IBM System Storage

Notice Regarding Storage Encryption

GA32-0642-01

IBM System Storage

Notice Regarding Storage Encryption

GA32-0642-01

IBM Notice Regarding Storage Encryption

Thank you for acquiring an IBM storage device that includes encryption technology. It is important that you read this document which contains important information regarding the use of such a device. By making use of an Encryption Machine, you acknowledge, on behalf of your enterprise, that you have read this notice, understand the risks of using an Encryption Machine described herein, and accept the IBM disclaimers as set forth below.

1. Introduction

Encryption technology plays a vital role in protecting sensitive data. Encryption can protect information from unauthorized access, even from individuals who otherwise have access to your information technology systems. Encryption can also protect information while it is in transit from one system to another, or when stored on removable or transportable media.

Proper protection and management of encryption keys is a critical element of implementing encryption in your information technology environment. Failure to properly protect and manage your encryption keys can result in the inability to retrieve associated encrypted data. For additional information on implementing encryption in environments using IBM and/or non-IBM environments, please read IBM's white paper which can be accessed through the following link:

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101479

2. Definitions

Encryption Machine -- a data storage Machine configured with the capability to perform encryption of data. Such encryption may be provided through a feature or as a standard capability of the Machine.

Encryption Deadlock –all key servers within a computing environment are rendered inoperable because key server data is stored on an Encryption Machine that is dependent on the key server to access the data (i.e., the encryption keys themselves have been included within the data that was encrypted using those keys).

3. Encryption Considerations

You may elect to implement and configure your key server environment at the time of initial installation, or to reconfigure such environment following initial installation. The proper use of encryption technology is critical to the maintenance, security and accessibility of encrypted data.

You are hereby advised that the risks inherent in encryption technology include the following:

a. failure to properly implement, configure or maintain the encrypted storage environment or any encryption keys, encryption key management applications (for instance Tivoli Key Lifecycle Manager Program), or boot records for an attached server, may lead to the loss of encryption keys resulting in the irretrievability of the data encrypted using those keys;

b. improper implementation, configuration, or maintenance can cause an Encryption Deadlock, which may result in the irretrievability of all key-server-managed encrypted data at all installations in the computing environment; and

c. with the introduction of Machine-based encryption and other encryption technologies at different levels of the storage environment, the likelihood of an Encryption Deadlock can increase significantly.

4. IBM Encryption Support Services

IBM offers and recommends IBM Encryption Support Services to assist you with the implementation of your storage encryption configuration. Upon your request, IBM will provide you with information regarding such service offering.

5. IBM Disclaimer

The limitation of liability terms in effect between you and IBM are supplemented by the following additional disclaimers of IBM's potential liability regarding storage encryption:

a. You are solely responsible for selecting and properly implementing the configuration of your key server environment. IBM is not liable for any damages resulting from improper implementation of an encryption environment or any modification to such an environment if the implementation or modification was not made by IBM; and

b. If you configure or reconfigure your key server environment following IBM Encryption Support Services, you are solely responsible for any damages resulting from improper implementation, configuration or reconfiguration.

IBM oznámení o šifrování úložišť

Děkujeme Vám, že jste si zakoupili úložné zařízení IBM, které zahrnuje šifrovací technologii. Je velmi důležité, abyste si přečetli tento dokument, který obsahuje důležité informace vztahující se na užívání takového zařízení. Užíváním Šifrovacího stroje potvrzujete jménem Vašeho podniku, že jste si toto oznámení přečetli, že chápete rizika vyplývající z užívání Šifrovacího stroje, který je v tomto dokumentu popsán a že akceptujete právní doložky IBM, jak jsou uvedeny níže.

1. Úvod

Šifrovací technologie hraje v ochraně citlivých dat významnou roli. Šifrování může chránit informace před neoprávněným přístupem, a to i před přístupem jednotlivců, kteří jinak mají přístup k Vašim IT systémům. Šifrování může ochránit informace rovněž v případě jejich přenosu z jednoho systému na jiný nebo při jejich ukládání na vyjímatelná nebo přenosná média.

Řádná ochrana a správa šifrovacích klíčů je základním prvkem implementace šifrování ve Vašem prostředí informačních technologií. Nedostatečná ochrana a chybná správa šifrovacích klíčů může vést k nemožnosti načíst související šifrovaná data. Další informace o implementaci šifrování v prostředích od IBM a/nebo jiných dodavatelů najdete v dokumentu IBM White Paper, který je dostupný prostřednictvím následujícího odkazu:

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101479

2. Definice

Šifrovací stroj -- Stroj používaný jako úložiště dat, který disponuje funkcí šifrování dat. Takové šifrování může být prováděno prostřednictvím nějaké vlastnosti nebo jako standardní schopnost stroje.

Uváznutí procesu šifrování (Encryption Deadlock) – všechny klíčové servery v rámci výpočetního prostředí jsou ve stavu neprovozuschopnosti, jelikož data klíčového serveru jsou uložena na Šifrovacím stroji, který je závislý na schopnosti klíčového serveru přistupovat k datům (tj. šifrovací klíče samy o sobě jsou zahrnuty do dat šifrovaných pomocí takových klíčů).

3. Pokyny týkající se šifrování

Můžete se rozhodnout, že budete prostředí Vašeho klíčového serveru implementovat a konfigurovat v okamžiku počáteční instalace nebo že po provedení počáteční instalace toto prostředí překonfigurujete. Základním a nezbytným předpokladem pro údržbu, zabezpečení a přístupnost šifrovaných dat je správné použití šifrovací technologie.

Je třeba vzít na vědomí, že rizika spojená s šifrovací technologií zahrnují:

a. neschopnost řádně implementovat, konfigurovat nebo udržovat prostředí šifrovaného úložiště nebo šifrovací klíče, aplikace pro správu šifrovacích klíčů (například program Tivoli Key Lifecycle Manager) nebo zavádět záznamy pro připojený server, což může vést ke ztrátě šifrovacích klíčů a následné neschopnosti načíst data šifrovaná pomocí takových klíčů;

b. nesprávná implementace, konfigurace nebo údržba může způsobit uváznutí procesu šifrování, což může vést k neschopnosti načíst veškerá šifrovaná data typu "key-server-managed" na všech instalacích ve výpočetním prostředí; a

c. se zavedením šifrování na bázi stroje a jiných šifrovacích technologií na různých úrovních prostředí úložišť může pravděpodobnost uváznutí procesu šifrování výrazně stoupnout.

4. Služby IBM Encryption Support Services

IBM nabízí a doporučuje služby IBM Encryption Support Services, jež Vám pomohou s implementací Vaší konfigurace šifrování úložišť. Na Vaši žádost Vám IBM poskytne informace týkající se nabídky těchto služeb.

5. Vyloučení záruky

Podmínky týkající se omezení odpovědnosti, jež platí pro smluvní vztah mezi Vámi a IBM, jsou doplněny o následující dodatečná vyloučení případné odpovědnosti IBM ve vztahu k šifrování úložišť:

a. Nesete výhradní odpovědnost za výběr a řádnou implementaci konfigurace prostředí Vašeho klíčového serveru. IBM nenese odpovědnost za žádné škody, jež jsou důsledkem nesprávné implementace šifrovacího prostředí nebo nějaké modifikace takového prostředí, jestliže takovou implementaci nebo modifikaci nebyla učiněna IBM; a

b. jestliže po službách IBM Encryption Support Services následně nakonfigurujete nebo překonfigurujete prostředí Vašeho klíčového serveru, ponesete výhradní odpovědnost za jakékoli škody, jež budou důsledkem nesprávné implementace, konfigurace nebo překonfigurace.

Notice IBM concernant le chiffrement du stockage

Nous vous remercions d'avoir choisi une unité de stockage IBM qui inclut une technologie de chiffrement. Il est important que vous lisiez ce document qui contient des informations essentielles sur l'utilisation d'une telle unité. En utilisant une machine de chiffrement, vous reconnaissez, au nom de votre entreprise, que vous avez bien lu cette notice, compris les risques, décrits dans ce document, liés à l'utilisation d'une machine de chiffrement et que vous acceptez l'exclusion de la responsabilité d'IBM décrite ci-dessous.

1. Introduction

La technologie de chiffrement joue un rôle essentiel dans la protection des données sensibles. Le chiffrement permet de protéger vos informations d'un accès non autorisé, et ce, même de la part des personnes qui bénéficient d'un droit d'accès à vos systèmes informatiques. Le chiffrement permet également de protéger des informations transférées d'un système à un autre ou des informations sauvegardées sur un support amovible ou pouvant être transporté.

Une gestion et une protection convenables des clés de chiffrement sont essentielles à l'implémentation du chiffrement dans votre environnement informatique. Si la protection ou la gestion de vos clés de chiffrement est incorrecte, il est parfois impossible de récupérer les données chiffrées correspondantes. Pour plus d'informations sur l'implémentation d'un chiffrement dans des environnements utilisant ou non des environnements IBM, veuillez consulter le livre blanc d'IBM, accessible grâce au lien suivant :

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101479

2. Définitions

Machine de chiffrement : machine de stockage de données configurée afin de pouvoir chiffrer ces données. Un tel chiffrement peut être fourni en tant qu'option ou en tant que fonction standard de la machine.

Blocage du chiffrement –tous les serveurs de clés d'un environnement informatique sont inexploitables car les données de ces serveurs sont stockées sur une machine de chiffrement qui dépend d'un serveur de clés pour accéder aux données (en d'autres termes les clés de chiffrement ont été incluses dans les données chiffrées à l'aide de ces clés).

3. Remarques relatives au chiffrement

Vous pouvez choisir d'implémenter et de configurer votre environnement de serveurs de clés au moment de l'installation initiale ou bien de le reconfigurer après l'installation initiale. Une bonne utilisation de la technologie de chiffrement est indispensable à la maintenance, à la sécurité et à l'accessibilité des données chiffrées.

Ce document vous informe que les risques liés à la technologie de chiffrement incluent les suivants :

a. Une implémentation, une configuration ou une gestion incorrecte de l'environnement de stockage chiffré ou des clés de chiffrement, des applications de gestion des clés de chiffrement (par exemple le programme Tivoli Key Lifecycle Manager), ou des enregistrements de démarrage pour un serveur joint, peuvent provoquer la perte des clés de chiffrement ; les données chiffrées à l'aide de ces clés sont alors irrécupérables ;

b. Une implémentation, une configuration ou une gestion incorrecte peut générer un blocage du Chiffrement, qui peut donner lieu à la perte irrémédiable de toutes vos données chiffrées, gérées par un serveur de clés, et stockées sur les installations de l'environnement informatique ; par ailleurs,

c. Avec l'introduction du chiffrement par machine et d'autres technologies de chiffrement à différents niveaux de l'environnement de stockage, le risque de blocage du chiffrement peut fortement augmenter.

4. Services IBM d'assistance au chiffrement (IBM Encryption Support Services)

IBM vous propose et vous recommande d'avoir recours aux services IBM d'assistance au chiffrement destinés à vous aider pour l'implémentation de la configuration du chiffrement du stockage. IBM vous fournit, sur simple demande, des informations concernant cette offre de services.

5. Exclusion de responsabilité d'IBM

Les dispositions de la limitation de responsabilité en vigueur entre vous et IBM sont complétées par les clauses supplémentaires suivantes relatives à la responsabilité potentielle d'IBM dans le chiffrement du stockage :

a. Vous êtes seul responsable du choix et de la bonne implémentation de la configuration de votre environnement de serveurs de clés. IBM décline toute responsabilité pour tout dommage dû à une implémentation inadaptée d'un environnement de chiffrement ou pour toute modification apportée à cet environnement si l'implémentation ou la modification n'a pas été effectuée par IBM ; d'autre part,

b. Si vous configurez ou reconfigurez votre environnement de serveurs de clés après l'intervention des Services IBM d'assistance au chiffrement, vous serez seul responsable des dommages dus à une implémentation, à une configuration ou à une reconfiguration inadaptée.

IBM Hinweis zur Speicherverschlüsselung

Vielen Dank, dass Sie sich für eine IBM Speichereinheit entschieden haben, die mit Verschlüsselungstechnologie arbeitet. Bitte lesen Sie dieses Dokument aufmerksam durch. Es enthält wichtige Informationen zur Nutzung der Speichereinheit. Durch die Nutzung eines Verschlüsselungssystems bestätigen Sie im Namen Ihres Unternehmens, dass Sie diesen Hinweis gelesen haben, die darin beschriebenen Risiken der Verwendung eines Verschlüsselungssystems kennen und den nachstehend genannten IBM Haftungsausschlüssen zustimmen.

1. Einführung

Für den Schutz sensibler Daten sind Verschlüsselungstechnologien unverzichtbar. Durch Verschlüsselung können Informationen vor unbefugtem Zugriff geschützt werden, sogar vor dem Zugriff von Einzelpersonen, die ansonsten auf Ihre IT-Systeme zugreifen können. Darüber hinaus werden durch Verschlüsselung Informationen bei der Übertragung von einem System auf ein anderes System oder bei der Speicherung auf wechselbaren oder transportablen Datenträgern geschützt.

Ein wichtiger Bestandteil der Verschlüsselung in Ihrer IT-Umgebung ist der richtige Schutz und die richtige Verwaltung von Verschlüsselungsschlüsseln. Wenn Verschlüsselungsschlüssel nicht ordnungsgemäß geschützt und verwaltet werden, kann dies dazu führen, dass die zugehörigen verschlüsselten Daten nicht abgerufen werden können. Weitere Informationen über die Implementierung von Verschlüsselungstechnologien in Umgebungen mit Systemen von IBM und/oder anderen Herstellern erhalten Sie im thematisch zugehörigen White Paper von IBM, das unter folgendem Link verfügbar ist:

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101479

2. Begriffsbestimmungen

Verschlüsselungssystem – Ein System für die Datenspeicherung, das mit Funktionalität für die Datenverschlüsselung konfiguriert ist. Diese Verschlüsselung kann im Rahmen eines Features oder einer Standardfunktion des Systems bereitgestellt werden.

Verschlüsselungsdeadlock – Alle Key-Server in einer IT-Umgebung sind nicht funktionsfähig, da Key-Serverdaten auf einem Verschlüsselungssystem gespeichert sind, das für den Datenzugriff den Key-Server benötigt (d. h., die Verschlüsselungsschlüssel sind in den Daten enthalten, die mit diesen Schlüsseln verschlüsselt wurden).

3. Überlegungen hinsichtlich Verschlüsselung

Sie können Ihre Key-Serverumgebung entweder zum Zeitpunkt der Erstinstallation implementieren und konfigurieren oder diese Umgebung nach der Erstinstallation rekonfigurieren. Für die Verwaltung und die Sicherheit verschlüsselter Daten und den Zugriff darauf ist die ordnungsgemäße Nutzung der Verschlüsselungstechnologie entscheidend.

Die Verschlüsselungstechnologie bringt unter anderem folgende Risiken mit sich:

a. Eine nicht ordnungsgemäße Implementierung, Konfiguration oder Verwaltung der verschlüsselten Speicherumgebung oder von Verschlüsselungsschlüsseln, von Anwendungen für das Management von Verschlüsselungsschlüsseln (z. B. Tivoli Key Lifecycle Manager Program) oder von Bootsätzen für verbundene Server kann zum Verlust von Verschlüsselungsschlüsseln und damit dazu führen, dass die mit diesen Schlüsseln verschlüsselten Daten nicht mehr abgerufen werden können.;

b. Eine nicht ordnungsgemäße Implementierung, Konfiguration oder Verwaltung kann zu einem Verschlüsselungsdeadlock und damit dazu führen, dass alle vom Key-Server verwalteten verschlüsselten Daten an allen Installationen in der IT-Umgebung nicht mehr abgerufen werden können.

c. Durch die Einführung einer systembasierten Verschlüsselung und anderer Verschlüsselungstechnologien auf verschiedenen Ebenen der Speicherumgebung kann die Wahrscheinlichkeit eines Verschlüsselungsdeadlocks erheblich zunehmen.

4. IBM Encryption Support Services

IBM bietet und empfiehlt IBM Encryption Support Services, um Sie bei der Implementierung Ihrer Konfiguration für die Speicherverschlüsselung zu unterstützen. Auf Anforderung stellt Ihnen IBM gerne weitere Informationen über ein solches Serviceangebot zur Verfügung.

5. IBM Haftungsausschluss

Die Haftungsbedingungen zwischen Ihnen und IBM werden durch die folgenden zusätzlichen Ausschlüsse im Zusammenhang mit der möglichen Haftung von IBM hinsichtlich Speicherverschlüsselung ergänzt:

a. Der Kunde ist für die Auswahl und ordnungsgemäße Implementierung der Konfiguration seiner Key-Serverumgebung allein verantwortlich. IBM übernimmt keine Haftung für Schäden, die aus der nicht ordnungsgemäßen Implementierung einer Verschlüsselungsumgebung oder einer Änderung einer solchen Umgebung resultieren, wenn die Implementierung oder Änderung nicht von IBM vorgenommen wurde.

b. Wenn der Kunde seine Key-Serverumgebung mit Unterstützung von IBM Encryption Support Services konfiguriert oder rekonfiguriert, ist er für Schäden, die aus der nicht ordnungsgemäßen Implementierung, Konfiguration oder Rekonfiguration resultieren, allein verantwortlich.

Ειδοποίηση της IBM σχετικά με την Κρυπτογράφηση Αποθηκευμένων Δεδομένων

Σας ευχαριστούμε για την αγορά της συσκευής αποθήκευσης IBM που περιλαμβάνει τεχνολογία κρυπτογράφησης. Είναι ιδιαίτερα σημαντικό να διαβάσετε το παρόν έγγραφο, το οποίο περιλαμβάνει σημαντικές πληροφορίες αναφορικά με τη χρήση τέτοιων συσκευών. Κάνοντας χρήση μιας Μηχανής Κρυπτογράφησης, βεβαιώνετε, εκ μέρους της επιχείρησής σας, ότι διαβάσατε την παρούσα ειδοποποίηση, κατανοείτε τους κινδύνους που ενέχει η χρήση μιας Μηχανής Κρυπτογράφησης όπως περιγράφονται στην παρούσα, και αποδέχεστε τις δηλώσεις αποποίησης της IBM που παρατίθενται παρακάτω.

1. Εισαγωγή

Η τεχνολογία κρυπτογράφησης παίζει έναν κρίσιμο ρόλο στην προστασία ευαίσθητων δεδομένων. Με την κρυπτογράφησή πληροφοριών μπορείτε να προστατέψετε τις εν λόγω πληροφορίες από μη εξουσιοδοτημένη πρόσβαση, ακόμα και από άτομα που έχουν κανονική πρόσβαση στα πληροφοριακά σας συστήματα. Μπορείτε επίσης, μέσω της κρυπτογράφησης πληροφοριών, να προστατέψετε τις εν λόγω πληροφορίες κατά τη μεταβίβασή τους από το ένα σύστημα στο άλλο, ή όταν αποθηκεύονται σε αφαιρέσιμα ή κινητά μέσα αποθήκευσης.

Η σωστή προστασία και διαχείριση κλειδιών κρυπτογράφησης αποτελεί κρίσιμο παράγοντα στην υλοποίηση τεχνολογιών κρυπτογράφησης στο περιβάλλον πληροφορικής της επιχείρησής σας. Η ανεπαρκής προστασία και διαχείριση κλειδιών κρυπτογράφησης μπορεί να έχει ως αποτέλεσμα να μην είστε πλέον σε θέση να ανακτήσετε τα αντίστοιχα κρυπτογραφημένα δεδομένα. Για περισσότερες πληροφορίες σχετικά με την υλοποίηση τεχνολογιών κρυπτογράφησης σε περιβάλλοντα IBM ή/και μη IBM, σας παρακαλούμε να διαβάσετε το σχετικό έγγραφο "white paper" της IBM, στο οποίο μπορείτε να έχετε πρόσβαση μέσω της ακόλουθης διασύνδεσης:

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101479

2. Ορισμοί

Μηχανή Κρυπτογράφησης (Encryption Machine) – μια Μηχανή αποθήκευσης δεδομένων στην οποία έχει υλοποιηθεί η δυνατότητα κρυπτογράφησης δεδομένων. Η εν λόγω κρυπτογράφηση μπορεί να παρέχεται μέσω κάποιου πρόσθετου εξοπλισμού ή/και λογισμικού ή να περιλαμβάνεται στις δυνατότητες που παρέχει η Μηχανή.

Κρυπτογραφικό Αδιέξοδο (Encryption Deadlock)– όλοι οι εξυπηρετητές κλειδιών (key servers) ενός περιβάλλοντος πληροφορικής έχουν τεθεί εκτός λειτουργίας επειδή τα δεδομένα των εξυπηρετητών κλειδιών έχουν αποθηκευτεί σε μια Μηχανή Κρυπτογράφησης που βασίζεται στους ίδιους τους εξυπηρετητές κλειδιών για την πρόσβαση στα δεδομένα (με άλλα λόγια, τα ίδια τα κλειδιά κρυπτογράφησης περιλαμβάνονται στα δεδομένα που κρυπτογραφήθηκαν με χρήση των εν λόγω κλειδιών).

3. Ζητήματα σχετικά με την Κρυπτογράφηση

Μπορείτε να επιλέξετε την υλοποίηση και διαμόρφωση του περιβάλλοντος του (των) εξυπηρετητή(-ών) κλειδιών σας κατά την αρχική εγκατάσταση, ή μπορείτε να διαμορφώσετε το εν λόγω περιβάλλον μετά την αρχική εγκατάσταση. Η σωστή χρήση της τεχνολογίας κρυπτογράφησης είναι κρίσιμης σημασίας για τη συντήρηση, την ασφάλεια και την προσβασιμότητα των κρυπτογραφημένων δεδομένων.

Για το λόγο αυτό επισημαίνεται ότι οι κίνδυνοι που ενέχονται στην τεχνολογία κρυπτογράφησης είναι οι εξής:

α. Η μη κατάλληλη υλοποίηση, διαμόρφωση ή συντήρηση του περιβάλλοντος κρυπτογράφησης αποθηκευμένων δεδομένων, των κλειδιών κρυπτογράφησης, των εφαρμογών διαχείρισης κλειδιών κρυπτογράφησης (για παράδειγμα, το Πρόγραμμα Tivoli Key Lifecycle Manager Program) ή των εγγραφών εκκίνησης (boot records) ενός συνδεδεμένου εξυπηρετητή, μπορεί να οδηγήσει στην απώλεια κλειδιών κρυπτογράφησης, με αποτέλεσμα να μην είναι πλέον δυνατή η ανάκτηση των δεδομένων που κρυπτογραφήθηκαν με τα εν λόγω κλειδιά.

β. Η μη κατάλληλη υλοποίηση, διαμόρφωση ή συντήρηση μπορεί να προκαλέσει ένα Κρυπτογραφικό Αδιέξοδο, το οποίο ενδέχεται να καθιστά αδύνατη την ανάκτηση οποιωνδήποτε κρυπτογραφημένων δεδομένων που ελέγχονται από τον εξυπηρετητή κλειδιών σε οποιαδήποτε από τις εγκαταστάσεις του περιβάλλοντος πληροφορικής σας, και

γ. Με την εισαγωγή της κρυπτογράφησης μέσω Μηχανής (Machine-based encryption) ή οποιωνδήποτε άλλων τεχνολογιών κρυπτογράφησης σε διαφορετικά επίπεδα του περιβάλλοντος αποθήκευσης δεδομένων, η πιθανότητα να προκύψει κάποιο Κρυπτογραφικό Αδιέξοδο αυξάνεται σημαντικά.

4. Υπηρεσίες Υποστήριξης Κρυπτογράφησης της IBM (IBM Encryption Support Services)

Η IBM σας προσφέρει και σας προτείνει τις Υπηρεσίες Υποστήριξης Κρυπτογράφησης που παρέχει ώστε να σας βοηθήσει στην υλοποίηση του δικού σας περιβάλλοντος κρυπτογράφησης δεδομένων. Κατόπιν αιτήματός σας, η IBM θα σας παράσχει περισσότερες πληροφορίες σχετικά με τις εν λόγω υπηρεσίες.

5. Δηλώσεις Αποποίησης της IBM

Οι όροι περί περιορισμού ευθύνης που βρίσκονται σε ισχύ ανάμεσα σε εσάς και την IBM συμπληρώνονται από τις ακόλουθες πρόσθετες δηλώσεις αποποίησης αναφορικά με τη δυνητική ευθύνη της IBM σε ό,τι αφορά την κρυπτογράφηση αποθηκευμένων δεδομένων:

α. Εσείς είστε αποκλειστικά υπεύθυνοι για την επιλογή και την κατάλληλη υλοποίηση της διαμόρφωσης του περιβάλλοντος του (των) εξυπηρετητή(-ών) κλειδιών σας. Η IBM δεν φέρει ευθύνη για οποιεσδήποτε ζημίες προκύψουν από τη μη κατάλληλη υλοποίηση του περιβάλλοντος κρυπτογράφησης ή την τροποποίηση ενός τέτοιου περιβάλλοντος εάν η εν λόγω υλοποίηση ή τροποποίηση δεν πραγματοποιήθηκε από την IBM, και

β. Εάν προβείτε στη διαμόρφωση ή εκ νέου διαμόρφωση του περιβάλλοντος του (των) εξυπηρετητή(-ών) κλειδιών σας μετά την παροχή Υπηρεσιών Υποστήριξης Κρυπτογράφησης από την IBM, θα είστε αποκλειστικά υπεύθυνοι για οποιεσδήποτε ζημίες προκύψουν από τη μη κατάλληλη υλοποίηση, διαμόρφωση ή εκ νέου διαμόρφωση.

IBM Avviso relativo alla Crittografia della Memoria

Grazie per aver acquisito un dispositivo di memoria IBM che include tecnologia di crittografia. E' importante leggere questo documento che contiene informazioni di rilievo relative all'utilizzo di tale dispositivo. Utilizzando una Macchina di Crittografia, si riconosce, per conto del proprio gruppo aziendale, di aver letto questo avviso, compreso i rischi derivanti dall'utilizzo di una Macchina di Crittografia qui descritta, e si accettano le rinunce IBM come stabilito di seguito.

1. Introduzione

La tecnologia di crittografia ha un ruolo vitale nel proteggere i dati sensibili. La crittografia può proteggere le informazioni da accessi non autorizzati, anche da individui che in altro modo hanno accesso ai sistemi di tecnologia informativa. Inoltre, la crittografia può proteggere le informazioni mentre transitano da un sistema all'altro, o quando memorizzate su supporti rimovibili o trasportabili.

Una protezione e gestione appropriata delle chiavi di crittografia è un elemento cruciale dell'implementazione della crittografia nel proprio ambiente di tecnologia informativa. La mancata protezione e gestione delle chiavi di crittografia può portare all'incapacità di richiamare i dati crittografati associati. Per ulteriori informazioni sull'implementazione della crittografia in ambienti che utilizzano ambienti IBM e/o non-IBM, leggere il white paper di IBM cui è possibile accedere dal seguente link:

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101479

2. Definizioni

Macchina di Crittografia -- una Macchina per la memorizzazione dei dati configurata con la capacità di eseguire crittografia dei dati. Tale crittografia può essere fornita tramite una funzione o come capacità standard della Macchina.

Deadlock di Crittografia –tutti i principali server all'interno di un ambiente di computing sono resi inoperabile perchè i dati del server principale sono memorizzati su una Macchina di Crittografia che dipende dal server principale per accedere ai dati (cioè, le chiavi di crittografia stesse sono state incluse all'interno dei dati crittografati utilizzando quelle chiavi.

3. Considerazioni sulla Crittografia

E' possibile scegliere di implementare e configurare il proprio ambiente del server principale al momento dell'installazione iniziale o di riconfigurare tale ambiente in seguito all'installazione iniziale: L'uso appropriato della tecnologia di crittografia è fondamentale alla manutenzione, sicurezza e accessibilità dei dati crittografati.

Con il presente, si è avvisati che i rischi inerenti la tecnologia di crittografia includono quanto segue:

a. mancata implementazione, configurazione o conservazione appropriate dell'ambiente di memoria crittografata o delle chiavi di crittografia, delle applicazioni per la gestione della chiave di crittografia (ad esempio, il Programma Tivoli Key Lifecycle Manager), o dei record di avvio per un server collegato,possono portare alla perdita delle chiavi di crittografia determinando l'irrecuperabilità dei dati crittografati utilizzando quelle chiavi;

b. implementazione inappropriata, configurazione o manutenzione possono causare un Deadlock di Crittografia, che possono determinare l'irrecuperabilità di tutti i dati crittografati gestiti dal server principale in tutte le installazioni nell'ambiente di computing; e

c. con l'introduzione della crittografia basata su Macchina e altre tecnologie di crittografia a diversi livelli dell'ambiente di memorizzazione, la probabilità di un Deadlock di Crittografia può aumentare notevolmente.

4. Servizi di Supporto della Crittografia IBM

IBM offre e consiglia i Servizi di Supporto Crittografia IBM per assistenza nell'implementazione della propria configurazione di crittografia della memoria. Su richiesta, IBM fornirà le informazioni riguardanti tale offerta del servizio.

5. Rinuncia IBM

La limitazione delle clausole di responsabilità in vigore tra le parti sono integrate dalle seguenti rinunce aggiuntive della potenziale responsabilità di IBM relativa alla crittografia della memoria:

a. E' propria la responsabilità nella scelta e implementazione appropriata della configurazione dell'ambiente del server principale. IBM non è responsabile di danni derivanti da una inappropriata implementazione di un

ambiente di crittografia o di qualsiasi modifica a tale ambiente se l'implementazione o la modifica non sono state apportate da IBM; e

b. Se si configura o riconfigura l'ambiente del server principale in base ai servizi di Supporto della Crittografia IBM, si è l'unico responsabile di qualsiasi danno derivante da inappropriata implementazione, configurazione o riconfigurazione.

IBM ストレージ暗号化に関する通知書

暗号化テクノロジーを含む IBM ストレージ・デバイスを取得いただき、ありがとうございます。 このデバイスの使用に関する重要な情報が含まれている本文書をお読みいただくことが重要です。 お客様は、暗号化マシンを使用することにより、自己の企業グループを代表して、本注意事項を読み、ここに記載された暗号化マシンの使用のリスクを理解し、以下に示す IBM 免責条項に同意することを承諾するものとします。

1. 概要

暗号化テクノロジーは、機密データの保護に不可欠な役割を果たします。 暗号化は、お客様の情報テクノロジー・システムにアクセス権を持たないはずの個人からのも含めた、許可されていないアクセスから情報を保護できます。 暗号化はまた、情報をあるシステムから別のシステムへ移行する間や、取り外し可能や可搬式のメディアに保管する時にも保護できます。

暗号鍵の適切な保護および管理は、お客様の情報テクノロジー環境に暗号化を実装するのに非常に重要な要素です。 暗号鍵を適切に保護および管理しない場合、関連する暗号化データの再取り出しができなくなるおそれがあります。 IBM 環境および/または他社製の環境における暗号化の実装についての詳細は、以下のリンクからアクセスできる IBM のホワイト・ペーパーを参照してください。

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101479

2. 定義

暗号化マシン -- データの暗号化を実行できるように構成されたデータ・ストレージ・マシン。 この暗号化は、マシンの機能を通じて、またはマシンの標準機能として提供されます。

暗号化デッドロック – 鍵サーバーのデータが、そのデータへのアクセスを鍵サーバーに依存する暗号化マシンに格納されているために、コンピューター環境内のすべての鍵サーバーが作動不能であること (つまり、暗号鍵自体が、それらの鍵を使用して暗号化されたデータ内に含まれています) 。

3. 暗号化の考慮事項

お客様は、初期インストールの際にお客様の鍵サーバー環境を実装および構成するか、または初期インストール後にそのような環境を再構成するかを、選択することができます。 暗号化テクノロジーを適切に使用することは、暗号化データの維持、セキュリティーおよびアクセス可能性にとって重要です。

お客様は、本文書により、暗号化テクノロジーに以下のような特有のリスクが含まれることを承知するものとします。

a. 暗号化ストレージ環境や暗号鍵、暗号鍵管理アプリケーション (Tivoli Key Lifecycle Manager プログラムなど)、または接続されたサーバーのブート・レコードを適切に実装、構成または保守しなかった場合、暗号鍵が損失し、それらの鍵を使用して暗号化されたデータの再取り出しができなくなるおそれがあります。

b. 実装、構成または保守が不適切な場合、 暗号化デッドロックが生じて、コンピューター環境におけるすべてのインストールで、鍵サーバーが管理する暗号化データのすべての再取出しができなくなる結果をもたらす可能性があります。

c. ストレージ環境の異なるレベルでのマシンベースの暗号化と他の暗号化テクノロジーの実装により、暗号化デッドロックの可能性が著しく高まるおそれがあります。

4. IBM 暗号化サポート・サービス

IBM は、お客様のストレージ暗号化構成の実装を支援するために、IBM 暗号化サポート・サービスを提供および推奨します。 お客様の依頼により、IBM はかかるサービスについての情報を提供します。

5. IBM の免責条項

お客様と IBM 間で有効な責任の制限の条項は、以下の追加的なストレージ暗号化に関する IBM の潜在的責任の免責条項によって補足されます。

a. お客様は、お客様の鍵サーバー環境の構成を選択し、適切に実装することについて、単独で責任を負います。 IBM は、暗号化環境の不適切な実装または暗号化環境の変更によって生じた損害について、その実装または変更が IBM によるものでない場合、責任を負いません。

b. お客様が、IBM 暗号化サポート・サービス後にお客様の鍵サーバー環境を構成または再構成した場合、お客様は、不適切な実装、構成または再構成によって生じた損害について、単独で責任を負います。

저장 장치 암호화 관련 **IBM** 주의사항

암호화 기술이 포함된 IBM 저장 장치를 취득해 주셔서 감사합니다. 해당 디바이스 사용에 관한 중요한 정보가 들어 있는 이 문서를 읽어야 합니다. 암호화 기계를 사용함으로써 귀하는 해당 기업진단을 대신하여 이 주의사항을 읽었고, 이 문서에 설명된 암호화 기계 사용의 위험을 이해하고 있으며, 다음과 같은 IBM 면책사항을 승인함을 확인하는 것입니다.

1. 소개

암호화 기술은 중요한 데이터를 보호하는 데 필수적 역할을 합니다. 암호화는 무단 액세스는 물론 정보 기술 시스템에 대한 액세스 권한이 있는 개인으로부터 정보를 보호할 수 있습니다. 또한 한 시스템에서 다른 시스템으로 전환 중이거나 이동식 또는 전송 가능한 미디어에 저장된 경우 정보를 보호할 수 있습니다.

암호화 키를 적절하게 보호하고 관리하는 것은 정보 기술 환경에서 암호화를 구현하는 데 있어 중요한 요소입니다. 암호화 키를 적절하게 보호하고 관리하지 못하면 관련 암호화 데이터를 복구할 수 없게 될 수 있습니다. IBM 및/또는 비IBM 환경을 사용하여 환경에서 암호화를 구현하는 방법에 대한 자세한 내용은 다음 링크를 통해 액세스할 수 있는 IBM 백서를 참조하십시오.

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101479

2. 정의

암호화 기계 -- 데이터 암호화를 수행하는 기능으로 구성된 데이터 저장 장치 기계입니다. 이 암호화는 기계의 피처를 통해 제공되거나 기본 성능으로 제공될 수 있습니다.

암호화 교착 상태 – 키 서버 데이터는 데이터에 액세스할 수 있는 키 서버에 종속된 암호화 기계에 저장되기 때문에 컴퓨팅 환경 내의 모든 키서버는 작동하지 않게 됩니다(즉, 암호화 키 자체가 해당 키를 사용하여 암호화된 데이터 내에 포함됨).

3. 암호화 주의사항

초기 설치 시 키 서버 환경을 구현 및 구성하거나 초기 설치에 이어 해당 환경을 다시 구성하도록 선택할 수 있습니다. 적절한 암호화 기술 사용은 암호화 데이터의 유지보수, 보안 및 액세스 가능성에 중요한 요소입니다.

암호화 기술에 내재된 위험은 다음과 같습니다.

a. 암호화된 저장 장치 환경, 암호화 키, 암호화 키 관리 응용프로그램(예: Tivoli Key Lifecycle Manager Program) 또는 연결된 서버의 Boot Record를 적절하게 구현, 구성 또는 유지보수하지 못하면 암호화 키가 손실되어 해당 키를 사용하여 암호화된 데이터를 복구하지 못하게 됩니다.

b. 부적절한 구현, 구성 또는 유지보수는 암호화 교착 상태를 초래하여 컴퓨팅 환경에서 모든 설치를 수행할 때 모든 키-서버-관리 암호화 데이터를 복구하지 못하게 될 수 있습니다.

c. 저장 장치 환경의 서로 다른 레벨에 기계 기반 암호화 및 기타 암호화 기술을 도입하면 암호화 교착 상태가 크게 증가할 수 있습니다.

4. IBM 암호화 지원 서비스

IBM은 저장 장치 암호화 구성의 구현을 지원하기 위해 IBM 암호화 지원 서비스를 제공 및 권장합니다. 귀하가 요청하면 IBM이 해당 서비스 오퍼링(Offering)에 관한 정보를 제공합니다.

5. IBM 면책사항

귀하와 IBM 간에 적용되는 책임 제한 조항은 저장 장치 암호화 관련 IBM의 잠재적 책임에 대한 다음과 같은 추가 면책사항으로 보충됩니다.

a. 키 서버 환경 구성을 선택하고 적절하게 구현하는 것은 귀하의 책임입니다. IBM은 암호화 환경의 부적절한 구현 또는 해당 환경의 수정이 IBM에 의해 수행되지 않은 경우 해당 구현 또는 수정으로 인해 발생하는 어떠한 손해에도 책임을 지지않습니다.

b. IBM 암호화 지원 서비스에 따라 키 서버 환경을 구성 또는 재구성하는 경우 부적절한 구현, 구성 또는 재구성으로 인해 발생하는 모든 손해는 귀하의 책임입니다.

IBM pranešimas dėl duomenų saugyklų šifravimo

Dėkojame, kad įsigijote IBM duomenų saugyklos įrenginį su šifravimo technologija. Būtinai perskaitykite šį dokumentą, nes jame pateikta svarbi informacija apie tokio įrenginio naudojimą. Naudodami Šifravimo įrenginį jūs savo įmonės vardu patvirtinate, kad perskaitėte šį pranešimą, supratote čia aprašytą šifravimo įrenginio naudojimo riziką ir sutinkate su toliau nurodytu IBM atsakomybės atsisakymu.

1. Įvadas

Šifravimo technologija yra gyvybiškai svarbi apsaugant svarbius duomenis. Šifravimas gali apsaugoti, kad informacijos neteisėtai negalėtų pasiekti net tie asmenys, kurie kitais atvejais turi prieigą prie informacinių technologijų sistemų. Šifravimas taip pat gali apsaugoti informaciją ją perkeliant iš vienos sistemos į kitą, saugant keičiamosiose arba perkeliamose laikmenose.

Diegiant šifravimą jūsų informacinių technologijų aplinkoje svarbiausia yra užtikrinti tinkamą šifravimo raktų apsaugą ir tvarkymą. Netinkamai saugant ir tvarkant šifravimo raktus gali nepavykti nuskaityti susijusių šifruotų duomenų. Norėdami gauti papildomos informacijos apie šifravimo diegimą aplinkose, kuriose naudojamos IBM ir ne IBM aplinkos, skaitykite IBM baltąjį dokumentą, kurį rasite spustelėję šį saitą:

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101479

2. Apibrėžimai

Šifravimo įrenginys – duomenų saugojimo Įrenginys, kuriame sukonfigūruota galimybė šifruoti duomenis. Šifruoti naudojant įrenginyje esančią priemonę arba standartinę galimybę.

Šifravimo aklavietė – situacija, kai visi kompiuterinės aplinkos raktų serveriai atvaizduojami kaip neveikiantys, nes raktų serverio duomenys yra saugomi Šifravimo įrenginyje, kuris priklauso nuo prie duomenų prieinančio raktų serverio (t. y. šifravimo raktai yra duomenyse, kurie buvo užšifruoti naudojant šiuos raktus).

3. Šifravimo aplinkybės

Galite nuspręsti diegti ir konfigūruoti savo raktų serverio aplinką pradinio diegimo metu arba konfigūruoti šią aplinką iš naujo atlikę pradinį diegimą. Tinkamai naudoti šifravimo technologiją ypač svarbu tvarkant, apsaugant ir naudojant šifruotus duomenis.

Šiuo pranešimu esate įspėjami, kad su šifravimo technologija yra susijusi tokia rizika :

a. Trikdžiai, neleidžiantys tinkamai diegti, konfigūruoti arba tvarkyti šifruotos saugyklos aplinkos arba bet kurių šifravimo raktų, šifravimo raktų valdymo taikomųjų programų (pavyzdžiui, „Tivoli Key Lifecycle Manager“ programos) arba prijungto serverio paleisties įrašų, todėl galite prarasti šifravimo raktus, o duomenys užšifruoti naudojant šiuos raktus gali tapti nebenuskaitomi;

b. Netinkamai diegiant, konfigūruojant arba tvarkant gali susidaryti Šifravimo aklavietė, dėl kurios visose kompiuterinės aplinkos įdiegtyse esantys visi raktų serverių valdomi šifruoti duomenys gali tapti nebenuskaitomi; ir

c. Skirtinguose saugyklos aplinkos lygmenyse naudojant Įrenginiu pagrįstą šifravimą ir kitas šifravimo technologijas, Šifravimo aklavietės tikimybė gali žymiai padidėti.

4. IBM šifravimo palaikymo paslaugos

IBM siūlo ir rekomenduoja naudotis IBM Šifravimo palaikymo paslaugomis, skirtomis padėti jums diegti saugyklos šifravimo konfigūraciją. Gavusi jūsų užklausą, IBM suteiks informacijos apie šią paslaugą.

5. IBM atsakomybės atsisakymas

Galiojančių jūsų ir IBM atsakomybės sąlygų apribojimas papildomas toliau nurodytu galimos IBM atsakomybės, susijusios su saugyklos duomenų šifravimu, papildomu atsakomybės atsisakymu:

a. Esate visiškai atsakingi už raktų serverio aplinkos konfigūracijos pasirinkimą ir tinkamą diegimą. IBM neatsako už jokią žalą, atsiradusią dėl netinkamo šifravimo aplinkos diegimo arba bet kokio tokios aplinkos modifikavimo, jeigu diegimą arba modifikavimą atliko ne IBM; ir

b. Jeigu konfigūruojate arba pakartotinai konfigūruojate raktų serverio aplinką naudodamiesi IBM šifravimo palaikymo paslaugomis, esate visiškai atsakingi už žalą, atsiradusią dėl netinkamo diegimo, konfigūravimo arba pakartotinio konfigūravimo.

Uwagi IBM na temat szyfrowania pamięci masowej

Dziękujemy za zakup urządzenia pamięci masowej IBM zawierającego technologię szyfrowania. Prosimy o uważne przeczytanie niniejszego dokumentu. Zawiera on bowiem ważne informacje na temat korzystania z tego urządzenia. Korzystając z Urządzenia Szyfrującego, Klient potwierdza w imieniu swego przedsiębiorstwa, że przeczytał niniejszą uwagę, jest świadomy ryzyka związanego z używaniem Urządzenia Szyfrującego opisanego w niniejszym dokumencie oraz zaakceptował zastrzeżenia IBM zamieszczone poniżej.

1. Wprowadzenie

Technologia szyfrowania odgrywa istotną rolę w zabezpieczaniu danych objętych szczególną ochroną. Szyfrowanie zabezpiecza informacje przed dostępem bez uprawnień, nawet w przypadku osób fizycznych, które posiadają dostęp do systemów informatycznych Klienta. Szyfrowanie może również zabezpieczać informacje w trakcie przenoszenia ich z jednego systemu na inny bądź w czasie przechowywania na nośnikach wymiennych lub przenośnych.

Właściwe zabezpieczenie kluczy szyfrowania oraz zarządzanie nimi jest newralgicznym elementem implementacji szyfrowania w środowisku informatycznym. Jakiekolwiek niepowodzenie w tym zakresie może uniemożliwić odtworzenie zaszyfrowanych danych. Więcej informacji na temat implementacji szyfrowania w środowiskach korzystających z oprogramowania IBM oraz innych producentów zawiera opracowanie IBM dostępne pod poniższym adresem:

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101479

2. Definicje

Urządzenie Szyfrujące oznacza urządzenie pamięci masowej umożliwiające szyfrowanie danych. Szyfrowanie takie może być przeprowadzone z wykorzystaniem dodatkowych opcji lub w ramach standardowych możliwości urządzenia.

Zakleszczenie Szyfrowania oznacza, że wszystkie serwery kluczy w środowisku obliczeniowym nie działają, ponieważ dane serwera kluczy zapisane są w Urządzeniu Szyfrującym, które z kolei potrzebuje serwera kluczy, aby uzyskać dostęp do danych (tzn. same klucze szyfrowania zawarte są w danych, które zostały zaszyfrowane z użyciem tychże kluczy).

3. Aspekty szyfrowania

Klient może zdecydować się na implementację i konfigurację środowiska serwera kluczy w czasie wstępnej instalacji bądź też na rekonfigurację takiego środowiska po wstępnej instalacji. Właściwe korzystanie z technologii szyfrowania ma newralgiczne znaczenie dla utrzymania, bezpieczeństwa i dostępności zaszyfrowanych danych.

Warto pamiętać o poniższych czynnikach ryzyka wynikających z zastosowania technologii szyfrowania:

a. niemożność właściwej implementacji, skonfigurowania lub serwisowania środowiska zaszyfrowanej pamięci masowej lub kluczy szyfrowania, aplikacji zarządzania kluczami szyfrowania (na przykład programu Tivoli Key Lifecycle Manager Program) lub rekordów startowych dla podłączonego serwera może prowadzić do utraty kluczy szyfrowania, a to z kolei może uniemożliwić odtworzenie danych zaszyfrowanych za pomocą tych kluczy;

b. niewłaściwa implementacja, skonfigurowanie lub serwisowanie mogą spowodować Zakleszczenie Szyfrowania, które z kolei może uniemożliwić odtworzenie wszystkich danych zaszyfrowanych kluczem zarządzanym przez serwer we wszystkich instalacjach w środowisku obliczeniowym;

c. dzięki wprowadzeniu szyfrowania z użyciem Urządzenia i innych technologii szyfrowania na różnych poziomach środowiska pamięci masowej prawdopodobieństwo Zakleszczenia Szyfrowania zdecydowanie maleje.

4. Usługi wsparcia IBM świadczone w zakresie szyfrowania

IBM oferuje i rekomenduje usługi wsparcia świadczone w zakresie szyfrowania jako pomoc przy wdrażaniu konfiguracji dla szyfrowania pamięci masowej. IBM dostarczy na żądanie informacje na temat oferty takich usług.

5. Zastrzeżenia IBM

Poniższe dodatkowe zastrzeżenia uzupełniają zakres odpowiedzialności ponoszonej przez Klienta i IBM w zakresie szyfrowania pamięci masowej:

a. Klient ponosi wyłączną odpowiedzialność za wybór i właściwą implementację konfiguracji środowiska serwera kluczy. IBM nie ponosi odpowiedzialności za szkody wynikające z niewłaściwej implementacji środowiska szyfrowania lub modyfikacji takiego środowiska, jeśli taka implementacja lub modyfikacja nie zostały przeprowadzone przez IBM.

b. Jeśli Klient konfiguruje lub rekonfiguruje swoje środowisko serwera kluczy korzystając z usług wsparcia IBM w zakresie szyfrowania, to ponosi on wyłączną odpowiedzialność za wszelkie szkody wynikające z niewłaściwej implementacji, konfiguracji oraz rekonfiguracji.

Aviso da IBM Relativo a Criptografia de Armazenamento

Obrigado por adquirir um dispositivo de armazenamento da IBM que inclui tecnologia de criptografia. É importante que o Cliente leia este documento que contém informações importantes em relação ao uso de tal dispositivo. Ao usar uma Máquina de Criptografia, o Cliente reconhece, em nome de sua empresa, que leu este aviso, entende os riscos de usar uma Máquina de Criptografia descrita aqui e aceita as renúncias de responsabilidade da IBM conforme definido abaixo.

1. Introdução

A tecnologia de criptografia representa uma função vital na protecção/proteção de dados sensíveis. A criptografia pode proteger informações de acesso não autorizado, mesmo de indivíduos que, de outra forma, tenham acesso a seus sistemas de tecnologia da informação. A criptografia pode também proteger informações enquanto estas estão em trânsito de um sistema ao outro ou quando armazenadas em mídia/suporte media removível ou transportável.

A protecção/proteção adequada e a gestão/gerenciamento de chaves de criptografia é um elemento crítico da implementação de criptografia em seu ambiente de tecnologia da informação. A falha em proteger adequadamente e gerenciar suas chaves de criptografia pode resultar na incapacidade de recuperar dados criptografados associados. Para obter informações adicionais sobre implementação de criptografia em ambientes usando ambientes IBM e/ou não IBM, leia o "white paper" da IBM, o qual pode ser acedido/acessado por meio do seguinte link:

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101479

2. Definições

Máquina de Criptografia -- uma máquina de armazenamento de dados configurada com a capacidade de executar criptografia de dados. Tal criptografia pode ser fornecida por meio de um recurso ou como uma capacidade padrão da Máquina.

Conflito de Criptografia –todos os servidores chave em um ambiente de computação são disponibilizados inoperáveis porque os dados do servidor chave são armazenados em uma Máquinade Criptografia que é dependente do servidor chave para aceder/acessar os dados (ex., as chaves de criptografia em si foram incluídas nos dados que foram criptografados usando essas chaves).

3. Considerações de Criptografia

O Cliente pode decidir implementar e configurar seu ambiente de servidor chave no momento da instalação inicial ou reconfigurar tal ambiente seguindo a instalação inicial. O uso adequado de tecnologia de criptografia é crítico para a manutenção, segurança e acessibilidade de dados criptografados.

O Cliente está advertido aqui de que os riscos inerentes na tecnologia de criptografia incluem o seguinte:

a. a falha em implementar, configurar ou manter adequadamente oambiente de armazenamento criptografado ou quaisquer chaves de criptografia, aplicativos de gerenciamento/gestão de chave de criptografia (por exemplo, Programa Tivoli Key Lifecycle Manager) ou registros/registos de inicialização para um servidor conectado, pode levar à perda de chaves de criptografia resultando na impossibilidade de recuperar de dados criptografados usando essas chaves;

b. a implementação, configuração ou manutenção imprópria pode causar um Conflito de Criptografia, o qual pode resultar na irrecuperabilidade de todos os dados criptografados gerenciados pelo servidor chave em todas as instalações no ambiente de computação;e

c. com a introdução de criptografia baseada em Máquinae outras tecnologias de criptografia em níveis diferentes do ambiente de armazenamento, a probabilidade de um C onflitode Criptografia pode aumentar de forma significativa.

4. Serviços de Suporte de Criptografia da IBM

A IBM oferece e recomenda os Serviços de Suporte de Criptografia da IBM para assistir o Cliente com a implementação de sua configuração de criptografia de armazenamento. Mediante seu pedido, a IBM fornecerá informações relativas à oferta de tal serviço.

5. Renúncia de Responsabilidade da IBM

Os termos de limitação de responsabilidade em vigor entre o Cliente e a IBM são suplementados pela responsabilidade das renúncias adicionais da IBM a seguir:

a. O Cliente é o único responsável por seleccionar/selecionar e implementar adequadamente a configuração de seu ambiente de servidor chave. A IBM não é responsável por quaisquer danos resultantes de implementação imprópria de um ambiente de criptografia ou qualquer modificação a tal ambiente se a implementação ou modificação não tiver sido feita pela IBM; e

b. Se o Cliente configurar ou reconfigurar seu ambiente de servidor chave seguindo os Serviços de Suporte de Criptografia da IBM, o Cliente será o único responsável por quaisquer danos resultantes de implementação, configuração ou reconfiguração imprópria.

Замечание IBM относительно Шифрования в Системах Хранения

Благодарим вас за приобретение устройства хранения данных IBM, оснащенного технологией шифрования данных. Внимательно ознакомьтесь с этим документом, который содержит важные сведения об использовании подобных устройств. Используя Машину с Шифрованием, вы тем самым от имени вашего предприятия подтверждаете, что ознакомились с настоящим замечанием, осознаете описанные в нем риски использования Машины с Шифрованием, и соглашаетесь с отказом IBM от ответственности, приведенным ниже.

1. Введение

Технологии шифрования играют важную роль в защите конфиденциальных данных. С помощью шифрования можно защитить данные от несанкционированного доступа, даже если несанкционированный доступ осуществляют те лица, которые в иных случаях имеют доступ к ИТ-системам предприятия. Шифрование также позволяет защитить данные при их передаче из одной системы в другую и при хранении на съемных или переносных носителях.

Особо важным условием внедрения шифрования в вашу ИТ-среду является надежная защита ключей шифрования и надлежащее управление ими. Недостаточная защита ключей шифрования, так же как и неправильное управление ими, может привести к невозможности получения данных, зашифрованных с помощью этих ключей. Чтобы получить дополнительные сведения о реализации шифрования в средах, в которых используются решения IBM и/или других производителей, ознакомьтесь с технической публикацией IBM, к которой можно перейти по следующей ссылке:

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101479

2. Определения

Машина с Шифрованием – Машина хранения данных с настроенной возможностью шифрования данных. Шифрование может быть реализовано в виде дополнительной функции или в качестве стандартной возможности Машины.

Неустранимая Блокировка Шифрования – ситуация, в которой все серверы ключей шифрования в вычислительной среде становятся недоступными из-за того, что данные этих серверов хранятся на Машине с Шифрованием, которой для доступа к данным требуется обращаться к серверу ключей шифрования (то есть ключи шифрования оказались среди данных, зашифрованных с помощью этих ключей).

3. Что нужно принять во внимание при Шифровании

Вы можете решить создать и сконфигурировать вашу среду серверов ключей шифрования при первоначальной установке, либо настроить ее позже. Правильное использование технологии шифрования является особо важным для технического обслуживания, безопасности и доступности зашифрованных данных.

Настоящим сообщаем вам о том, что риски присущие технологиям шифрования, включают следующее:

a. невозможность правильно внедрять, конфигурировать или обслуживать среду хранения зашифрованных данных или любые ключи шифрования, приложения для управления ключами шифрования (например, Tivoli Key Lifecycle Manager) или загружать записи для подключенных серверов может привести к потере ключей шифрования, из-за чего данные, зашифрованные с использованием этих ключей, будут безвозвратно утрачены;

b. неправильное внедрение, конфигурирование или обслуживание может стать *причиной* Неустранимой Блокировки Шифрования, из-за чего все данные, зашифрованные с использованием серверов ключей шифрования, на всех установках в вычислительной среде будут безвозвратно утрачены; и

c. при реализации шифрования с использованием Машины и других технологий шифрования на разных уровнях среды хранения данных вероятность возникновения Неустранимой Блокировки Шифрования значительно возрастает.

4. Услуги IBM по Поддержке Шифрования (IBM Encryption Support Services)

IBM предлагает и рекомендует Услуги IBM по Поддержке Шифрования (IBM Encryption Support Services) для содействия вам во внедрении вашей конфигурации шифрования данных в системах хранения. Дополнительные сведения об этих услугах IBM предоставляются по запросу.

5. Отказ IBM от ответственности

Положения об ограничении ответственности, действующие между вами и IBM, дополняются следующими отказами IBM от возможной ответственности в отношении шифрования данных в системах хранения.

a. Вы несете полную ответственность за выбор и правильную реализацию конфигурации среды серверов ключей шифрования. IBM не несет ответственности ни за какой ущерб, возникший в результате неправильной реализации среды шифрования или любого изменения такой среды, если реализация среды или ее изменение не производились специалистами IBM; и

b. В случае если вы конфигурируете или изменяете конфигурацию вашей среды серверов ключей шифрования после оказания Услуг IBM по Поддержке Шифрования, вы несете полную ответственность за любой ущерб, возникший в результате неправильной реализации, конфигурирования или изменения конфигурации.

IBM 有关存储加密的声明

感谢您购买包含加密技术的 IBM 存储设备。请务必阅读本文，本文包含有关这类设备使用的重要信息。 您一旦使用加密机器，即表示您承认已代表您的企业阅读了本声明、理解使用本文所述的加密机器可能招致的风险，并且接受下面阐明的 IBM 免责声明。

1. 简介

加密技术在保护敏感数据方面起到重要作用。加密可保护信息免受未经授权的访问，即使是原本有权访问信息技术系统的人也不例外。加密还可在信息从一个系统传输至另一个系统时，或者存储在可移动或可运送介质上时，为信息提供保护。

加密密钥的妥善保护和管理是在信息技术环境中实施加密的关键要素。如未能妥善保护和管理加密密钥，则可能导致无法恢复相关的加密数据。有关在 IBM 和/或非 IBM 环境中实施加密的更多信息，请阅读可从下面的链接获得的 IBM 白皮书：

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101479

2. 定义

加密机器— 配备数据加密能力的数据存储机器。此类加密可通过某种功能部件提供，也可作为机器的标配功能提供。

加密死锁 – 计算环境中的所有密钥服务器，因为密钥服务器数据存储在加密机器中，而这些加密机器又依赖于密钥服务器来访问这些数据（即，加密密钥本身包含在用这些密钥加密的数据之中），因而呈现不可运行状态。

3. 加密注意事项

您可以选择在初始安装时实施并配置密钥服务器环境，也可以在初始安装之后重新配置此类环境。 正确使用加密技术对于加密数据的维护、安全性和可访问性至关重要。

因此，我们向您提出，加密技术本身的固有风险包括以下这些：

a. 如未能正确实施、配置或维护加密存储环境，或者任何加密密钥、加密密钥管理应用程序（例如，Tivoli Key Lifecycle Manager Program）或所连服务器的引导记录，那么这都可能导致加密密钥丢失，从而造成使用这些密钥加密的数据无法恢复；

b. 不正确的实施、配置或维护可能造成加密死锁，而加密死锁可导致计算环境中安装的所有设备上的所有通过密钥服务器管理的加密数据不可恢复；

c. 如果在存储环境的不同级别引入基于机器的加密以及其他加密技术，那么加密死锁的可能性可能明显增高。

4. IBM 加密支持服务

IBM 提供并推荐 IBM 加密支持服务来协助您实施存储加密配置。 IBM 将根据您的请求提供与此类服务有关的信息。

5. IBM 免责声明

以下涉及存储加密的 IBM 潜在责任附加免责声明是贵方与 IBM 之间生效的责任限制条款的补充：

a. 选择并正确实施密钥服务器环境配置的责任完全由您承担。对于因加密环境实施不当，或者对此类环境的任何修改而造成的任何损失，如果实施或修改行为并非 IBM 所为，则 IBM 不承担任何责任；

b. 如果您在 IBM 加密支持服务之后配置或重新配置了密钥服务器环境，那么对于因不正确的实施、配置或重新配置而造成的任何损失，将由您独自承担。

IBM-ovo obvestilo o šifriranju pomnilnika

Zahvaljujemo se vam za nakup IBM-ove pomnilniške naprave s šifrirno tehnologijo. Ta dokument morate prebrati, saj vsebuje izredno pomembne informacije o uporabi takšne naprave. Z uporabo šifrirne naprave v imenu podjetja potrjujete, da ste se seznanili s tem obvestilom, razumete tveganja pri uporabi šifrirne naprave, opisane v tem dokumentu, in sprejemate IBM-ove omejitve odgovornosti, kot je določeno v nadaljevanju.

1. Predstavitev

Šifrirna tehnologija igra pomembno vlogo pri varovanju občutljivih podatkov. Šifriranje varuje informacije pred nepooblaščenim dostopanjem in tudi pred posamezniki, ki sicer imajo dostop do vaših sistemov informacijske tehnologije. Poleg tega šifriranje varuje informacije tudi med prenosom iz enega sistema v drugega ali shranjevanjem na odstranljiv ali prenosen medij.

Ustrezna zaščita in upravljanje šifrirnih ključev je izredno pomemben element pri implementaciji šifriranja v okolju informacijske tehnologije. Posledica nepravilne zaščite in upravljanja šifrirnih ključev je lahko nezmožnost pridobivanja povezanih šifriranih podatkov. Dodatne informacije o implementaciji šifriranja v okoljih z IBM-ovimi okolji ali okolji, ki niso IBM-ova, najdete v IBM-ovi beli knjigi, na naslednji povezavi:

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101479

2. Definicije

Šifrirna naprava - naprava za shranjevanje podatkov, ki je konfigurirana z zmožnostjo izvajanja šifriranja podatkov. Takšno šifriranje je lahko zagotovljeno s funkcijo ali standardno zmožnostjo naprave.

Zastoj šifriranja – vsi strežniki ključev v okolju ne delujejo, ker so podatki strežnika ključev shranjeni na šifrirni napravi, ki je za dostopanje do podatkov odvisna od strežnika ključev (npr. šifrirni ključi so bili vključeni v podatke, ki so bili šifrirani s temi ključi.

3. Pomisleki pred uporabo šifriranja

Okolje strežnika ključev lahko implementirate in konfigurirate ob začetni namestitvi ali pa to storite pozneje. Pravilna uporaba šifrirne tehnologije je bistvenega pomena za vzdrževanje, zaščito in dostopnost do šifriranih podatkov.

Z naslednjimi informacijami vas obveščamo o tveganjih, ki so del šifrirne tehnologije, in vključujejo naslednje:

a. nepravilna implementacija, konfiguracija ali vzdrževanje okolja šifriranega pomnilnika ali šifrirnih ključev, aplikacij za upravljanje šifrirnih ključev (na primer Tivoli Key Lifecycle Manager Program) ali zagonskih zapisov za priključeni strežnik lahko vodi do izgube šifrirnih ključev in s tem do nezmožnosti pridobivanja podatkov, ki so bili šifrirani s temi ključi;

b. nepravilna implementacija, konfiguracija ali vzdrževanje lahko povzroči zastoj šifriranja, kar lahko pomeni, da ne boste mogli pridobiti vseh šifriranih podatkov, ki so upravljani s strežnikom ključev, pri vseh namestitvah v okolju računalnika, in

c. z uvedbo šifriranja, ki temelji na napravi, in drugih šifrirnih tehnologij na različnih ravneh okolja pomnilnika se verjetnost zastoja šifriranja lahko znatno poveča.

4. IBM-ove storitve za podporo šifriranja

IBM nudi in priporoča IBM-ove storitve za podporo šifriranja kot pomoč pri implementaciji konfiguracije šifriranja pomnilnika. Na vašo zahtevo vam bomo priskrbeli informacije o tej storitveni ponudbi.

5. IBM-ova omejitev odgovornosti

Veljavni pogoji omejitve odgovornosti med vami in IBM-om so podprti z naslednjimi dejstvi o omejitvi odgovornosti, ki se nanašajo na IBM-ovo potencialno odgovornost v zvezi s šifriranjem pomnilnika:

a. izbira in pravilna implementacija konfiguracije okolja strežnika ključev je vaša odgovornost. IBM ni odgovoren za kakršno koli škodo, ki nastane pri nepravilni implementaciji šifrirnega okolja, ali kakršne koli spremembe takšnega okolja, če implementacije ali prilagoditve ni izvedel IBM; in

b. če konfigurirate ali ponovno konfigurirate okolje strežnika ključev v skladu z IBM-ovimi storitvami za podporo šifriranja, ste sami odgovorni za kakršno koli škodo, ki nastane zaradi nepravilne implementacije, konfiguracije ali vnovične konfiguracije.

Aviso de IBM sobre el Cifrado de Almacenamiento

Gracias por adquirir un dispositivo de almacenamiento de IBM que incluye tecnología de cifrado (encriptación). Es importante que lea este documento, que contiene información importante sobre el uso de este dispositivo. Al utilizar una Máquina de Cifrado, reconoce en nombre de su empresa que ha leído este aviso, que comprende los riesgos que se describen en el presente documento referentes al uso de una Máquina de Cifrado, y que acepta la renuncia declaraciones de limitación de responsabilidad de IBM que se establece a continuación.

1. Introducción

La tecnología de cifrado desempeña un papel fundamental en la protección de datos sensibles. El cifrado puede proteger la información de los accesos no autorizados e incluso de las personas que tengan acceso de cualquier otra forma a sus sistemas de tecnologías de la información. El cifrado también puede proteger la información cuando se transfiere de un sistema a otro, o cuando se almacena en soportes extraíbles o transportables.

La protección y la gestión adecuadas de las claves de cifrado son elementos de gran importancia al implementar el cifrado en el entorno de tecnologías de la información. Si no protege y gestiona las claves de cifrado de forma correcta es posible que no pueda recuperar sus datos cifrados asociados. Para obtener información sobre la implementación de cifrado en entornos IBM y no IBM, lea la documentación técnica de IBM, a la que se puede acceder a través del enlace siguiente:

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101479

2. Definiciones:

Máquina de Cifrado: Máquina de almacenamiento de datos configurada con la función de cifrado de datos. Dicho cifrado debe realizarse mediante un dispositivo o como función estándar de la Máquina.

Punto Muerto de Cifrado: todos los servidores de claves del entorno informático dejan de estar operativos porque los datos del servidor de claves se almacenan en una Maquina de Cifrado que depende del servidor de claves para acceder a los datos (es decir, las claves de cifrado se han incluido en los datos cifrados utilizando dichas claves).

3. Consideraciones de cifrado

Puede optar por implantar y configurar el entorno de servidor de claves en cualquier momento durante la instalación inicial, o volver a configurarlo una vez realizada la instalación inicial. El uso adecuado de la tecnología de cifrado resulta de vital importancia para el mantenimiento, la seguridad y la accesibilidad de los datos cifrados.

Mediante el presente documento, se le notifica que la tecnología de cifrado incluye los siguientes riesgos inherentes::

a. el incumplimiento de la correcta implantación, configuración o mantenimiento del entorno de almacenamiento cifrado o de las claves de cifrado, las aplicaciones de gestión de claves de cifrado (como el programa Tivoli Key Lifecycle Manager), o los registros de arranque para un servidor adjunto, puede ocasionar que se pierdan las claves de cifrado y que no se puedan recuperar los datos cifrados con dichas claves;;

b. la implantación, configuración o mantenimiento inadecuados pueden causar un Punto Muerto de Cifrado (ncryption Deadlock), lo que puede resultar en la imposibilidad de recuperación de todos los datos cifrados gestionados por servidores de claves en todas las instalaciones del entorno informático;

c. con la implantación de cifrado basado en la Máquina y otras tecnologías de cifrado en diferentes niveles del entorno de almacenamiento, la posibilidad de un Punto Muerto de Cifrado aumenta de forma considerable.

4. Servicios de Soporte IBM de Cifrado

IBM ofrece y recomienda los Servicios de Soporte de IBM de Cifrado, que le ayudarán a implantar la configuración de cifrado de almacenamiento. Si se lo solicita, IBM le proporcionará información sobre esta oferta de servicios.

5. Renuncia de responsabilidad de IBM

Los términos de limitación de responsabilidad en vigor entre usted e IBM se complementan por las siguientes renuncias de responsabilidad referentes a la posible responsabilidad de IBM sobre el cifrado de almacenamiento:

a. Usted es el único responsable de seleccionar e implantar de forma correcta la configuración del entorno de servidor de claves. IBM no se responsabiliza de ningún daño que resulte de la implantación inadecuada de un entorno de cifrado ni de la modificación de dicho entorno si la implementación o la modificación no han sido realizadas por IBM; y

b. en caso de que Usted configure o reconfigure su entorno de servidor de claves con la ayuda de los Servicios de Soporte de IBM de Cifrado, usted sólo será responsable de los daños que resulten de la implantación, la configuración o reconfiguración inadecuadas.

IBM 有關儲存體加密之注意事項

感謝 貴客戶取得 IBM 儲存裝置，此裝置內含加密技術。請務必閱讀本文件，本文件內含使用該裝置之相關重要資訊。貴客戶藉由使用「加密機器」而代表 貴客戶所屬之企業確認： 貴客戶已詳閱本注意事項文件，瞭解本文件所述有關使用「加密機器」之風險，並接受以下載明之 IBM 免責聲明。

1. 簡介

加密技術在保護機密資料上扮演重要之角色。「加密」可保護資訊避免遭受未獲授權之存取，即使是對於 貴客戶技術系統擁有存取權之個人，加密亦有相同之保護功效。「加密」亦可保護資訊從某一系統傳輸至另一系統，或保護資訊儲存在抽取式或可攜式媒體。

適當的保護與管理加密金鑰，對於在 貴客戶之資訊環境中建置加密，至爲重要。未能適當保護及管理 貴客戶之加密金鑰，可能致使無法擷取相關加密資料。如需有關在 IBM 及/或非 IBM 之環境中建置加密之其他資訊，請閱讀 IBM 白皮書，該白皮書可透過下列鏈結取得：

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101479

2. 定義

加密機器 -- 具備執行資料加密功能之資料儲存機器。該加密可透過特別功能提供之，亦可作爲機器之標準功能而提供之。

加密死結 – 當金鑰伺服器之資料係儲存在依賴金鑰伺服器以存取資料之加密機器時，亦即（加密金鑰本身已納入先前使用該等金鑰加密之資料中），將使運算環境中之一切金鑰伺服器均變成無法運作。

3. 加密考量

貴客戶可於初次安裝時建置及配置 貴客戶之金鑰伺服器環境，亦可於初次安裝後重新配置該環境。適當使用加密技術，對於加密資料之維護、安全及可存取性相當重要。

因此，提醒 貴客戶加密技術含有以下各項之風險：

a. 未能適當建置、配置或維護所連接伺服器之加密儲存環境或任何加密金鑰、加密金鑰管理應用程式（例如：Tivoli Key Lifecycle Manager 程式）、或開機記錄，可能導致加密金鑰滅失，進而導致無法擷取使用該等金鑰進行加密之資料；

b. 不當建置、配置或維護加密儲存環境或任何加密金鑰可能導致發生加密死結，進而導致所有在運算環境中一切已安裝而受管理金鑰伺服器加密之資料無法被擷取。

c. 若引進以機器爲基礎之加密措施及不同儲存環境層級之其他加密技術，會大幅提高發生「加密死結」之可能性。

4. IBM 加密支援服務

IBM 提供並建議 貴客戶採用 IBM 加密支援服務，以協助 貴客戶建置 貴客戶之儲存體加密配置。若 貴客戶提出要求，IBM 將提供 貴客戶有關該服務供應項目之資訊。

5. IBM 免責聲明

下列有關儲存體加密之 IBM 潛在責任額外免責聲明，係 貴客戶與 IBM 雙方立約生效之賠償限制條款之補充：

a. 貴客戶應自行負責選取及適當建置 貴客戶金鑰伺服器環境之配置。因不當之加密環境建置或因該環境之任何修改而產生任何損害時，如該建置或修改並非 IBM 所爲者，IBM 對該等損害概不負責；及

b. 若 貴客戶於 IBM 提供加密支援服務後自行配置或重新配置 貴客戶之金鑰伺服器環境，因該不當建置、配置或重新配置所產生之損害，由 貴客戶自行負責。

Part Number: 45W6389

Printed in USA

(1P) P/N: 45W6389

GA32-0642-01