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

Sichere Datenübertragung für Ihr Unternehmen

Highlights

- Bietet eine äußerst sichere Datenübertragung mit Partnern, Lieferanten und Kunden
- Ermöglicht die Verschlüsselung mit Schlüsselverwaltung für Band und Platte
- Kann große Datenmengen zur Remote-Archivierung verschlüsseln
- Nutzt Schlüsselverwaltungsfunktionen von IBM® z/OS
- Ermöglicht eine langfristige Schlüsselverwaltung für archivierte Daten an Remote-Standorten
- Bietet erhöhte Flexibilität mit Unterstützung des OpenPGP-RFC 4880 Formats
- Unterstützt Komprimierung mit den ZIP- und ZLIB-Algorithmen und nutzt z Data Compression (zEDC), sofern verfügbar.

Der Schutz sensibler Daten ist für Unternehmen auf der ganzen Welt von großer Bedeutung. Der Schutz kritischer Unternehmensdaten und Kundeninformationen ist so wichtig, dass seine Bedeutung bis in die Unternehmensspitze zu spüren ist, da ein mangelhafter Schutz von Gütern und Vermögenswerten zu hohen direkten Kosten und was noch wichtiger ist, zum Verlust von Kunden und dem Vertrauen der Anleger führen kann. Datenschutz kann auch gemäß brancheninternen oder gesetzlichen Regelungen und vertraglichen Verpflichtungen gegenüber Geschäftspartnern erforderlich sein. Unabhängig davon, ob Daten durch das Netzwerk oder auf einem Band in einem Fahrzeug durch die ganze Stadt übertragen werden, müssen sie vor unberechtigten Nutzern geschützt und rechtmäßigen Nutzern zugänglich sein.

Die IBM® Encryption Facility for z/OS® V1.2 kann Mainframe Encryption Services einsetzen, die seit über 20 Jahren zum Schutz von Geldautomaten eingesetzt werden, um ruhende Daten zu schützen. Kunden können die zentrale Schlüsselverwaltung von z/OS nutzen, um einen äußerst sicheren Austausch von Schlüsseln zu ermöglichen. Würden wichtige Inhalte, die für einen vertrauenswürdigen BP vorgesehen waren, in die falschen Hände gelangen, könnten die Daten erst mit dem privaten Schlüssel des Partners entschlüsselt werden.

Mit der IBM Encryption Facility for z/OS können Sie die Daten auf Ihrem z/OS System für den Transport zu Ihrem Partner oder Kunden verschlüsseln, selbst wenn diese nicht über ein z/OS System verfügen. Partner mit z/OS können die Encryption Facility, einen Java™-basierten Client, den Decryption Client for z/OS oder ein mit OpenPGP RFC 4880 kompatibles Programm einsetzen, um die Daten zu entschlüsseln.

Partner ohne z/OS können den Java-basierten Client oder ein mit OpenPGP RFC 4880 kompatibles Programm zum Entschlüsseln und Verschlüsseln von Daten einsetzen.

Die Encryption Facility for z/OS setzt sich aus zwei kostenpflichtigen optionalen Features zusammen:

- Das **Encryption Services Feature** unterstützt die Ver- und Entschlüsselung bestimmter Dateiformate unter z/OS. Mit diesem Feature können Sie Daten an Remote-Standorte Ihres Unternehmens oder an Partner und Lieferanten übertragen sowie archivieren. Das Encryption Services Feature bietet Unterstützung für das IBM z Systems-Format (mit Encryption Facility for z/OS V1.1 eingeführt) sowie für das OpenPGP-Format (mit Encryption Facility for z/OS V1.2 bereitgestellt). Das z Systems Format unterstützt hardware-beschleunigte Komprimierung vor der Verschlüsselung .
- Das **DFSMSdss-Encryption Feature** ermöglicht die Verschlüsselung von DFSMSdss-Speicherauszugsdateien. Dieses Feature unterstützt hardware-beschleunigte Komprimierung vor der Verschlüsselung.

State-of-the-art-(SOTA-)Verschlüsselung und zentrale Schlüsselverwaltungsfunktionen, die von z/OS und den z Systems Servern bereitgestellt werden, unterstützen den Schutz der Daten.

Encryption Services Feature

z Systems Format

Das Encryption Services Feature ermöglicht es Ihnen, Daten zu verschlüsseln, so dass sensible Daten plattformübergreifend mit Partnern, Lieferanten und Kunden ausgetauscht werden können. Sie können das Encryption Services Feature auch zur Verschlüsselung bestimmter Dateien für die Archivierung verwenden. Diese Funktion kann die Schlüsselverwaltung von z/OS und die Zugriffsauthentifizierung verwenden, die im Rahmen der Integrated Cryptographic Services Facility (ICSF) bereitgestellt wird, sowie die Hardwarekomprimierung und die hardwareunterstützten kryptografischen Funktionen der z Systems Server.

Das Encryption Services Feature unterstützt die Datenverschlüsselung mit TDES-Schlüsseln (dreifache Länge) oder 128-Bit AES (Advanced Encryption Standard) Schlüsseln. RSA (Rivest Shamir Adleman) öffentliche/private Schlüssel können als Key Wrap spezifiziert werden, um die AES- und TDES Schlüssel, die für die Verschlüsselung der Datei verwendet wurden, zu ver- oder entschlüsseln. Die durch Key Wrap geschützten Schlüssel werden im Datei-Header gespeichert. Mit dieser Technik können sehr viele Dateien unter Verwendung verschiedener Schlüssel erzeugt werden und sollten auch nach Jahren der Archivierung noch lesbar sein. Das Encryption Services Feature unterstützt auch die Verwendung eines Kennwort-Schlüsselderivationssystems.

Das Encryption Services Feature unterstützt Eingaben von physischen sequenziellen Eingabedateien, von Membern partitionierter Dateien (partitioned data sets, PDS) und erweiterten partitionierten Dateien (PDSE) sowie von Dateien, die in z/OS UNIX® System Services Dateisystemen abgelegt wurden. Die Eingabedateien können vor der Verschlüsselung und dem Schreiben der Ausgabedateien komprimiert werden. Durch Verwendung des Large Block Interface zur Ausgabe von Dateien, die auf Band geschrieben wurden, kann das Encryption Services Feature auch zur Optimierung von Leistung und Platzbedarf für Speichermedien beitragen.

OpenPGP RFC4880 Format
Mit der Einführung der V1.2 unterstützt die Encryption Facility for z/OS jetzt auch das OpenPGP-Format. OpenPGP-Unterstützung bietet noch mehr Auswahl und Flexibilität für den Datenaustausch mit BPs. Die OpenPGP Unterstützung der Encryption Facility wird den Anforderungen des OpenPGP-Standards gerecht und ist mit anderen, OpenPGP-(RFC 4880-)konformen Produkten kompatibel. So können Sie verschlüsselte, komprimierte und/oder digital signierte Dateien zwischen Ihren internen Rechenzentren (RZ) sowie mit externen Geschäftspartnern (BP) und Lieferanten austauschen, die einen OpenPGP-(RFC 4880-)konformen Client auf z/OS und einem anderen Betriebssystem (OS) betreiben. Die Encryption Facility OpenPGP Unterstützung beinhaltet eine große Zahl neuer Funktionen, wie z. B. Passphrase-basierte Verschlüsselung eines zufällig generierten Session-Schlüssels, asymmetrische Verschlüsselung eines nach dem Zufallsprinzip generierten symmetrischen Schlüssels mittels RSA- und ElGamal-Algorithmen, digitale Signaturen von Daten und eine Reihe weiterer Funktionen, die ausgehend von Ihrer Betriebsumgebung und Ihren Anforderungen wichtig sein können.

Die Unterstützung für das z/OS V1.2 OpenPGP-Format nimmt mehr CP-Kapazität als die Unterstützung der Encryption Facility für das z Systems Format in Anspruch. Die Encryption Facility kann dabei jedoch so konfiguriert werden, dass mehrere CPs genutzt und dadurch eine parallele Verarbeitung ermöglicht wird. Die Auswirkungen der verstärkten CPU-Auslastung für die OpenPGP-Formatunterstützung der Encryption Facility können durch die Nutzung der z Integrated Information Processor (zIIP) Prozessoren auf z13 und der zIIP zEnterprise Application Assist Processors (zAAP) Prozessoren der früheren Generationen reduziert werden. Da die OpenPGP-Formatunterstützung in Java geschrieben ist und Java-Workloads für den Spezialprozessor zulässig sind, sind Softwareeinsparungen möglich. Bei manchen Konfigurationen, wie z. B. einer Konfiguration mit vier oder mehr Online-CPUs, kann sich daher der Einsatz der Encryption Facility für das OpenPGP-Format im Vergleich zur Encryption Facility für das z Systems Format positiv auf die Verarbeitungszeit auswirken.

Diese Funktionen können die Integrated Cryptographic Services Facility (ICSF) und Hardware-Kryptografie nutzen. Die Hardware-Kryptografie setzt eine entsprechende Umgebung und eventuell ein installiertes kryptografisches Modul voraus.

Die Encryption Facility for z/OS V1.2 ist auf derzeit unterstützten z Systems und z/OS Releases verfügbar.

DFSMSdss Encryption Feature

Das Data Facility Storage Management Subsystem (DFSMSdss) Encryption Feature kann die Verschlüsselung von DFSMSdss-Speicherauszugsdateien auf Band oder Platte ermöglichen. Diese Funktion dient zur Nutzung der z/OS Schlüsselverwaltung und Zugriffsauthentifizierungsfunktionen sowie der hardwareunterstützten Kryptografie und Komprimierungsfunktionen von z Systems.

DFSMSdss Encryption unterstützt die Datenverschlüsselung mit TDES Schlüsseln (dreifache Länge) oder 128-Bit AES-Schlüsseln. Wie das Encryption Services Feature unterstützt auch dieses Feature die Verwendung von RSA öffentlichen/privaten Schlüsseln als Key Wrap für AES und TDES Datenschlüssel zur Verschlüsselung von Dateien sowie die AES- und TDES-Schlüsselgenerierung mit einem bestimmten Kennwort. Sie können auch festlegen, dass DFSMSdss Daten vor der Verschlüsselung komprimiert.

Das DFSMSdss Encryption Feature umfasst zwei Funktionen, eine für die Datenverschlüsselung während der Verarbeitung eines DUMP-Befehls und die andere zur Datenentschlüsselung während der Verarbeitung eines RESTORE-Befehls.

Encryption Facility for z/OS Client unter Verwendung des z Systems Format
Der Encryption Facility for z/OS Client ist ein getrennt lizenziertes Programm, das ohne jegliche Gewährleistung zur Verfügung gestellt wird. Es ermöglicht den Austausch verschlüsselter Daten zwischen z/OS Systemen, auf denen die Encryption Facility installiert ist sowie zwischen Systemen, die auf z/OS oder anderen Plattformen mit den erforderlichen Funktionen ausgeführt werden.

Der Encryption Facility for z/OS Client setzt sich folgendermaßen zusammen:

- **Java-basierter Client.** *Der Java-basierte Client kann sowohl unter z/OS als auch jeder anderen Plattform, die Java unterstützt, eingesetzt werden.* Der Java-basierte Client unterstützt sowohl die Entschlüsselung von Daten, die im Encryption Facility z Systems Format auf einem z/OS-System verschlüsselt wurden, als auch die Verschlüsselung von Daten, die an ein z/OS-System gesendet werden sollen, wo sie mit Hilfe des Encryption Facility z Systems Formats entschlüsselt werden. Anmerkung: Daten, die mit dem Java-basierten Client verarbeitet werden sollen, können nicht mittels Komprimierung erstellt werden.
- **Decryption Client for z/OS.** *Der Decryption Client for z/OS wird nur auf z/OS-Systemen unterstützt.* Der Decryption Client for z/OS unterstützt die Entschlüsselung von Daten, die im Encryption Facility z Systems Format auf einem z/OS-System verschlüsselt wurden. Daten, die mit dem Decryption Client for z/OS verarbeitet werden sollen, können mittels Komprimierung erstellt werden. Der Decryption Client bietet keine Unterstützung zur Verschlüsselung von Daten für die Rücksendung. Diese Option zeichnet sich durch bessere Leistungseigenschaften aus und kann den Einsatz wenigerer Medien für den Datenaustausch erforderlich machen. Sie ermöglicht es Ihren BP jedoch nicht, die Daten in einem verschlüsselten Format an Sie zurückzusenden.

Der Wert von Mainframe-Verschlüsselung

IBM Mainframe Encryption Services basieren auf Hardware- und Software-Integration: der Verschlüsselungs- und Kompressionstechnologien der Mainframe-Server und der zentralen Schlüsselverwaltungsfunktionen des z/OS Betriebssystems.

Die Manframe Verschlüsselungs-Hardware bietet zwei Schlüssel-Funktionen: Sie ermöglicht die Beschleunigung der Verschlüsselung im Vergleich zu Software-basierter Verschlüsselung und beinhaltet mit den entsprechenden Funktionen auch Secure Key Services. Hochleistungsfähige Verschlüsselungsbeschleunigung wird durch die CP Assist for Cryptographic Function (CPACF) ermöglicht, die in die zentralen Prozessoren der IBM z Systems Server integriert ist. Auf dem IBM System z10® Enterprise Class Server (z10 EC®) und neueren Modellen wurden unter anderem zusätzliche Erweiterungen wie die Unterstützung des SHA-512-Hash-Algorithmus und bis hin zum 256 Bit Advanced Encryption Standard (AES-256), der sich schnell zu einem De-facto-Standard für Verschlüsselung entwickelt, integriert.

Die optionalen Features Crypto Express2, Crypto Express3, Crypto Express4 und Crypto Express5 bieten die Secure Key Technologien, die einen vertrauenswürdigen Austausch mit öffentlichen und privaten Schlüsseln ermöglichen. Secure Key ist wichtig für Bankfunktionen, wie die Kommunikation zwischen Host und Geldautomat. Crypto Express2 unterstützt Triple-DES und Trusted Key Entry und bietet so Secure Key Optionen. Crypto Express3 unterstützt Triple-DES und AES 128-, 192- und 256-Bit-Verschlüsselung. Die neueste Generation Crypto Express5 bringt eine verbesserte Performance mit, die von der z/OS Encryption Facility zusammen mit den Leistungsverbesserungen der z13 CPACF genutzt werden kann.

Die ICSF Funktion von z/OS stellt die Schnittstelle zwischen den Anwendungen, die Verschlüsselung benötigen, und den Hardwareverschlüsselungsdiensten bereit. ICSF hat sich seit über 20 Jahren bei Mainframe Kunden weltweit im Einsatz bewährt und unterstützt Unternehmen dabei, Verschlüsselungscodes zu schützen und zu verwalten. Dies beinhaltet die Generierung von Schlüsseln, die Verwaltung von Schlüsseln auf der Basis von Kundenrichtlinien und die Wiederherstellung von Schlüsseln. Ein weiteres wichtiges Merkmal von ICSF ist die Möglichkeit, bei einer Überprüfung Informationen zur Einhaltung gesetzlicher Vorschriften und zu Zugriffskontrollen bereitzustellen.

Diese Verschlüsselungsfunktionen werden durch die Ausfallsicherheit und Verfügbarkeit des IBM Mainframe zusätzlich erweitert. Die Hochverfügbarkeit (HA), Skalierung, Widerstandsfähigkeit und die Möglichkeit zur Remote-Wiederherstellung des Mainframe macht sie zur besten Wahl für die Speicherung und Verwaltung von Verschlüsselungscodes. Die Verschlüsselungsfunktionen der IBM-Mainframe Server kann zusammen mit den integrierten Sicherheitsfunktionen des z/OS Betriebssystems dazu beitragen, eine hervorragende Grundlage für langfristige Schlüsselverwaltung zu schaffen. Die Encryption Facility for z/OS (V1.2) ist darauf ausgelegt, ein umfassendes Konzept für die Datenverschlüsselung auf Band und/oder Platte zu bieten.

Andere IBM Verschlüsselungsfunktionen

IBM bietet eine breite Palette von Verschlüsselungslösungen, die entwickelt wurden, um Ihren Anforderungen an die Datensicherheit zu entsprechen.

IBM System Storage Solution
Die IBM System Storage® TS1120 Bandlaufwerke und die neueren Modelle bieten leistungsstarke flexible Datenspeicherung mit Unterstützung für Datenverschlüsselung. Diese Verschlüsselungsfunktion ist standardmäßig auf allen neu bestellten TS1120 Bandlaufwerken oder neueren Modellen integriert. Bei aktivierter Verschlüsselung bieten die TS1120-Bandlaufwerke und neueren Modelle eine Datenschutzlösung, die die Verschlüsselungsfunktion vom Server auf das Bandlaufwerk auslagert (wodurch Server Overhead vermieden wird) und so eine kostengünstige Verschlüsselungslösung für die Archivierung und Sicherung großer Datenmengen darstellt. Bei Einsatz mit z/OS kann das TS1120-Bandlaufwerk oder ein neueres Modell zudem die Vorteile der herausragenden Sicherheits- und Verschlüsselungsfunktionen von z Systems nutzen und so eine leistungsstarke Lösung für die unternehmensweite Schlüsselspeicherung und -verwaltung bieten.

IBM Security Key Lifecycle Manager (ISKLM)
IBM Security Key Lifecycle Manager (ISKLM) for z/OS arbeitet mit verschlüsselungsfähigen Bandlaufwerken und System Storage Einheiten von IBM. ISKLM unterstützt die Erzeugung, den Schutz, die Speicherung und die Verwaltung von Verschlüsselungscodes, die für die Verschlüsselung von auf Einheiten zu schreibenden Daten und die Entschlüsselung der von dort zu lesenden Daten verwendet werden. ISKLM bietet ein Command Line Interface (CLI) zur Verwaltung der Schlüssel für diese Einheiten. Außerdem unterstützt ISKLM for z/OS die Bandlaufwerke 3592 und Linear Tape-Open® (LTO®) mit aktivierter Verschlüsselung. Die folgenden Laufwerkstypen werden unterstützt:

- TS1120, TS1130 und TS1140 Bandlaufwerke mit aktivierter Datenverschlüsselung
- Für LTO Ultrium® 4 und LTO Ultrium 5 Bandlaufwerke mit aktivierter Datenverschlüsselung wird die Verschlüsselung bei voller Leitungsgeschwindigkeit nach Komprimierung im Bandlaufwerk durchgeführt.

ISKLM for z/OS unterstützt zudem den IBM DS8000® Storage Controller mit der entsprechenden Mikrocode Bundle-Version auf dem DS8000 Storage Controller, Lizenzierter interner Code (LIC) Level 64,2 oder höher.

Data Encryption for IMS and DB2 Database Solution
IBM Data Encryption for IMS® and DB2® Databases bietet Ihnen ein Datenverschlüsselungstool für sowohl IMS als auch DB2 für z/OS Datenbanken in einem einzigen Produkt. Dieses Produkt ist so konzipiert, dass es Ihnen den Schutz von vertraulichen und persönlichen Daten für IMS auf Segmentebene und für DB2 auf Zeilenebene ermöglicht. IBM Data Encryption for IMS and DB2 Databases erfolgt über Standard IMS- und DB2-Exits, die die kryptografische Hardware von z Systems zur Datenverschlüsselung für die Archivierung und Datenentschlüsselung für die Anwendungsnutzung aufrufen.

Alle diese Lösungen bieten Ihnen eine Vielzahl von Verschlüsselungsmöglichkeiten, die jeweils zum Schutz spezifischer Elemente Ihrer Umgebung konzipiert sind. Um zu bewerten und zu bestimmen, welche dieser Verschlüsselungslösungen am besten geeignet ist, um Ihren Sicherheitsanforderungen gerecht zu werden, wenden Sie sich bitte für weitere Informationen an Ihren IBM Vertriebsbeauftragten oder den BP vor Ort.

Hardwarevoraussetzungen:

Die Encryption Services und die DFSMSdss Encryption Features der Encryption Facility for z/OS können auf den folgenden IBM Servern ausgeführt werden:

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

Die Hardware-Kryptografie-Optionen haben die folgenden Mindestanforderungen gemäß der IBM Deutschland Ankündigung 207-008 vom 16. Januar 2007

Bitte lesen Sie die folgende Ankündigung für Einzelheiten dazu: **ibm.com**/common/ssi/rep_ca/8/897/ENUS207-008/ENUS207008.PDF

Weitere Informationen

Weitere Informationen zur Sicherheit von IBM Mainframes finden Sie unter: **ibm.com**/systems/z/security/

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter **ibm.com**

ZSD01450-DEDE-04