

FDRCRYPT ENCRYPTED BACKUPS

z/OS Storage Management



The protection of backup data is now required by many of today's government, industry and corporate privacy and security laws and regulations, such as the European Data Protection Directive, HIPAA, Sarbanes-Oxley, and DOD requirements, among others in Europe, the USA and other countries.

Data encryption now plays a key role in the protection of your backups – particularly any backups that are destined to go outside of your organisation...



Key Benefits

- Protect your FDR/ABR backups against unauthorised access...by encrypting the backup data using advanced and efficient encryption routines.
- Reduce the risk of data exposure due to lost, stolen and mislaid backup tapes.
- Protect your IDCAMS sequential copies of your data created with REPRO.



Hardware Encryption

FDRCRYPT and FDRCAMS support the following hardware encryption and hardware assists:

- AES hardware encryption on IBM z9 BC/EC processors (and their successors)
- TDES on z890, z990 and z9 processors (and their successors).
- The z/9 hardware assist (CPACF), which is a standard, no-cost feature on the z/9

Utilisation of these hardware instructions can significantly reduce the CPU and elapsed time overheads usually associated with encryption.



Software Encryption

In addition to the hardware encryption described above, FDRCRYPT and FDRCAMS also offer various types of software encryption of varying strength. This allows you to balance the sensitivity of the data with the additional cost in CPU and elapsed time to encrypt that data.



FDRCRYPT Encrypted Backups

FDRCRYPT can encrypt FDR and ABR backups, protecting those backups against unauthorised access by anyone who does not possess the proper encryption keys.

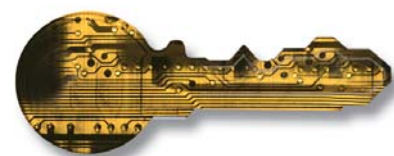
FDRCRYPT also supports master keys, which allow encrypted backups to be restored even if the individual keys are not available.



FDRCAMS Encrypted Sequential files

FDRCAMS is a sub-module included with FDRCRYPT, which acts as a front-end to IBM's IDCAMS and allows a REPRO command to encrypt its output sequential data sets and decrypt them when reading them back in again.

This allows sequential copies of your VSAM, IAM and PS files (created with IDCAMS REPRO) to be encrypted prior to shipment to other companies or government agencies.



FDRCRYPT ENCRYPTED BACKUPS



Encryption Algorithms

FDRCRYPT and FDRCAMs offer various levels of software encryption:

- **TDES** Triple Data Encryption Standard, uses the DES algorithm 3 times, with 3 different keys of 64 bits each (192 bits total) to encrypt the data.
- **AES** Uses a 128, 192 or 256-bit encryption key to do a repetitive transformation of the data. AES is the current standard for US government encryption.
- **CIPHER** also uses a substitution table, and then each byte is moved to a different location in the data block.

Innovation would make the following recommendations:

- z890 or z990 – use **TDES**
- z/9 or z/10 – use **AES128**
- Other – use **Cipher**

All encryption algorithms are implemented entirely within FDRCRYPT and FDRCAMs and do not depend on any other installed encryption hardware or software. This ensures that the data can be decrypted (by FDRCRYPT or FDRCAMs) at any disaster site.

FDRCRYPT encryption is supported on all full volume, incremental, application and data set backups created by FDR, ABR and FDRAPPL.

Key Management

FDRCRYPT includes secure key management. It generates a different key for each backup, thereby increasing the security on those backups. A master key, which is kept in a secure place and limited to a few trusted individuals, is available in the event that the key file is lost or destroyed.

RSA Keys

As an alternative to the standard master keys described above, FDRCAMs can optionally use an RSA “public” key. At decryption time, a matching RSA “private” key is then used to decrypt the encrypted key.

User Experience

“We use FDRCRYPT encryption on all our FDR/ABR backups that go offsite – even if they are just being moved to another secure location. We also use it on our IDCAMS REPROs when exchanging data with other organisations...”

“We use FDRCAMs to create an encrypted copy and Innovation provides our client a free copy of FDRDECRY to decrypt the tape. This allows us to send ENCRYPTED data to any of our clients regardless of the installed hardware or software they have...!”

Most Electronic Data Must be Protected by One or More of These Regulations:

FDRCRYPT will help you maintain compliance.

- HIPAA
- **PCI DSS**
- GLBA
- SOX 802
- ISO 17799 Int'l IT Security
- European Union Data Protection

*If you have credit card data, you must comply with **PCI DSS!***

FDRCRYPT provides encryption for full volume, incremental, archive, application and data set backups. FDRCAMs provides encryption for VSAM, Sequential and IAM datasets.

Want to Know More About FDRCRYPT? For a No-Obligation FREE Trial or to request a FREE Concepts & Facilities Guide, ask your local sales representative or visit: <http://www.innovationdp.fdr.com>



CORPORATE HEADQUARTERS: 275 Paterson Ave., Little Falls, NJ 07424 • (973) 890-7300 • Fax: (973) 890-7147
E-mail: support@fdrinnovation.com • sales@fdrinnovation.com • <http://www.innovationdp.fdr.com>

EUROPEAN OFFICES:	FRANCE 01-49-69-94-02	GERMANY 089-489-0210	NETHERLANDS 036-534-1660	UNITED KINGDOM 0208-905-1266	NORDIC COUNTRIES +31-36-534-1660
--------------------------	--------------------------	-------------------------	-----------------------------	---------------------------------	-------------------------------------