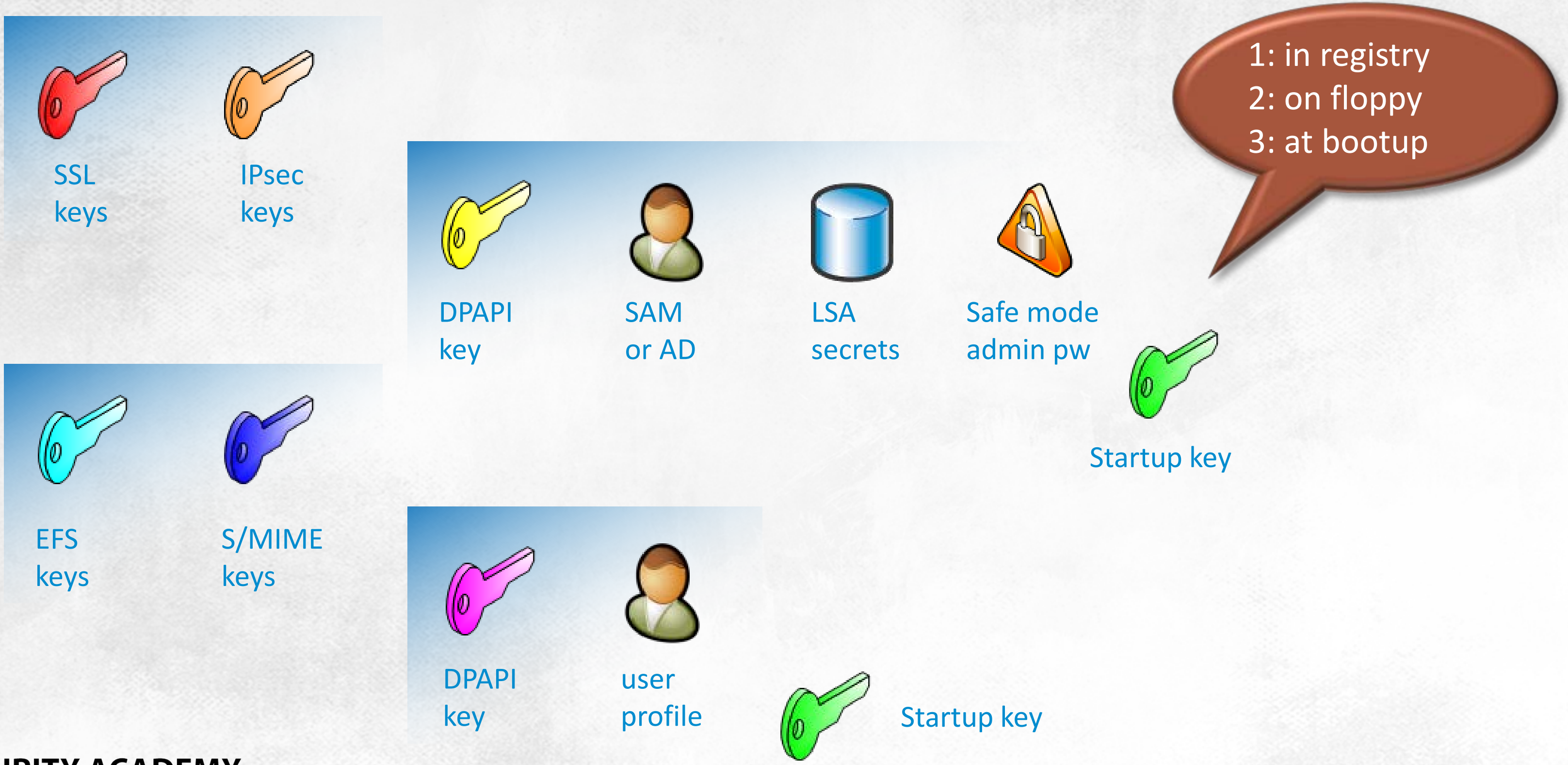
Encryption

Key protection in windows



SSL keys

IPsec keys

EFS keys

S/MIME keys

DPAPI key

SAM or AD

LSA secrets

Safe mode admin pw

Startup key

1: in registry
2: on floppy
3: at bootup

DPAPI key

user profile

Startup key

Drive Encryption

Introduction

Drive encryption should ensure data stored on encrypted disks is secure and confidential

Ciphertext security depends on these four factors:

- The confidentiality of decryption key
- The quality of encryption algorithm
- The length of the key used to encrypt data
- The length of a single data block and the way in which encrypted data is split into fixed-length blocks (block cipher mode)

Drive Encryption

Introduction

Drive encryption programs should:

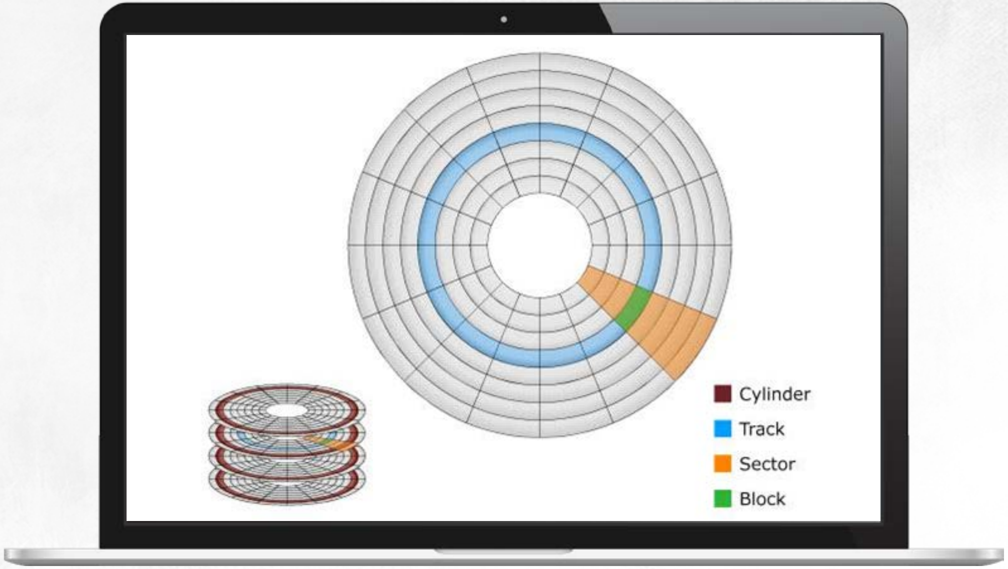
- Encrypt all hard drive sectors at writing and decrypt them at reading
- Encrypt and decrypt in real time, and the overall computer performance decrease should not exceed several per cent
    - A CPU takes from 50 to 100 clocks in the time needed to read one byte of data on a hard drive
    - Encryption/decryption per a byte cannot exceed 35 clocks
    - AES in CBC mode requires about 20 cycles/byte
    - The diffuser used in BitLocker needs 10
    - In most cases performance drops by no more than 5%

Drive Encryption

Introduction

From an administrative standpoint, encryption applications should:

- Enable remote installation, configuration and administration
- Enable remote management, particularly enable emergency access to drives if user forgets a password
- Enable access to encrypted data if a key irrevocably lost

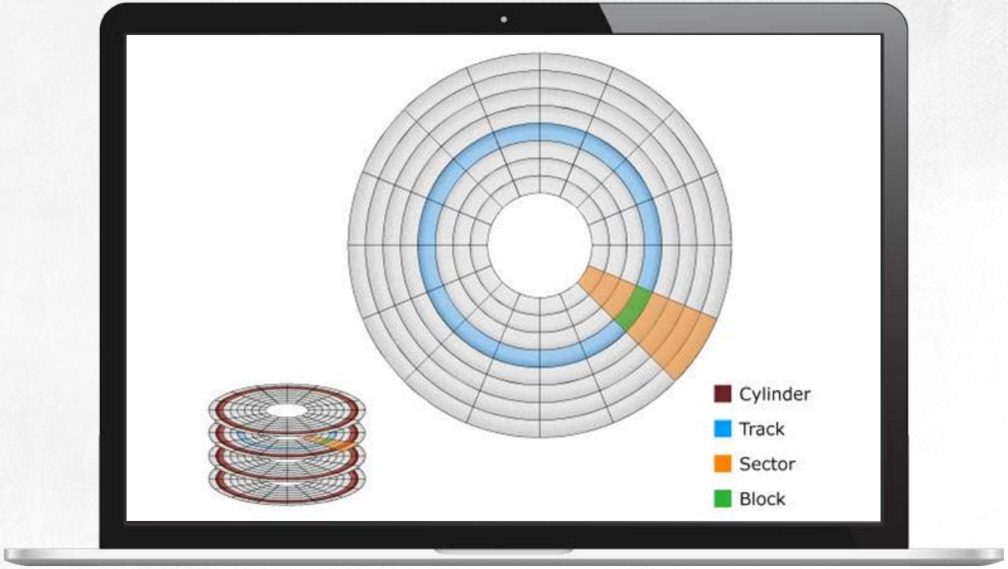


Drive Encryption

Introduction

Some drive encryption applications offer the following features: data authenticity check, data hiding and computer integrity check

Checking the authenticity of encrypted data is in particular of vital importance



Drive Encryption

Authenticity

Data authenticity is checked by adding a message authentication code (MAC) to it

For sector-based encryption, adding MACs to ciphertexts is not possible

Because a sector has a fixed length (512 bytes), a ciphertext cannot be longer than the plaintext data to be encrypted. If it was, part of the ciphertext written to one sector would depend on the part written to another sector on a drive

Drive Encryption

Authenticity

Additionally, some programs presume data written to different sectors is independent from each other
You could "increase" the size of a sector from 512 to 1,024 bytes…

To ensure the authenticity of ciphertexts:

- The change of one byte causes the pseudorandom change of all remaining bytes in the same block or sector
- Each sector is encrypted using a different key, which makes it harder to move ciphertexts across sectors without authorisation

Drive Encryption

Ciphers

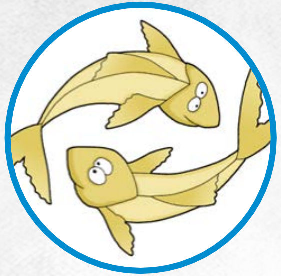
AES is a symmetric-key block cipher, a winner in the 1997 competition held by NIST

Verifiably secure

Speed (for 256-bit keys it is smaller by 40% than for 128-bit keys)
Immune to execution time and power consumption analyses
Verifiably resistant to differential cryptanalysis and linear cryptanalysis

Serpent is a symmetric-key block cipher that provides a comparable security level to the one provided by AES

The difference is that it is much slower than AES



Twofish is a symmetric-key block cipher that encrypts data in rounds.

Nearly as fast as AES (may be faster in some implementations) and according to some experts it offers better security

Drive Encryption

BitLocker

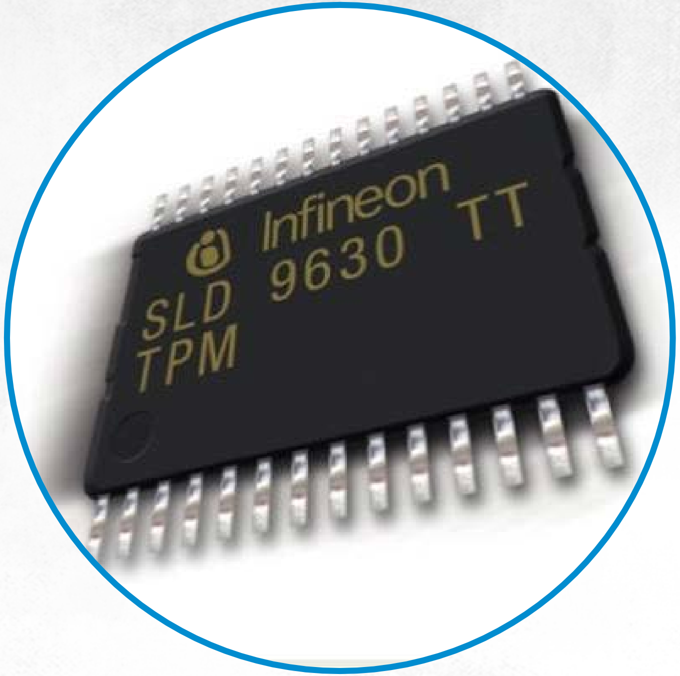
TPM generates and stores keys

TPM chips implement RSA, SHA-1, HMAC and AES

The key will only be made available when host integrity is verified

The TPM computes SHA-1 hashes of PCR values at each system start

Moving an encrypted drive from one host to another or starting your computer from a different boot disk (for example from a DVD disc) means you will not be able to access the key



Drive Encryption

BitLocker

The TPM measures all PCRs

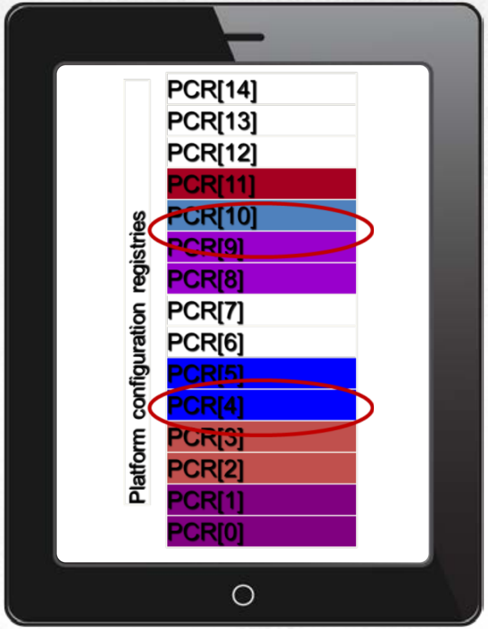
By default, BitLocker uses PCR 4, 8, 9, 10, 11

If you add more, it may cause the system to not be loaded

ROM 2 and 3: Any change will block the system from starting

… this includes connecting a USB drive

BIOS ROM 0 and 1: Updating the BIOS will block the system from starting



Drive Encryption

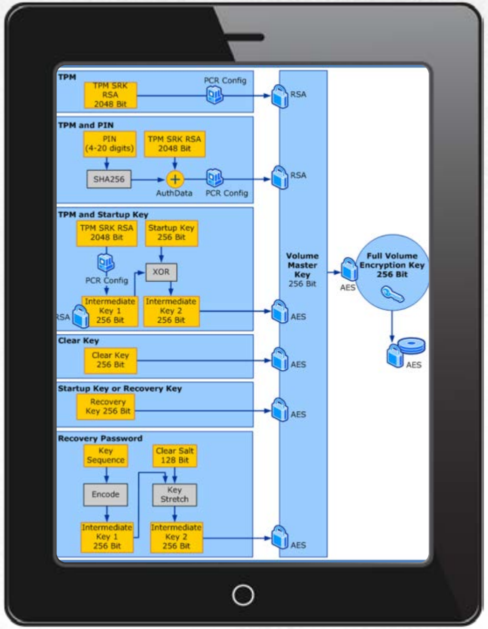
BitLocker

BitLocker is a full disk encryption tool that uses AES in CBC mode

You can also diffuse encrypted data using an algorithm called Elephant

The Storage Root Key (SRK) is stored in the TPM

The SRK is used to encrypt the Volume Master Key (VMK) stored on the boot drive, while the VMK itself secures the Full Volume Encryption Key (FVEK)



IT SECURITY ACADEMY

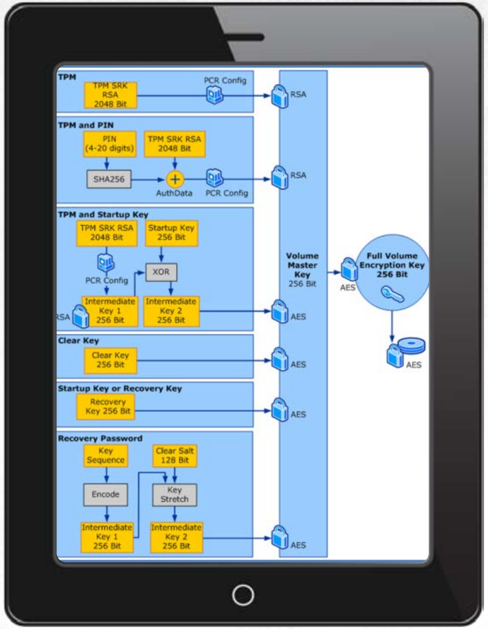
www.SecAcademy.com

Drive Encryption

BitLocker

If the VMK was only encrypted with the SRK, changing computer settings would entail a permanent loss of all encrypted data. To avoid this situation, a copy of the VMK is encrypted with a 48-digit recovery key you must submit if the system disk-protecting VMK is lost

You can save the recovery key on a USB drive



Drive Encryption

BitLocker

You can also consider protecting the VMK additionally with a PIN-secured smart card or a combination of the methods mentioned earlier

In the most widely-used TPM mode:

- The BIOS measures PCR values
- A SRK is generated from selected PCR values
- Windows uses the SRK to decrypt a VMK
- The VMK is used to decrypt an FVEK
- The FVEK is used to decrypt disk sectors when read

Drive Encryption

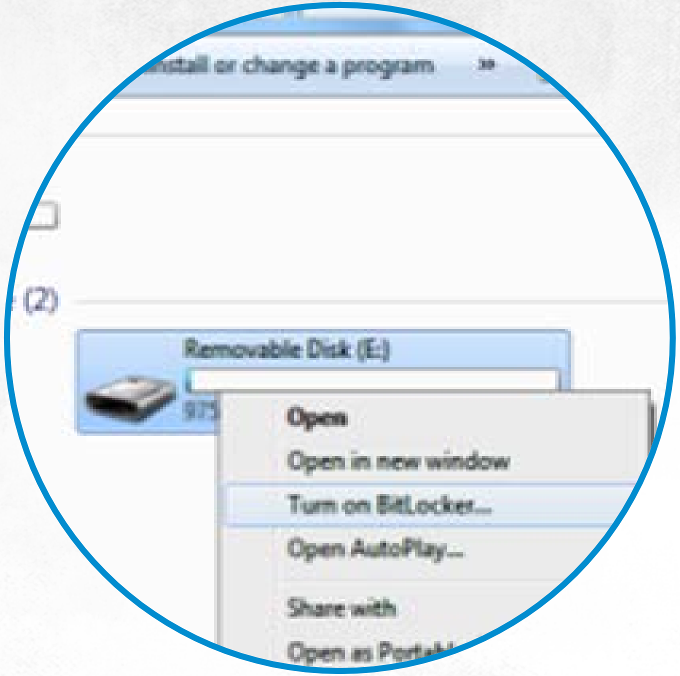
BitLocker To Go Reader

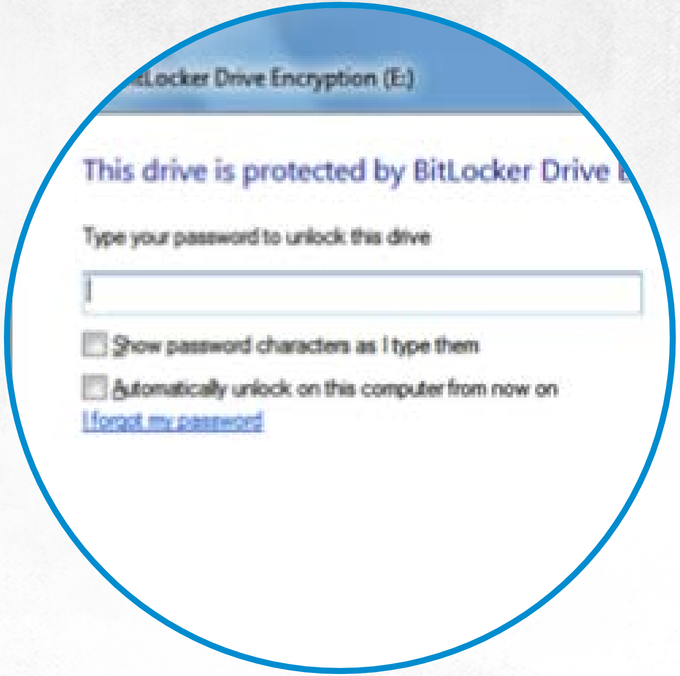
In Windows 7 also external USB drives may be encrypted

Encryption and decryption in this case does not require the TPM. To access encrypted USB files, you just need to submit the password that protects them or use a smart card containing the right key

Encrypting 1 GB takes up to several minutes

After you insert an encrypted drive to a computer running Windows Vista SP1 or XP SP3, you will be able to read its contents





tLocker Drive Encryption (E:)

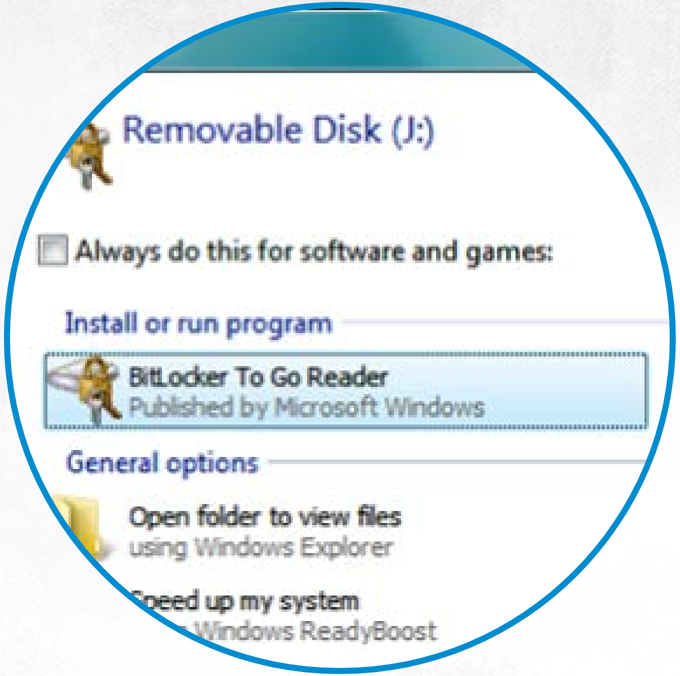
This drive is protected by BitLocker Drive

Type your password to unlock this drive

□ Show password characters as I type them

□ Automatically unlock on this computer from now on

I forgot my password



Removable Disk (J:)

□ Always do this for software and games:

Install or run program

BitLocker To Go Reader
Published by Microsoft Windows

General options

Open folder to view files
using Windows Explorer

Speed up my system
Windows ReadyBoost

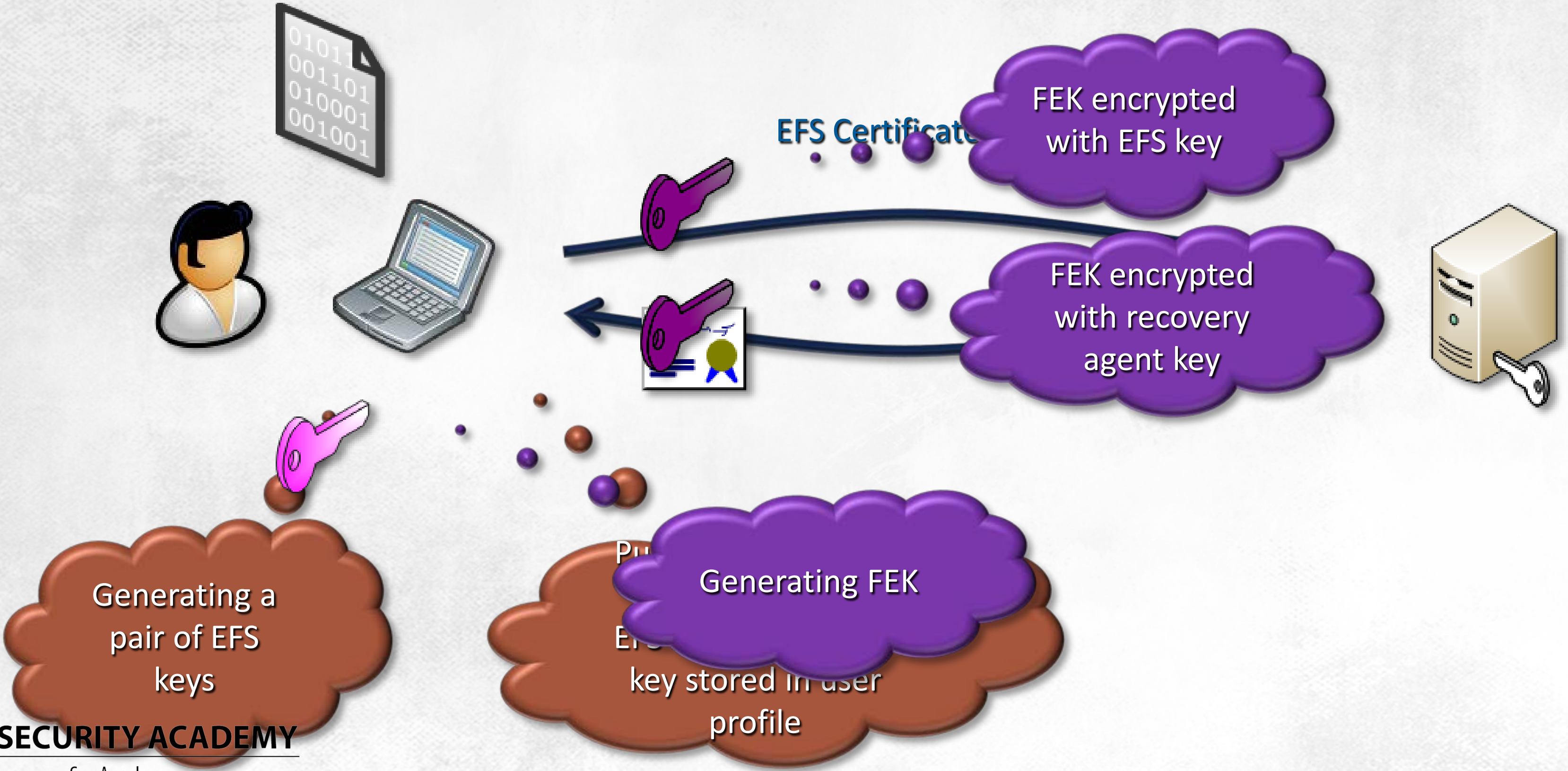
Drive Encryption

BitLocker vs. TrueCrypt

Feature or function	BitLocker	TrueCrypt
Manufacturer	Microsoft	TrueCrypt Foundation
Release date	2006-11-08	2004-02-02
License	Commercial	Open Source
OS	Windows Vista and newer	Linux 2.4-2.6, Windows 2000 and newer, Mac OS X
Hidden container	No	Yes
Authentication	TPM, password, key and combinations	Password or key
Computer integrity check	Yes (requires TPM)	No
TPM support	Yes	No
Multiple keys	Yes	No
Hardware-based encryption	No	No
Physical disk encryption	No	Yes
Logic disk encryption	Yes	Yes
Virtual disk encryption	No	Yes
Ciphers	AES	AES, Serpent, Twofish and their combinations
Block cipher modes	CBC with secret IVs	XTS, CBC with predictable IVs, LRW
Ciphertext authenticity check	Yes (Elephant)	Partial

File and Folder ENcryption

EFS



EFS Certificate

FEK encrypted with EFS key

FEK encrypted with recovery agent key

Generating a pair of EFS keys

Pu

Ef

key stored in user profile

Generating FEK

File Encryption

EFS

The EFS driver, a component of the NTFS driver, is the agent responsible for encryption

Encryption:

- Requests sent to the EFS driver are passed to the FeClient DLL
- Next, a file is checked if it may be encrypted
- A log file called efs0.log file is created in the System Volume Information folder
- A 16-byte FEK is generated
- The FEK is encrypted with a user’s public key
- If a data recovery agent is defined, Data Recovery Fields (DRFs) are created
- DDF and DRF field hash is computed and saved in the file header (in the $EFS attribute)
- A backup is created (the efs0.tmp file)
- The content of the encrypted file is copied to a backup file
- The content of the encrypted file is deleted
- At this stage the original file is labelled as encrypted, and that’s why data copied back to the backup file will be encrypted before they are saved
- Efs0.log now contains information about the successful encryption, and the efs0.tmp backup file is deleted
- The efs0.log file is deleted, which ends the file encryption procedure

File Encryption

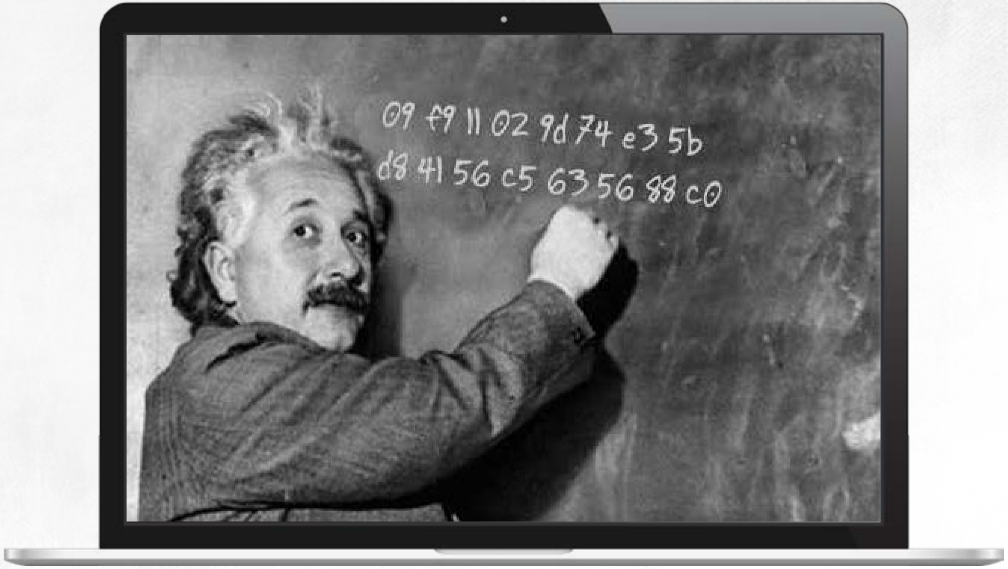
EFS

Backups of the encrypted file will be encrypted with the same FEK

A user who has access to the file when the backup file is created and who loses this access later will be able to decrypt the files in the backup

Exercise

Data encryption



Using EFS

THANKS