

File encryption

- Confidential files (e.g. documents) are protected by encryption.
- Access to encrypted data is restricted to authorised users.



If files are to be protected against unauthorised access, encryption is the tool of choice.



CCE - Citizen Card Encrypted

- CCE is a tool, to en-/decrypt files using the citizen card.
- A-SIT promotion:
https://demo.a-sit.at/buergerkarte/cce2_tool/index.html offers a tool to encrypt and store data in a container using the Citizen Card.
- Files can be en-/decrypted using the CCE manager or using the context menu of the Windows Explorer.
- CCE uses the format S/MIME which guarantees the compatibility to E-Mail-Clients such as Outlook, Thunderbird or Evolution.
- Using S/MIME as a file format, CCE decrypts e-mails encrypted by this standard.
- CCE supports secure deletion of files. This guarantees that no residual unencrypted data remains.



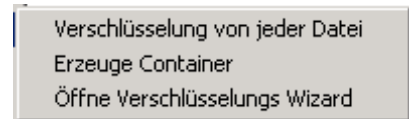
Encryption certificates

- A file can be encrypted for different users. Therefore the recipient's encryption certificates are used.
- CCE offers several ways to retrieve the encryption certificates:
 - Certificates can be imported from a citizen card, from files, or downloaded from LDAP-servers.
 - Directory services such as LDAP-servers store the certificates of their customers. The directory service of A-Trust contains the certificates of citizens who activated their bank card "Bankomatkarte" as citizen card, the directory service of the Main Association of the Social Insurance Institutions holds the certificates of the health insurance card "e-card", respectively.
 - These LDAP-servers are preconfigured with CCE and queries can be made with data (e.g., the name or part of the name) of the desired person.
- CCE holds certificates in its certificate store. Groups of certificates can be build that contain certificates of several users.



Encryption of files

- Using the Explorer context menu: Marked files can be encrypted using the explorer context menu (to open, click the right mouse button). If several files are marked, each file can be encrypted separately (Verschlüsselung von jeder Datei) or the marked files are stored together in an encrypted container (Erzeuge Container).



- Using the CCE-Manager: Use the Windows start menu to start the CCE-Manager. Files can be added and encrypted using the button "Datei Verschlüsselung".

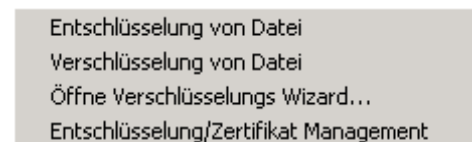


The default settings of CCE perform a secure deletion of plaintext files after the data have been encrypted. This prevents residual plaintext data on the harddisk.



Decryption of files

- CCE can decrypt files using the citizen card or a software key. Before decoding the user has to enter the PIN code of the citizen card or the password of the software key store.
- Using the Explorer context menu: the marked files can be decrypted using the Windows explorer context menu (click the right mouse button).



- Using the CCE Manager: Use the Windows start menu to start the CCE-Manager. Encrypted files can be added and decrypted using the button "Datei Entschlüsselung".



Secure deletion of files

- If a file is deleted, the data usually remain physically on the disk and can be restored.
- In the case of sensitive data it is important that the files are deleted in a way that nobody can restore it any more.
- CCE implements an algorithm that overwrites a file multiple times before it is deleted. This prevents any restoring of deleted data.
- CCE is configured to delete plaintext files safely after its encryption.



Files must be deleted securely after its encryption to prevent restoring of the plain text.



Hardware token / Software token

- The storage of the private key is important for the security of encrypted data. There are two kinds of tokens: hardware tokens and software tokens.
- Hardware token: The Citizen Card is a hardware token. The private key is stored on the card and cannot be read in general. All operations using the key are implemented directly on the hardware token.

- Software token: The key is stored on a data medium (e.g., the harddisk). The key file is usually protected by a password. If an attacker gets access to this key file, he can try to crack the password and thus gets access to the private key.
- CCE supports hardware- and software tokens. Software tokens are stored in a key memory which is secured by a password.



Backup key

- If data is encrypted with the Citizen Card, the file can no longer be decrypted in case of lost or defective cards.
- It is recommended to use at least a second certificate for encryption.
- The second certificate can be either another citizen card or a software-token.
- If a software token is used as backup key, it must be stored separately from the encrypted data.

To prevent data loss in case of a lost or damaged Citizen Card it is important to use a backup key or an additional card.

If the backup key is a software key, do not store it together with the encrypted data.



Further questions

Send an e-mail to:

technology@a-sit.at

www.a-sit.at

2010-06



CCE - file encryption using the Austrian Citizen Card

E-Government Flyer Nr.208 EN

CCE - Citizen Card Encrypted - file encryption tool

- File encryption
- CCE - tool
- Encryption certificates
- Encryption of files
- Decryption of files
- Secure deletion of files
- Hardware token / Software token
- Backup key

DIGITAL  AUSTRIA