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 **Iokaler** 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.	Anla	ge eines neuen Benutzers	2
	1.1	Registerkarte Allgemein	2
	1.2	Registerkarte Umgebung	3
	1.3	Registerkarte Mitgliedschaft	4
2.	Star	skript anlegen und NTFS Berechtigungen vergeben	5
2	2.1	Startskript anlegen	5
2	2.2	NTFS Berechtigung für Internet Explorer vergeben	5
3.	RDP	Terminaldienste konfigurieren	6
3	3.1	Berechtigung für den RDP Dienst vergeben und den "biometrie" User hinzufügen	6
	3.1.1	Registerkarte Berechtigungen	6
3	3.2	RDP Anmeldung am Server erlauben	7
	3.2.1	Registerkarte Citrix Einstellungen	7
4.	Prof	ileinstellungen für den lokalen "biometrie" User	7
4	4.1	Bildschirmschoner ausschalten	7
4	4.2	Internet Explorer Proxy ausschalten	8
4	4.3	Internet Explorer Startseite festlegen	8
5.	ICA	Terminaldienste konfigurieren	9
Ę	5.1	Berechtigung für den ICA Dienst vergeben und den "biometrie" User hinzufügen	9
	5.1.1	Registerkarte Berechtigungen	9
Ę	5.2	ICA ThinClient Anmeldung für den User "biometrie" am SIA Server erlauben	10
	5.2.1	Registerkarte ICA-Einstellungen	10
6.	Tasł	manager über Richtlinie für den "biometrie" User deaktivieren	10
7.	Anw	endung (OSsecure - Biometrie) in der Scout Console je GS erstellen	11
8.	Anla	ge Fehlermeldung	12
9.	Ums	chalten 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

E Computerverwaltung						
📃 Datei Aktion Ansicht	Eenster <u>?</u>					_ 8 ×
⇐ ⇒ 🗈 💽 🗙 😭	8 8 0					÷.
Computerverwaltung (Lokal)	Nar	ne	Vollständig	ger Name	Besch	reibung
🖻 🌇 System	1	ALF			Vorde	finiertes Konto für Gastzugrif
Ereignisanzeige		biometrie	biometrie			
E Kale Benutzer und	Gruppe	Ctx_ConfigMgr	Ctx_Confi	gMgr ucer		
Benutzer		ctx_cpsvcaser ctx_cpuuser	ctx couus	er		
Gruppe Eigenso	haften von	biometrie	AAAA SISMAA	100) 	U.	? 🗙 s Konto für die Verwal
Geräte-Mar	mataiibaruw	obuna I T	orminaldian	stoprofil	Finuäblen	ito für Hilfe- und Supp
🖃 🎦 Datenspeicher 🛛 🗛	emein M	italiedschaft	Profil	Umaebuna		en
🕀 🔐 Wechselme	_				I energy	
	🖗 biometr	ie				
🕀 🎲 Dienste und An	9					
<u>⊻</u> oli:	ständiger Nam	ie: biometrie				
Bes	chreibung:					
Г	Benutzer mus	s Kennwort bei d	ler nächsten	Anmeldung är	ndem	
	Benutzer kann	n Kennwort <u>n</u> icht	ändern			
	Kennwort läuf	t nie ab				
	Konto ist deak	tiviert				
	– Konto ist aesp	ent				
And a						
			ОК	Abbrechen	0 <u>b</u> ernehr	men
				2	13.1	

1.2 Registerkarte Umgebung

💻 Computerverwaltung				_ 🗆 ×
📃 Datei Aktion Ansicht Eenstei	r <u>2</u>			_ 8 ×
← → 🗈 🖬 🗙 📽 😫 🖆	ያ ⊡			
🗐 Computerverwaltung (Lokal)	Name	Vollständiger Name	Beschreib	ung
🖹 🛱 🎇 System			Vordefinie	rtes Konto für Gastzugrif
	biometrie	biometrie		
E Freigegebene Ordner	Ctx_ConfigMgr	Ctx_ConfigMgr		
	ttx_cpsvcuser	ctx_cpsvcuser		
	A Ctx cpuuser	ctx cpuuser	2 .	
Eigenscharter	i von biometrie			to für Hilfe- und Suppr
Geräte-Mar Remoteut	perwachung	Terminaldiensteprofil	Einwählen	
Datenspeicher Allgemein	Mitgliedschaft	Profil Umgebung	Sitzungen	ļ
🔐 Defragmen I Sie können	die Startumgebung fü	ir die Terminaldienste konfiqu	urieren. Diese	
🛛 🔚 Datenträge Einstellunge	in setzen die Clienteir	nstellungen außer Kraft. 🦷		
🗄 😼 Dienste und An	starten			
	ndes Programm beim	Anmelden starten:		
Progra	ะกาก:			
Starte	n in:			
/			-	
			12	
	te			
🗖 Beim	Anmelden Verbindun	g zu Clientjaufwerken herstel	llen	
🗖 Beim	An nelden Verbindun	g zu Client <u>d</u> ruckern herstelle	n	
🗖 Stand	da dmäßig den <u>H</u> aupt	drucker des Clients verwend	len	
-			Ē.	4
		OK Abbrechen	Ubernehmen	
1 m				

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.

🞑 C:\Programme\Biometrie					_ 🗆 🗙
Datei Bearbeiten Ansicht Eavoriten	E <u>x</u> tras	s <u>2</u>			1
🔇 Zurück 🔹 🕥 🕣 🍠 🔎 Suchen 🥫) Ordne	er 🖽 🕶			
Adresse 🛅 C:\Programme\Biometrie					💌 📄 Wechseln zu
Ordner	x	Name 🔺	Größe	Тур	Geändert am
 		start.cmd	1 KB	Windows-Befehlsskript	24.05.2011 16:01

Inhalt der "start.cmd":

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

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

Datei Bearbeiten Ansicht Ea	voriten Extras ?		
🗅 Zurück 🔹 🍙 👻 🎲 🛛 🔎 Suc			
dresse 🗁 C:\Programme			💌 🔁 Wechs
Ordner	× Name *	Größe Typ	Geändert am
 	Actuate7	Dateiordn Dateiordn Dateiordn	er 16.01.2008 11:33 er 15.03.2011 23:54 er 07.07.2008 21:52
	ng Citrix	Ing Eigenschaften von Internet Explor Allgemein Freigabe Sicherheit Ar <u>G</u> ruppen- oder Benutzernamen:	er 🤋 🕅
 Borland Broadcom Citrix Common Files ComPlus Applicatio CSI DDMI Agent 	Ins	ions Side Administratoren (SIA Citrix Server) ions Side T311125-IntExpl (V998DPV1) Sig SYSTEM	er\Administratoren) metrie) eT311125-IntExpl)
 delage32 Eldo5 Eraser Finanzportal24 FirefoxPortable FULStTab Gemeinsame Date Hyperwave IAS IBM InstallShield Instal Internet Explorer IZArc 	en Eraser Finanzportal24 FirefoxPortable FULStTab Gemeinsame Dat Hyperwave IAS InstallShield Inst InstallShield Inst Internet Explore IZArc Java Lexmark	H Berechtigungen für biometrie eien Vollzugriff Ändern Lesen, Ausführen Ordnerinhalt auflisten Lesen allatior Lesen r Schreiben Klicken Sie auf "Erweitert", um spezi Berechtigungen oder erweiterte Einstanzuzeigen.	nzufügen Entfernen Zulassen Verweigern U U

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

🚔 tscc - [Terminaldienstekonfigura	tion\¥erbindu	ngen]				_ 🗆 🗵
Datei Aktion Ansicht ?						
← → 🖻 🖬 🗙 📽 😫 🔮						
🙀 Terminaldienstekonfiguration	Verbindung	Übertragung	Тур	Kommentar	Î.	
Verbindungen	ICA-tcp	tcp	Citrix ICA 3.0		_	
E Servereinstellungen	RDP-Tcp	tcp	Microsoft RDP 5.2			
	Eigen	schaften von R	DP-Tcp		ŶX	
		Umgebung	Remoteüberwachung	Client	einstellungen	
		Allgemein	Anmeldeeinstellung	gen	Sitzungen	
		Netzwerkadapter	Berechtigungen	Citrix	Einstellungen	
	G	ruppen- oder Benu				
		😰 Administratorer	I (SIA Citrix Server VAdmini	istratoren)		
		😰 biometrie (SIA)	Citrix Server\biometrie)			
		🕫 LOKALER DIE	NST			
		🕵 NETZWERKD	IENST			
		🕵 SYSTEM				
			E	linzufügen	Entfernen	
		و میر			Variation	
	B	erechtigungen für t	piometrie	Zulasser		
		Vollzugriff				
		Benutzerzugriff				
		Gastzugriff Specialle Percekt	2110-200			
		opozielie Delecht	gangett			
Beamtenver	sorgung					
🗁 Biometrie						
🕀 🛅 Borland						
	KI	icken Sie auf "Erw	eitert", um spezielle			
	ie Bi	erechtigungen ode nzuzeigen.	r erweiterte Einstellungen			

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.

		-
Jesigns Desktop		gen
Bildschirmschon		
(Kein) Wartezeit	Einstellungen Vors	chau vierung

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

rnetoptionen	? ×
	AN-Einstellungen
Verbindungen III Sichen III Verbindungen IIII Klicken Sie auf "Einri Internetverbindung Einstellungen für VPN- und W	Automatische Konfiguration Die automatische Konfiguration kann die manuellen Einstellungen überlagern. Deaktivieren Sie sie, um die Verwendung der manuellen Einstellungen zu garantieren. Automatische Suche der Einstellungen Automatisches Konfigurationsskript verwenden Adresse
Klicken Sie auf "Einstellunge Proxyserver für die Verbindi	Proxyserver Proxyserver für LAN verwenden (diese Einstellungen gelten nicht für VPN- oder Wählverbindungen) Adresse: localhost Port: 1234 Erweitert. Proxyserver für lokale Adressen umgehen
C Nur wählen, wenn keine C Immer Standardverbind	OK Abbreche
Aktueller Standard: Keine	Als Standard
LAN-Einstellungen	
Die LAN-Einstellungen gelten n	nicht für 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.

<u>Achtung</u>: 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

tscc - [Terminaldienstekonfigu	ation\Verbind	lungen]				_ 0
<u> 2</u> atei Ak <u>t</u> ion <u>A</u> nsicht <u>?</u>						
- → 🖻 🔟 🗡 📽 😫 (§ 🖪					
🖞 Terminaldienstekonfigurati	Verbindung	Übertragung	Тур	Kommentar		
	☐ ICA-tcp	tcp	Citrix ICA 3.0			
⊡	RDP-Tcp	tcp	Microsoft RDP 5.2			
	Eige	enschaften von IC	A-tcp		? ×	
		Umgebung	Remoteüberwachung	Clier	nteinstellungen	
		Allgemein	Anmeldeeinstellun	gen	Sitzungen	
		Netzwerkadapter	Berechtigunger	n ICA	-Einstellungen	
		Gruppen- oder Benu	Izernamen:			
		Administratorov	(CIA Citrix Convort Adm	inistratoron)		
		C biometrie (SIA	Citrix Server biometrie)	riisuatorerij		
			(SIA Citrix Server\ob. c	reveueer		
			NST	psycusery		
			IENST			
		Remotedeskto	obenutzer (SIA Citrix Ser	vertRemoted	esktophenu	
		5 S-2-6-1-32065	7503-184784221830836	1042	and a	
			Ŀ	linzufügen	<u>E</u> ntfernen	
	100	Berechtigungen für t	iometrie	Zulassen	Verweigern	
		Vollaugriff				
		Reputzerzugriff				
		Gastzugriff			H	
	- Aller - Aller					

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

5.2.1 Registerkarte ICA-Einstellungen

Terminaldienstekonfiguration	Verbinduna	Übertragung	Тур	Kommentar	
Verbindungen	PICA-tcp	tcp	Citrix ICA 3.0		
Servereinstellungen	RDP-Tcp	tcp	Microsoft RDP 5.2		
	Eiger	nschaften von IC	A-tcp		? ×
		Umgebung	Remoteüberwachung	Clier	nteinstellungen
		Allgemein	Anmeldeeinstellung	ien	Sitzungen
	1200	Netzwerkadapter	Berechtigunger	IC4	A-Einstellungen
		Gering Bei dieser Einstellu Waveform-Daten v komprimiert. Diese abgespielte Tonqu die Zentraleinheit u die geringere Dater Bandbreite.	ng werden die an den Clier or der Übermittlung auf en Komprimierung bewirkt, da altät wesentlich schlechter nd die Vorteile ähneln den nrate ermöglicht jedoch Ve ollte für alle Verbindungen	t gesendeten Maximum vor ss die auf dem ist. Die Anfore en der Einstelli bindungen mit mit niedriger B	eispiel 116 KB/Sek. Clientgerät derungen an ung 'Mittel'; t geringer andbreite,
		einschließlich aller	Modemverbindungen, ben	utzt werden.	
	-	Clientdruckeroption	Modemverbindungen, beni	utzt werden.	
		clientdruckeroption	Modemverbindungen, ben n ig wird nur der Hauptdruck	utzt werden. er des Clients	verbunden
		Clientdruckeroption	Modemverbindungen, ben n ig wird nur der Hauptdruck	utzt werden. er des Clients	verbunden

6. Taskmanager über Richtlinie für den "biometrie" User deaktivieren

Um den Taskmanager für den User "biometrie" zu deaktivieren, benötigt dieser <u>temporäre</u> 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:
 - o 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)



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).

Anmelde	rneldung
<u>.</u>	Sie müssen über die Zugriffsberechtigung für Terminalserverbenutzer auf diesem Computer verfügen, um sich remote anmelden zu können. Standardmäßig verfügen Mitglieder der Gruppe "Remotedesktopbenutzer" ober diese Berechtigung. Wenn Sie kein Mitglied der Gruppe "Remotedesktopbenutzer" oder einer anderen Gruppe, die über diese Berechtigung verfügt, sind bzw. wenn die Gruppe "Remotedesktopbenutzer" nicht über diese Berechtigung verfügt, muss Ihnen die entsprechende Berechtigung manuell zugewiesen werden.
	ск
	Yerbindungsfehler 🛛
	Dieser Desktop steht derzeit nur Administratoren zur Verfügung. Wenden Sie sich an Ihren Administrator, um sicherzustellen, dass die richtigen Optionen für Ihre Clientverbindung eingestellt wurden.

9. Umschalten der ICA-Sessions am Thinclient

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

