Beschreibung:

Zusätzliche ICA Session am ThinClient für Zugriff auf OSsecure Systeme mittels Internet Explorer ohne Benutzerwechsel.

Auf den SIA Citrix Servern der Sparkasse wird ein **lokaler** Benutzer „baugleich“ angelegt, bei dem das Kennwort nicht abläuft und einige Sicherheitseinstellungen und Optionen im Profil vergeben werden. Im Admin Tool der ThinClients (Scout-Konsole) wird eine zweite ICA-Session erstellt, die das jeweilige OSsecure-System (z.B. Tagestresor) im Internet Explorer bedient.

Inhalt

1. Anlage eines neuen Benutzers 2

1.1 Registerkarte Allgemein 2

1.2 Registerkarte Umgebung 3

1.3 Registerkarte Mitgliedschaft 4

2. Startskript anlegen und NTFS Berechtigungen vergeben 5

2.1 Startskript anlegen 5

2.2 NTFS Berechtigung für Internet Explorer vergeben 5

3. RDP Terminaldienste konfigurieren 6

3.1 Berechtigung für den RDP Dienst vergeben und den „biometrie“ User hinzufügen 6

3.1.1 Registerkarte Berechtigungen 6

3.2 RDP Anmeldung am Server erlauben 7

3.2.1 Registerkarte Citrix Einstellungen 7

4. Profileinstellungen für den lokalen „biometrie“ User 7

4.1 Bildschirmschoner ausschalten 7

4.2 Internet Explorer Proxy ausschalten 8

4.3 Internet Explorer Startseite festlegen 8

5. ICA Terminaldienste konfigurieren 9

5.1 Berechtigung für den ICA Dienst vergeben und den „biometrie“ User hinzufügen 9

5.1.1 Registerkarte Berechtigungen 9

5.2 ICA ThinClient Anmeldung für den User „biometrie“ am SIA Server erlauben 10

5.2.1 Registerkarte ICA-Einstellungen 10

6. Taskmanager über Richtlinie für den „biometrie“ User deaktivieren 10

7. Anwendung (OSsecure - Biometrie) in der Scout Console je GS erstellen 11

8. Anlage Fehlermeldung 12

9. Umschalten der ICA-Sessions am Thinclient 12

1. Anlage eines neuen Benutzers

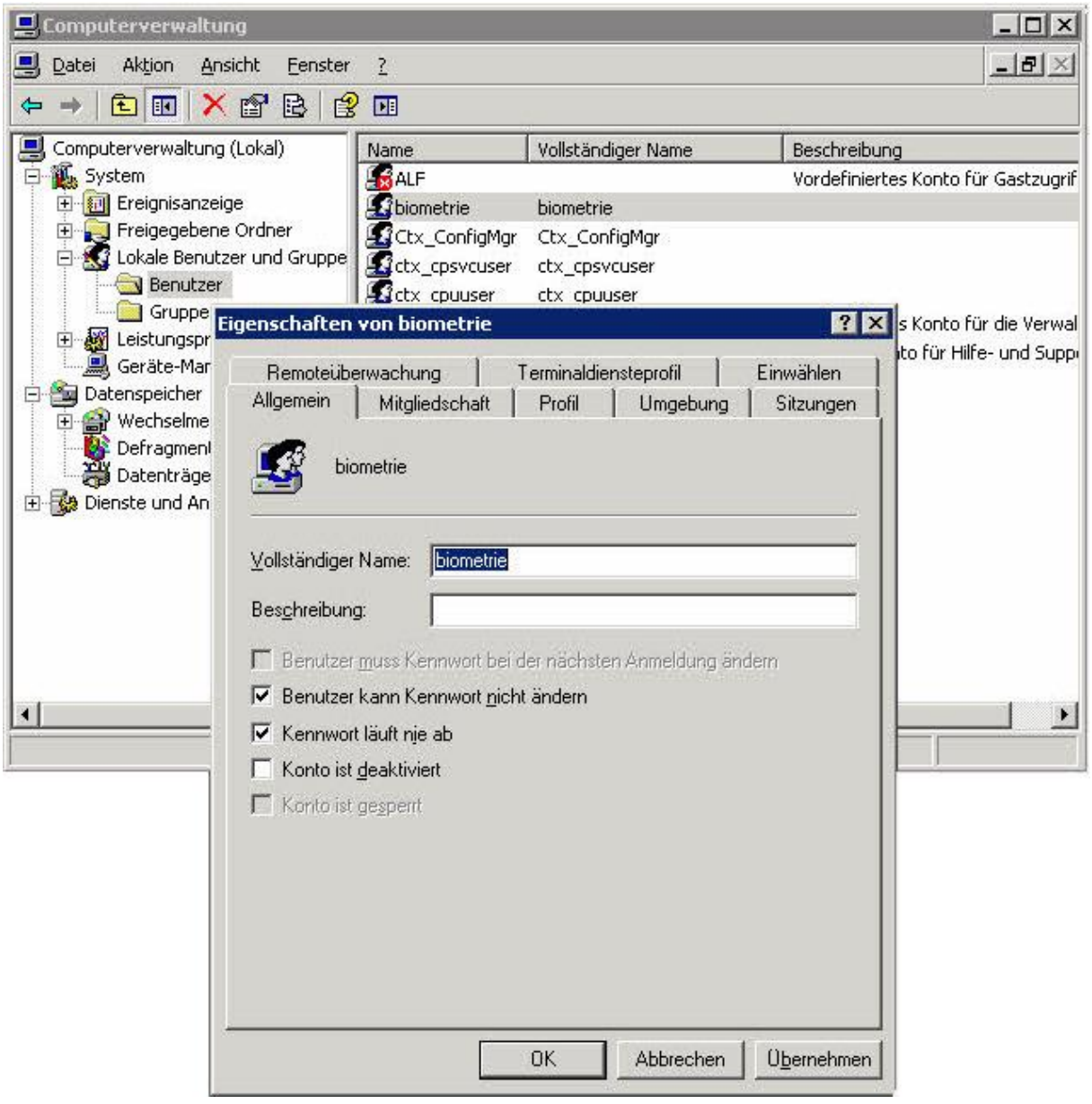
Anlage eines lokalen Benutzers auf den SIA Citrix Servern mit folgenden Eigenschaften.

Benutzername: *biometrie*

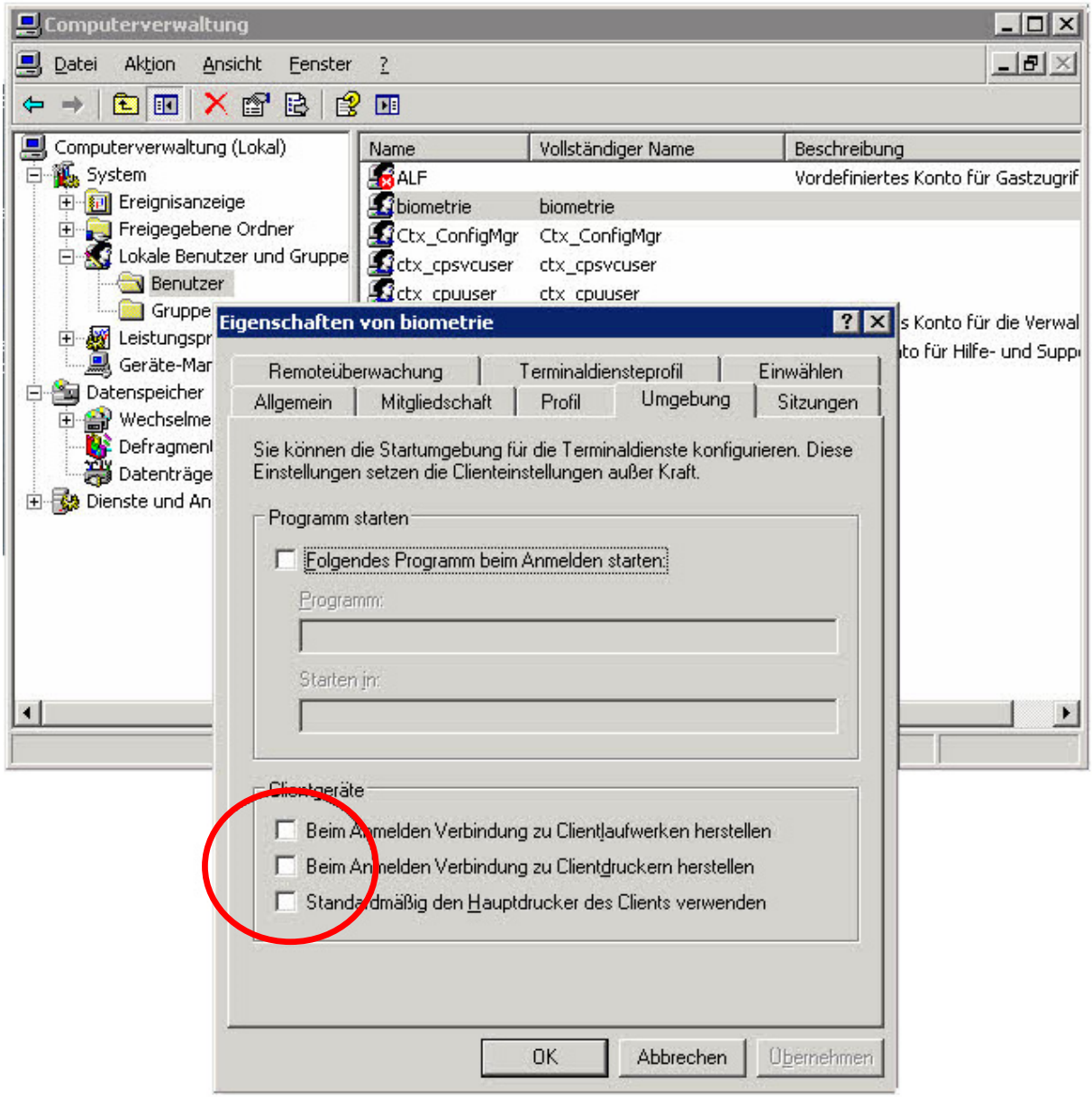
Kennwort: *xxxxxxx*

Computerverwaltung ► System ► Lokale Benutzer ► Eigenschaften (des Users „biometrie“) ►

1.1 Registerkarte Allgemein

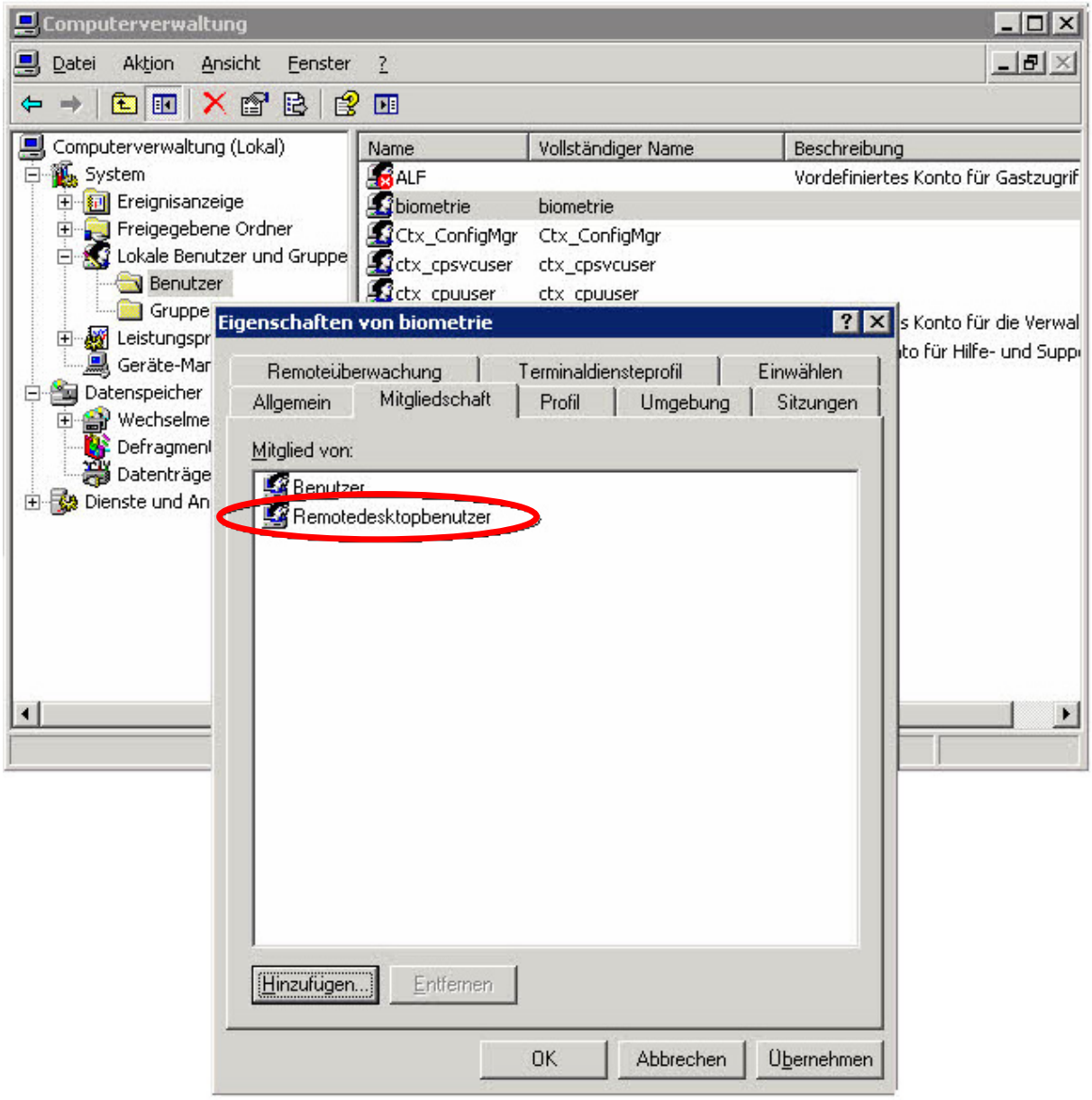


1.2 Registerkarte Umgebung



1.3 Registerkarte Mitgliedschaft

User „biometrie“ muss für ICA Anmeldung Mitglied der Gruppe Remotedesktopbenutzer sein, ansonsten wird er beim Anmeldevorgang mit Fehlermeldung abgewiesen.

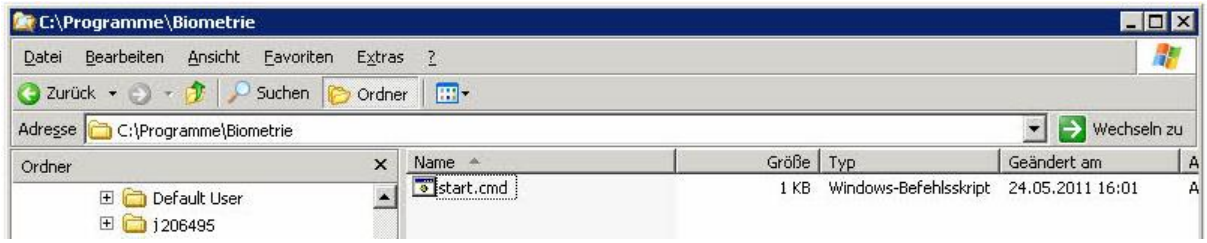


2. Startskript anlegen und NTFS Berechtigungen vergeben

Erstellen Sie Sie im Programmverzeichnis einen Ordner „Biometrie“. Die Verzeichnisrechte müssen für diesen Ordner nicht angepasst werden.

2.1 Startskript anlegen

Erstellen Sie ein Startskript oder legen Sie die fertige und dieser Beschreibung beigefügte Datei „start.cmd“ in dem erstellen Ordner ab.

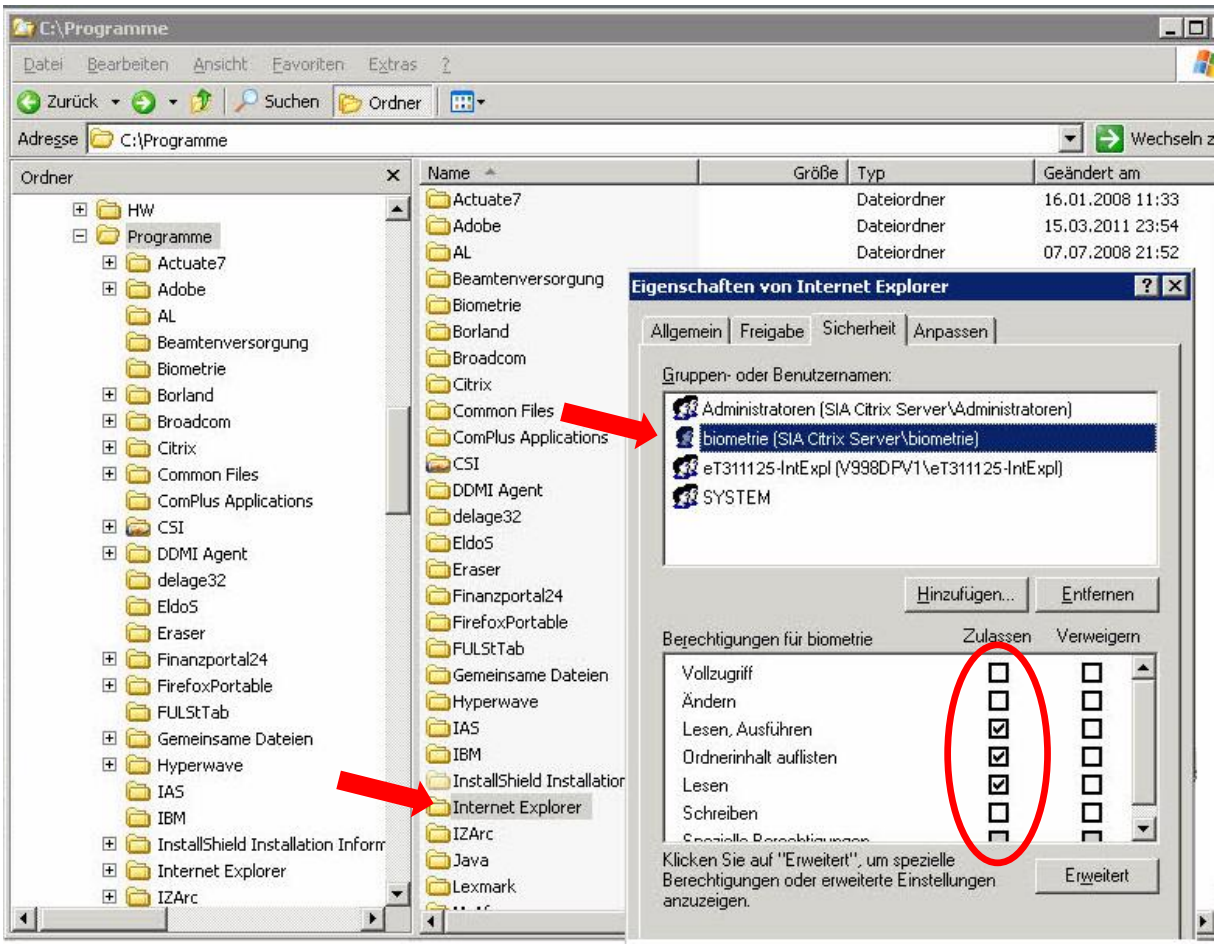


Inhalt der „start.cmd“:

```
@echo off
rem Wird von einer Scout ICA Session aufgerufen
rem OSsecure IE Zugriff
"c:\programme\internet explorer\iexplore.exe" -k -nohome "%1"
exit
```

Der Internetexplorer wird mit dem Parameter (-k) im Kiosk-Mode (Vollbild) und mit dem Parameter (-nohome) ohne Startseite (weiße Seite) gestartet.

2.2 NTFS Berechtigung für Internet Explorer vergeben (Eigenschaften ► Sicherheit)



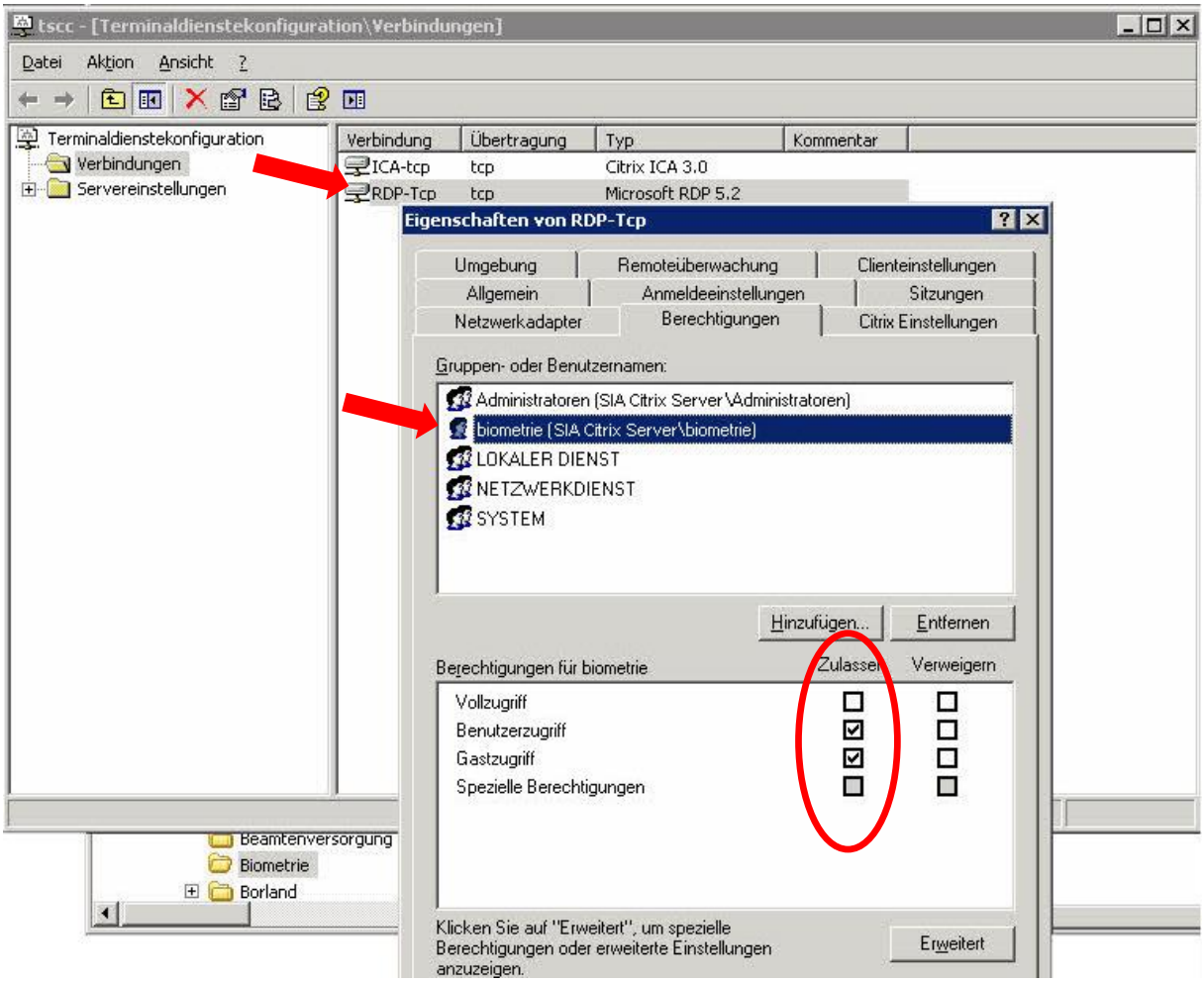
3. RDP Terminaldienste konfigurieren

Für die Einstellung des Userprofiles muss der RDP Terminaldienst konfiguriert werden. Die „Management-Konsole“, bzw. die „Terminaldientekonfiguration\Verbindungen“ wird an den SIA Servern per Kommandozeilenaufruf über „**tscc.msc**“ gestartet.

3.1 Berechtigung für den RDP Dienst vergeben und den „biometrie“ User hinzufügen

tscc.msc ► Verbindungen ► RDP ► Eigenschaften ►

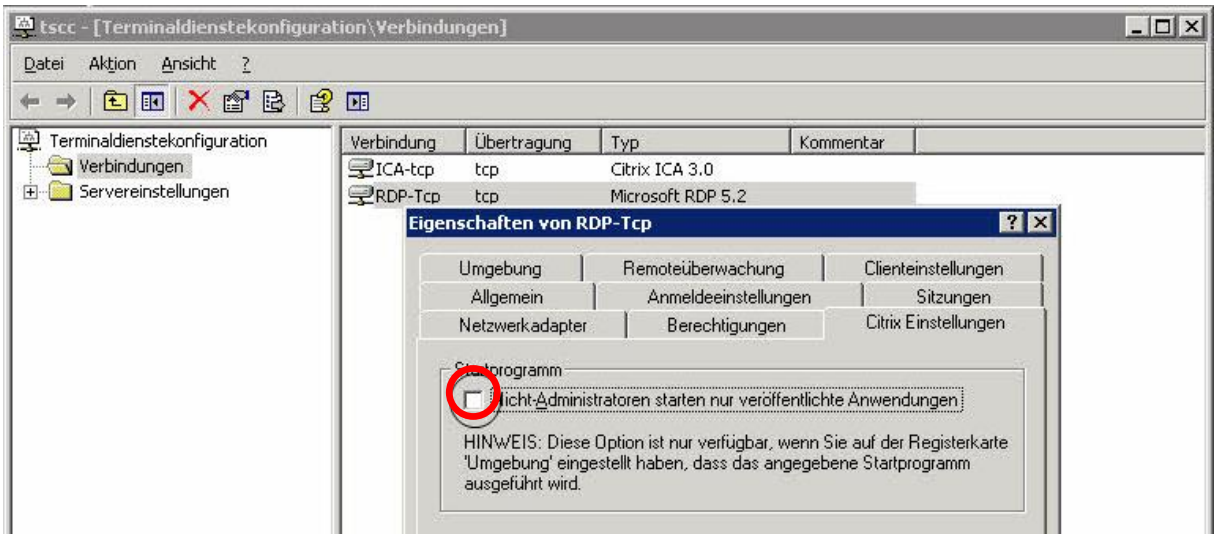
3.1.1 Registerkarte Berechtigungen



3.2 RDP Anmeldung am Server erlauben

Die RDP Anmeldung muss am Server erlaubt werden, ansonsten kann sich der „biometrie“ User zur Einstellung seines Anwenderprofiles nicht anmelden. **Nach Einstellung der Profiloptionen, sollte Haken wieder gesetzt werden**.

3.2.1 Registerkarte Citrix Einstellungen

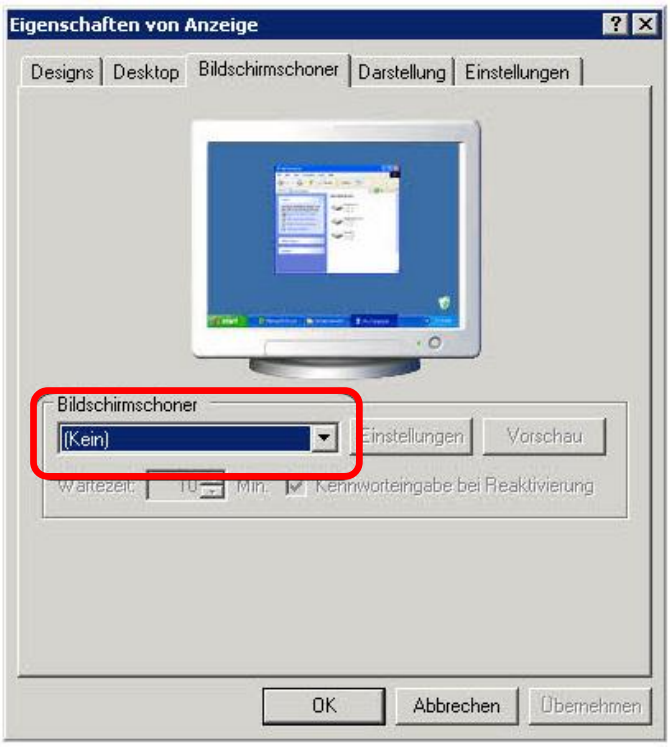


4. Profileinstellungen für den lokalen „biometrie“ User

Anmeldung lokal am Server mit dem User „biometrie“ über die Konsole und den Befehl „mstsc /v:*IP-ADRESSE*“ (IP-Adresse des jeweiligen SIA Servers) durchführen.

4.1 Bildschirmschoner ausschalten

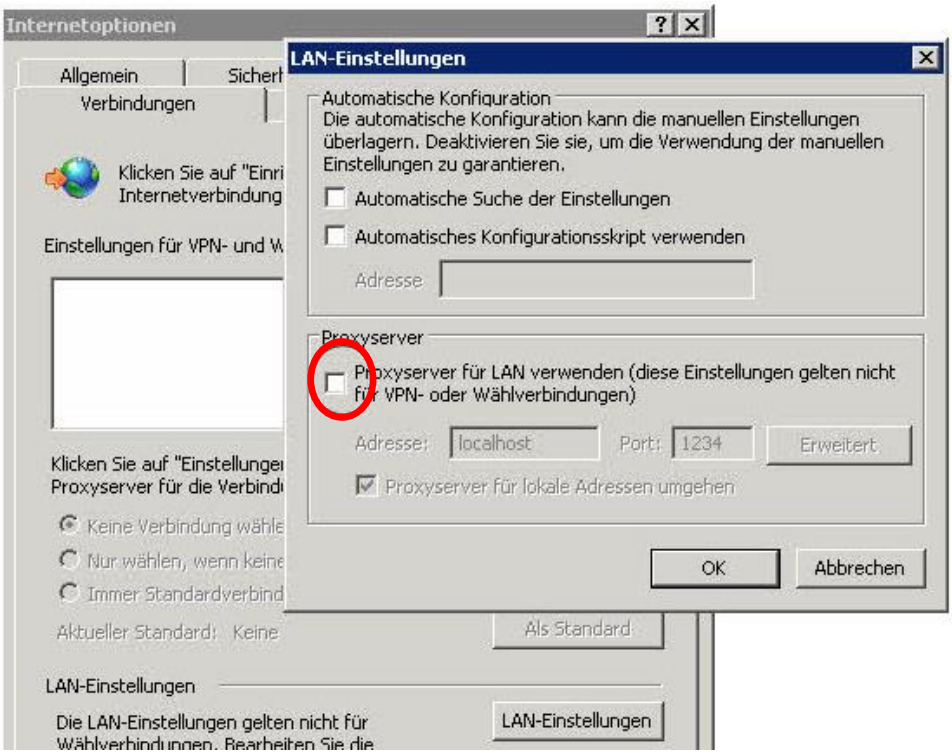
Der User „biometrie“ bleibt immer angemeldet, verfällt nicht in den Bildschirmschoner und wird auch nicht von einem GPO (Gruppenrichtlinienobjekt) überschrieben.



4.2 Internet Explorer Proxy ausschalten

Der Proxy des Internet Explorers muss abgeschaltet werden, ansonsten hat der User „biometrie“ kein Browserzugriff auf die lokalen Adressen (IP-Adresse oder Hostname) der OSsecure-Systeme (Tagestresor, Schleuse, Schlösser).

Internet Explorer ► Extras ► Internet Optionen ► Verbindungen ► LAN Einstellungen



4.3 Internet Explorer Startseite festlegen

Beim Aufruf der „start.cmd“ (siehe Punkt 7) wird die Startseite der Tagestresore mitgegeben. Falls ein Anwender in der ICA Session am ThinClient die Tastenkombination <Alt> <Pos1> drückt, erhält er die „about:blank“ Seite. Mit rechter Maustaste kann er wieder zurück navigieren bzw. den Browser mit <Alt> <F4> schließen um sich komplett neu an der ICA Session anzumelden.

Achtung: **Nach Fertigstellung der Profileigenschaften, sollte die RDP Anmeldung wieder entzogen werden.**

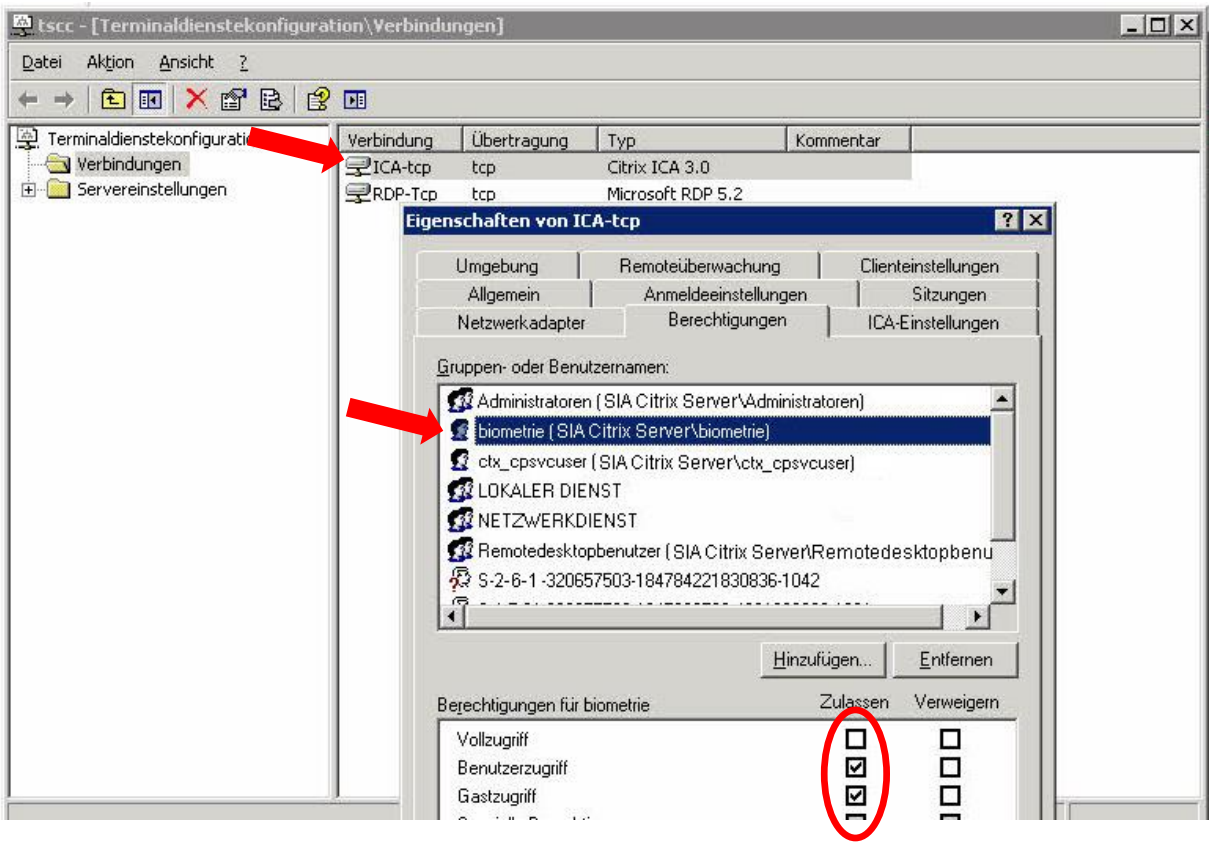
5. ICA Terminaldienste konfigurieren

Für die Einstellung des Userprofiles muss der ICA Terminaldienst konfiguriert werden (wird vom ThinClient verwendet). Die „Management-Konsole“, bzw. die „Terminaldientekonfiguration\Verbindungen“ wird an den SIA Servern per Kommandozeilenaufruf über „**tscc.msc**“ gestartet.

5.1 Berechtigung für den ICA Dienst vergeben und den „biometrie“ User hinzufügen

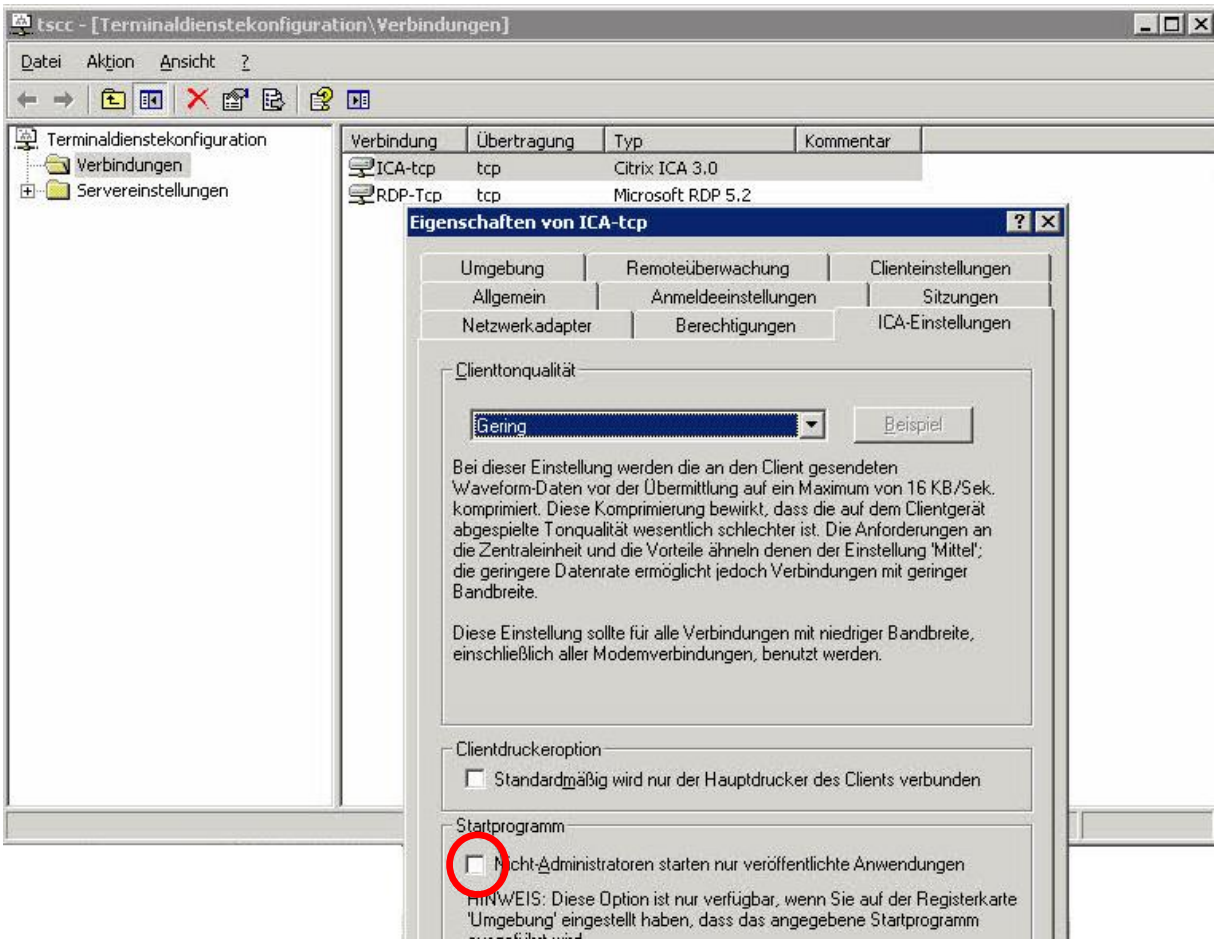
tscc.msc ► Verbindungen ► RDP ► Eigenschaften ►

5.1.1 Registerkarte Berechtigungen



5.2 ICA ThinClient Anmeldung für den User „biometrie“ am SIA Server erlauben

5.2.1 Registerkarte ICA-Einstellungen



6. Taskmanager über Richtlinie für den „biometrie“ User deaktivieren

Um den Taskmanager für den User „biometrie“ zu deaktivieren, benötigt dieser temporäre Adminrechte.

- Kommandozeilenaufruf an BEIDEN SIA Servern über regedt32.
- Schlüssel „System“ unter folgenden Pfad anlegen.

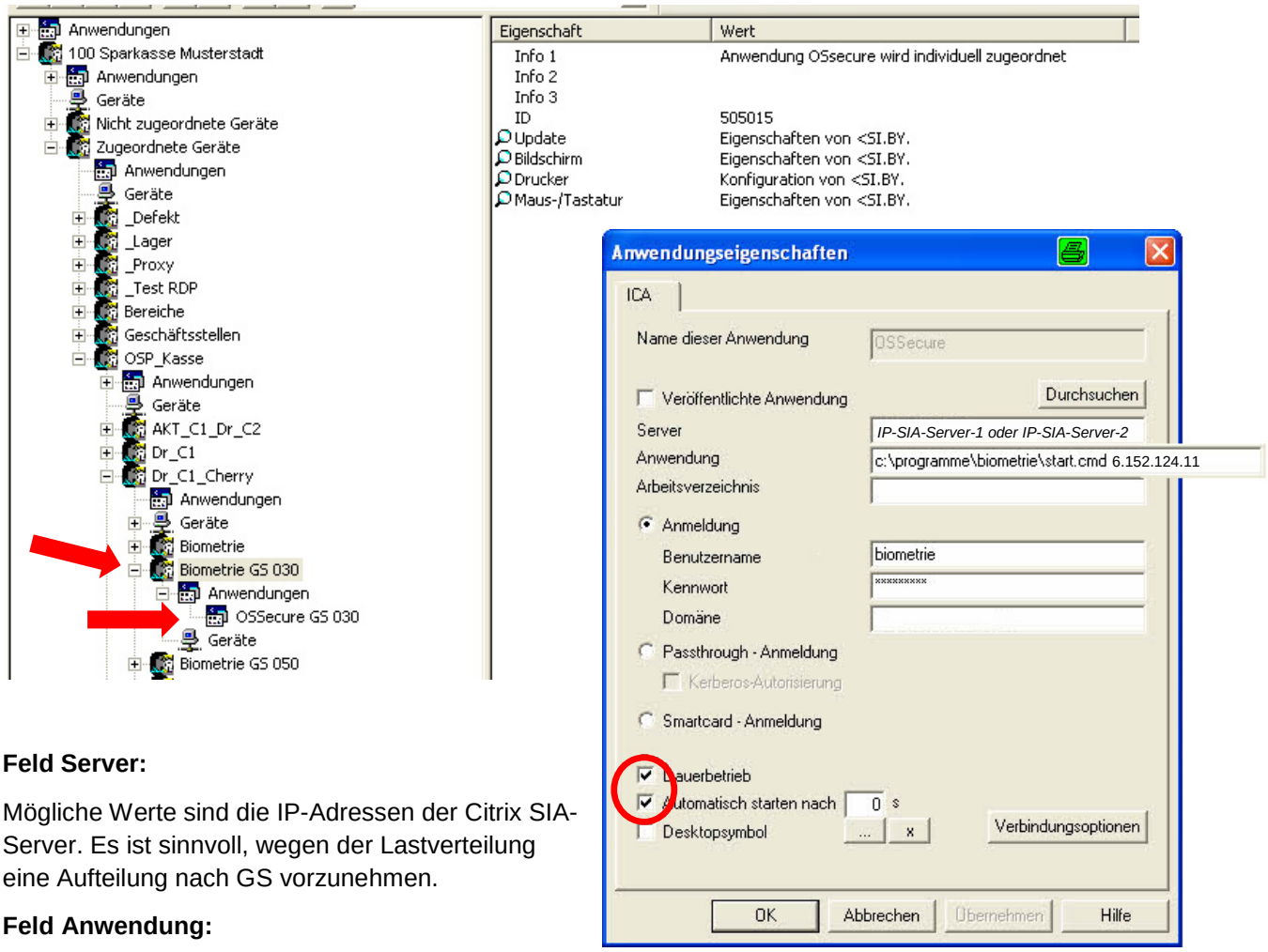
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System

DWORD-Wert mit dem Namen DisableTaskMgr neu erstellen.
DWORD-Wert mit dem Namen DisableLockWorkstation neu erstellen.
DWORD-Wert mit dem Namen DisableChangePassword neu erstellen.

Der Wert **1** sperrt die Funktion
Der Wert **0** oder ein Löschen des jeweiligen Eintrags gibt die Funktion wieder frei.

7. Anwendung (Biometrie) in der Scout Console je GS erstellen

- Anlage einer neuen OE unter …/OSP_Kasse/Dr_C1_Cherry mit dem Namen „**Biometrie GS xxx**“
- Anlage einer neuen Anwendung unterhalb der Biometrie-OE mit dem Namen „OSsecure GS xxx“ und folgenden Eigenschaften:
  - Server: **IP-Adresse 1** (Citrix SIA Server 1) oder **IP-Adresse 2** (Citrix SIA Server 1)
  - Anwendung: c:\programme\biometrie\start.cmd 6.152.xxx.11 (Tagestresor Beispiel)
  - Domäne: „**Hostname 1**“ (Citrix SIA Server 1) bzw. „**Hostname 2**“ (Citrix SIA Server 2)



Feld Server:

Mögliche Werte sind die IP-Adressen der Citrix SIA-Server. Es ist sinnvoll, wegen der Lastverteilung eine Aufteilung nach GS vorzunehmen.

Feld Anwendung:

Der „start.cmd“ wird die jeweilige IP-Adresse oder der Hostname des OSsecure-Gerätes (z.B. Tagestresor) mitgegeben. In diesem Beispiel *6.152.124.11*

Feld Domäne:

Mögliche Werte sind die Hostnamen der Citrix SIA-Server. Hier sollte der Hostname der jeweiligen Maschine stehen, welche unter „Feld Server“ eingetragen wurde („ping –a *IP-SIA-Server*“ würde als Resultat die Namensauflösung (Host-SIA-Server) bringen).

Bei „Dauerbetrieb“ und „Automatisch starten“ bitte Haken setzen, damit sich die ICA Session automatisch wieder startet, wenn der User z.B. den Internet Explorer mit <Alt> <F4> beendet.

In den Verbindungsoptionen sind keine weiteren Einstellungen notwendig, da wir nicht auf veröffentlichte Anwendungen von Citrix zugreifen wollen.

Anschließend den Kassen-ThinClient der Biometrie-GS in „Geräte“ verschieben!

8. Anlage Fehlermeldung

Wenn sich der Benutzer „biometrie“ nicht in der Gruppe Remotedesktopbenutzer befindet, bzw. der Haken in der RDP Terminaldienstekonfiguration (tscc.msc) bei „Nicht-Administratoren starten nur veröffentlichte Anwendungen“ gesetzt ist, dann kann sich der Benutzer nicht anmelden und wird beim Anmeldevorgang mit folgenden Fehlermeldungen abgewiesen (siehe Punkt 3).

9. Umschalten der ICA-Sessions am Thinclient

Tastenkombination: <Strg> + <Alt> + <Cursorpfeile> (nach oben oder nach unten)