From the overview module, you should have an understanding of the encryption support that is provided in the tape drive. You should be familiar with how encryption is requested at the host, and the terminology used in the encryption solution. You should also have an understanding of the encryption management flow between the drive and the encryption key manager and the role of the new proxy interface in IOS.

This module goes into additional detail on the encryption flow and terminology with more detailed examples provided.

Agenda

- **Symmetric and asymmetric encryption**
- **Encrypted data exchange with a business partner**
- **Encryption flow**
  - Write from beginning of tape (BOT)
  - Read or append from tape

© 2007 IBM Corporation
ON DEMAND BUSINESS™

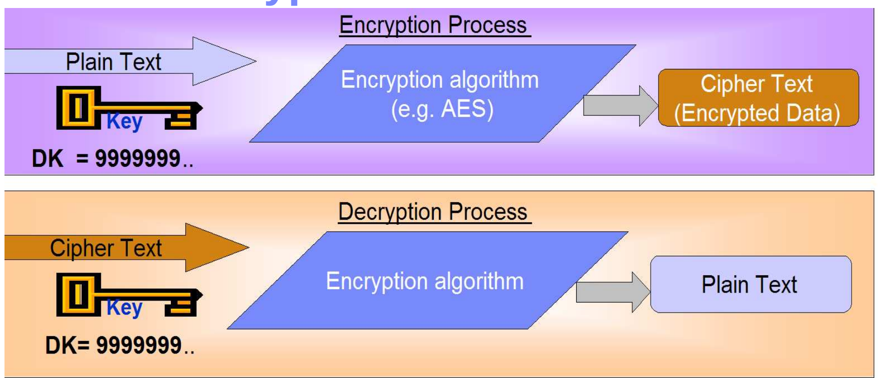
This module will start by going over symmetric and asymmetric encryption terminology with a discussion of how each plays a role in the 3592 Model E05 tape encryption support. Then it will walk you through a detailed example showing a business partner data exchange and what each company would have in its key store. You will see the steps involved in a write from the beginning of tape, followed by the steps involved in a tape read or an append.

IBM Systems & Technology Group

IBM

Symmetric encryption

For example, data key



- Data that is not encrypted – clear text
- Clear text is encrypted by processing with a “key” and an encryption algorithm
- Keys are bit streams
  - 128, 192, 256 bit key length
- Symmetric encryption – same key to encrypt and decrypt

© 2007 IBM Corporation

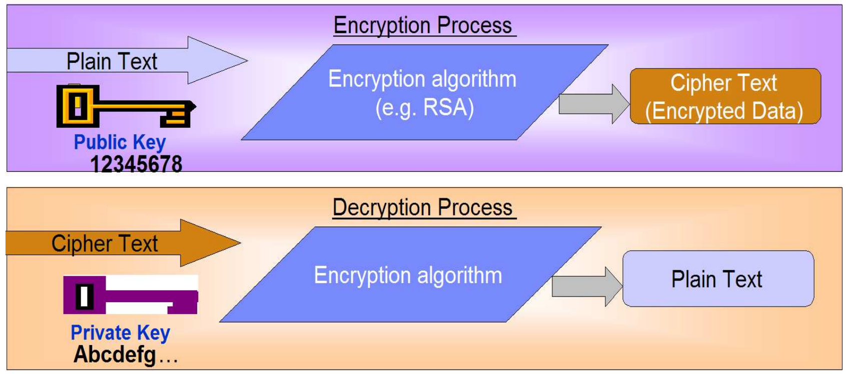
ON DEMAND BUSINESS™

The symmetric key also referred to as the “data key” in the tape encryption solution is used by the tape drive to encrypt and decrypt the data on the tape cartridge.

IBM Systems & Technology Group

Asymmetric encryption

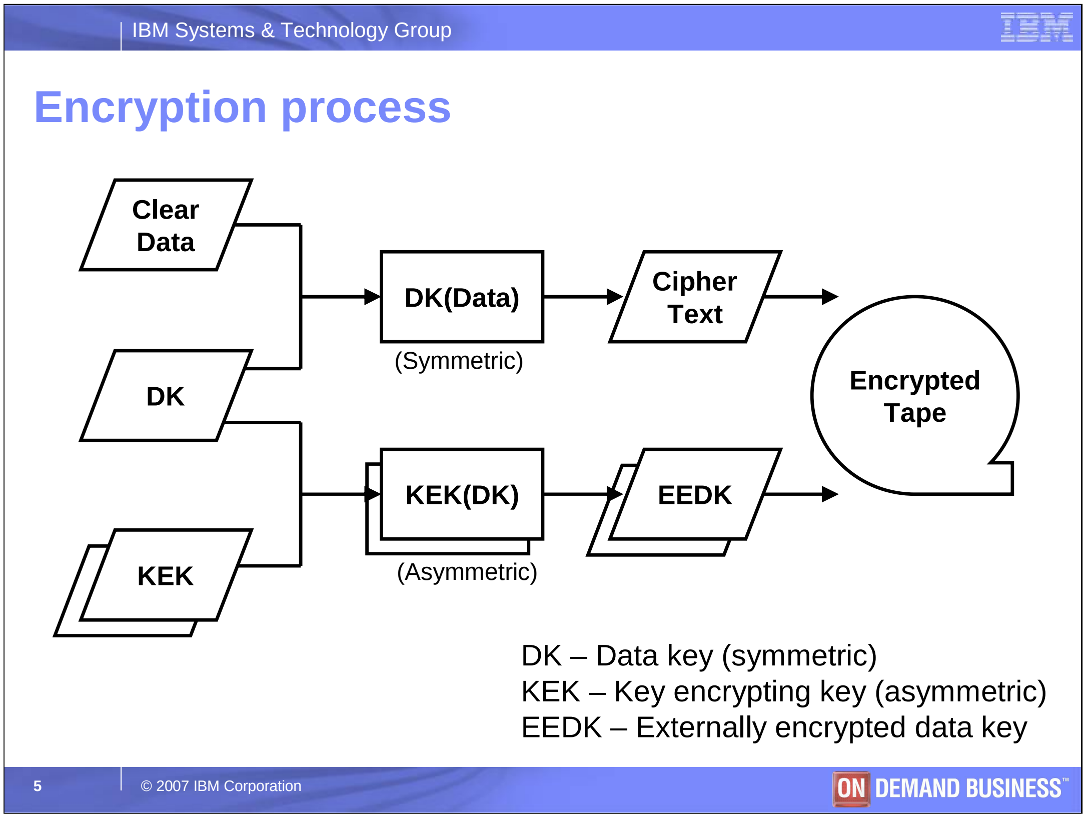
For example, key encrypting key (KEK)



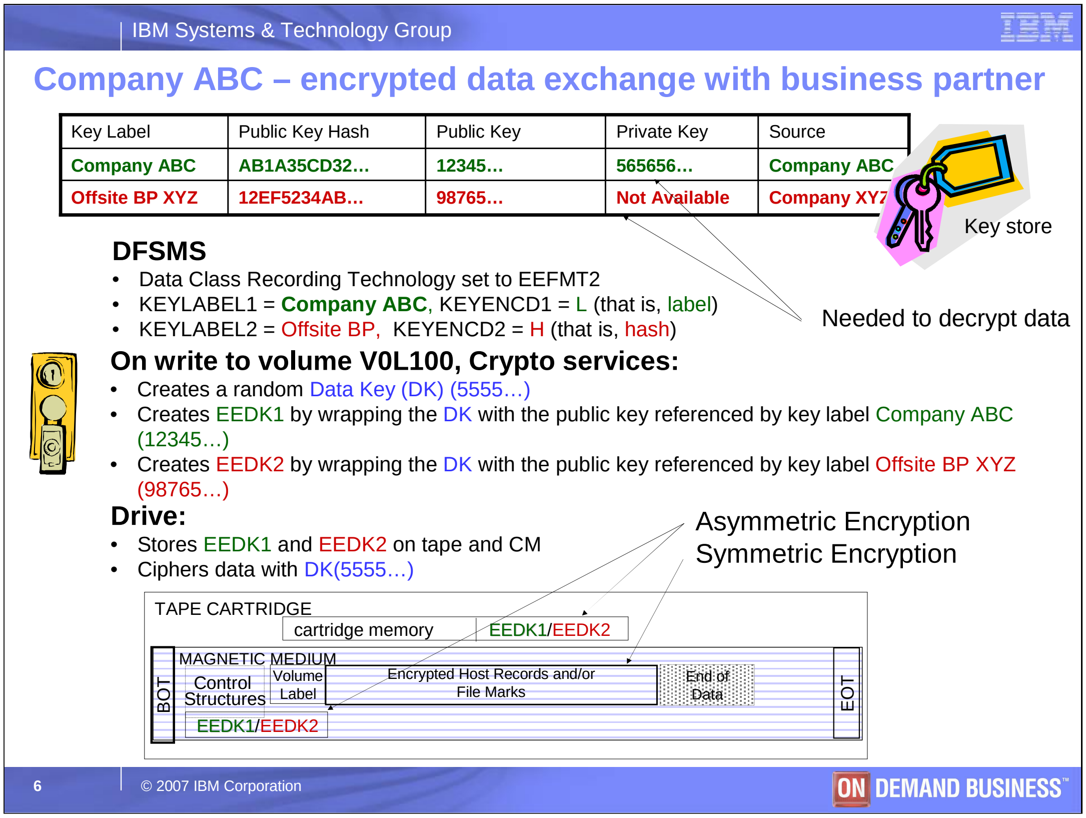
- The key used to encrypt is often referred to as the public key; for example, the KEKs used to wrap the DK and create the EEDKs.
- The public key may be made widely available without fear of compromise.
- The key used to decrypt is referred to as the private key.
- Private keys must be secured against unauthorized access.
- Public / private encryption is widely used for exchange of data between organizations.

4 © 2007 IBM Corporation ON DEMAND BUSINESS™

The asymmetric key also referred to as a public/private key pair is used in the tape encryption solution to encrypt “wrap” and decrypt the data key. The public key is used to encrypt the data key and the private key is used to decrypt the data key. The encrypted data key is stored on the tape cartridge in a structure referred to as the externally encrypted data key (EEDK).



This picture shows the role that the data key has in encrypting the data stored on the tape cartridge and the role that the key encrypting key plays in encrypting the data key. When the encryption process completes not only is encrypted data placed on the tape cartridge, but along with the data, the drive also stores the encrypted data key.



The example above shows “Company ABC” needing to write to tape cartridge VOL100 not only for its own use, but also for a business partner data exchange with company “Company XYZ”.

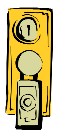
Company XYZ – encrypted data exchange with business partner

Key Label	Public Key Hash	Public Key	Private Key	Source
Offsite BP ABC	**AB1A35CD32…**	**12345…**	**Not Available**	**Company ABC**
Company XYZ	**12EF5234AB…**	**98765…**	**787878…**	**Company XYZ**

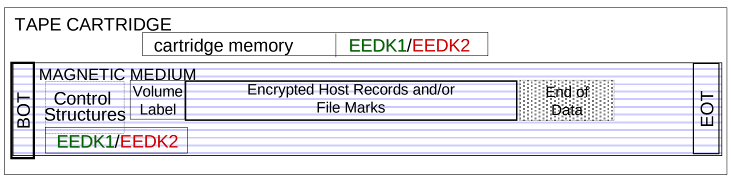
Key store

Key label for the same public key is different at BP

On read from volume VOL100:



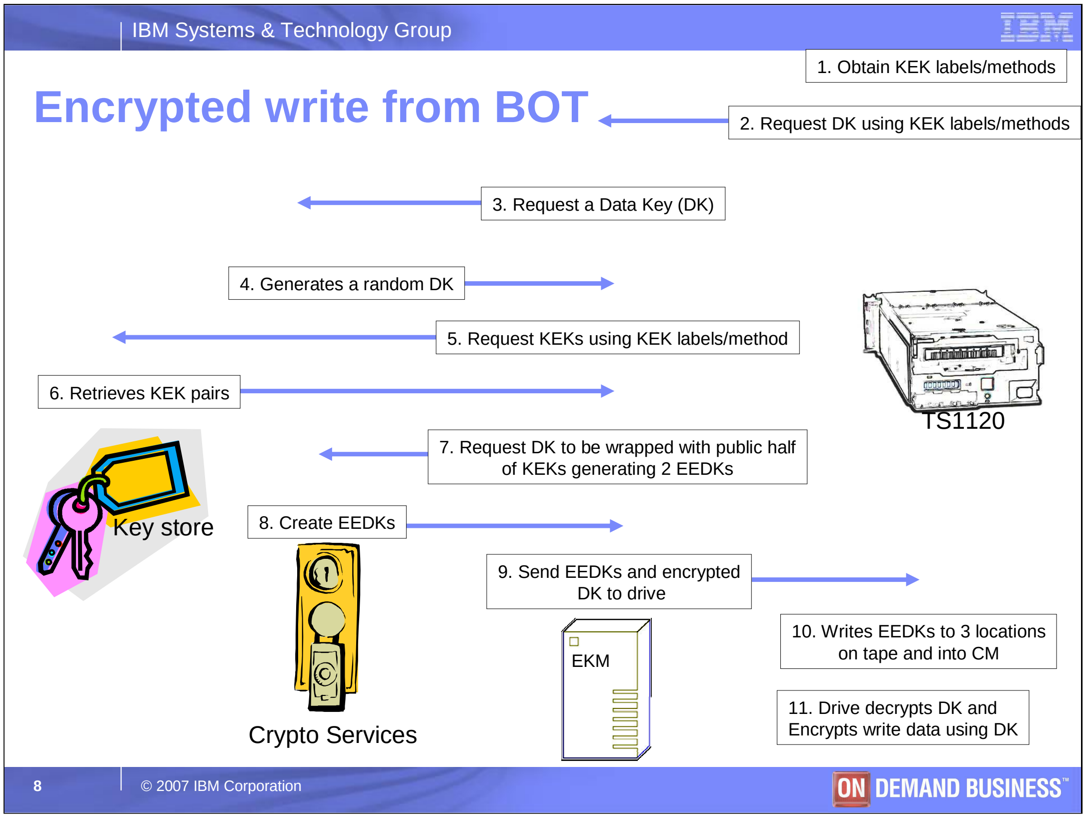
- Drive retrieves EEDK1 and EEDK2 from tape or CM
- Crypto Services attempts to unwrap DK from EEDK1 with the private key referenced by key label Offsite BP ABC. No match found in key store.
- Crypto Services attempts to unwrap DK from EEDK2 with the private key referenced by hash of key label Company XYZ (12EF5234AB…). Match found in key store.
- Drive deciphers data with DK(5555…)



 © 2007 IBM Corporation

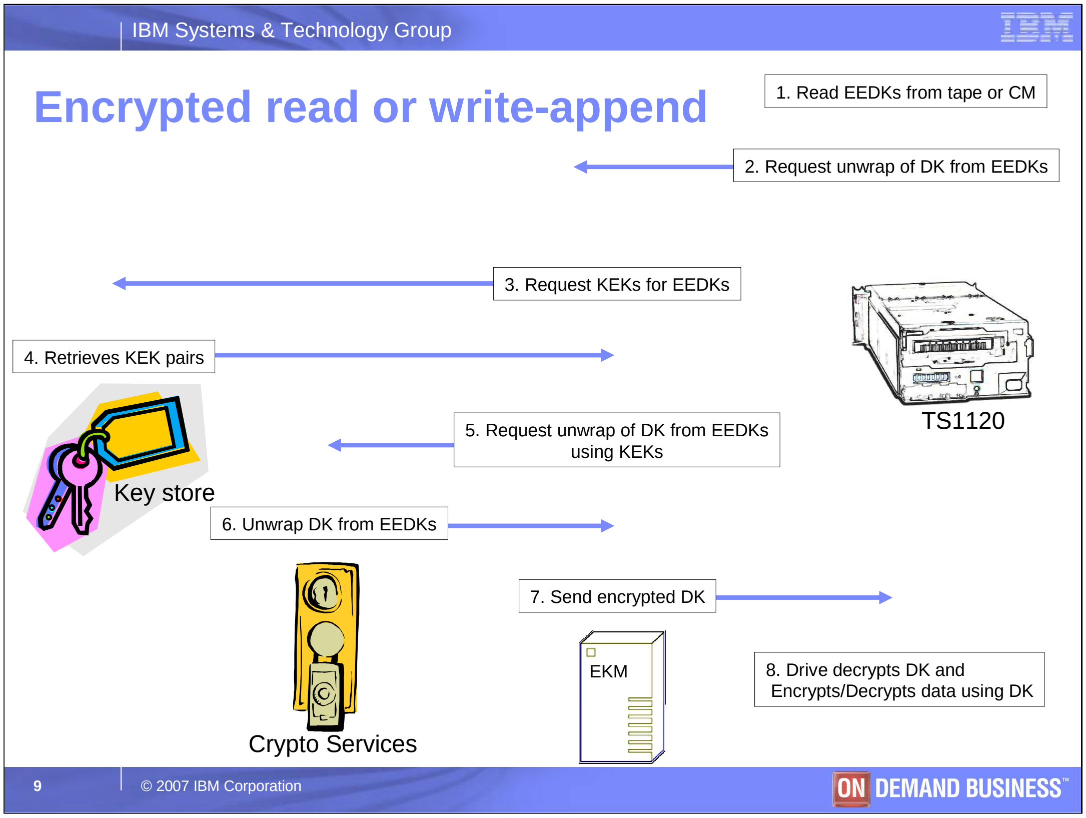
This example shows business partner “Company XYZ” reading the tape generated by “Company ABC”.

This slide and the last one illustrate different key labels referencing the public/private key pair in each of the key stores as “Company ABC” and “Company XYZ”. They also show that “hash” was used for the second key label’s encoding mechanism when the tape was originally created. Also illustrated is the fact that “Company ABC” would only have its business partner’s public key and never their corresponding private key in their own key store.



This is a high level view of some of the steps involved in an encrypted write. In this case the write is from the beginning-of-tape (BOT) and shows the roles that the tape drive, the EKM, crypto services and the key store play in the overall solution.

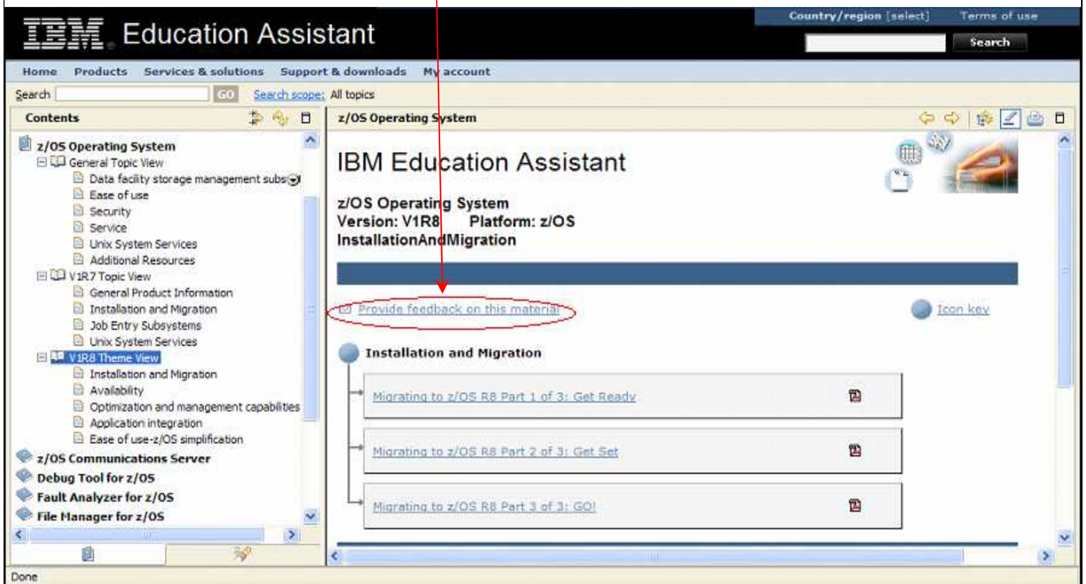
The flow starts from the top right corner with item #1 and proceeds through the numbered steps. In step 1, the host has indicated to the drive that encryption is requested and has passed any key encrypting key (KEK) labels to the drive. The drive then requests a data key (DK) from the key manager and passes the host specified key labels to the key manager. The key manager requests that a data key be generated. Crypto services generates a random data key that is then encrypted with the public key referenced by the passed key labels generating two EEDK structures. The EEDK structures are then sent to the drive to be stored on the tape cartridge along with an encrypted version data key that the drive can decrypt. The drive then decrypts the data key and encrypts the data using the generated data key.



This is a high level view of some of the steps involved in an encrypted read or write-append. It also shows the roles that the tape drive, the EKM, crypto services and the key store play in the overall solution. The flow starts from the top right corner with item #1 and proceeds through the numbered steps. In step 1, the drive detects that the data on the tape is encrypted and requests that the key manager unwrap the data key from the EEDK structures on the tape. The EEDK structures are passed to the key manager. The key manager, using the key label encoding mechanism information (label or hash) stored within the EEDK structures interacts with the key store to obtain the needed key encrypting key. Crypto services using the private key portion of the key encrypting key unwraps the data key from the EEDK structure. The key manager is able to send an encrypted version of this data key back to the drive that the drive can then decrypt. The drive then decrypts the data key and encrypts/decrypts the data on the tape cartridge.

Did you find this IBM Education Assistant module useful?

Provide feedback and specify the module title on your response.



 © 2007 IBM Corporation

In your feedback to IBM, answer these three questions:

How helpful was this IEA presentation? Give it a rating from 1 to 5 where 1 = very helpful and 5 = not at all helpful

Did this presentation save you a service call to IBM? Yes or No

What other topics would you like to see covered in z/OS IEA?

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

AIX*	IBM*	Tivoli*
DFSMS	IBM eServer	VM/ESA*
DFSMSrmm	IBM logo*	z/OS*
e-business logo	Redbooks*	z/VM*
ESCON*	System I	z/VSE
FICON*	System p	zSeries*
I5/OS*	System x	
I5/OS (logo)	System z	

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Intel is a registered trademark of the Intel Corporation in the United States, other countries or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

HP is a registered trademark of Hewlett-Packard Development Company, L.P.

Sun is a registered trademark of Sun Microsystems, Inc., in the United States and other countries.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

 © 2007 IBM Corporation