

| 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 and 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.</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          | 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> .<br><br>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 API's 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 algorithms 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 to ensure that only the FIPS validated CCK is used within the software. |
| 2  |                  | X X | Product shall be NIAP certified  | IMPORTANT         | 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.   |
| 3  | X                | X   | Product shall be compliant with American Disabilities Act Section 508.   | IMPORTANT         | 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.   |
| 4  | X                | X   | Product shall be in the NIAP certification process   | DESIRABLE         | <see response to requirement #2>  |
| <b>ENCRYPTION</b>  |                  |     |  |                   |   |
| 5  |                  | X X | The product provides Full Disk Encryption (FDE), File/Folder Encryption System (FES), or Integrated FDE and FES.   | CRITICAL          | 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          | 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<br>USB: All Attached Storage, including Thumb Drives, iPod's, Camera's, external drives, etc.<br>PDA's: SmartPhones (see OS Compatability section for complete list)<br>CD/DVD: Nero and Roxio controls available Summer of 2007<br>Additionally, with minimal user interaction, Credant can secure documents for Tapes Storage, Email, FTP, CD/DVD, or shared drives.   |
| 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          | N/A. Credant is not a FDE product.  |

| DAR ENCRYPTION TECHNICAL & FUNCTIONAL REQUIREMENTS FOR DoD and other FEDERAL AGENCIES |                  |     |   |                   |  |
|---|------------------|-----|---|-------------------|--|
| Requirement Number  | Product Category |     | Technical & Functional Requirements   | Category Rankings | <i>Instructions to Offerors - Vendors please follow intructions 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 &amp; Functional Requirements in this document, or provide a table of cross references.</i>  |
|   | FDE              | FES |   |                   |  |
| 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          | <i>For all 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 definies password strength) for easier interoperability with exchanging Files to non-Credant Enabled and non-Managed External Systems as outlined requirement #13.</i>  |
| 9   | X                | X   | The product's process for encryption and decryption of data is configurable to be transparent to user   | IMPORTANT         | <i>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.</i> |

| 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         | 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         | 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         | 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         | 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         | 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         | 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         | <see response to technical requirement #14>  |
| 17  |                  | X   | Product is capable of file compression and encryption in a single step by the user  | DESIRABLE         | Credant does not increase or decrease file size significantly. In some cases, Credant may increase file size by up to 32 Bytes, but this is an extremely small rounding. Credant does not compress files, but is capable of encrypting compressed files.   |
| <b>AUTHENTICATION</b>   |                  |     |   |                   |  |
| 18  | X                |     | Product provides boot authentication  | CRITICAL          | N/A. Credant is not a full disk solution.  |
| 19  | X                |     | Product must support use of DoD CAC or PIV II compliant Smartcard for boot authentication with no modification of card required   | CRITICAL          | N/A. Credant is not a full disk solution.  |
| 20  | X                |     | Product must support use of DoD CAC or PIV II compliant Smartcard on a Government approved token for boot authentication  | CRITICAL          | N/A. Credant is not a full disk solution.  |
| 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          | N/A. Credant is not a full disk solution.  |
| 22  | X                |     | Product supports password based pre-boot authentication   | IMPORTANT         | N/A. Credant is not a full disk solution.  |
| <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          | N/A. Credant is not a full disk solution.  |

| 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 intructions 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          | N/A. Credant is not a full disk solution.   |
| 25  | X                |     | Product shall have the capability to allow administrators to provide remote assistance to users who are locked out   | CRITICAL          | N/A. Credant is not a full disk solution.   |
| 26  | 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          | N/A. Credant is not a full disk solution.   |
| 27  | X                | X   | Product shall prohibit vendor's ability to access, modify, or decrypt data   | CRITICAL          | The 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          | 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          | <see response to Technical Requirement #28>   |
| 30  | X                | X   | Product does not interfere with full disk data erasure tools   | CRITICAL          | <see response to Technical Requirement #28>   |
| 31  | X                | X   | The product is capable of secure escrow and recovery of the symmetric encryption key   | CRITICAL          | 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 can never 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          | 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          | N/A. Credant is not a full disk solution.   |
| 34  | X                | X   | The product's encryption/decryption process must occur without loss or corruption of data or content modification  | CRITICAL          | 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   | Product will be capable of encrypting swap, free, slack, temp, and Internet temp files   | CRITICAL          | 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          | N/A. Credant is not a full disk solution.   |
| 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         | N/A. Credant is not a full disk solution.   |

| 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 |  |                   |   |
| 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         | N/A. Credant is not a full disk solution.   |
| 39  | X                |     | Product has the ability to allow administrators to maintain administrator password for pre-boot authentication for each system   | IMPORTANT         | N/A. Credant is not a full disk solution.   |
| 40  | X                | X   | Product does not change the content of the GINA.dll file   | IMPORTANT         | CREDANT does not modify or replace the GINA.dll file or affect the login process in any way.  |
| 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         | Host based security 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         | As a software-based solution, Credant is 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         | 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         | 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         | 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         | N/A. Credant is not a full disk solution.   |
| 47  | X                |     | Product allows authorized user to validate disk encryption has occurred and is maintained  | IMPORTANT         | N/A. Credant is not a full disk solution.   |
| 48  | X                |     | Product can support pre-boot integrity   | IMPORTANT         | N/A. Credant is not a full disk solution.   |
| 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         | 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         | <see response to Technical Requirement #41>. 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         | TPM functionality is on the roadmap with an estimated completion of Q4 2007. Credant will offer deep level interaction with Vista BitLocker - providing central management, control and BitLocker key management to the process. Credant will support TPM by leveraging BitLocker's support of TPM.   |
| 52  | X                | X   | Product must be compatible with standard applications, protocols, and communications within the Federal Government   | DESIRABLE         | Since Credant does not encrypt the application or system files there is 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.   |

| 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 intructions 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 |   |                   |  |
| 53  | X                |     | Product supports boot into multiple operating systems on a single device  | DESIRABLE         | N/A. Credant is not a full disk solution.  |
| 54  | X                | X   | Provides open APIs or an SDK to support application integration   | DESIRABLE         | SDKs are available   |
| 55  | X                |     | The product supports Single Sign-On (simultaneous pre-boot and O/S logon)   | DESIRABLE         | N/A. Credant is not a full disk solution.  |
| CENTRALIZED MANAGEMENT CONSOLE  |                  |     |   |                   |  |
| 56  | X                |     | The product's administrator management console allows for failover functionality (fault tolerance/redundancy)   | CRITICAL          | N/A. Credant is not a full disk solution.  |
| 57  | X                |     | The product's administrator management console supports capability to add/modify/delete admin users   | CRITICAL          | N/A. Credant is not a full disk solution.  |
| 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          | 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.   |
| 59  | X                |     | The product's administrator management console supports retrieval of computer, user, and user-group information from Active Directory   | CRITICAL          | N/A. Credant is not a full disk solution.  |
| 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          | N/A. Credant is not a full disk solution.  |
| 61  | X                |     | Product will support or integrate with existing asset/license tracking and management tools   | IMPORTANT         | N/A. Credant is not a full disk solution.  |
| 62  | X                |     | Product shall support secure remote management of devices to support remote users   | IMPORTANT         | N/A. Credant is not a full disk solution.  |
| 63  | X                |     | Product shall support secure remote access to the administrator management console for administrators   | IMPORTANT         | N/A. Credant is not a full disk solution.  |
| 64  | X                |     | The product's administrator management console must be scalable to support large enterprise environments  | IMPORTANT         | N/A. Credant is not a full disk solution.  |
| 65  | X                |     | The product's administrator management console permits multiple administrator logins for simultaneous access  | IMPORTANT         | N/A. Credant is not a full disk solution.  |
| 66  | X                |     | The product's administrator management console supports retrieval of computer, user, and user-group information from LDAP Servers   | IMPORTANT         | N/A. Credant is not a full disk solution.  |
| 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         | <see response to Technical Requirement #28>  |

| DAR ENCRYPTION TECHNICAL & FUNCTIONAL REQUIREMENTS FOR DoD and other FEDERAL AGENCIES |                  |     |  |                   |  |
|---|------------------|-----|--|-------------------|--|
| Requirement Number  | Product Category |     | Technical & Functional Requirements  | Category Rankings | <i>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 &amp; Functional Requirements in this document, or provide a table of cross references.</i> |
|   | FDE              | FES |  |                   |  |
| 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         | <i>N/A. Credant is not a full disk solution.</i>   |

| 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 |   |                   |   |
| 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. |                  |     |   |                   |   |
| 69  | X                | X   | Microsoft Windows 2000  |                   | Yes. SP3, SP4.  |
| 70  | X                | X   | Microsoft Windows 2003  |                   | No.   |
| 71  | X                | X   | Microsoft Windows XP  |                   | Yes. SP1, SP2 and XP Tablet PC Edition SP2  |
| 72  | X                | X   | Microsoft Windows Vista   |                   | Credant Vista support will be available on Version 5.4 which is scheduled for Late September 2007.  |
| 73  | X                | X   | UNIX / Sun Solaris  |                   | No.   |
| 74  | X                | X   | Mac OS X  |                   | This is on the roadmap, but not supported today.  |
| 75  | X                | X   | Windows Mobile 5.0  |                   | Yes. Windows Mobile 5 and Windows Mobile 5 Smartphone.  |
| 76  | X                | X   | Windows CE  |                   | Yes. Credant supports Windows Mobile 2002/2003 for PPC and Smartphone.  |
| 77  | X                | X   | RIM/Blackberry  |                   | Yes. Blackberry Java OS 4.0 and 4.1   |
| 78  | X                | X   | Palm  |                   | Yes. Palm 5.x.  |
| 79  | X                | X   | Symbian   |                   | Yes. Symbian OS 7.0s, Nokia Series 80.  |
| 80  | X                | X   | Linux to include Red Hat, SuSE  |                   | No.   |
| GENERAL AND TECHNICAL SUPPORT   |                  |     |   |                   |   |
| 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          | CREDANT notifies customers of new releases and patches and provides a web link for the client to download them.   |
| 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          | Customers receive a written description of each upgrade enhancement and feature.  |
| 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          | We will comply.   |
| 84  | X                | X   | Vendor must provide several technical support delivery options, to include phone, online, onsite, etc.  | CRITICAL          | Credant supplies phone, on site and online technical support. All development and support personnel are located in the US.  |
| 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          | 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          | Credant complies with this requirement one major release back from each release. Customers who have not upgraded for more than one major release are required to upgrade multiple releases by going through the major patch upgrade chain.  |
| 87  | X                | X   | Provide troubleshooting guidance for product  | CRITICAL          | CREDANT provides troubleshooting guidance as a standard help desk procedure   |
| 88  | X                | X   | Product must provide user-friendly feedback messages when errors or warnings occur  | IMPORTANT         | CREDANT provides user-friendly error messages or uses standard Windows error messages   |
| 89  | X                | X   | System installation documentation should include steps to verify proper operation upon completion of installation.  | IMPORTANT         | Credant documentation verifies that installation is done properly. Credant self-verifies through its audit capabilities   |
| 90  | X                | X   | Provide SIN (Special Item Number) 132-51 for professional services offered  | DESIRABLE         | Working on getting this from ID GSA Schedule...   |

| 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          | According to the Credant End User License Agreement Organizations 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 credant server/userbase to another.  |
| 92  | X                | X   | Provide license pricing that is user based and includes secondary-use rights.                                 | CRITICAL          | 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.  |
| 93  | X                | X   | Product licenses are perpetual  | CRITICAL          | 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          | Licenses are priced on a per device and a per user option.  |
| 95  | X                | X   | Price of annual software maintenance  | CRITICAL          | 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         | See attached price list   |
| 97  | X                | X   | Product training is available for system administrators as separate price                                     | IMPORTANT         | Product Training is available for Systems Administrators in the DC and Dallas areas. For larger classes there are also options for having a certified Credant Trainer visit the Government Location and perform localized training.   |
| 98  | X                | X   | Provide license pricing that is device-based regardless of the number of users                                | IMPORTANT         | 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         | 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         | CREDANT is transparent to end users, no user training is required to secure data.   |
| 102   | X                | X   | Onsite product training is available  | IMPORTANT         | Onsite training is available.   |
| 103   | X                | X   | Vendor shall provide virtual web-based training for the product   | IMPORTANT         | Credant has periodic Seminars that provide web-based instructor-led introductory classes on Credant capabilities, features, functions and admin interface.  |