are not changed during any encryption processing.
35	X	X	Product will be capable of encrypting swap, free, slack, temp, and Internet temp files	CRITICAL	<b>Meets Requirement.</b> Credant encrypts the Windows swap file, the Windows password hash, temporary files, and temporary Internet files without the overhead of encrypting the full disk. Legacy files or residual clear-text on a drive can be rendered unreadable with up to seven-pass overwrite as defined in the CMG Policy Server. Once Credant is installed, all data is encrypted in-stream as it is written to the media. This means that no unprotected clear text files will be created once Credant is installed on a device, and all slack space will contain either no data, or residual encrypted data.
36	X		Product allows modification of boot authentication screen by administrators to reflect Federal Agency warning banners	CRITICAL	<b>Meets Requirement.</b> Drive Manager provides the specific legal notices, policy notifications and help screens. These can be customized per group or at the enterprise level by defining the policy within the Policy Server. These warnings may be presented both at installation time as well pre-boot.

DAR ENCRYPTION TECHNICAL & FUNCTIONAL REQUIREMENTS FOR DoD and other FEDERAL AGENCIES					
Requirement Number	Product Category		Technical & Functional Requirements	Category Rankings	Instructions to Offerors - Vendors please follow instructions and respond to each technical requirement with a response in the appropriate section below (you may delete the instructions and replace with proposed response), reference an attachment, or state 'No Response'. When referencing attachments, use the same Requirement Numbers in the same order as the Technical & Functional Requirements in this document, or provide a table of cross references.
	FDE	FES			
37	X		When only password authentication is used for boot authentication, the product shall allow the administrator to enforce complex passwords to include a minimum of 9 characters in length, upper and lower case, alphanumeric, and special characters	IMPORTANT	<b>Meets Requirement.</b> One of the many options for authentication within Drive Manager is fixed password. When utilizing fixed passwords administrators can configure policies within the Policy Server, to enforce the following fixed password customizable options: [1] password length (configurable from 1 to 255 characters required), [2] password retention (configurable from 0 to 24 previous passwords prevented from re-use), [3] how many alpha, numeric, and/or special characters can or must be used, [4] case sensitivity, [5] and frequency of forced password changes (configurable from 1 to 5,000 days).
38	X		Product supports ability for administrators to require / restrict which pre-boot authentication mechanism will be used (i.e. CAC, Smartcard, token or password only)	IMPORTANT	<b>Meets Requirement.</b> Drive Manager provide complete control over the authorized authentication methods. Methods can be set per enterprise, per group and per platform. Available authentication methods include password, PIN, RSA, CAC, color passcode, remote authentication, web token, and X9.9 token. The administrator selects which ones will be available to the user at login time.
39	X		Product has the ability to allow administrators to maintain administrator password for pre-boot authentication for each system	IMPORTANT	<b>Meets Requirement.</b> Drive Manager provides named administrators the ability to log in to systems for authorized purposes. All access to systems is logged in the central audit log on the Policy Server. There is no upper limit on the number of named administrators, and administrators can be granted access to groups of machines based on any level of the hierarchy including Enterprise, Group level or sub-group.
40	X	X	Product does not change the content of the GINA.dll file	IMPORTANT	<b>Meets Requirement.</b> Neither FDE or our FES products modify the existing GINA file. Drive Manager utilizes a chaining methodology in order to pass through credentials from pre-boot without modifying the GINA.dll file.
41	X	X	Product should not conflict with the host based security solutions running simultaneously on a mobile computing device such as Host Intrusion or Prevention Systems (HIDS or HIPS), Firewalls, and Anti-virus.	IMPORTANT	<b>EXCEEDS REQUIREMENTS.</b> Credant does not conflict with host based security solutions including HIDS, HIPS, Firewalls, Anti-virus and Patch Management. Those solutions operate at a different level in the stack and at a different moment in time than the Credant encryption process. The main objective of Credant is to encrypt user-oriented sensitive data. Host based security solutions protect operating processes from maliciously accessing sensitive OS functions.
42	X	X	Product is capable of silent and remote installation and updates of the product	IMPORTANT	<b>Meets Requirement.</b> Credant is completely transparent to the end-user. Credant installation and updates are pushed out through standard installation processes, such as Windows MSI Files. While Credant uses user account information and CAC/PIV tie-ins for security and authentication the installation and the associated registration are device-based and require no user-interaction. The user will receive their encryption keys and encryption policy the first time they login to the network.
43	X	X	During the product's encryption/decryption process, if the process is interrupted, the product is capable of resuming the process from point of disruption	IMPORTANT	<b>Meets Requirement.</b> Credant operates on a file-by-file basis. If there is a break in the encryption process for any reason Credant will not lose any information. It will re-start the encryption process for that file without impacting the rest of the machine or any other files.
44	X	X	Product will support or have built-in auditing, monitoring, analysis, and reporting capabilities	IMPORTANT	<b>Meets Requirement.</b> Credant has the functionality to be implemented in compliance with Audit and Accountability section of NIST SP 800-53. Credant conforms to storage capacity, audit processing, audit monitoring, analysis and reporting, audit reduction and report generation, time stamp, protection of audit information, non-repudiation capability and audit retention requirements.
45	X	X	Product shall allow logging of access events to the product and encrypted data (success and failure)	IMPORTANT	<b>Meets Requirement.</b> Credant logs successful and unsuccessful attempts to log into the device that contains the protected data. Credant also logs the current policy and the encryption status of all users who have logged onto the device. Credant supports NIST SP 800-53.
46	X		Product allows export of encrypted file that contains system generated full volume encryption key	IMPORTANT	<b>Meets Requirement.</b> Drive Manager provides complete key escrow of all encryption keys on the central Policy Server and allows for authorized decryption and recovery of data, as long as authentication can establish a network connection to the Policy Server for validation. Credant also, provides a bootable Utility CD that can communicate via a network connection to provide server based authentication to approve data recovery. Mobile Armor does not expose volume encryption key directly to an end user or administrator to prevent compromise of that key through mismanagement such as unauthorized duplication.
47	X	X	Product allows authorized user to validate disk encryption has occurred and is maintained	IMPORTANT	<b>Meets Requirement.</b> Drive Manager provides central audit logging of all activities on enterprise systems that can be easily reported on including encryption status, background encryption speed, and device encryption completion. Also, each user's system tray will have a Credant logo'd shield that if pointed to by the mouse arrow, will display current encryption percentage. If this icon is double-clicked users can receive details of encryption status.
48	X		Product can support pre-boot integrity	IMPORTANT	<b>Meets Requirement.</b> Drive Manager performs a real time status check at boot time to insure the integrity of the pre-boot operating system. The integrity check checks for tampering with the pre-boot operating system, files, or authentication information.

DAR ENCRYPTION TECHNICAL & FUNCTIONAL REQUIREMENTS FOR DoD and other FEDERAL AGENCIES					
Requirement Number	Product Category		Technical & Functional Requirements	Category Rankings	Instructions to Offerors - Vendors please follow instructions and respond to each technical requirement with a response in the appropriate section below (you may delete the instructions and replace with proposed response), reference an attachment, or state 'No Response'. When referencing attachments, use the same Requirement Numbers in the same order as the Technical & Functional Requirements in this document, or provide a table of cross references.
	FDE	FES			
49	X	X	Product allows administrators the option to install and configure the product on systems and devices not requiring DoD CAC or PIV II compliant Smartcard for boot authentication and/or encryption	IMPORTANT	<b>Meets Requirement.</b> Administrators can designate which authentication mechanism is appropriate for which users or groups in the same manner they do today. Credant does not affect the boot or login process in any way. Credant supports CAC, token or Smartcards use in an organization but does not stop the authentication of users who are not required to use them.
50	X	X	Product can be integrated into Federal Agency host-based security solutions as a module running on an endpoint computer	DESIRABLE	<b>Meets Requirement.</b> Credant can be seamlessly integrated with host-based security solutions. Credant does not conflict with host based security solutions including HIDS, HIPS, Firewalls, Anti-virus and Patch Management. Those solutions operate at a different level in the stack and at a different moment in time than the Credant encryption process. The main objective of Credant is to encrypt user-oriented sensitive data. Host based security solutions protect operating processes from maliciously accessing sensitive OS functions. There is also an API for Credant that can be extended to work with specific products, as well as inherent configuration security for OS Locations, device types, application data, SWAP Data, Temp Files, etc.
51	X	X	Product supports Trusted Platform Module (TPM) chip version 1.2 or higher	DESIRABLE	<b>Meets Requirement.</b> Credant CMG offers the ability to enroll, manage and report on TPM and BitLocker activity.
52	X	X	Product must be compatible with standard applications, protocols, and communications within the Federal Government	DESIRABLE	<b>Meets Requirement.</b> There are no compatibility issues with standard applications, protocols and communications including disk defragmenters, deleted/damaged file recovery tools, SMS, Tivoli, NetOps Tools, MS AD, Exchange 2003 & 2007, and system integration, since Credant does not encrypt the application or system files
53	X	X	Product supports boot into multiple operating systems on a single device	DESIRABLE	<b>Meets Requirement.</b> Drive Manager provides the ability to boot into multiple operating systems on the same machine. The process works like this, each time a laptop is turned on or re-booted, the Drive Manager pre-boot authentication will load and upon successful login the laptop will perform a soft reboot in which any pre-OS requests including which OS to load can be presented. Regardless of which OS you load they will all be encrypted and have Drive Manager drivers running in the background to decrypt/encrypt on the fly.
54	X	X	Provides open APIs or an SDK to support application integration	DESIRABLE	<b>Meets Requirement.</b> We do not currently provide an SDK. Support for government developed application integration is accomplished through administrative settings without the use of an SDK. In addition, Credant proscribes to LDAP and Windows file/folder APIs. Any product that can write to these open APIs will integrate with Credant.
55	X		The product supports Single Sign-On (simultaneous pre-boot and O/S logon)	DESIRABLE	<b>Meets Requirement.</b> Drive Manager provides single sign on against LDAP servers including Active Directory. The pre-boot operating system provides authentication against the LDAP server even enforcing, real-time password expiration and password change rules. This even allows for password changes from the Mobile Armor pre-boot authentication environment.
CENTRALIZED MANAGEMENT CONSOLE					
56	X	X	The product's administrator management console allows for failover functionality (fault tolerance/redundancy)	CRITICAL	<b>Meets Requirement.</b> The management Console provides remote access to the Policy Server to change policies, add users, run reports, or any other required activity. The management console is entirely self contained and can be run on any Windows machine with TCP/IP access to the central Policy Server. The PolicyServer uses Microsoft Server 2003/2008 with an SQL Database which provides fail-over/redundancy capabilities. If redundant Policy Servers are desired, they can simply be setup to communicate to the same back-end SQL database.
57	X	X	The product's administrator management console supports capability to add/modify/delete admin users	CRITICAL	<b>Meets Requirement.</b> Drive Manager utilizes a 4 tier hierarchy of assignment per user: Enterprise Administrators, Group Administrators, Group Authenticators, and End-Users (There is also an Enterprise Authenticator). The management console provides named administrators the ability to modify users, polices and devices on an authority level limited basis (configurable by policy). All access to systems is logged in the central audit log on the PolicyServer. There is no upper limit on the number of named administrators, and administrators can be granted access to groups of machines based on any level of the hierarchy including Enterprise, Group level. For example, an Enterprise administrator has the ability to modify all levels of the hierarchy but a group administrator is limited to his group or below. Authenticators do not have access to policies at their level. They can only assist users with remote authentication and review logs (i.e., help-desk personnel).
58	X	X	The product shall provide the capability to set a limit on the number of unsuccessful consecutive logon attempts to the administrator management console and invokes lockout for exceeding the limit	CRITICAL	<b>Meets Requirement.</b> Credant supports the CAC-specified lock-out parameter, or provides a custom Gina for non-CAC environments that can limit logon attempts based on administrator defined settings. Credant also offers the ability to delete data or hard reset the device when the Credant Shield is installed on mobile devices such as a Smart Phone.

DAR ENCRYPTION TECHNICAL & FUNCTIONAL REQUIREMENTS FOR DoD and other FEDERAL AGENCIES					
Requirement Number	Product Category		Technical & Functional Requirements	Category Rankings	Instructions to Offerors - Vendors please follow instructions and respond to each technical requirement with a response in the appropriate section below (you may delete the instructions and replace with proposed response), reference an attachment, or state 'No Response'. When referencing attachments, use the same Requirement Numbers in the same order as the Technical & Functional Requirements in this document, or provide a table of cross references.
	FDE	FES			
59	X		The product's administrator management console supports retrieval of computer, user, and user-group information from Active Directory	CRITICAL	<b>Meets Requirement.</b> The Policy Server provides central management for all users, groups and provides integration with Active Directory to allow for the retrieval of users and groups from the LDAP without requiring any schema modification to the existing Active Directory Schema. The Policy Server uses a "snap-in" functionality to plug in the Active Directory interface into the Policy Server.
60	X		The product's administrator management console must support ability to secure the PK-enabled administrative interface by using the DoD CAC or PIV II compliant Smartcard for authentication	CRITICAL	<b>Meets Requirement.</b> Policy Server management console can support the ability to authenticate to the console using a DoD CAC or PIV II compliant smartcard. The management console allows an administrator to register the certificate during the setup of the administrator account. Once the administrator has registered the certificate, the administrator may authenticate to the console using the CAC or PIV II smartcard.
61	X	X	Product will support or integrate with existing asset/license tracking and management tools	IMPORTANT	Credant's CMG or Drive Manager does not interfere with asset tracking and licensing tools initiated after pre-boot authentication.
62	X	X	Product shall support secure remote management of devices to support remote users	IMPORTANT	<b>Meets Requirement.</b> Both Drive Manager and CMG provides complete management of remote devices by the Policy Server over TCP/IP. DataArmor attempts to contact the PolicyServer for policy changes at boot time and at a configured interval after boot up (allowing updates to be pulled after VPN access is up). All communication is fully encrypted in XML (using AES-256) over port 80 (default).
63	X	X	Product shall support secure remote access to the administrator management console for administrators	IMPORTANT	<b>Meets Requirement.</b> The management console is a stand alone application that can be run on any Windows machine or VMWare and connects via TCP/IP to the central Policy Server. All communications between the console and the Policy Server are encrypted.
64	X	X	The product's administrator management console must be scalable to support large enterprise environments	IMPORTANT	<b>Meets Requirement.</b> The management console is a stand alone application that can be run on any Windows machine or VMWare and connects via TCP/IP to the central Policy Server. All communications with the Policy Server occur via the same Web Services interface used by all clients, allowing for unlimited hardware and software scalability options. As a general rule, a single Policy Server can support 30,000 users.
65	X	X	The product's administrator management console permits multiple administrator logins for simultaneous access	IMPORTANT	<b>Meets Requirement.</b> The management console is a stand alone application that can be run on any Windows machine or VMWare and connects via TCP/IP to the central Policy Server. There are no limitations for simultaneous administrator access buy authorized administrators.
66	X	X	The product's administrator management console supports retrieval of computer, user, and user-group information from LDAP Servers	IMPORTANT	<b>Meets Requirement.</b> The Policy Server can retrieve user and group information from the LDAP servers, however computer information is self generated during installation without user and/or administrator action.
67	X	X	The product or encryption system must be configurable to not interfere with remote distribution and full installation of applications, patches, and updates while connected to the network, and without user intervention	IMPORTANT	<b>Meets Requirement.</b> CREDANT does not interfere with existing administration processes, to include remote distribution and full installation of applications, patches, and updates. Credant is transparent to the user, administrative processes do not require user intervention.
68	X		The product or encryption system shall allow administrator to configure product to enforce zeroization, 'wipe' or key destruction to render the data unusable.	IMPORTANT	Drive Manager provides remote wiping and destruction capabilities for Windows. The Policy Server has policies that can be defined to wipe devices by the following 3 ways: [1] based on # of failed login attempts, [2] a pre-defined "dead-man-switch" or kill phrase, and [3] set required sync time intervals for client to speak with Policy Server.

DAR ENCRYPTION TECHNICAL & FUNCTIONAL REQUIREMENTS FOR DoD and other FEDERAL AGENCIES					
Requirement Number	Product Category		Technical & Functional Requirements	Category Rankings	Instructions to Offerors - Vendors please follow instructions and respond to each technical requirement with a response in the appropriate section below (you may delete the instructions and replace with proposed response), reference an attachment, or state 'No Response'. When referencing attachments, use the same Requirement Numbers in the same order as the Technical & Functional Requirements in this document, or provide a table of cross references.
	FDE	FES			
<b>SUPPORTED OPERATING SYSTEM, HARDWARE, FIRMWARE - NOTE: It is CRITICAL that product supports at least one of the following operating systems. It is IMPORTANT that product supports more than one of the following operating systems. It is DESIRABLE that product supports 3 or more operating systems. Of the list below, identify all operating systems supported to include version.</b>					
69	X	X	Microsoft Windows 2000		<b>EXCEEDS the Critical, Important, and Desirable requirements by supporting 7 OS.</b> Yes, with SP3, SP4.
70	X	X	Microsoft Windows 2003		<b>EXCEEDS the Critical, Important, and Desirable requirements by supporting 7 OS.</b> No.
71	X	X	Microsoft Windows XP		<b>EXCEEDS the Critical, Important, and Desirable requirements by supporting 7 OS.</b> Yes. SP1, SP2 and XP Tablet PC Edition SP2
72	X	X	Microsoft Windows Vista		<b>EXCEEDS the Critical, Important, and Desirable requirements by supporting 7 OS.</b> Yes.
73	X	X	UNIX / Sun Solaris		<b>EXCEEDS the Critical, Important, and Desirable requirements by supporting 7 OS.</b> No.
74	X	X	Mac OS X		<b>EXCEEDS the Critical, Important, and Desirable requirements by supporting 7 OS.</b> Yes, 10.x
75	X	X	Windows Mobile 5.0		<b>EXCEEDS the Critical, Important, and Desirable requirements by supporting 7 OS.</b> Yes. Windows Mobile 5 and Windows Mobile 5 Smartphone.
76	X	X	Windows CE		<b>EXCEEDS the Critical, Important, and Desirable requirements by supporting 7 OS.</b> Yes. Credant supports Windows Mobile 2002/2003 for PPC and Smartphone.
77	X	X	RIM/Blackberry		<b>EXCEEDS the Critical, Important, and Desirable requirements by supporting 7 OS.</b> No.
78	X	X	Palm		<b>EXCEEDS the Critical, Important, and Desirable requirements by supporting 7 OS.</b> Yes. Palm 5.x.
79	X	X	Symbian		<b>EXCEEDS the Critical, Important, and Desirable requirements by supporting 7 OS.</b> Yes. Symbian OS 7.0s, Nokia Series 80.
80	X	X	Linux to include Red Hat, SuSE		<b>EXCEEDS the Critical, Important, and Desirable requirements by supporting 7 OS.</b> No.
<b>GENERAL AND TECHNICAL SUPPORT</b>					
81	X	X	Under software maintenance agreement, vendors must notify the Government and deliver product within 10 working days of commercial release for new updates	CRITICAL	<b>EXCEEDS REQUIREMENT.</b> Within 5-7 days of commercial release, CREDANT notifies all customers of new patches and updates and provides a web link for the client to download the update.
82	X	X	For every product patch or upgrade release, vendor will provide verification that the product still meets all of the initial critical requirements	CRITICAL	<b>Meets Requirement.</b> Customers receive a detailed written report of each patch or upgrade enhancement and feature. This response was clarified by the DAR Team on Question Number A86, Dated 5 February 2007.
83	X	X	Vendor will maintain disclosure-requirements to the DoD when any commercial acquisitions of or by their company affects foreign ownership or influences foreign controls of that company.	CRITICAL	<b>Meets Requirement.</b> We will comply with this requirement. ID's business model is nearly 100% government focused with specialization in the DOD and Intelligence space, therefore we do not foresee any change in ownership that would be controlled by a foreign entity. ID is controlled by our CEO who is the single stock holder. ID's product OEM, Credant is a wholly owned U.S. company.
84	X	X	Vendor must provide several technical support delivery options, to include phone, online, onsite, etc.	CRITICAL	<b>EXCEEDS REQUIREMENT.</b> ID is offering Credant's telephonic, on site, online, email, and facsimile technical support. All development and support personnel are located in the US. In addition, ID will be providing all onsite support of trained and cleared personnel to augment Credant's capabilities.
85	X	X	Provide one (1) administrator & one (1) user's guide in hard copy and in electronic formats (PDF) with unlimited reproduction privileges for internal purposes per order	CRITICAL	<b>Meets Requirement.</b> Credant will provide an administrator guide in both formats. Credant is transparent to the end user and therefore has no user guide.
86	X	X	For every patch or upgrade release, new product releases will be backward compatible and be capable of using or decrypting previously encrypted data	CRITICAL	<b>Meets Requirement.</b> Credant complies with this requirement. Customers who have not upgraded for more than one major release are required to upgrade multiple releases by going through a sequential patch upgrade chain of only the Major Patches. As long as the system administrators are installing patches in a timely manner, there will be no compatibility issues of decrypting previously encrypted data.
87	X	X	Provide troubleshooting guidance for product	CRITICAL	<b>Meets Requirement.</b> CREDANT retains a knowledge base of troubleshooting issues and has documented steps in place to walk a customer through identifying the problem and providing recommended remediation guidelines to resolve the issue. Credant has help desk professionals that are tiered in Level one, two and three help desk procedures. This includes the accessibility to Credant engineers and SMEs. Most commonly identified issues can be addressed and resolved through Credant's online support portal ( <a href="http://support.credant.com/">http://support.credant.com/</a> ). This portal includes FAQ, Knowledge Base, Downloads, Discussion Forums, Search Engine and other valuable tools to assist in resolving issues.
88	X	X	Product must provide user-friendly feedback messages when errors or warnings occur	IMPORTANT	<b>Meets Requirement.</b> CREDANT provides user-friendly messaging to alert the user of any errors or warnings and provides a description of the issue. Users can access the help function or go online to get further detail and/or clarification of the issue and alert their administrator.

DAR ENCRYPTION TECHNICAL & FUNCTIONAL REQUIREMENTS FOR DoD and other FEDERAL AGENCIES					
Requirement Number	Product Category		Technical & Functional Requirements	Category Rankings	Instructions to Offerors - Vendors please follow instructions and respond to each technical requirement with a response in the appropriate section below (you may delete the instructions and replace with proposed response), reference an attachment, or state 'No Response'. When referencing attachments, use the same Requirement Numbers in the same order as the Technical & Functional Requirements in this document, or provide a table of cross references.
	FDE	FES			
89	X	X	System installation documentation should include steps to verify proper operation upon completion of installation.	IMPORTANT	<b>EXCEEDS REQUIREMENT.</b> Credant documentation describes the process and validation of each step of the installation process. Credant self-verifies the installation through its audit capabilities, which is an automated check that occurs every time the user connects to the network.
90	X	X	Provide SIN (Special Item Number) 132-51 for professional services offered	DESIRABLE	<b>Meets Requirement.</b> ID offers 37 labor categories that fall under Special Item Number 132-51 from ID's GS-35F-4153D. For the primary labor category supporting the implementation of Credant, ID is offering labor category "Consultant Software Category I" as listed in our GSA FSS 70 Schedule. Complete details for these labor categories is provided in Attachment 1.

DAR ENCRYPTION TECHNICAL & FUNCTIONAL REQUIREMENTS FOR DoD and other FEDERAL AGENCIES					
Requirement Number	Product Category		Technical & Functional Requirements	Category Rankings	Instructions to Offerors - Vendors please follow instructions and respond to each technical requirement with a response in the appropriate section below (you may delete the instructions and replace with proposed response), reference an attachment, or state 'No Response'. When referencing attachments, use the same Requirement Numbers in the same order as the Technical & Functional Requirements in this document, or provide a table of cross references.
	FDE	FES			
<b>LICENSING &amp; COSTING</b>					
91	X	X	Licenses are transferable within each Federal Agency	CRITICAL	<u>Meets Requirement.</u> Federal Agencies that purchase Credant can move licenses from one installation to another. There are no technical limitations that prevent end-user licenses from moving from one credit server/userbase to another.
92	X	X	Provide license pricing that is user based and includes secondary-use rights.	CRITICAL	<u>Meets Requirement.</u> Licenses are priced on a per user basis. Users are permitted to have an unlimited number of devices, both at work and at home. This licensing is based on LDAP/AD users and as users are added or deleted secondary use rights apply.
93	X	X	Product licenses are perpetual	CRITICAL	<u>Meets Requirement.</u> Credant Licenses are sold as perpetual licenses with annual recurring maintenance based on the license price and the level of tech support required (24X7 vs. 8X5)
94	X	X	Price of product licenses	CRITICAL	<u>Meets Requirement.</u> Licenses are priced on a per device and a per user option. The prices in Attachment 1 include significant discounts and concessions from Intelligent Decisions' Authorized Federal Supply Schedule INFORMATION TECHNOLOGY SCHEDULE PRICELIST found at: <a href="http://www.intelligent.net/publicweb/federal/contract_search.cfm">http://www.intelligent.net/publicweb/federal/contract_search.cfm</a> Our GSA contracting officer is Tessa Dorsey ( <a href="mailto:tessa.dorsey@gsa.gov">tessa.dorsey@gsa.gov</a> ) 703-605-2791
95	X	X	Price of annual software maintenance	CRITICAL	<u>Meets Requirement.</u> The price of annual Software Updates/Upgrades/Support is provided for two levels: Gold and Standard. Gold includes 24X7 support and Standard provides typical business hours. See attached pricing for price breakdown.
96	X	X	Price of all tiered support options	IMPORTANT	<u>Meets Requirement.</u> See Attachment 1 to Exhibit B for the complete price structure.
97	X	X	Product training is available for system administrators as separate price	IMPORTANT	<u>Meets Requirement.</u> Product Training is available for Systems Administrators in the DC and Dallas areas. ID includes an option for having a certified Credant Trainer visit the Government Location and perform localized training for larger classes.
98	X	X	Provide license pricing that is device-based regardless of the number of users	IMPORTANT	<u>Meets Requirement.</u> See attached pricing on a per device basis. Users are permitted to license devices both at work and at home. This licensing is based on the number of devices that are connecting into the server for registration and ongoing audit/reporting.
99	X	X	When maintenance is included with the purchase of a license, support begins at the time of installation phase	IMPORTANT	Support for the Credant product line begins at the time of purchase, according to the GSA Terms and Conditions, unless a specific "turn-on time" is established at the point of award.
100	X	X	Licenses include home-use rights	DESIRABLE	<u>Meets Requirement.</u> Licenses include home-use rights, but are tied to specific hardware that are installed and registered through the managed network. All devices that connect into the managed network are capable of installing the full Credant product subject to user or device-based licensing agreement. Non-managed devices can leverage the power of Credant2Go in order to access and secure sensitive documents.
<b>TRAINING</b>					
101	X	X	Users should require minimal or no training to utilize the product	IMPORTANT	<u>EXCEEDS REQUIREMENT.</u> CREDANT is transparent to end users, no user training is required to secure data.
102	X	X	Onsite product training is available	IMPORTANT	<u>Meets Requirement.</u> ID has Credant trained engineers that are available for training at onsite locations. ID also offers a large training center at our Ashburn, Virginia facility to train onsite if desired by the customer. ID currently has regularly scheduled training class in the Washington D.C. Metro area and in Dallas, Texas.
103	X	X	Vendor shall provide virtual web-based training for the product	IMPORTANT	<u>Meets Requirement.</u> ID has taped training that is available via the web and can be accessed from any computer that has access to the Internet. Credant also has periodic Seminars that provide web-based instructor-led introductory classes on Credant capabilities, features, functions and admin interface.