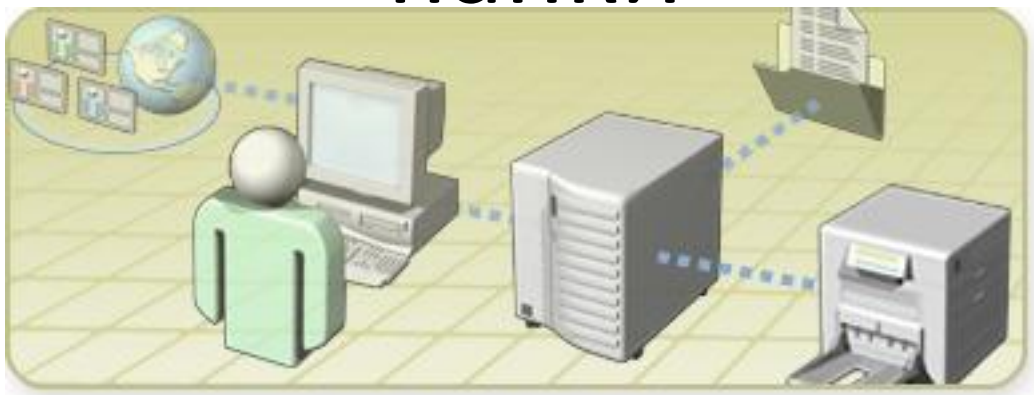
Споделяне и сигурност за данни. Конфигуриране на достъпа до файлове и папки



План

- Промяна на позволенията за файл и папка
- NTFS позволения
- Задаване на NTFS позволения
- Ефективни NTFS позволения
- Позволения след копиране и местене
- Криптиране на файлове и папки с EFS
- BitLocker To Go
- Пълно криптиране на диск с BitLocker
- Задаване на дискови квоти
- Позволяване на файлове за мобилни потребители
- Distributed File System (DFS)
- NTFS позволения
- Encrypting File System (EFS)

Видове атаки

Условно атаките се разделят на два типа:

- **Външни атаки** – източникът на атаката се намира извън периметъра на разглежданата мрежа;
- **Вътрешни** - атаката е стартирана от мрежови сегмент или система, която се намира в периметъра на дадената мрежа.

- Границите на мрежите се размиват - използват се облачни услуги, виртуални частни мрежи (VPN), мобилни устройства и др., като това води до по-трудно дефиниране дали атаката е вътрешна за мрежата или външна.

Външни атаки

- Сканиране на портове, операционни системи, използвани услуги и др.;
- Опити за пробив на системите за сигурност чрез атака на потребителски или административни пароли;
- Използване на технологични или други пропуски (bug) за получаване на неоторизиран достъп до устройства;
- Отказ на услуги - DoS (Denial of Service) и DDoS (Distributed Denial of Service);
- SPAM и др.

Вътрешни атаки

- Сканиране на мрежови ресурси, протоколи и системи;
- Подслушване и събиране на пакети;
- DoS;
- Пренасочване на портове;
- DNS spoofing;
- ARP poisoning;
- Опити за неоторизиран достъп до ресурси, чрез атака на парола или потребителски профил и много др.

Структурирани/неструктурирани атаки

Друго разделяне на мрежовите атаките:

- **Структурирана** – целенасочена атака, изпълнена от силно мотивирани и опитни лица, насочена към конкретна организация или система;
- **Не-структурирана** – случайни опити за атака, които нямат точно дефинирана цел.

Нива и технологии за защита

Споделяне на папки

- Споделяне с Windows Explorer
- Инсталиране на сървърна роля File Services
- Използване на Provision a Shared Folder Wizard
- Достъпване на споделена папка

Демонстрация

Промяна на позволенията за файл и папка

- Принципът, който трябва да се следва е потребителите да получават минимално необходимите им позволения, за да могат да си свършат възложените задачи
- NTFS - файловата система по подразбиране за Windows – позволява реализирането на Принципа на минималните позволения
- Позволенията могат да се задават на потребител или на потребителска група (за предпочитане)
- Файловете и папките използват едни и същи (с малки изключения) NTFS позволения, но те се проявяват по различен начин

NTFS позволения

- Базови NTFS позволения
  - Full Control (Modify, Read & Execute, List Folder Contents, Read, Write)
    - Позволява на потребителя да прави всичко с файл или папка, включително да променя позволения
    - Единственото стандартно позволение, което позволява на потребителя да променя позволения за файл или папка
    - Потребителите могат да вземат собствеността върху файл или папка (take ownership)
  - Modify (Read & Execute, List Folder Contents, Read, Write)
    - Позволява на потребителя да чете, пише, променя и изтрива файлове и папки

NTFS позволения

- Базови NTFS позволения
  - Read & Execute (List Folder Contents, Read)
    - Позволяват на потребителя да достъпва файл или папка и да изпълнява програма от папката
  - List Folder Contents
    - Прилага се само към папка
    - Позволява на потребителя да вижда съдържанието на папка – файлове и подпапки
  - Read
    - Може да чете съдържанието на папка или да достъпва файл (и да вижда позволенията и атрибутите (Read-Only, Hidden, Archive и System)
    - Не позволява на потребителя да изпълнява програми
  - Write
    - Папки: Потребителят може да добавя файлове и папки в тази папка
    - Файлове: Потребителят може да променя файл, но не може да го изтрива

NTFS позволения

- Наследени (Inherited) позволения
  - Когато се създава нов файл или папка, те приемат позволенията от родителската папка
  - Процесът се нарича наследяване (inheritance) и може да доведе до усложнени позволения
- Наследяването може да се изключи

Задаване на NTFS позволения

- Всеки обект файл или папка върху NTFS дисков дял има таб Security когато му се избере Properties
  - От този таб може да се види текущата конфигурация на позволенията за обекта
- Може да се използва и помощна програма от командния ред icacls
- В Магна АС трябва да се направи следното:
  - Всички потребители, които са членове на група Marketing трябва да достъпват с позволение Modify локалната папка Marketing (да се направи с GUI)
  - Да се зададе на членовете на група Sales позволение Modify до локална папка Sales (icacls)
    - icacls c.\sales /grant gm\sales:(oiXci)m
  - Да се забрани достъп до папка Sales за групата Marketing (GUI)

Демо

Ефективни NTFS позволения

- Възможно е NTFS позволенията да си противоречат
  - На потребител да сме задали позволение Read за конкр.папка, а в същото време той да има позволение Write по силата на членство в група
- С едно изключение NTFS позволенията са кумулативни
  - В горния пример потребителят ще получи ефективно позволение Read и Write
  - Изключение
    - Ако потребителят има изрично зададена забрана (Deny) за група или индивидуално, Deny е по-силно от всичко друго

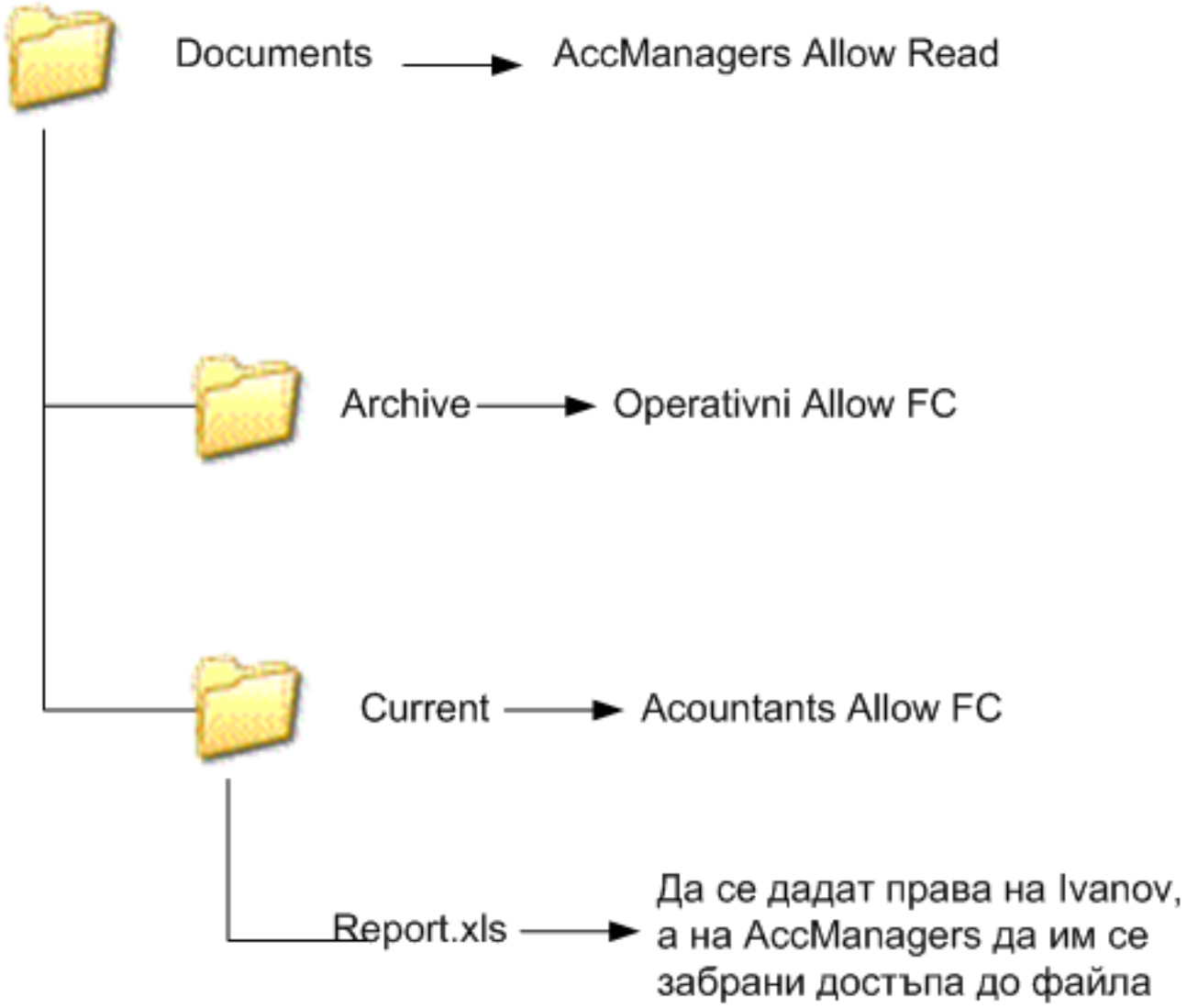
Ефективни NTFS позволения

- В Магна АД трябва да се разбере защо потребителят Сава Костов може да променя съдържанието на документи в папката C:\Accounting
- Използвайки таба effective permissions ще определим какъв достъп му е бил зададен и защо може да прави промени

Позволения след копиране и местене

- Местенето и копирането на файлове и папки може да промени NTFS позволенията
  - Когато се копират обекти на ново място, те приемат позволенията от новото място
  - Когато се местят обекти
    - Към място на същия дял/диск
      - Те запазват съществуващите си позволения
    - Към място на различен дял/диск
      - Те наследяват позволенията от новата папка

Задача


Documents
AccManagers Allow Read
Archive
Operativni Allow FC
Current
Acountants Allow FC
Report.xls
Да се дадат права на Ivanov,
а на AccManagers да им се
забрани достъпа до файла

Дискови квоти

- С използване на Windows Explorer
- Hard квота / Soft квота
- С използване на File Server Resource Manager /роля File and Storage Services /

Демонстрация

Offline Files

- Offline файловете позволяват на мобилни клиенти да работят с кеширано копие на файлове от споделени папки, когато не са свързани с мрежата, и да ги синхронизират със сървъра, когато се свържат към мрежата.
- Offline файловете са почти прозрачни за потребителите

Демонстрация

Distributed File System (DFS)

- В големи компании може да е трудно на потребителите да помнят местата на файловете (къде да ги открият)

- DFS създава едно общо пространство, което потребителите да използват, за да достъпват всички споделени папки без да знаят на кой точно сървър са разположени шеърите

- DFS се използва и за redundancy. Имаме копие на данните на повече от едно място. Потребителите ще се свържат към най-близкия сървър, който има копие на данните.

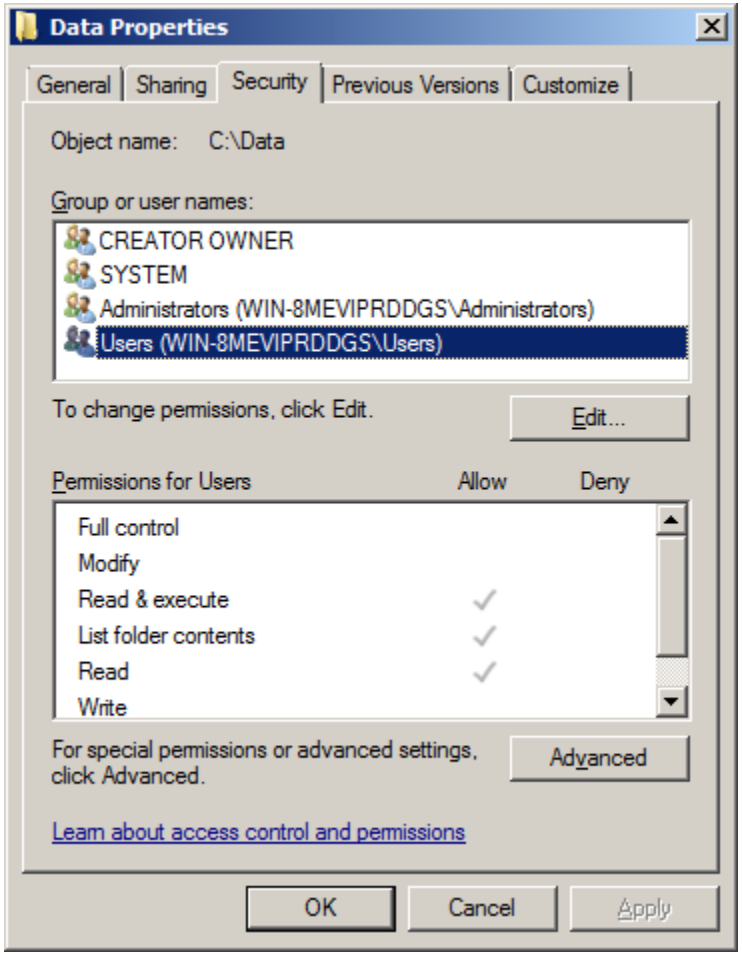
Демонстрация

Сигурност за данните

- NTFS позволения
- Encrypting File System (EFS)

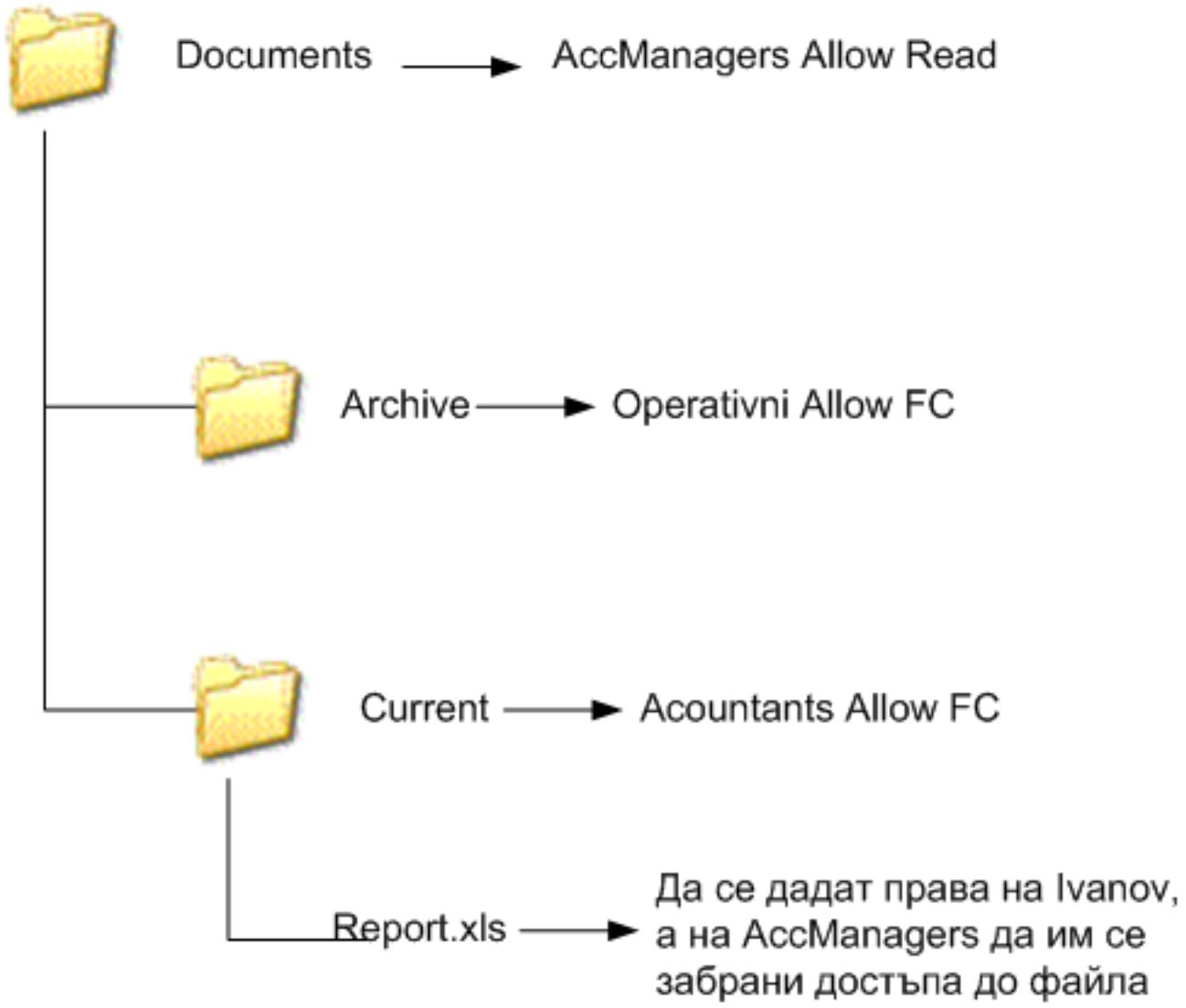
NTFS Permissions

- NTFS позволенията могат да се задават за папки и файлове
- Позволенията могат да се задават за потребители или групи
- Позволенията са кумулативни
- Deny е по-силно от Allow



Демонстрация

Задача


Documents
AccManagers Allow Read
Archive
Operativni Allow FC
Current
Acountants Allow FC
Report.xls
Да се дадат права на Ivanov,
а на AccManagers да им се
забрани достъпа до файла

Encrypting File System (EFS)

- NTFS позволенията осигуряват защита в рамките на Windows, но ако се получи физически достъп до твърдия диск и той се използва в не-Windows среда, то NTFS позволенията ще се изгубят
- EFS добавя допълнително ниво на защита чрез криптиране на данните на диска. Така те стават нечитаеми за други операционни системи
- EFS се поддържа от Windows 2000 и нагоре

Криптография

- Криптографията е концепция за прилагане на алгоритъм към обикновен текст, който да го конвертира в криптиран текст.

- Алгоритъм: добавяне на 2 букви
- Михаил Радев → Окчвкн Твжзд

Криптография

- Повечето алгоритми са известни
- Това, което се променя в алгоритъма е ключа

- Пример: Алгоритъмът е добавяне на х букви.
- Ключът е “х”

- Ако х=2, тогава Михаил Радев → Окчвкн Твжзд

- Ако х=5, тогава Михаил Радев → Снъенр Хейкж

Криптография

- EFS използва два различни типа криптиране.
- Криптиране със симетричен ключ
  - Един и същ ключ се използва за криптиране и декриптиране на данните
- Криптиране с публичен ключ (асиметрично)
  - Използва двойка ключове
  - Единият ключ се използва за криптиране, а другият – за декриптиране

Криптиране с публичен ключ

- Всеки потребител има двойка ключове

- Единият е достъпен само за конкретния потребител и се нарича частен ключ
- Другият е публично достъпен и се нарича публичен ключ.

Криптиране с публичен ключ

- Пример:
  - Ако имаме 20 потребители, те биха имали общо 40 ключа. 20 от тях ще са частни и достъпни само за конкретния потребител и 20 ще са публични и достъпни за всички.
  - Всеки потребител ще има достъп до 21 ключа – 20 публични и 1 частен
  - Всеки ключ може да се използва за криптиране на данни
  - Само ключ, чифт с криптиращия може да се използва за декриптиране на данни.

Криптиране с публичен ключ

Андрей иска да изпрати криптирани данни за Мария

Андрей криптира данните с публичния ключ на Мария
Андрей изпраща данните на Мария
Единствения ключ, който може да ги декриптира е частния ключ на Мария
Мария декриптира данните с частния си ключ

Частен Публичен

Частен Публичен

Криптиране с публичен ключ

Андрей иска да изпрати аутентикирани данни за Мария
/тя да е сигурна, че той ги изпраща/

Андрей криптира данните със своя частен ключ
Андрей изпраща аутентикираните данни на Мария
Мария проверява данните, като ги декриптира
с публичния ключ на Андрей
Всеки може да декриптира данните – така се
проверява автентичността на данните. Това се нарича
още и цифрово подписване на данните

Частен Публичен

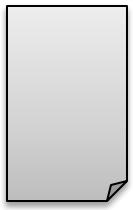
Частен Публичен

Как работи EFS

- EFS използва криптиране със симетричен и с публичен ключ
- Първо файла се криптира със симетричен ключ (FEK – File Encryption Key)
- След това се прави копие на FEK за recovery agent/във всяка мрежа има RA – user account, който има достъп до всички EFS криптирани данни/, за потребителя, който криптира файла и за потребителите, които могат да достъпват файла
- Накрая всяко копие на FEK се криптира със съответния публичен ключ на потребителя, който трябва да достъпи този файл.

Как работи EFS

- Андрей иска да е сигурен, че само той и Мария ще имат достъп до определен файл.



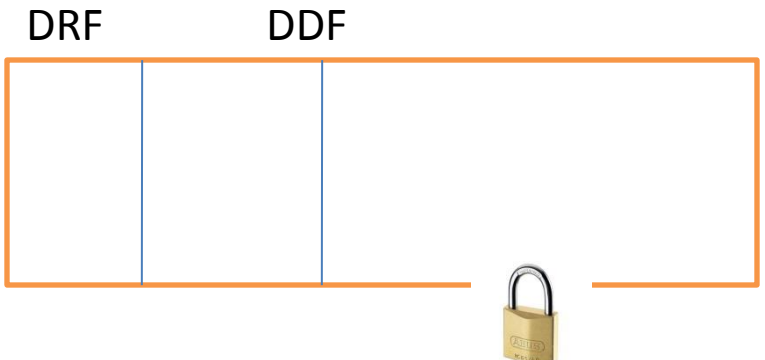
Файл

FEK

Публичен ключ Андрей

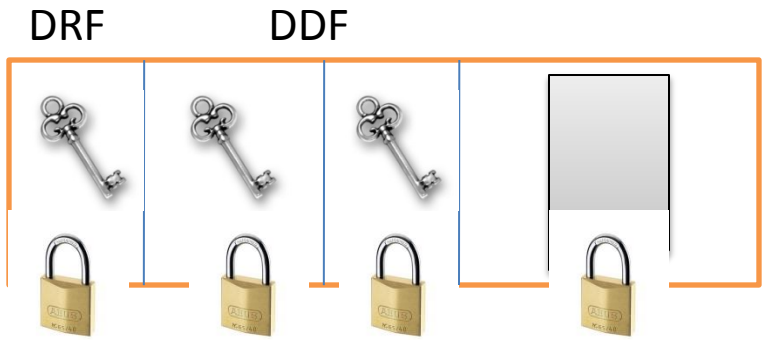
Публичен ключ Мария

Публичен ключ Recovery Agent



Как работи EFS

- Достъп до криптираните данни – ако някой се опита да достъпи файла ще стигне до 4 заключени кутии



Въпроси?

Консултации
– сряда от 14:00 до 16:00 в кабинет 2-401
- петък от 13:00 до 15:00 в кабинет 530

Email: radev@ue-varna.bg