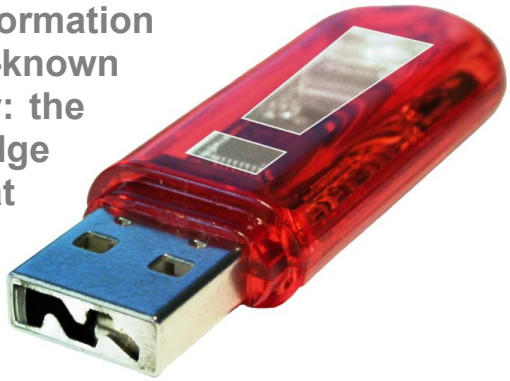
ENCRYPTION "TO GO"

CENTRALLY DEFINED REQUIREMENTS FOR CONFIDENTIALITY AND REAL USER ENVIRONMENT IN THE AREA OF CONFLICT

PROTECTING CONTENT ON REMOVABLE DATA STORAGE USING ENCRYPTION



The protection of company-owned information during transportation entails a well-known area of conflict in information security: the user himself may be able to best judge the sensibility of the information but at the same time, he neither has the expertise in the usage of encryption technologies nor the time for a "special treatment" of the information according to centrally defined security requirements. This calls for products which connect the central, network-wide security management and are characterized by easy usability and appropriate individualization according to the company guidelines. In the following, we will describe different use cases in this area of conflict and the resulting requirements as well as solutions that are able to solve these.

Established solutions for the encryption en-route, which have been offered for some time e.g. by Utimaco, Pointsec or Safe Boot, using a partition encryption with the help of company keys, show significant user deficits in the outlined area of conflict. In the following, we will outline different use cases which prove that they do not meet some significant requirements.

Use Case „Mobility“: Sales employees would like to transport sensible customer data to the customer and there, hand them over on a Memory Stick or another data storage device without facing a security risk in case of loss or theft of the data storage device. Obviously, the sales employee may not disclose the secret company key – as far as he even knows it – or leave it on an external system because e.g. entering the key into an external system is an insecure data entry due to “keyboard sniffers” and with that, would endanger the total data and network of the own company.

Therefore, the described sales employee needs a customer specific key. This requirement could generally be met by a pre-converted PKI or products that offer user-sided key entries. In this case, though, a PKI is not an option because the infrastructure requirements for spontaneous data transportation are too high and mostly, a jointly usable infrastructure does not exist. The products for the key entry call for user action **before** the exportation of the data – depending on the quality, the user can actively ask for the encryption by using the context menu (i.e. right mouse click.) This action requires not only awareness on the user’s side but also time and therefore patience. Finally, another problem arises through the fact that each data storage device needs a separate key for the partition encryption.

Use Case „Multi Key“: In addition to the above described requirement, the sales employee obviously would like to store all customer data on his personal Memory Stick. At the same time, he would like to only disclose specific customer related data to each client – regardless whether he hands over the key and the data storage device directly to the customer or whether he enters a customer specific key into an external and therefore insecure system that decodes parts of the device.
This requirement cannot be met by solutions that only provide one single key for the whole partition, e.g. by entering a PIN for the encrypted Memory Sticks with a high degree of security offered e.g. by the company Kobil.
The requirement for the easy usability has already been mentioned earlier. Which concrete requirements result from this? First of all, the user should not have to deal with any planning tasks but all activities and user decisions would need to be fully automated and integrated in the standard processes. Due to the fact that we are dealing with security during data transportation we differentiate between the export out of a secure environment and the import into a secured environment. Both situations require existing key material. Experience tells us that the employee’s mind is the best storage area because, naturally, he is always present at the point of action. So called “Escrow”-requirements do normally not exist for the following reason: during the confidential data transportation, the original data always remains unchanged in a secure environment; only data copies are used for transportation. For several reasons it is recommended not to directly change the data on the mobile data storage device, e.g. by opening the file with Word, because a short contact outfall to the saving device can lead to a loss of the original data (exceptions are U3-solutions which are not widely available at this point in time). Therefore, those products which offer the deletion of originals as an option cannot be recommended.

Use Case “Data Export“: Regardless of the application chosen in the Microsoft™ environment (“drag&drop”, “cut&paste” or context menu), the user guidance for the data export needs to be outlined in a few simple steps within the defined standard

processes. These security measures must not be avoided. Company-specific security requirements (e.g. complexity of encryption keys) must be presented by user-guidance at the point of usage in real time.

Use Case "Data Import": The target system must not require a special installation because most users are not entitled to install programs on their computer. At the same time, it is obviously necessary for the decryption tool to be automatically installed to the data storage device when encrypting the data.
Every company has data that can be easily communicated without any security requirements, e.g. company brochures, product descriptions and other publicly accessible information which are part of each sales employee's standard equipment. As always, the right dosage of security is significant in order to avoid an erosion of the sense of security. Therefore, it makes sense to allow the storage of unencrypted data onto data storage devices, e.g. Memory Sticks or rewritable CDs or DVDs. When exporting image data for viewing to digital cameras, image printers or other devices, encryption must actually be avoided because the devices may not work otherwise. Therefore, the encryption must be adapted according to central guidelines and depending on the individual target device and the files. It is necessary to not only check the file name but also the file content in order to make sure that no renamed or sensible contents leave the company network unencrypted.
Therefore, the decision about which data needs to be encrypted does not only depend on the target of the copying operation but also on the content. It cannot only be made on the basis of the file type but also needs to incorporate the possibility of a content check and pattern check.

Use Case "Encryption depending on the choice of target": An unencrypted data export is mandatory for digital cameras, photo printers or other image related devices.

Use Case "Encryption depending on the choice of content": Company brochures may be exported unencrypted.

Depending on the company guidelines, generally all data must be encrypted and only specially defined files may be exported unencrypted (White List Policy) or generally all files may be exported unencrypted with the exception of some special data that must be encrypted (Black List Policy). The differentiation by content also helps to keep processes lean, because employees only have to take the additonal step of encrypting data, where it is really necessary.

Use Case "Sole usage of company-owned data storage devices": Companies also require the ability to personalize and individualize external data storage devices. These two functions support the work for small groups (management board and back office) or big groups (projects) with extremely confidential information. Export and access to individualized media is supported depending on the content and the authorization of the user in order to technically reflect project responsibilities, e.g. for finance or patents.

Use case »beginning of the head physician's shift« This shows the connection between cost savings, usability and security: The relevant patient data of the previous night shift can be loaded fully automatically and revision secure onto his

PDA or handheld computer. The head physician only needs to place the PDA next to his computer. The synchronization via Bluetooth starts automatically where the basic conditions like, for example, the correct encryption of the PDA, the authentication of all relevant devices and users and many other system set-ups, are automatically checked in advance.

Market analysis: All previously outlined requirements are actually met by the software product PDWatch from the company itWatch (www.itWatch.de.) The combination of content check of exporting data through the product XRayWatch from the same producer, companies are able to centrally manage and realize "exotic" requirements throughout the whole network. For example, it can be defined to encrypt Word documents which contain the "company confidential" footnote. On the other hand, non-sensible data can be exported unencrypted. A study case of the use of the content filter of the XRayWatch product has already been presented at the Microsoft Police Conference [Wust2006].

Requirements for the confidential transportation of data in brief:

1. Encryption with different keys on one data storage device
   a. If required, the keys will be chosen by the user
   b. Unencrypted and encrypted files are stored beside each other on one data storage device
1. Central definition of the key strengths, possibly of the encryption methods and guidelines
   a. Who may export unencrypted data?
   b. The characteristics of a strong key must be centrally defined.
   c. Which files/contents may be exported unencrypted?
   d. Data may be exported unencrypted onto which devices? An encryption is mandatory for which devices?
   e. Does the transfer require a protocol or shadowing?
3. Fully automated integration into Windows operating system: all standard Windows mechanisms for the file management need to automatically lead to encryption
   a. "Drag&drop"
   b. "Cut&paste"
   c. Context menu operations
4. No bypass of security set-ups for sensible data
5. Decryption software needs to be provided automatically and must not require any installation onto the target system

The tool »DeviceWatch« takes care of the device security, "DevCon" helps to automize device-related actions without user-interaction, by that achieving lean business processes.

We would like to especially outline the positive characteristic of the products - that underlines the actual philosophy of IT managers to "support but not to limit" the fully automated functions of the Windows™ operating system – which implements a solution for all user groups without the requirement of technical knowledge or special awareness. Therefore, the company's Data Protection Officer or Information Security Officer is able to, for example, demand an encryption when exporting data respecting a simple Security Policy. Some Security Policies are already integrated in PDWatch by standard. E.g. the case that a user has been entitled by the central management to export data unencrypted, he takes on the responsibility by his personal action to approve the unencrypted export in each individual case – which is reported in a log file.

Sources:

[Wust2006] Digitale photography on XP-workstations of the Bavarian. Police, , 11. Microsoft Police Congress April 3rd/4th 2006 in Bad Homburg

Find out in detail about our innovation and contact us at

Info@itWatch.de or +49 (0) 89 / 620 30 100.

itWatch GmbH
Aschauer Str. 30
D-81549 Munich
www.itWatch.info