IBM Encryption Facility for z/OS (5655-P97)

Per il trasferimento sicuro dei dati a disposizione dell'azienda

Caratteristiche principali

- Assicura il trasferimento ultrasicuro dei dati con partner, fornitori e clienti
- Offre funzioni di crittografia con gestione delle chiavi per nastro e disco
- Consente la crittografia di elevati volumi di dati per l'archiviazione in siti remoti
- Adopera le funzionalità di gestione delle chiavi di IBM® z/OS
- Consente la gestione delle chiavi a lungo termine per i dati archiviati in siti remoti
- Aumenta la flessibilità con il supporto del formato OpenPGP RFC 4880
- Supporta la compressione con gli algoritmi ZIP e ZLIB e la funzione z Data Compression (zEDC), se disponibile.

La protezione dei dati sensibili è un problema che affligge aziende di ogni parte del globo. La salvaguardia dei dati critici per il business e delle informazioni sui clienti preoccupa anche le più alte cariche aziendali, poiché gli errori commessi in questo campo si traducono in costi vivi molto alti e, cosa ancora più importante, nella perdita della fiducia di clienti e investitori. La protezione dei dati potrebbe essere imposta anche da normative pubbliche e private e obblighi contrattuali con partner commerciali. Quando si muovono in rete o si spostano, depositati su un nastro, da un capo all'altro della città, i dati devono essere protetti da visualizzazioni indesiderate e risultare accessibili solo al personale autorizzato.

IBM Encryption Facility for z/OS V1.2 consente di proteggere i dati at rest con l'ausilio di servizi di crittografia di livello mainframe, adoperati per la sicurezza dei Bancomat da oltre 20 anni. I clienti possono utilizzare la gestione centralizzata delle chiavi di z/OS per garantire lo scambio ultrasicuro delle chiavi di crittografia. Qualora importanti contenuti destinati a un partner affidabile dovessero cadere nelle mani sbagliate, potrebbero essere decrittografati solo con la chiave di crittografia privata del partner.

Con IBM Encryption Facility for z/OS potrete crittografare i dati sul sistema z/OS per inviarli a partner o clienti, anche se questi ultimi non posseggono un sistema z/OS. Per decrittografare i dati, i partner in possesso di z/OS hanno la possibilità di utilizzare Encryption Facility, il client basato su Java™, il Decryption Client for z/OS o un programma compatibile con OpenPGP RFC 4880. Per crittografare e decrittografare

i dati, i partner che non dispongono di z/OS possono invece utilizzare il client basato su Java o un programma compatibile con OpenPGP RFC 4880.

Encryption Facility for z/OS include due funzioni opzionali a pagamento:

- **Encryption Services**, che consente di crittografare e decrittografare alcuni formati file su z/OS, per permettervi di trasferire o archiviare file in siti remoti interni all'impresa o di partner e fornitori. Encryption Services supporta sia il formato IBM z Systems (originariamente introdotto in Encryption Facility for z/OS V1.1) sia il formato OpenPGP (reso disponibile con Encryption Facility for z/OS V1.2). Il formato z Systems supporta la compressione con accelerazione hardware prima della crittografia
- **DFSMSdss Encryption feature**, che consente la crittografia di set di dati dump DFSMSdss e supporta la compressione con accelerazione hardware prima della crittografia.

Alla protezione dei dati contribuiscono anche funzionalità di crittografia e gestione centralizzata delle chiavi all'avanguardia fornite da z/OS e dai server z Systems.

Encryption Services

Formato z Systems

Encryption Services consente di crittografare i dati per condividere informazioni sensibili su piattaforme diverse con partner, fornitori e clienti. La funzione può essere adoperata anche per crittografare determinati file a scopo di archiviazione. Encryption Services può adoperare la gestione delle chiavi di z/OS, le funzionalità di autenticazione dell'accesso ICSF (Integrated Cryptographic Services Facility) e la compressione hardware e le funzionalità crittografiche hardware dei server z Systems.

Supporta inoltre la crittografia dei dati mediante chiavi TDES a tre passaggi o AES a 128 bit. Per cifrare e decifrare le chiavi AES e TDES impiegate per la crittografia del file, possono essere specificate chiavi pubbliche/private RSA (Rivest Shamir Adleman). Le chiavi cifrate verranno archiviate in un'intestazione file. Con queste tecnica è possibile generare molti file – utilizzando diverse chiavi di crittografia – ciascuno leggibile anche dopo anni di archiviazione. Encryption Services supporta anche l'uso di uno schema di derivazione della chiave password.

Encryption Services supporta input provenienti da file di input sequenziali, membri di set di dati partizionati (PDS) e set di dati partizionati estesi (PDSE) e file archiviati in file system z/OS UNIX® System Services. La funzione può comprimere i file di input prima di crittografarli e scrivere i file di output. Grazie all'impiego dell'interfaccia a grandi blocchi per i file di output scritti su nastro, Encryption Services può anche ottimizzare le prestazioni e lo spazio disponibile sui supporti.

Formato OpenPGP RFC4880
Con l'introduzione della V1.2, Encryption Facility for z/OS offre ora il supporto del formato OpenPGP. OpenPGP assicura maggiore possibilità di scelta e flessibilità per lo scambio di dati con i BP. Il formato OpenPGP supportato da Encryption Facility è conforme ai requisiti dello standard OpenPGP ed è compatibile con altri prodotti compatibili con OpenPGP (RFC 4880). Questo supporto consente di scambiare un file crittografato, compresso e/o firmato in digitale tra il data center di un'azienda e i BP o i fornitori esterni che dispongono di un client compatibile con OpenPGP (RFC 4880) dotato di sistema operativo z/OS o di altro tipo. Il supporto OpenPGP di Encryption Facility prevede una lunga lista di nuove funzionalità, come la crittografia basata su passphrase di una chiave di sessione generata a caso, la crittografia asimmetrica di chiavi simmetriche generate a caso adoperando algoritmi RSA e ElGamal, la firma digitale dei dati e diverse altre funzioni che possono essere più o meno importanti a seconda dell'ambiente operativo e dei requisiti dell'azienda.

Il formato OpenPGP supportato da Encryption Facility for z/OS V1.2 consuma più risorse CP del formato z Systems di Encryption Facility. Può essere inoltre configurato per utilizzare più CP mediante una maggiore elaborazione parallela. L'impatto del maggiore utilizzo di risorse CPU può essere però ridotto con l'impiego di processori zIIP (z Integrated Information Processor) su z13 e zIIP e zAAP (zEnterprise Application Assist Processor) sui sistemi di precedente generazione. Poiché il supporto del formato OpenPGP è scritto in Java e il carico di lavoro Java è idoneo ai processori di tipo "motore specialistico", è possibile tagliare i costi software. Per alcune configurazioni, come quelle che prevedono quattro o più CPU attive, il tempo impiegato per un'attività dal supporto OpenPGP può essere quindi più favorevole di quello del supporto del formato z Systems.

Queste funzioni possono sfruttare l'Integrated Cryptographic Service Facility (ICSF) e la crittografia hardware. La crittografia hardware richiede un ambiente corretto e potrebbe richiedere l'installazione di un modulo crittografico.

Encryption Facility for z/OS V1.2 è disponibile sulle versioni di z Systems e z/OS attualmente supportate.

DFSMSdss Encryption

Data Facility Storage Management Subsystem (DFSMSdss) Encryption consente di crittografare set di dati dump DFSMSdss scritti su nastro e disco. La funzione è progettata per utilizzare la gestione delle chiavi e le funzionalità di autenticazione dell'accesso di z/OS, oltre alle funzionalità di compressione e crittografia hardware di z Systems.

Supporta inoltre la crittografia dei dati mediante chiavi TDES a tre passaggi o AES a 128 bit. Come Encryption Services, anche DFSMSdss Encryption supporta l'uso di chiavi pubbliche/private RSA per cifrare e decifrare le chiavi dati AES e TDES impiegate per la crittografia dei file e consente di generare chiavi AES e TDES mediante una specifica password. È possibile configurare DFSMSdss perché comprima i dati prima di crittografarli.

DFSMSdss Encryption include due funzioni, una per crittografare i dati durante l'elaborazione di comandi DUMP e l'altra per decrittografare i dati durante l'elaborazione di comandi RESTORE.

Encryption Facility for z/OS Client con impiego del formato z Systems
Encryption Facility for z/OS Client, programma con licenza separata (offerto così com'è, senza alcuna garanzia), è progettato per consentire lo scambio di dati crittografati tra sistemi z/OS dotati di funzione Encryption Facility e sistemi che eseguono z/OS o altre piattaforme e hanno bisogno delle funzioni supportate.

Encryption Facility for z/OS Client include i seguenti componenti:

- **Java-based Client.** *Java-based Client, scritto in Java, può essere utilizzato su z/OS e su qualsiasi altra piattaforma che supporti Java.*Java-based Client supporta sia la decrittografia dei dati creati su z/OS mediante il formato Encryption Facility z Systems sia la crittografia dei dati da inviare a un sistema z/OS in cui il file verrà decrittografato con il formato Encryption Facility z Systems. Nota: i dati che devono essere elaborati mediante Java-based Client non possono essere creati con la compressione
- **Decryption Client for z/OS.** *Decryption Client for z/OS è supportato solo su sistemi z/OS.* Decryption Client for z/OS supporta la decrittografia dei dati creati su z/OS con il formato Encryption Facility z Systems. I dati che devono essere elaborati mediante Decryption Client for z/OS possono essere creati con la compressione. Decryption Client non supporta la crittografia dei dati per il percorso di ritorno. Questa opzione potrebbe avere vantaggi prestazionali e richiedere meno supporti per lo scambio, ma non consente al BP di restituire i dati in formato crittografato.

Il valore della crittografia mainframe

I servizi di crittografia mainframe IBM si basano sull'integrazione di hardware e software – le tecnologie di crittografia e compressione dei server mainframe e la gestione centralizzata delle chiavi del sistema operativo z/OS.

L'hardware di crittografia mainframe ha due caratteristiche essenziali: assicura l'accelerazione della crittografia rispetto alla crittografia software e, con le funzioni giuste, offre anche servizi Secure Key. L'accelerazione della crittografia ad alte prestazioni è assicurata dalla CP Assist for Cryptographic Function (CPACF), integrata nei processori centrali dei server IBM z Systems. Sul server IBM System z10 Enterprise Class (z10 EC) e versioni successive, nuovi miglioramenti includono il supporto dell'algoritmo di hashing SHA-512 e della tecnologia Advanced Encryption Standard fino a 256 bit (AES-256), che sta diventando rapidamente lo standard di crittografia de facto.

Le funzioni opzionali Crypto Express2, Crypto Express3, Crypto Express4 e Crypto Express5 forniscono le tecnologie Secure Key che consentono scambi affidabili mediante coppie di chiavi pubbliche e private. Secure Key è essenziale per funzioni di banking come la comunicazione tra l'host e il Bancomat. Crypto Express2 supporta Triple-DES e Trusted Key Entry, offrendovi opzioni Secure Key. Crypto Express3 supporta chiavi di crittografia dati Triple-DES e AES a 128, 192 e 256 bit. L'ultima generazione Crypto Express5 offre prestazioni migliorate che possono essere sfruttate dall'Encryption Facility z/OS insieme ai miglioramenti apportati alla CPACF di z13.

La funzione ICSF di z/OS rappresenta l'interfaccia tra le applicazioni che hanno bisogno della crittografia e i servizi di crittografia hardware. Con oltre 20 di collaudato impiego da parte di clienti mainframe di ogni parte del globo, ICSF aiuta le imprese a proteggere e gestire le chiavi di crittografia, con operazioni di generazione delle chiavi, gestione delle chiavi basata su criteri aziendali e ripristino delle chiavi. ICSF consente anche di fornire informazioni di conformità agli audit e controlli degli accessi.

Queste funzionalità di crittografia vengono ulteriormente estese grazie alla resilienza e alla disponibilità del mainframe IBM. L'alta disponibilità (HA), la scalabilità, la resilienza e le funzionalità di ripristino remoto che lo caratterizzano rendono il mainframe la scelta più logica per l'archiviazione e la gestione delle chiavi di crittografia. Le funzionalità di crittografia presenti nei server mainframe IBM, insieme alla sicurezza integrata nel sistema operativo z/OS, rappresentano una solida base per la gestione delle chiavi a lungo termine. Encryption Facility for z/OS (V1.2) è progettato per fornire uno strumento completo per la crittografia dei dati su nastro e/o disco.

Altre funzionalità di crittografia IBM

IBM offre ora un'ampia gamma di soluzioni di crittografia progettate per soddisfare le vostre esigenze di protezione dei dati.

IBM System Storage Solution

IBM System Storage TS1120 e le unità nastro successive assicurano storage flessibile ad alte prestazioni con il supporto della crittografia dati. Questa funzionalità di crittografia viene fornita di serie su tutte le unità nastro TS1120 o di modello successivo ordinate di recente. La TS1120 e le unità nastro successive con funzione di crittografia sono progettate per offrire una soluzione di protezione dati capace di spostare il processo di crittografia dal server all'unità nastro (evitando il sovraccarico del server) e garantire operazioni efficaci sui grandi volumi di dati coinvolti nei processi di archiviazione e backup. Se utilizzata con z/OS, la TS1120 o le unità nastro di modello successivo sfruttano le straordinarie funzioni di crittografia e sicurezza di z Systems per garantire un'efficace soluzione per lo storage e la gestione delle chiavi di crittografia nell'intera impresa.

IBM Security Key Lifecycle Manager (ISKLM)

IBM Security Key Lifecycle Manager (ISKLM) for z/OS funziona con le unità nastro e i dispositivi di storage IBM abilitati alla crittografia. ISKLM permette di generare, proteggere, salvare e gestire le chiavi di crittografia utilizzate per crittografare le informazioni che vengono scritte su questi dispositivi e per decodificare le informazioni lette da questi stessi dispositivi. Una Command Line Interface (CLI) consente di gestire la fornitura di queste chiavi ai dispositivi. ISKLM for z/OS supporta inoltre unità nastro 3592 e Linear Tape-Open® (LTO®) abilitate alla crittografia. Sono supportati i seguenti tipi di unità:

- Unità nastro TS1120, TS1130 e TS1140 capaci di crittografare i dati
- Unità nastro LTO Ultrium® 4 e LTO Ultrium 5 capaci di crittografare i dati (la crittografia viene eseguita a velocità full line nell'unità nastro dopo la compressione).

ISKLM for z/OS supporta anche IBM DS8000 Storage Controller con la versione bundle del microcodice appropriata, livello Licensed Internal Code (LIC) 64.2 o superiore.

Data Encryption for IMS and DB2 Database Solution

L'IBM Data Encryption per database IMS e DB2 offre uno strumento di crittografia dati per database IMS e DB2 per z/OS in un solo prodotto. La soluzione è progettata per consentirvi di proteggere i dati sensibili e privati a livello di segmento per i database IMS e a livello di riga per i database DB2. L'IBM Data Encryption per database IMS e DB2 viene implementata tramite uscite IMS e DB2 standard che richiamano l'hardware di crittografia z Systems per crittografare i dati per lo storage e decrittografarli per l'uso applicativo.

Tutte queste soluzioni offrono svariate funzionalità di crittografia, ciascuna progettata per proteggere specifici elementi dell'ambiente. Per valutare quale di queste soluzioni di crittografia sia la più adatta ai vostri requisiti di sicurezza, contattate il vostro rappresentante di vendita IBM di fiducia o un BP locale per maggiori informazioni.

Requisiti hardware:

Le funzioni Encryption Services e DFSMSdss Encryption di Encryption Facility for z/OS vengono eseguite sui seguenti server IBM:

- IBM z13
- IBM zEnterprise EC12 (zEC12) o zBC12
- IBM zEnterprise 196 (z196) o z114
- IBM System z10 Enterprise Class (z10 EC) o z10 BC
- IBM System z9 Enterprise Class (z9 EC) o z9 BC.

Le opzioni di crittografia hardware prevedono i seguenti requisiti minimi riportati nell'annuncio IBM per gli Stati Uniti 207-008, datato 16 gennaio 2007

Per ulteriori informazioni consultate il seguente annuncio: **ibm.com**/common/ssi/rep_ca/8/897/ENUS207-008/ENUS207008.PDF

Ulteriori informazioni

Per ulteriori informazioni sulla sicurezza mainframe IBM visitate il seguente sito: **ibm.com**/systems/z/security/

IBM Italia S.p.A
Circonvallazione Idroscalo
20090 Segrate (Milano)
Italia

La home page IBM è disponibile all'indirizzo **ibm.com**/it

Si prega di riciclare

ZSD01450-ITIT-04