

**Philips Crypto B.V.**

To:Everyone concerned

From:

Ir. M.C.M. Muijen

Department:
Systems & Architectures

Tel: +31 (0)40 27 22 600

Fax: +31 (0)40 27 23 658

Ref: CYR-990727.MCM.doc

Date: 2000-02-28

Subject: V-Kaart release notes Build 1.1 / Known problems and workarounds

*V-Kaart Systems***1. Formatting floppy-disks I**

V-Kaart Systems can not format unformatted floppy disks.

2. Formatting floppy-disks II

V-Kaart Systems cannot handle the 'Cancel' button on the format progress-bar. Clicking the 'Cancel' button will lead to a BSOD (Blue Screen of Death).

3. Microsoft Office and findfast.exe

When Microsoft Office is installed on a V-Kaart System, it installs also a program called 'findfast.exe'. This program creates and accesses index-files during the session without user interaction. Automatic re-/declassification can occur whenever such an index-file is accessed on a different classification level (or with other categories). To stop this from happening, remove the 'findfast.exe' executable from the 'Startup' folder.

4. Microsoft Office and the Personal folder

V-Kaart Systems cannot create V-Kaart Encrypted User Files in the Personal folder. Microsoft Office, and other programs, saves its user-files by default in the Personal folder. These user-files will be of the V-Kaart Encrypted System File type. This implies that no Signatures and / or V-Kaart Access Control Lists can be added. The Microsoft Office default path can be redefined (MS Word: 'Tools' -> 'Options' -> 'File locations' -> 'Modify').

5. Changing CD-ROMs during boot-time

V-Kaart Systems cannot handle CD-ROM (re-) insertions and removals during boot-time. Inserting and removing CD-ROMs during boot-time can lead to a BSOD.

6. Changing CD-ROMs during the session

V-Kaart Systems cannot handle a CD-ROM removal and an insertion of another CD-ROM during the session. Inserting and removing CD-ROMs during the session can lead to an Explorer crash.

7. CD-ROM autorun feature

V-Kaart Systems, depending on the platform and CD-ROM player brand, may not support the CD-ROM autorun feature.

8. Removing a V-Kaart Token

Removing a V-Kaart Token, on a V-Kaart System, before the system asks you to, will lead to a hang-up.

9. Inserting a V-Kaart Token

Inserting a V-Kaart Token, on a V-Kaart System, requires the user to logon within approx. 2 minutes. Otherwise, the system will give a BSOD on the V-Kaart Logon dialogbox time-out.

*cpqwest?**voor afsluiten*



CYR -Release notes 1.11(aangepast)
page 2

10. System Restart Button

On some V-Kaart Systems pressing the Restart Button after a system shutdown may lead to a BSOD.

11. Trash-can

Using the trashcan on V-Kaart Systems can give numerous error-messages. Temporary solution: turn the trash-can off (i.e. files are deleted instantly).

12. Standalone V-Kaart Systems

Standalone V-Kaart Systems rely on several RPC services. These services will only be installed if Windows NT networking is installed (which is in contradiction with being standalone!). Therefore, after installing Windows NT networking, probably with a non-existing network-card, perform the following actions:

- Remove all network-cards from the 'Adapter' tab (located on the Network Neighborhood property page).
- Remove all network-protocols from the 'Protocols' tab.
- Remove all network-services, except for 'RPC Configuration', from the 'Services' tab.
- Ignore error-message and reboot the V-Kaart System.

13. Performance I

Some 'older' Pentium systems (e.g. Pentium 133Mhz/32Mb) may cause synchronization problems during boot-time. If this is the case, the following message will be displayed:

*Kan het sleutel materiaal niet laden.
Het systeem zal worden afgesloten.
Last error: e0500019*

Appending the 'DependOnService' registry entry with the value 'RPCSS' (the type equals REG_MULTI_SZ and is created with 'regedt32.exe') to the 'VkMdsService' and 'VkSmuService' keys in the 'HKLM\System\CurrentControlSet\Services\' hive, may fix the synchronisation problems.

14. Performance II

Standalone V-Kaart Systems performance may appear less compared with V-Kaart Systems in a network.

15. Uploading audit files

Uploading audit files from a V-Kaart System to a V-Kaart Security File Server using the V-Kaart Session Management Utility will fail when the local audit backup directory does not contain two audit files (the cyclic and non-cyclic). A temporary fix for this problem is to newly create the missing audit file with zero length.

16. Converting to NTFS

Converting a FAT partition, on a V-Kaart System, to NTFS can corrupt encrypted files making them inaccessible.

17. Windows NT guest account

Logging on to a V-Kaart System using the Windows NT guest account fails due to constraint access-rights for the registry (i.e. only read-access is allowed but read- / write-access is required). Adding the Administrator group-right to the Guest-account can solve this problem.

18. Novell

The current V-Kaart release does not support transparent file-encryption for drives mapped on a Novell server. To prevent the V-Kaart System from filtering network mapped drives the following parameters need to be reconfigured:

- Using the Service Control Manager, change the start-up value of the 'V-Kaart FileSystem Drive Notifier' service from 'automatic' to 'manual'.
- Using the registry editor, remove the registry value 'VkfsNet' from the 'HKLM \ Software \ Microsoft \ Windows \ CurrentVersion \ Run' key.
- Using the registry editor, change the registry value 'Login When NWGina Not Loaded' of the 'HKLM \ Software \ Novell \ Network Provider \ Initial Login' key from 'yes' to 'no'.



CYR -Release notes 1.11(aangepast)
page 3

In case the parameters are NOT reconfigured, when a Novell Client is installed, the V-Kaart System will become unstable resulting in (amongst others) BSODs.

19. Changing file security attributes and adding V-ACLs in one operation

Adding a V-ACL to a V-Kaart Encrypted User File and changing the file's security attributes in one operation can fail. The V-Kaart Encrypted User File security attributes must be changed first. When the file's security attributes are changed and are covered by the session's security attributes, then the V-ACL can be added to a V-Kaart Encrypted User File without any problem.

20. File sharing with users from another Security Domain

The current V-Kaart release does not support file sharing between users of different security domains. File sharing using the import / export mechanism, and in future releases via EMAIL, is supported.

21. Missing access denied messages

No error message "access denied" is being displayed on the console, when deleting the following Windows NT files:

- \WINNT\SYSTEM32\NTDLL.DLL
- \WINNT\SYSTEM32\SMSS.EXE
- \WINNT\SYSTEM32\DRIVERS\LNKSPX.SYS

These files are opened before the V-Kaart FileSystem is active. Therefore, the V-Kaart FileSystem does not know that they are opened already. However, the files are not deleted because Windows NT has locked them.

22. Files on UNC paths are not en- / decrypted

Files create by means of UNC paths are always plain. Encrypted files can become corrupted when data is written to them using a UNC path (the data added will be in plain).

23. Unmapping network drives */mapping*

Unmapping network drives manually can cause the V-Kaart System to become unstable. Therefore, let Windows NT unmap network drives on shutdown.

24. Remote Management

Remote Management of V-Kaart System is not supported in this release. V-Kaart Systems should be made inaccessible for remote access (set the corresponding user-right!).

25. Power Management

Power Management on laptops and desktops must be configured in such away that under no circumstance the power supply to the V-Kaart Card and the smart card reader is interrupted.

26. Administrator rights

All local Windows NT accounts used by V-Kaart must have the Administrator privilege (for now).

27. Installing Windows NT Service Packs I

Windows NT Service Packs must be applied before the V-Kaart Software is installed.

28. Installing Windows NT Service Packs II

Installing Windows NT Service Pack 5 can lead to floppy access problems on some systems (only seen on a Dell Optiplex Gxpro).

29. Access denied on the CL_PAVK.DAT cache-list file

Adding a VACL to a V-Kaart Encrypted User File can cause the CL_PAVK.DAT cache-list file to become corrupted. Each time the file is referenced, you will get a 'Access denied' error from the file-system. This file can be removed by hand (DOS). After the VKS is rebooted, it is automatically recreated.

30. Installing Lotus Notes



CYR -Release notes 1.11(aangepast)
page 4

The extensions '*.LCK' and '*.NBF' should be added to the V-Kaart Encrypted System File extension list (using the V-Kaart Update System Utility) prior to installing Lotus Notes. Otherwise these files will become of the V-Kaart Encrypted User File type and can therefore cause access problems depending on the session attributes.

31. Upper case filenames problem

The VKaart System changes upper case characters in filenames to lower case characters. Therefore, all files will be stored on disk by their filename in lower case.

V-Kaart Security Management Systems

32. Setting the Suspended Session Timer

V-Kaart Systems do not support the Suspended Session Timer. Therefore, do not set the V-Kaart Security Management System's Suspended Session Timer, leave it on infinite.

33. Retrieving audit-files from the V-Kaart Security File Server

V-Kaart Security Management Systems may need an explicit logon (i.e. logon using the Network Neighborhood) to the V-Kaart Security File Server to access the audit-files (having an identical Windows NT account on both the V-Kaart Security Management System and the V-Kaart Security File Server is required).

34. Password Validity Period

V-Kaart Systems cannot detect the end of a V-Kaart Password Validity Period.

35. System groups cannot be infinitely nested

V-Kaart Security Management Systems cannot nest System groups infinitely. For now, only one System group within a System group is allowed.

36. Invalid audit messages

V-Kaart Systems generate occasionally invalid audit messages. These message are filled with binary zeros and are marked as incorrect after conversion on a V-Kaart Security Management System. While converting, just ignore the error-messages.

37. Replace key material

V-Kaart Security Management System's option "Vervang Sleutel Materiaal" will be implemented in a future release and may therefore not be selected. *waarschijnlijk niet.*

38. Managers with audit rights

The first created manager, in the Managers list, who has audit rights, must be used to perform all audit activities. Working with multiple audit managers is not yet supported.

39. Classification-, Category-, and user-name length

The Classification-, Category-, and user-name length must NOT exceed 19 characters. This rule applies to all 20 character bounded names in the V-Kaart System. Exceeding the 19 characters will lead to all kinds of strange behaviour by the VKSMS and VKS.

40. Authentication on more than one file

When using the V-Kaart Authentication Utility to authenticate more than one file, by selecting multiple entries in the explorer, some files may not be authenticated correctly.

41. Mix-up of files when importing confidentiality keys

When importing confidentiality keys the system asks to insert the disk with the file INTEGRITY.RSA in drive A:. The VKSMS actually checks the existence of INTEGRITY.RSA, but then imports CONFIDENTIALITY.RSA.

General



CYR -Release notes 1.11(aangepast)
page 5

42. DE/PE 100 PCMCIA smart card reader

Release 2 of the De La Rue PE-100/DE-100 PC-Card smart-card adapter drivers do not work, use the beta release instead.

43. DE/PE 100 PCMCIA smart card reader

V-Kaart Systems with a DE/PE 100 PCMCIA smart card reader installed, get an error-message on boot-time indicating that a particular service / driver is not started. This error-message can be discarded by removing the 'DependOnService' value from the 'HKLM\System\CurrentControlSet\Services\CTNT4 SCR ' registry-key. This only holds for the beta release of the DE/PE 100 PCMCIA smart card reader drivers.

44. RPC failures

Windows NT tries to resolve numeric computer names to network addresses. For example, 692055 will be treated as a network address (a non-existent one i.e.) instead of a computer name. Communication with the security management and the certificate book database is based on RPC. These RPCs will fail whenever a numeric computer name is used.