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

为企业提供安全的数据传输

要点

- 让您与合作伙伴、供应商和客户进行高度安全的数据传输
- 通过磁带和磁盘的密钥管理支持加密
- 支持远程站点档案的高容量数据加密
- 利用 IBM z/OS 密钥管理功能
- 支持远程站点归档数据的长期密钥管理
- 通过支持 OpenPGP RFC 4880 格式提高灵活性
- 支持采用 ZIP 和 ZLIB 算法以及适用时利用 z Data Compression （zEDC） 进行的压缩

敏感数据保护是全球各个公司普遍关注的问题。确保关键业务数据和客户信息安全非常重要，已引起公司董事会的注意，这是因为未能保护这些资产可以招致高昂的现付成本，更重要的是，可能还会导致客户流失和投资者信心丧失。行业或政府法规及与业务合作伙伴的合同义务中可能也要求数据保护。数据无论是在网络上移动还是存储在磁带上利用卡车在城镇中运送，都必须受到保护，以免未经授权的用户访问并确保目标用户易于访问。

IBM® Encryption Facility for z/OS® V1.2 可以采用大型机加密服务来保护静态数据，这种服务 20 多年来一直帮助保护 ATM。客户可以使用 z/OS 集中式密钥管理提供高度安全的加密密钥交换。如果提供给可靠业务合作伙伴的重要内容落入他人之手，只有采用该合作伙伴所掌握的私有加密密钥才能解密该数据。

凭借 IBM Encryption Facility for z/OS，您可以在 z/OS 系统上加密数据以传输给合作伙伴或客户，即使他们不具有 z/OS 系统也能如此。拥有 z/OS 的合作伙伴可以选择使用 Encryption Facility、

Java-based Client、Decryption Client for z/OS 或符合 OpenPGP RFC 4880 的程序解密数据。没有 z/OS 的合作伙伴可以使用基于 Java 技术的客户端或符合 OpenPGP RFC 4880 的程序解密和加密数据。

Encryption Facility for z/OS 包含两种已定价的选配特性：

- **Encryption Services** 特性支持在 z/OS 上加密和解密某些文件格式。这使您能够将文件传输至企业内的远程站点、合作伙伴和供应商，或对它们进行归档。Encryption Services 特性既支持 IBM z Systems™ 格式（最初在 Encryption Facility for z/OS V1.1 中推出），又支持 OpenPGP 格式（凭借 Encryption Facility for z/OS V1.2 推出）。z Systems 格式支持加密前的硬件加速压缩。
- **DFSMSdss™ Encryption** 特性能够加密 DFSMSdss 转储数据集。此特性支持加密前的硬件加速压缩。

z/OS 功能和 z Systems 服务器特性提供领先加密和集中式密钥管理功能，有助于保护数据安全。

Encryption Services 特性

z Systems 格式

Encryption Services 特性可以使您对有助于跨平台与合作伙伴、供应商和客户共享敏感信息的数据进行加密。您还可以使用 Encryption Services 特性加密某些要归档的文件。该特性可以使用 Integrated Cryptographic Services Facility （ICSF） 中提供的 z/OS 密钥管理和访问认证功能以及 z Systems 服务器的硬件压缩和硬件加密功能。

Encryption Services 特性支持使用 TDES 三倍长密钥或 128 位 AES 密钥进行数据加密。RSA 公钥/私钥可用于封装和解封用于加密文件的 AES 和 TDES 数据密钥。封装的密钥将存储在文件头中。这种技术可以使用不同的加密密钥生成很多文件，且每种文件都有望在归档存储数年后依然能够阅读。Encryption Services 特性还支持采用密码密钥派生机制。

Encryption Services 特性支持通过物理序列输入文件、分区数据集（PDS） 中的成员和分区数据集拓展 （PDSE） 数据集以及存储在 z/OS UNIX System Services 文件系统上的文件进行输入。它可以压缩输入文件，然后对它们进行加密并写入输出文件。通过将大型块级接口用于写入磁带的输出文件，Encryption Services 特性还可以帮助优化性能和介质空间。

OpenPGP RFC4880 格式
由于 V1.2 的推出，Encryption Facility for z/OS 现在可以支持 OpenPGP 格式了。OpenPGP 支持为进行业务合作伙伴数据交换提供更多选择和灵活性。Encryption Facility OpenPGP 支持旨在符合 OpenPGP 标准要求并与符合 OpenPGP （RFC 4880） 的其他产品相兼容。这种支持使您与外部业务合作伙伴和供应商（安装有在 z/OS 和其他操作系统上运行且符合 OpenPGP （RFC 4880） 的客户端）一起，使用 Encryption Facility 提供的 OpenPGP 支持在内部数据中心之间交换经过加密、压缩且/或数字签署的文件。Encryption Facility OpenPGP 支持包括一长串新功能，例如随机生成的会话密钥基于密码的加密、使用 RSA 和 ElGamal 算法随机生成的对称密钥进行的不对称加密、数据的数字签名以及可能非常重要的若干其他功能（基于您的操作环境和要求）。

Encryption Facility for z/OS V1.2 OpenPGP 格式支持将比 Encryption Facility z Systems 格式支持占用更多 CP。它可以进行配置，以通过增加并行处理利用多个 CP。Encryption Facility for OpenPGP 格式支持导致 CUP 利用率提高，由此造成的影响可以通过 z13 上的 z Integrated Information Processor （zIIP）处理器以及前几代产品上的 zIIP 和 zEnterprise Application Assist Processors （zAAP） 处理器加以降低。由于 OpenPGP 格式支持采用 Java 写入，而 Java 工作负载符合专用引擎处理器的要求，您可以实现潜在的软件节约。因此，对于某些配置来说，例如具有 4 个或更多在线 CPU 的配置，就处理一项任务所需的时间而言，OpenPGP 支持可能优于 Encryption Facility z Systems 格式支持。

上述功能可以利用 ICSF 和硬件加密。硬件加密需要合适的环境，可能还需要安装加密模块。

Encryption Facility for z/OS V1.2 在目前受支持的 z Systems 和 z/OS 版本上提供。

DFSMSdss Encryption 特性

DFSMSdss Encryption 特性可以使您加密写入磁带和磁盘的 DFSMSdss 转储数据集。该特性旨在利用 z/OS 密钥管理和访问认证功能以及 z Systems 的硬件加密和压缩功能。

DFSMSdss Encryption 支持使用 TDES 三倍长密钥或 128 位 AES 密钥进行的数据加密。与 Encryption Services 特性一样，该特性支持使用 RSA 公钥/私钥封装和解封用于加密文件的 AES 和 TDES 数据密钥以及使用指定密码进行 AES 和 TDES 密钥生成。您还可以将 DFSMSdss 指定为在加密前压缩数据。

DFSMSdss Encryption 特性包含两种功能，一种是在处理 DUMP（转储）命令时加密数据，另外一种是在处理 RESTORE（还原）命令时解密数据。

采用 z Systems 格式的 Encryption Facility for z/OS Client
Encryption Facility for z/OS Client 是一款经过单独许可的程序（按原样提供，不带保证），旨在支持在已安装 Encryption Facility 的 z/OS 系统与在 z/OS 或需要受支持功能的其他平台上运行的系统间进行加密数据交换。

Encryption Facility for z/OS Client 包含下列特性：

- **Java-based Client**。Java-based Client 采用 Java 编写，可以在 z/OS 和任何支持 Java 的平台上使用。Java-based Client 既支持解密在 z/OS 系统上采用 Encryption Facility z Systems 格式创建的数据，也支持加密拟发送至 z/OS 系统的数据（这种情况下，文件将采用 Encryption Facility z Systems 格式解密）。注：拟使用 Java-based Client 进行处理的数据不能采用压缩功能创建。
- **Decryption Client for z/OS.**Decryption Client for z/OS 仅在 z/OS 系统上才会受到支持。Decryption Client for z/OS 支持解密在 z/OS 系统上采用 Encryption Facility z Systems 格式创建的数据。拟使用 Decryption Client for z/OS 进行处理的数据不能采用压缩功能创建。Decryption Client 不支持回程数据加密。该选件可能具有性能优势，且需要较少的介质就能实现交换目的，但不允许业务合作伙伴以加密格式将数据返回给您。

大型机加密的价值

IBM 大型机加密服务基于硬件和软件集成，即大型机服务中的加密与压缩技术，以及 z/OS 操作系统中的集中式密钥管理功能。

大型机加密硬件提供两种重要功能：与基于软件的加密相比，它提供加密加速度，且凭借相应的特性提供安全密钥服务。高性能加密加速度在 IBM z Systems 服务器中央处理器中内置的 CP Assist for Cryptographic Function （CPACF）中提供。在 IBM System z10® Enterprise Class （z10 EC™）服务器和后续版本中，新的增强功能包括对 SHA-512 哈希算法乃至 256 位高级加密标准 （AES-256）（正快速发展成为实际上的加密标准）的支持。

Crypto Express2、Crypto Express3、Crypto Express4 和 Crypto Express5 选配特性提供支持使用公钥/私钥可靠交换的安全密钥技术。安全密钥对银行业务功能（比如主机到 ATM 的通信）来说非常重要。Crypto Express2 支持三重数据加密标准和 Trusted Key Entry，从而为您提供安全密钥选项。Crypto Express3 支持三重数据加密标准以及 AES 128、192 和 256 位数据加密密钥。最新一代 Crypto Express5 带来 z/OS Encryption Facility 可以利用的增强性能以及 z13 CPACF 中的性能提升。

z/OS 的 ICSF 功能为寻求加密的应用程序与硬件加密服务提供接口。随着全球大型机客户 20 多年久经验证的使用，ICSF 帮助企业保护和管理加密密钥。这包括密钥生成，按照客户策略管理密钥以及密钥恢复。ICSF 的另外一个特性是能够提供审计合规信息和访问控制。

IBM 大型机的弹性和可用性会进一步拓展上述加密功能。大型机的高可用性、规模、弹性和远程恢复功能使其成为了存储和管理加密密钥的合理选择。IBM 大型机服务器提供的加密功能，加上 z/OS 操作系统固有的安全性，可以帮助为长期密钥管理提供卓越的基础。Encryption Facility for z/OS （V1.2） 旨在为磁带和/或磁盘提供全面的数据加密方案。

其他 IBM 加密功能

IBM 现在提供广泛的加密解决方案，旨在满足您的数据保护需求。

IBM System Storage Solution

IBM System Storage® TS1120 或后来的磁带驱动器提供支持数据加密的高性能灵活数据存储。这种加密功能是所有最近订购的 TS1120 或后续磁带驱动器型号上的标配。TS1120 及支持加密的后续磁带驱动器旨在提供具有下列特征的数据保护解决方案：能够将加密功能从服务器转移到磁带驱动器上（避免服务器开销），并为数据归档和备份的大量数据提供经济高效的加密解决方案。与 z/OS 搭配使用时，TS1120 或后续磁带驱动器型号利用 z Systems 独特的安全和加密特性，为企业级的加密密钥存储和管理提供强大的解决方案。

IBM Security Key Lifecycle Manager (ISKLM)

IBM Security Key Lifecycle Manager （ISKLM） for z/OS 与 IBM 支持加密的磁带驱动器和系统存储设备协同工作。对于对写入设备的信息进行加密和对从设备中读出的信息进行解密的加密密钥，ISKLM 帮助进行生成、保护、存储和维护。有一个命令行接口供您管理向这些设备提供的密钥服务。此外，ISKLM for z/OS 支持能够加密的 3592 和 Linear Tape-Open （LTO） 磁带驱动器。下列驱动器类型会受到支持：

- 支持数据加密的 TS1120、TS1130 和 TS1140 磁带驱动器
- 支持数据加密的 LTO Ultrium 4 和 LTO Ultrium 5 磁带驱动器。压缩后在磁带驱动器上以全线速进行加密。

ISKLM for z/OS 还凭借 DS8000 Storage Controller 上相应的微码包、许可内码级别 （LIC） 级别 64.2 或以上支持 IBM DS8000® Storage Controller。

Data Encryption for IMS and DB2 Database Solution

IBM Data Encryption for IMS® and DB2® Databases 在单一产品中向您提供同时适用于 IMS 和 DB2 for z/OS 数据库的数据加密工具。此产品旨在使您能够保护 IMS 分区级和 DB2 行级的敏感和私有数据。IBM Data Encryption for IMS and DB2 Databases 将通过标配 IMS 和 DB2 出口进行实施。标配 IMS 和 DB2 出口调用 z Systems 加密硬件对拟存储和供应用程序使用的数据进行加密。

上述所有解决方案向您提供各种加密功能，每种功能都旨在保护您环境中特定元素的安全。如要评估和确定上述哪项/哪些加密解决方案最能满足您的安全要求，请联系 IBM 销售代表或当地的业务合作伙伴来了解详情。

硬件要求：

Encryption Facility for z/OS 的 Encryption Services 和 DFSMSdss Encryption 特性可以在下列 IBM 服务器上运行：

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

硬件加密选件具有 2007 年 1 月 16 日发布的 IBM 美国公告 207-008 中提出的下列最低要求

请参阅下列公告以了解详情:
ibm.com/common/ssi/rep_ca/8/897/ENUS207-008/ENUS207008.PDF

如需更多信息

如需有关 IBM 大型机安全性的更多信息，请访问:
ibm.com/systems/z/security/

Integrated Marketing Communications,
Server Group
Route 100
Somers, NY 10589

2015 年 1 月