

DataDesign Banking Application Components (DDBAC)

in Microsoft Terminal Server 2003-Umgebungen



Autor: Michael Goepper

Datei: DDBAC & Terminal Server 2003.doc

Version: 1-0-0

Status: Produktion

© DATADESIGN AG

A Inhaltsverzeichnis

1. MOTIVATION.....	2
1.1. Was ist HBCI/HBCI+/FinTS	2
2. VORAUSSETZUNGEN	2
2.1. Serverumgebung	2
2.2. Clientumgebung.....	2
2.3. Infrastrukturell.....	3
3. VORBEREITUNG.....	3
3.1. Installation der DDBAC-Komponenten auf dem Terminal Server	3
3.2. Installation des PC/SC-fähigen SmardCard-Lesers am Client	3
3.3. Installation der Remote Desktop Connection Software am Client	4
3.4. Aufrufen der Remote Desktop Connection Software	4
3.5. Einrichten des Chipkartenlesegeräts am Terminal Server	5
3.6. Einrichten von Kontakten	7
3.6.1. Mit Chipkarte	7
3.6.2. Mit RDH-Diskette	7
3.6.3. Mit PIN/TAN (HBCI+ oder FinTS)	8
4. BEKANNTE PROBLEME.....	8

B Änderungsverzeichnis

Version	Datum	Name	Änderungen/Kommentar
1-0-0	26. 01. 05	Michael Goepper	Erste freigegebene Version

C Abhängige Dokumente

Hyperlink	Dokument-Beschreibung

1. Motivation

Die Entwicklung hin zum wartungsfreundlicheren Terminal Server, insbesondere in kleinen Betrieben, Kanzleien und Büros, ist unverkennbar.

Daneben kommt häufig die DDBAC als Banking-Schnittstelle gerade in den o. g. Bereichen zum Einsatz.

Dieses Dokument soll Administratoren helfen, die optimale Konfiguration beim Einsatz der DDBAC in Terminal Server-Umgebungen zu wählen sowie die Installation zügig abzuwickeln.

1.1. Was ist HBCI/HBCI+/FinTS

HBCI ist eine vom Zentralen Kreditausschuss (ZKA = höchstes Organ der dt. Banken) verabschiedete Spezifikation für sicheres Online-Banking. Bankkunden können darüber zum einen über eine Standardschnittstelle mit der Bank kommunizieren (z. B. über Software für Rechnungswesen oder Zahlungsverkehrsprogramme) und zum anderen die gewohnten, bekannten und eingeführten Sicherheitsmechanismen verwenden. HBCI unterstützt dabei die Sicherheitsmedien RSA-SmartCard, DDV-SmartCard und RDH-Diskette, HBCI+ (das bekannte PIN/TAN-Verfahren) und in der Zusammenführung von HBCI und HBCI+ in FinTS.

Nahezu alle deutschen Kreditinstitute unterstützen diese Standard-Schnittstelle.

2. Voraussetzungen

2.1. Serverumgebung

- MS Terminal Server auf Basis von MS Windows 2003 Server.

Der Server muss dabei im Applikationsmodus (nicht im Verwaltungsmodus) laufen. Der Applikationsmodus wird ab der Standard Edition von MS Windows 2003 Server unterstützt (Web Edition ist nicht ausreichend).

2.2. Clientumgebung

- MS Remote Desktop Connection

Die MS Remote Desktop Connection Software wird standardmäßig mit Windows XP installiert. Bei anderen Betriebssystemen muss die entsprechende Software zusätzlich installiert werden.

Die aktuelle Version wird i.d.R. über den folgenden Link zur Verfügung gestellt: < <http://www.microsoft.com/windowsxp/downloads/tools/rdclientdl.msp> > (Stand: Jan. 2005).

- PC/SC fähiger SmartCard-Leser, wenn SmartCards verwendet werden sollen.

Ist die Verwendung von SmartCards zur Sicherung der Kommunikation mit der Bank vorgesehen, so muss am Arbeitsplatz (Client-System) ein PC/SC-fähiger Chipkartenleser installiert sein. Üblicherweise unterstützen alle am Markt befindlichen Geräte die PC/SC-Schnittstelle.

Die Unterstützung der PC/SC-Schnittstelle ist wichtig für die Kommunikation der serverseitig laufenden DDBAC mit dem clientseitig angeschlossenen SmartCard-Lesegerät.

Die DataDesign AG empfiehlt Geräte der Marke SCM (<http://www.chipdrive.de/>).

2.3. Infrastrukturell

Am Terminal Server muss eine **Verbindung in das Internet** möglich sein. Bei HBCI mit dem Sicherheitsverfahren PIN/TAN wird i.d.R. HTTPS – üblicherweise als TCP/IP via Port 443 - als Übertragungsprotokoll verwendet. HBCI mit SmardCard und im RDH-Diskettenverfahren verwendet ein HBCI-eigenes Übertragungsprotokoll, das auf TCP/IP basiert und i.d.R. über Port 3000 kommuniziert. Je nach Verfahren müssen die entsprechenden Bankrechner auf den angegebenen Ports erreichbar sein – d.h. Proxy-Server und Firewall-Systeme müssen ggf. darauf eingestellt werden.

3. Vorbereitung

Im Folgenden werden die Maßnahmen aufgezeigt, die einmal pro Server, bzw. Client durchzuführen sind.

3.1. Installation der DDBAC-Komponenten auf dem Terminal Server

Die Runtime-Komponenten der DDBAC müssen auf dem TerminalServer installiert werden. Die Installation kann nur ein Administrator, bzw. ein Benutzer mit Administrator-Rechten (Mitglied der Gruppe Administrator) durchführen.

Die jeweils aktuellste Version der Runtime-Komponenten der DDBAC ist über die Download-Seiten der DataDesign AG (<http://www.DataDesignAG.com/>) verfügbar.

Bei der Installation ist zu beachten, dass die Dateien DDBACCPL.CPL, DDBACCTM.CPL und DDBACCPL.CHM ggf. im falschen Verzeichnis abgelegt werden und deshalb händisch in das korrekte Verzeichnis verschoben werden müssen (siehe 4. Bekannte Probleme).

3.2. Installation des PC/SC-fähigen SmardCard-Lesers am Client

Am Client-System muss – wenn die Verwendung von SmartCards geplant ist – ein PC/SC-fähiger Kartenleser installiert werden.

Hierzu sind die Installationsanweisungen des jeweiligen Herstellers des Geräts zu beachten.

Der Einsatz gleicher SmartCard-Lesegeräte (auch bzgl. der Art des Anschlusses, z.B. alle Geräte einheitlich an USB angeschlossen) und gleicher Treiber-Versionen an allen Client-Geräten ist sinnvoll, da hierdurch Probleme unterschiedlicher Treiber und des Ansprechens unterschiedlicher Geräte vermieden werden.

Es ist zu beachten, dass die Installation des Treibers ggf. einen Neustart des Client-Rechners nötig macht. Bei auftretenden Problemen (z.B. Gerät kann nicht erkannt) ist ein Neustart des Client-Rechners unbedingt durchzuführen.

Die DataDesign AG empfiehlt Geräte der Marke SCM (<http://www.chipdrive.de/>). Bei diesen Geräten werden die PC/SC-Treiber mit der gewöhnlichen Treiberinstallation automatisch installiert. Für die Suche nach Ursachen bei auftretenden Fehlern liefert SCM i. d. R. entsprechende Analysesoftware mit den Treibern aus.

3.3. Installation der Remote Desktop Connection Software am Client

Die MS Remote Desktop Connection Software wird standardmäßig mit Windows XP installiert. Bei anderen Betriebssystemen muss die entsprechende Software zusätzlich installiert werden.

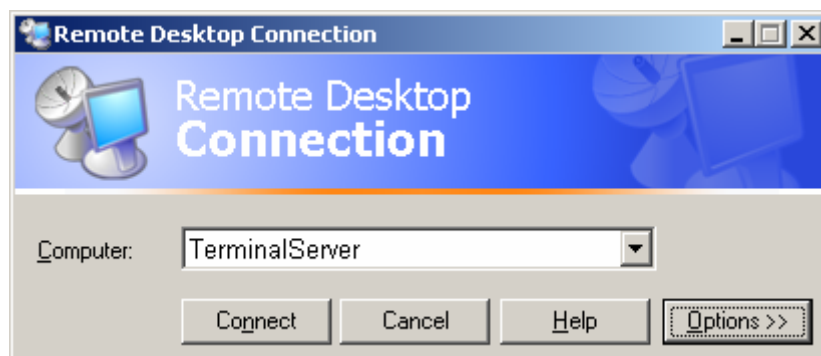
Die aktuelle Version wird i.d.R. über den folgenden Link zur Verfügung gestellt: <http://www.microsoft.com/windowsxp/downloads/tools/rdclientdl.msp> (Stand: Jan. 2005).

3.4. Aufrufen der Remote Desktop Connection Software

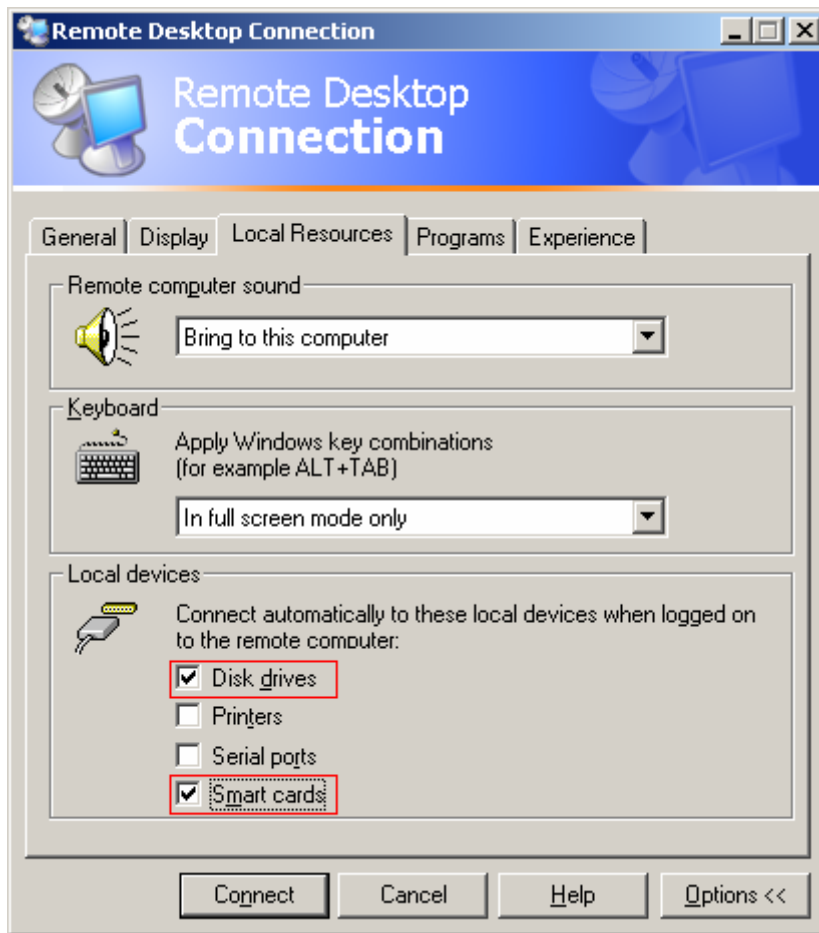
Das Starten der Software erfolgt durch den Aufruf über das Startmenü (Start – Alle Programme – Zubehör – Kommunikation – Remote Desktop Connection).

Die Verknüpfung eines Icons auf dem Desktop macht – bei häufiger Verwendung der Verbindung – Sinn.

Nach dem Aufruf der Remote Desktop Connection Software kann der entsprechend zu verwendende Terminal Server ausgewählt werden:



Damit (einmalig pro Client-System) weitere Optionen eingestellt werden können, ist der Button „Options >>“ zu klicken. Daraufhin können weitere Einstellungen vorgenommen werden.



Bei Auswahl des Reiters „Local Resources“ können weitere Einstellungen vorgenommen werden. Diese sind für die Arbeit mit RDH-Disketten oder bei der Verwendung SmartCards besonders zu beachten:

Smart cards (wird nur angezeigt, wenn ein PC/SC-fähiger Treiber des angeschlossenen SmartCard-Lesers installiert wurde) ist zu aktivieren, wenn das am Client angeschlossene SmartCard-Lesegerät gemeinsam mit HBCI-Chipkarten verwendet werden soll. Üblicherweise ist diese Einstellung aktiviert.

Disk drives ist zu aktivieren, wenn das RDH-Verfahren mit Schlüsseldiskette verwendet werden soll. Sie werden dabei darauf hingewiesen, dass die Verknüpfung mit lokalen Laufwerken ein Sicherheitsrisiko darstellen kann. Dieser Hinweis kann auch ausgeschaltet werden.

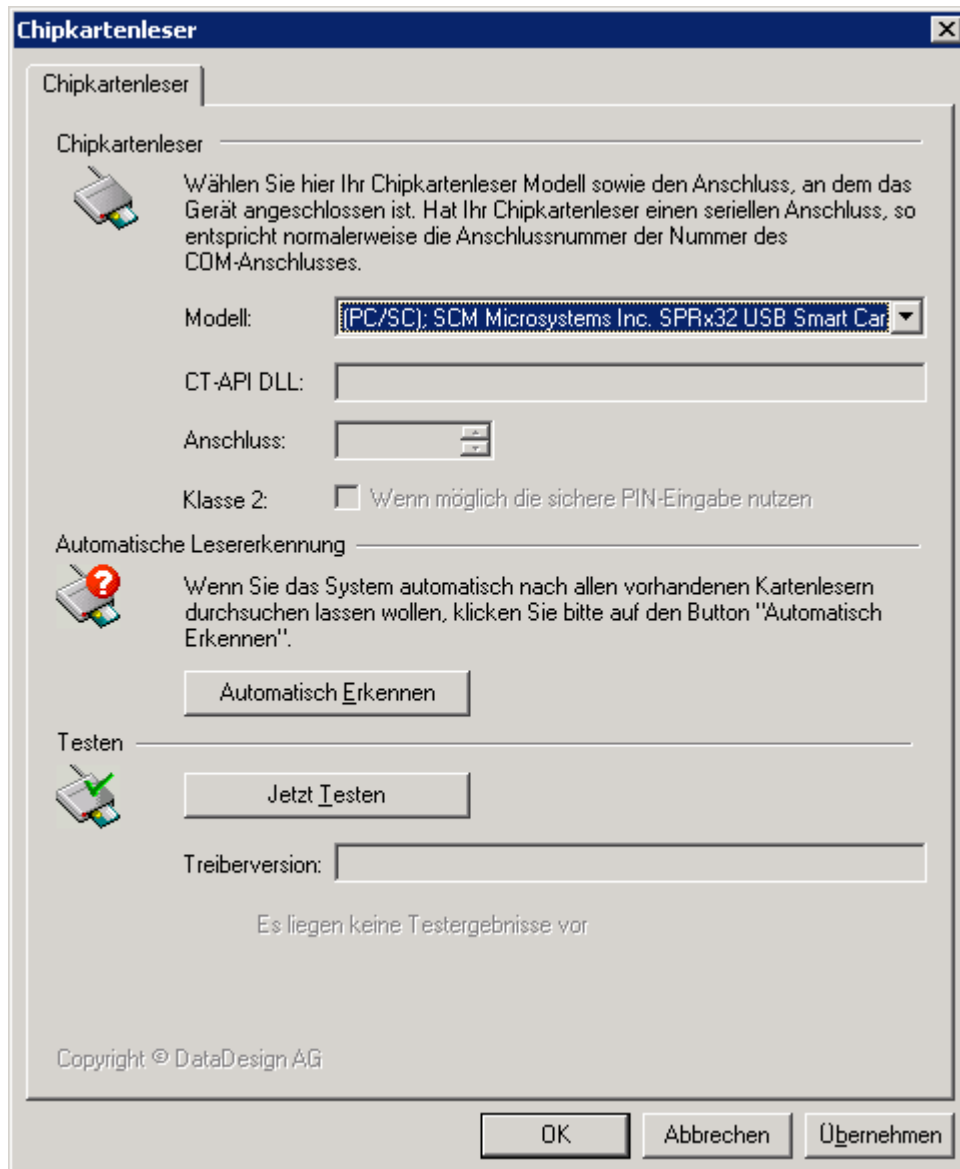
Die oben genannten Änderungen der Optionen werden normalerweise auch bei künftigen Verbindungen verwendet.

3.5. Einrichten des Chipkartenlesegeräts am Terminal Server

Nach Verbindung zum Terminal Server und erfolgreicher Anmeldung muss ggf. das SmartCard-Lesegerät eingerichtet werden.

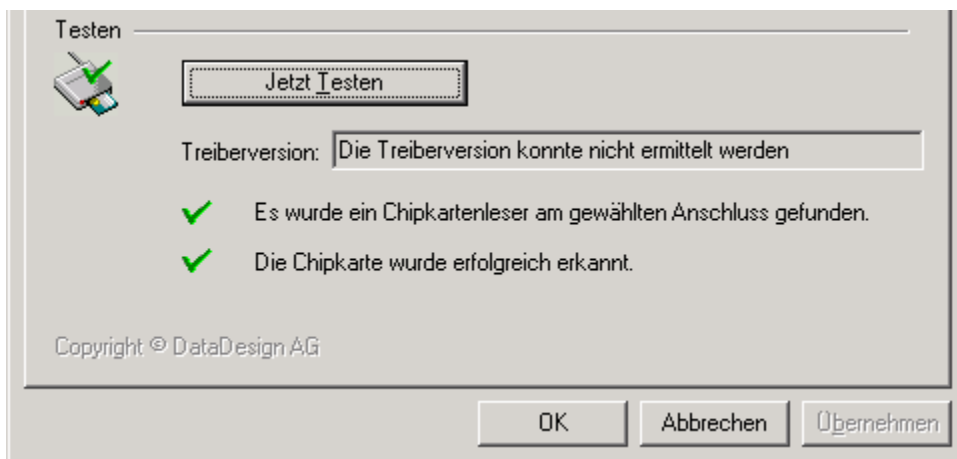
Dieser Schritt kann bei der Verwendung gleicher SmartCard-Lesegeräte und gleicher Treiber-Versionen auf den Client-Systemen entfallen, wenn mit einem anderen Client-System die Einrichtung schon erfolgt ist.

Zum Einrichten des SmartCard-Lesegeräts rufen sie bitte das Dienstprogramm Chipkartenleser aus der Systemsteuerung auf.



Das angeschlossene SmartCard-Lesegerät wird nach Drücken des Buttons „Automatisch Erkennen“ erkannt. In der obigen Abbildung wurde das Chipdrive PinPad des Herstellers SCM gefunden.

Zum Test des Lesers stecken sie bitte eine Karte in das SmartCard-Lesegerät und drücken sie den Button „Jetzt Testen“. Anhand der Rückmeldung des Dienstprogramms können sie erkennen, ob Chipkartenleser und Karte korrekt erkannt wurden.



Bei auftretenden Fehlern prüfen sie bitte die Konfiguration (siehe 3.2. Installation des PC/SC-fähigen SmartCard-Lesers am Client). Bei PC/SC-fähigen SmartCard-Lesegeräten kann i. d. R. die Treiber-version nicht ermittelt werden, die oben abgebildete Ausgabe stellt demnach eine erfolgreiche Kommunikation dar.

Bitte entfernen sie nach erfolgter Prüfung aus Sicherheitsgründen die Chipkarte aus dem SmartCard-Lesegerät.

3.6. Einrichten von Kontakten

Damit die Kommunikation mit den verschiedenen Banken stattfinden kann, muss für jeden Zugang zur Bank ein Kontakt eingerichtet werden.

Dies geschieht über den **Homebanking-Kontakte-Administrator** den sie in der Systemsteuerung auf dem Terminal Server finden.

Dabei gibt es einige – Terminal Server spezifische – Besonderheiten zu beachten:

3.6.1. Mit Chipkarte

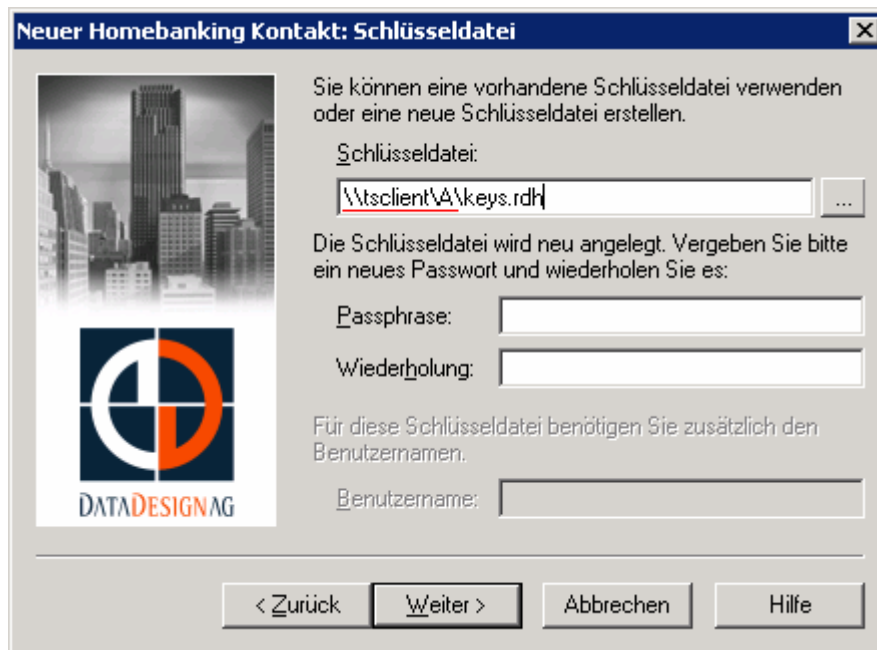
Grundsätzlich muss ein PC/SC-fähiges SmartCard-Lesegerät nebst PC/SC-fähigen Treibern installiert sein (beim Start der Remote Desktop Connection Software muss dabei „Smart cards“ aktiviert sein – siehe 3.4. Aufrufen der Remote Desktop Connection Software).

Bei korrekter Einrichtung (siehe 3.5. Einrichten des Chipkartenlesegeräts am Terminal Server) wird die eingelegte SmartCard ohne Probleme erkannt und verwendet.

In allen anderen Punkten verfahren Sie bitte wie gewohnt, bzw. wie aus der Online-Hilfe des Administrators ersichtlich.

3.6.2. Mit RDH-Diskette

Bei der Auswahl des Speicherplatzes der Schlüsseldatei muss das lokale Laufwerk des Clients eingegeben werden. \\tsclient\A bezeichnet das lokale Diskettenlaufwerk des Clients (beim Start der Remote Desktop Connection Software muss dabei „Disk drives“ aktiviert sein – siehe 3.4 Aufrufen der Remote Desktop Connection Software).



Dazu muss auf dem Client-System eine RDH-Schlüsseldiskette eingelegt sein. Auf gleichem Wege lassen sich auch neue Schlüssel auf einer Diskette erstellen.

In allen anderen Punkten verfahren Sie bitte wie gewohnt, bzw. wie aus der Online-Hilfe des Administrators ersichtlich.

3.6.3. Mit PIN/TAN (HBCI+ oder FinTS)

Beim Einrichten von PIN/TAN-Kontakten (HBCI+ oder FinTS) gibt es keine Terminal Server spezifische Besonderheiten zu beachten.

Bitte verfahren Sie bei der Einrichtung deshalb wie gewohnt, bzw. wie aus der Online-Hilfe des Administrators ersichtlich.

4. Bekannte Probleme

- Bei der Installation der DDBAC-Komponenten werden die Elemente für die Systemsteuerung auf dem Homeverzeichnis des Benutzers installiert. Entspricht das Laufwerk des Homeverzeichnisses (z.B. Z:) nicht dem Laufwerk des Systemverzeichnisses (z.B. C:), so kann der Windows Terminal Server diese Elemente nicht mehr finden und sie werden in der Systemsteuerung nicht angezeigt.

Die Dateien DDBACCPL.CPL, DDBACCTM.CPL müssen deshalb aus dem Unterverzeichnis \WINDOWS\System32\ auf dem Laufwerk des Homeverzeichnis händisch in das Verzeichnis C:\WINDOWS\System32 kopiert werden. Die Datei DDBACCPL.CHM ist in das Verzeichnis C:\WINDOWS\Help zu kopieren. C: bezeichnet dabei das Laufwerk des Systemverzeichnisses.

Mit der Version 3.9.x.x der DDBAC wird dieser Umstand behoben sein und es werden keine händischen Maßnahmen mehr erforderlich sein.

- Die Verwendung der PIN-Eingabe über das SmartCard-Lesegerät (Klasse-2-Leser mit Ziffernblock) wird über die PC/SC-Schnittstelle nicht unterstützt, so dass hierauf verzichtet werden muss und die PIN-Eingabe wie bei Klasse-1-Lesern über die gewöhnliche Tastatur erfolgt.