:datapol:

WinSafe.net

Administratorhandbuch

WinSafe.net

Administratorhandbuch

Hochsichere Verschlüsselung für Benutzergruppen

Windows® 2000
Windows® XP Home
Windows® Server 2003
Windows® XP Professional

Inhaltsverzeichnis

Kapitel 1

1 Das Sicherheitskonzept

WinSafe.net verwendet ein extrem einfaches Sicherheitskonzept, welches leicht verständlich ist. Es existieren lediglich zwei Arten von Benutzern innerhalb von *WinSafe.net*:

Standardbenutzer

Dieser Benutzer verfügt über die folgenden Berechtigungen:

- Änderung der PIN seiner eigenen SmartCard.
- Erstellen eines neuen Datentresors auf *WinSafe.net*-Servern auf denen seine SmartCard registriert ist.
- Verwalten von Mitbenutzungsrechten für eigene Tresore (der anlegende Benutzer ist immer der Besitzer des Tresors).
- Öffnen eines Datentresors für den er eine Berechtigung besitzt.
- Schließen eines geöffneten Datentresors.
- Löschen eigener Datentresore .

Administrator

Jeder als Administrator angelegte Benutzer kann mit seiner SmartCard zusätzlich folgende Operationen durchführen:

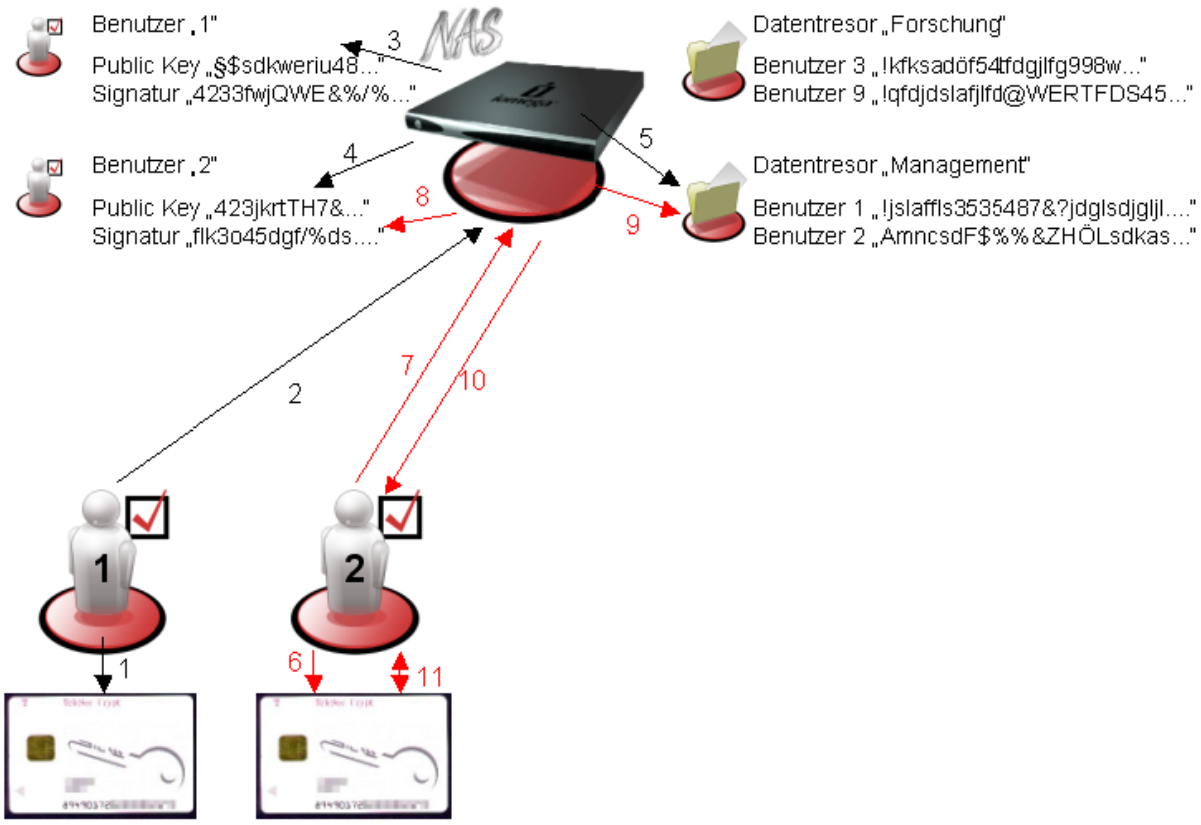
- Ausgeben einer SmartCard an einen neuen Benutzer.
- Ausgeben einer SmartCard an einen neuen Administrator.
- Löschen eines Benutzereintrags von sämtlichen existierenden Datentresoren.
- Löschen einer SmartCard.
- Austausch einer SmartCard (z.B. wenn ein Benutzer seine SmartCard vergessen hat).

Jede in *WinSafe.net* definierte SmartCard stellt, je nach zugewiesener Berechtigung, einen Benutzer oder Administrator dar. Alle in *WinSafe.net* festgelegten Berechtigungen beziehen sich dann auf die jeweilige SmartCard.

Da ein Administrator in *WinSafe.net* sehr viele Rechte hat, ist es wichtig, NUR vertrauenswürdigen Personen im Unternehmen eine SmartCard mit Administratorrechten auszugeben!

1.1 Arbeitsweise der Verschlüsselung

Das Arbeitsmodell von *WinSafe.net* ist in der folgenden Grafik näher dargestellt:



Vereinfacht erfolgt eine Verschlüsselung auf folgende Weise:

Anlegen eines neuen Datentresors und Vergabe der Berechtigung für Benutzer 2:

1. Prüfung der PIN der SmartCard von Benutzer 1
2. Herstellung einer Verbindung mit dem *WinSafe.net*-Server um den Datentresor "Management" anzulegen.
3. Prüfung der Signatur der SmartCard von Benutzer 1

3+4. Die Public-Keys von Benutzer 1 und Benutzer 2 werden aus der Datenbank gelesen

5. Der Datentresor wird angelegt und ein zufälliger Schlüssel für AES generiert. Dieser Schlüssel wird mit den Public-Keys aller zugelassenen Anwender (Benutzer 1 und 2) verschlüsselt im Datentresor gespeichert.

Nutzung des Datentresors "Management" durch den Benutzer 2:

6. Prüfung der PIN der SmartCard von Benutzer 2
7. Herstellung einer Verbindung mit dem *WinSafe.net*-Server um den Datentresor "Management" zu öffnen.
8. Prüfung der Signatur der SmartCard von Benutzer 2
9. Falls ein Benutzereintrag für den Benutzer 2 im Datentresor "Management" vorliegt wird der verschlüsselte Key gelesen.
10. Übertragung des verschlüsselten Keys zum Client
11. Die SmartCard führt eine RSA-Entschlüsselung des Keys durch und übermittelt das Resultat an den Client.

Ab jetzt werden alle Schreib- und Lesezugriffe von Benutzer 2 auf den Datentresor mit dem Key des Tresors auf dem Client ver- und entschlüsselt. Sobald die SmartCard aus dem Leser entfernt wird verliert die Session ihre Gültigkeit und der Prozess muss erneut durchlaufen werden.

1.2 Die Arbeitsweise von Rijandel

Für alle Kryptografie-Spezialisten empfehlen wir die offizielle Rijandel Spezifikation.

Eine grobe Beschreibung des Algorithmus:

Rijndael unterstützt Block- und Schlüssellängen von 128, 192 und 256 Bit. Sowohl der Schlüssel als auch die Blöcke werden als rechteckiges Feld von 4x4, 6x4 bzw. 8x4 Bytes interpretiert. Sämtliche Berechnungen werden byteweise durchgeführt, wobei die Bytes nicht als Zahlen, sondern als Elemente des finiten Felds GF(28) aufgefasst werden. Die Kombination aus Block- und Schlüssellänge bestimmt die Anzahl der Runden. Die Rundenfunktion ist für jede Runde (außer der letzen) gleich. Sie besteht aus den folgenden vier verschiedenen Operationen:

- **ByteSub**

8x8 S-Box, bewirkt Nichtlinearität

- **ShiftRow**

Verschiebung der Zeilen (abhängig von der Blocklänge), bewirkt Inter-Spalten-Diffusion

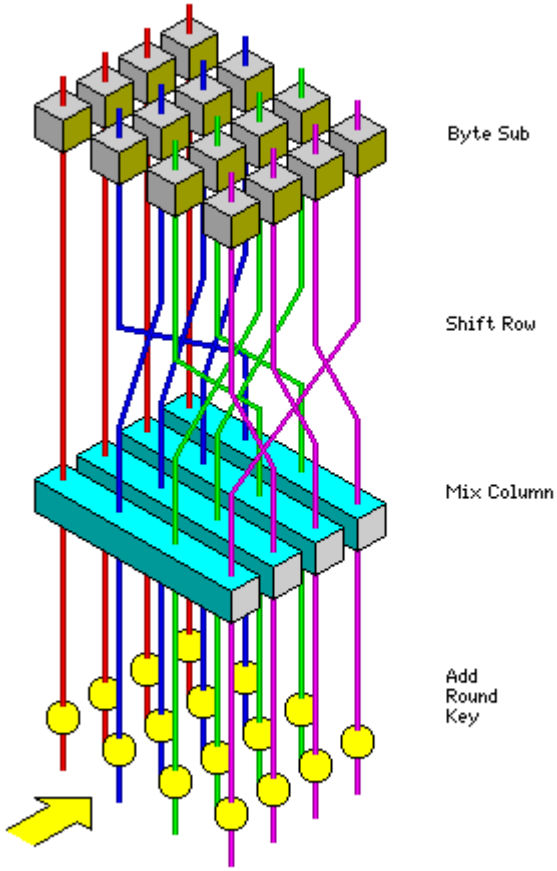
- **MixColumn**

Multiplikation der Spaltenvektoren mit einer 4x4-Matrix, bewirkt Intra-Spalten-Diffusion

- **AddKey**

Addition des Rundenschlüssels, bewirkt Schlüsselabhängigkeit

Vor der ersten Runde wird ein zusätzlich erzeugter Rundenschlüssel addiert, in der letzten Runde entfällt die MixColumn-Operation. Die Rundenschlüssel werden aus dem Hauptschlüssel durch eine Expansionsfunktion
erzeugt.



Quelle: A Cryptographic Compendium, http://home.ecn.ab.ca/~jsavard/crypto/jscrypt.htm

Kapitel II

2 Einrichtung und Installation

Die Installation und Einrichtung einer *WinSafe.net*-Umgebung sollte in folgenden Schritten durchgeführt werden:

- Installation der Serversoftware von *WinSafe.net*
- Installation von mindestens einem *WinSafe.net*-Client mit Administration
- Einstellung der Berechtigungen auf dem Server
- Hinzufügen der Clientlizenzen zu *WinSafe.net*
- Anlage des ersten Administrators
- Installation der restlichen Clients
- Anlage der weiteren Benutzer und Administratoren sowie Ausgabe der SmartCards
- Anlage der Tresore durch die Benutzer

2.1 Installation des Servers

Lesen Sie sich bitte vor der Installation die Systemvorrausetzungen für den Server durch.
Starten Sie das Setup über den entsprechenden Menüpunkt der mitgelieferten Installations-CD und folgen Sie den Anweisungen.
Für die Installation der Serverkomponente benötigen Sie Administratorrechte.
Während der Installation müssen Sie den Programmpfad, in dem der *WinSafe.net*-Server installiert werden soll, und das Verzeichnis für die Ablage der zukünftigen Tresore festlegen.
Nach der Installation ist ein Neustart des Servers notwendig.

2.2 Installation der Clients

Zur Installation eines *WinSafe.net*-Clients muss eine Verbindung mit dem *WinSafe.net*-Server zur Freigabe "dpcryclnt" hergestellt werden. Alternativ kann der *WinSafe.net*-Client auch von der mitgelieferten CD-ROM installiert werden.

Für die Installation der Clientsoftware werden Administratorrechte auf dem zu installierenden PC benötigt.

Vor der Installation des *WinSafe.net*-Clients muss der SmartCard-Leser auf dem System installiert werden. Machen Sie sich vor der Installation bitte mit den notwendigen Systemvorrausetzungen vertraut.
Unter Windows XP wird der von Datapol gelieferte Leser automatisch installiert. Für Windows 2000 benötigen Sie jedoch einen Treiber, welchen Sie unter der Freigabe "dpcryclnt" des *WinSafe.net*-Servers oder auf der Installations-CD finden.

Beachten Sie bitte, dass die Clientsoftware derzeit nur Windows 2000, XP oder höher unterstützt.

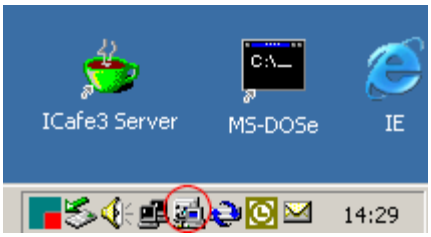
Starten Sie die Installation des *WinSafe.net*-Clients über den entsprechenden Menüpunkt der

Installations-CD.

Nach der Bestätigung der Lizenzbedingungen legen Sie den Installationspfad fest und entscheiden, ob auf dem Client auch die Administrationskomponente für *WinSafe.net* installiert werden soll. Dies ist nur auf Computern von Anwendern erforderlich, die SmartCards ausgeben und verwalten sollen.

Nach der Installation muss ein Neustart des PC erfolgen.

Nach dem Neustart erkennen Sie die erfolgreich verlaufene Installation am Vorhandensein des *WinSafe.net*-Tray-Icons.



2.3 Einstellen der Berechtigungen

Nach der Inbetriebnahme des *WinSafe.net*-Servers sollten Sie die NTFS-Berechtigungen sowie die Freigabeberechtigungen der Freigabe Winsafe$ definieren. Wie Sie den Server am Besten administrieren, können Sie im Serverhandbuch des jeweiligen Anbieters bzw. im Systemhandbuch des jeweiligen Windows-Betriebssystems nachlesen.

NTFS Berechtigungen:

Während der Installation des Servers haben Sie ein Verzeichnis für die Ablage der zukünftigen Tresore festgelegt.
Stellen Sie nun die NTFS-Berechtigungen dieses Verzeichnisses Ihren Bedürfnissen entsprechend ein. Achten Sie dabei darauf, dass jeder Benutzer mit einer gültigen SmartCard für *WinSafe.net* mit seinem Windows Benutzerkonto Vollzugriff auf dieses Verzeichnis erhält. Werden die Rechte eines Benutzers eingeschränkt, so kann er eventuell bestimmte Operationen, wie das Anlegen eines Tresors oder Schreiben von Dateien, nicht mehr durchführen.
Da eine administrative Freigabe im Netzwerk normalerweise unsichtbar ist, genügt es in vielen Fällen "Jeder" durch "Authentifizierte Benutzer" zu ersetzen.

Freigabeberechtigungen:

Jeder Benutzer einer SmartCard benötigt außerdem ausreichende Rechte bei den Freigabeberechtigungen. In der Regel bedeutet dies, dass alle Benutzer von *WinSafe.net* Vollzugriff auf die Freigabe Winsafe$ erhalten sollten.

Zur vereinfachten Administration können Sie Windows Gruppen verwenden.

2.4 Verwalten der Lizenzen

Das Lizenzmodell von *WinSafe.net*

WinSafe.net erfordert eine Lizenz je ausgegebener SmartCard auf dem *WinSafe.net*-Server. Auf den Clients müssen keine Lizenzen vergeben werden. Ist die maximale Anzahl von Benutzern erreicht, können keine weiteren SmartCards ausgegeben werden. Zur Erweiterung der Clientlizenzen folgen Sie bitte dem Abschnitt Hinzufügen von Clientlizenzen

Verwaltung der Lizenzen

Zum Verwalten Ihrer Lizenzen öffnen Sie den Benutzermanager des *WinSafe.net*-Servers.

Die Server-ID

Jeder *WinSafe.net*-Server verfügt über eine eigene eindeutige Server-ID.

Der Betrieb von mehreren *WinSafe.net*-Servern mit der gleichen Server-ID führt zu Störungen des Betriebs und stellt eine Verletzung der Lizenzbedingungen dar.

Maximale Anzahl Benutzer

Unter der Server-ID finden Sie die Anzahl der bereits ausgegeben und die maximal mögliche Anzahl SmartCards für den jeweiligen Server. Nach Erreichen der maximal möglichen Anzahl SmartCards können keine weiteren neuen Benutzer angelegt werden, bevor keine Erweiterungslizenz hinzugefügt wurde.

Hinzufügen von Clientlizenzen

Lizenzen für Ihren *WinSafe.net*-Server können Sie prinzipiell in 2 Formen erhalten:

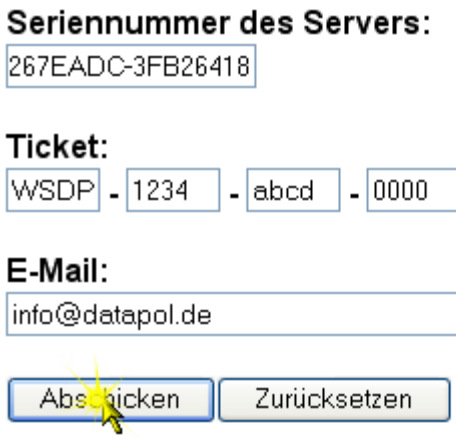
- als Lizenzdatei
- als Ticket

Sollten Sie die Lizenzen bereits in Form einer Datei erhalten haben, so klicken Sie auf den Button "Lizenz hinzufügen" im Über-Dialog des *WinSafe.net*-Benutzermanagers und verweisen auf die Lizenzdatei. Nun werden Ihrem Server die neuen Lizenzen zu den bereits vorhandenen hinzugefügt.

Falls Sie ein Ticket erhalten haben, müssen Sie die Lizenzen zuerst aktivieren. Dazu gehen Sie wie

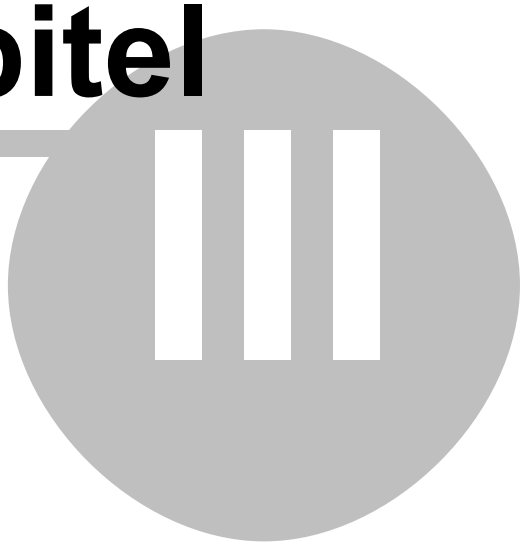
folgt vor:

- Öffnen Sie im Internet Browser die Adresse http://www.datapol-technologies.com/winsafe/licenses.htm.
- Geben Sie dort die Seriennummer (Server-ID) des *WinSafe.net*-Servers ein, zu dem Sie Lizenzen hinzufügen möchten
- Geben Sie das Ticket ein, das Sie beim Kauf der Lizenzen erhalten haben
- Geben Sie Ihre E-Mail Adresse an, an welche die neue Lizenzdatei geschickt werden soll
- Klicken Sie auf den Button "Abschicken"



Sie erhalten nun eine Lizenzdatei, sowohl zum sofortigen Download als auch zusätzlich noch an die angegebene E-Mail Adresse geschickt. Speichern Sie diese Datei ab.
Fügen Sie nun die Lizenzen, wie bereits am Anfang des Abschnitts Hinzufügen von Clientlizenzen beschrieben, dem *WinSafe.net*-Server hinzu.

Kapitel



3 Verwalten von SmartCards

Die Verwaltung der ausgegebenen SmartCards wird in *WinSafe.net* über die Benutzerverwaltung realisiert und erfolgt dezentral von einem beliebigen *WinSafe.net-Client* mit installiertem Administrationsmodul aus.
Bitte beachten Sie, dass ein korrekter Umgang mit den SmartCards der wichtigste Teil ist, den Sie beisteuern müssen, um eine sichere Umgebung zu schaffen und zu erhalten.

Sehen Sie die SmartCards wie einen Schlüssel zu einem sehr sicheren Tresor an. Bei diesem Vergleich kann der Hersteller des Tresors die allergrößte Sorgfalt, die besten Materialien und hochwertigsten Sicherheitskonzepte verwenden und trotzdem kann einem Einbrecher ein Zugriff gelingen, wenn er es schafft in den Besitz eines Schlüssels für den Tresor zu kommen.

Neben dem sicheren Umgang mit den Schlüsseln ist aber auch die sichere Ablage eines Reserve-Schlüssels für die Datentresore von essentieller Bedeutung. Denn im Gegensatz zu einem Tresor aus Stahl, der mit einem bestimmten Aufwand immer aufgebrochen werden kann, sind Datentresore unter *WinSafe.net* ohne einen gültigen Schlüssel mit dem derzeitigen Stand der Technik nicht mehr zu entschlüsseln.

Die verwendete Schlüsselstärke ist so hoch gewählt, dass, würde man alles Silizium, das derzeit auf der Erde existiert, zu modernen Pentium Prozessoren verarbeiten, die entstehende Rechenleistung immer noch nicht ausreichend wäre, um einen *WinSafe.net*-Datentresor innerhalb eines Jahres zu knacken.

Die Benutzerverwaltung stellt folgende Funktionen zur Verfügung:

- ***Benutzer/Administrator hinzufügen***
  Anlegen einer neuen SmartCard für einen Benutzer oder Administrator in *WinSafe.net*, wie in Anlegen eines Benutzers oder Administrators näher beschrieben.

- ***Benutzer/Administrator löschen***
  Entfernen einer SmartCard und damit des dazugehörigen Benutzers oder Administrators aus *WinSafe.net.* Dabei können zwei Optionen einzeln gewählt oder kombiniert werden:

  - *Benutzer von allen Tresoren entfernen* - Es werden lediglich die aktuellen Benutzerrechte aus allen bestehenden Tresoren gelöscht. Der Benutzer oder Administrator kann damit keine bereits zum Zeitpunkt des Löschens bestehenden Tresore mehr öffnen - auch seine eigenen nicht, jedoch weiterhin neue Tresore anlegen und auf diese zugreifen. Ein Administrator hat außerdem weiterhin die Möglichkeit SmartCards zu administrieren.

  - *Lösche diesen Benutzer aus der Datenbank* - die SmartCard wird aus der *WinSafe.net*-Datenbank entfernt. Damit sind mit dieser Karte keinerlei Aktionen mehr auf dem betreffenden Server möglich.

    Die Rechte dieser Karte bleiben jedoch in den Tresoren erhalten! Sollte diese Karte erneut ausgegeben werden, so "erbt" der neue Benutzer die vorher vorhandenen Rechte.

    Die an den jeweiligen Benutzer oder Administrator ausgegebene SmartCard bleibt dabei unberührt.

    Vor der Ausgabe an einen neuen Benutzer sollten die Daten auf solch einer Karte auf jeden Fall mit *Karte löschen* entfernt werden!

    Ansonsten erhält ein Benutzer, der die ehemalige Karte eines Administrators erhält, ebenfalls

Administratorrechte.

- ***Benutzer/Administrator bearbeiten***
  Bearbeiten der Benutzerinformationen eines Datenbankeintrags.

- ***Benutzer/Administrator ersetzen***
  Übertragen der Rechte eines Benutzers oder Administrators auf eine andere SmartCard. Dies wird notwendig, falls aus irgendeinem Grund ein Benutzer oder Administrator eine neue SmartCard benötigt (siehe auch Vergessene SmartCard), aber die Berechtigungen der alten Karte erhalten bleiben sollen. Die alte Karte ist für diesen Vorgang nicht erforderlich. Der ersetzte Benutzer oder Administrator bzw. dessen Karte kann dabei bei Bedarf gleich aus der Datenbank gelöscht werden. In diesem Fall gelten die gleichen Hinweise wie für die Funktion *Benutzer/Administrator löschen*

- ***Export der Benutzerinformationen in eine CSV-Datei***
  Exportieren der Daten aller Datenbankeinträge in eine Datei im CSV-Format, um diese z.B. in einer Tabellenkalkulation oder Datenbank weiterverwenden zu können.

- ***SmartCard löschen***
  Löschen der Daten auf einer SmartCard.

Falls diese Karte als Benutzer oder Administrator in *WinSafe.net* angelegt war, so bleibt die Karte als Datenbankeintrag erhalten und muss u.U. getrennt gelöscht werden!

- ***Hinzufügen von Lizenzen***
  Hinzufügen von Lizenzen zu Ihrem *WinSafe.net*-Server (Verwalten der Lizenzen)

3.1 Netzwerk- und Sicherheitsadministratoren

Eine der wichtigsten Anforderungen der Datensicherheit kann mit *WinSafe.net* erfüllt werden - die Trennung von Netzwerk- und Sicherheitsadministratoren.

Nur durch diese Trennung kann verhindert werden, dass z.B. über ein eingeschleustes "RootKit" trotz Verschlüsselung ein unberechtigter Zugriff auf geschützte Daten erlangt werden kann.

Daher ist es dringend erforderlich, dass die mitgelieferte Initial-SmartCard NICHT von einem Netzwerk- sondern vom Sicherheitsadministrator zur Verwaltung verwendet wird.

Für den Netzwerkadministrator, der die Installation durchführt, ist es also wichtig, die Clientsoftware mit der Option Administration von *WinSafe.net* auf dem PC des Sicherheitsadministrators zu installieren und die noch versiegelte Karte an diesen zu übergeben.

3.2 Anlegen der ersten Administratorkarte

Diese Operation sollte immer vom zuständigen Sicherheitsadministrator durchgeführt werden!

Zum Abschluss der Installation eines *WinSafe.net*-Servers ist es notwendig, die mitgelieferte Initial-SmartCard als erste Administratorkarte anzulegen.
Legen Sie die Initial-SmartCard, wie in Anlegen eines Benutzers oder Administrators beschrieben, als Administrator in *WinSafe.net* an.

Die PIN der neuen Initial-SmartCard ist im Auslieferungszustand grundsätzlich "000000".

Mit Hilfe dieser Karte können dann weitere Benutzer oder Administratoren angelegt werden.

3.3 Ausgabe weiterer SmartCards

Jeder Besitzer einer Administratorkarte kann beliebig neue Benutzer und Administratoren zu einem Server hinzufügen. Bitte beachten Sie deshalb als Sicherheitsadministrator von *WinSafe.net* folgende Regeln:

- **Erstellen Sie eine Reservekarte, die an einem sicheren Ort hinterlegt wird**
  Achten Sie darauf, dass mindestens eine SmartCard mit Administratorrechten an einem sicheren Ort, z.B. einem Tresor oder Schließfach, aufbewahrt wird.
  Ohne gültige Administratorkarte können keinerlei administrative Aufgaben, wie das Hinzufügen oder Entfernen von Benutzern, vorgenommen werden!

- **Trennung von Netzwerk- und Sicherheitsadministratoren**
  Wenn eine Trennung von Netzwerk- und Sicherheitsadministration vorgesehen wird, dürfen Netzwerkadministratoren keine SmartCards mit administrativen Rechten erhalten.

- **Ausgabe von Administratorkarten nur an Personen, die auch administrative Aufgaben wahrnehmen sollen**
  Die normale Arbeit mit *WinSafe.net* erfordert keine Administratorkarte. Da der Verlust einer solchen Karte ein sehr viel größeres Risiko darstellt als der Verlust einer Benutzerkarte, sollten auch Administratoren für die tägliche Arbeit mit *WinSafe.net* lediglich eine normale Benutzerkarte verwenden.

- **Dokumentation ausgegebener SmartCards**
  Zu Ihrer eigenen Sicherheit sollten Sie die Ausgabe aller SmartCards dokumentieren.

Administratoren

Legen Sie die Karte, wie in Anlegen eines Benutzers oder Administrators beschrieben, durch die Auswahl im Menü der Benutzerverwaltung *Administrator hinzufügen* als Administrator in *WinSafe.net* an.
Dieser Vorgang kann mit jeder bereits erstellten Administratorkarte durchgeführt werden.

Benutzer

Jeder Benutzer, der mit *WinSafe.net*-Tresoren arbeiten soll, benötigt ebenfalls eine persönliche SmartCard.
Die Anlage eines Benutzers ist praktisch identisch zum Anlegen eines Administrators. Im Menü des Benutzermanagers wählen Sie dann jedoch die Option *Benutzer hinzufügen*.

Sollten Sie zum Anlegen der Administratoren und Benutzer neue SmartCards verwenden, so befinden diese sich im NullPin-Modus. *WinSafe.net* erkennt dies und fragt beim Einlesen der Karte mit dem Benutzermanager keine PIN ab. Verwenden Sie hingegen schon einmal benutzte Karten, so benötigen Sie zum Einlesen jeweils deren PIN.

Auf jeden Fall sollten Sie eine SmartCard vor ihrer erneuten Verwendung löschen!

Damit werden nicht benötigte Informationen von der Karte entfernt und sichergestellt, dass bei der Ausgabe an einen neuen Benutzer keine unerwünschten Rechte auf der Karte erhalten bleiben. Des Weiteren wird die PIN auf die Standard-PIN zurückgesetzt.
Verfügt eine Karte bereits über eine (Standard-)PIN, so wird diese bei der Zuweisung zu einem Administrator oder Benutzer in *WinSafe.net* nicht verändert, d.h. die beim Einlesen abgefragte PIN bleibt weiterhin gültig. Wurde dagegen eine neue Karte im NullPin-Modus verwendet, dann erhält diese Karte automatisch die so genannte Standard-PIN.
Vor der Ausgabe einer Karte an den endgültigen Administrator oder Benutzer könnte es jedoch sinnvoll sein, die Standard-PIN bereits durch eine individuelle, z.B. per Zufall erzeugte PIN zu ersetzen. Dies würde verhindern, dass Benutzer oder - noch schlimmer - Administratoren Karten mit der Standard-PIN für die Arbeit mit *WinSafe.net* verwenden, da Sie der Aufforderung zur Vergabe einer persönlichen PIN nicht nachkommen.

Auf jeden Fall müssen Sie bei der Ausgabe einer Karte an einen Administrator oder Benutzer diesem die aktuelle PIN der Karte mitteilen!

Unabhängig mit was für einer PIN Sie eine SmartCard an einen Benutzer oder Administrator ausgeben, so sollten Sie diesen jedoch dazu auffordern, sofort die vorhandene PIN in eine nur ihm persönlich bekannte Nummer abzuändern. Falls eine SmartCard auf die Standard-PIN gesetzt ist, so wird der Benutzer bei jeder PIN-Eingabe automatisch auf einen Wechsel der PIN hingewiesen.

3.4 Anlegen eines Benutzers oder Administrators

Die Benutzerverwaltung von *WinSafe.net* wird durch einen Klick mit einer Maustaste auf das Tray-Icon aufgerufen.

Ist dieses Tray-Icon trotz installierten *WinSafe.net*-Clients nicht vorhanden, so lesen Sie bitte im Abschnitt Häufige Fragen (FAQ) nach.
Sollte die Option "*WinSafe.net*-Benutzermanager" nicht im Menü erscheinen, so wurde die optionale Administrationskomponente nicht installiert.

Es erscheint der Auswahldialog der *WinSafe.net*-Server:

Falls sich dieser Dialog nicht öffnet, so folgen Sie bitte den Anweisungen im Kapitel Problemlösungen.
Nachdem Sie den gewünschten Server ausgewählt haben, werden Sie aufgefordert Ihre SmartCard einzustecken und eine PIN für diese einzugeben. Zum Öffnen des Benutzermanagers benötigen Sie dafür eine SmartCard mit Administratorrechten. Beim Anlegen der ersten Administratorkarte ist dies die mitgelieferte Initial-SmartCard.

Die PIN der neuen Initial-SmartCard ist im Auslieferungszustand grundsätzlich "000000".

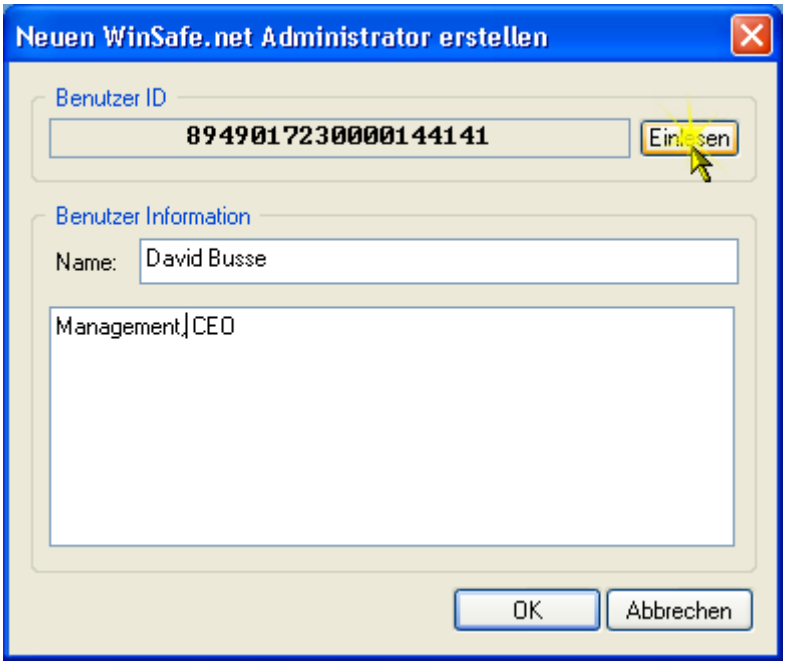
Beachten Sie bitte, dass Sie für die Eingabe der korrekten PIN bei einer SmartCard lediglich 3 Versuche zur Verfügung stehen.

Für weitere Informationen lesen Sie dazu bitte auch das Kapitel Gesperrte SmartCard.
Nachdem Sie die korrekte PIN eingegeben haben, erscheint der *WinSafe.net*-Benutzermanager:

Klicken Sie nun mit der rechten Maustaste in das weiße Feld und fügen einen Administrator oder Benutzer zum *WinSafe.net*-Server hinzu.
Stecken Sie nun die anzulegende Karte in den SmartCard-Leser und klicken auf *Einlesen*.

Klicken Sie nicht auf *Einlesen*, solange sich noch Ihre Administratorkarte im SmartCard-Leser befindet.

In diesem Fall würde die ID Ihrer Karte übernommen und mit den neuen Benutzerdaten überschrieben werden.
Sollte sich die Karte nicht im NullPin-Modus befinden oder die PIN-Eingabe bereits erfolgt sein (z.B. beim Anlegen der ersten Administratorkarte), so werden Sie nun zur Eingabe der PIN der neu anzulegenden Karte aufgefordert.
Falls dies noch nicht geschehen ist, so beachten Sie bitte auch die Ausführungen im Kapitel Ausgabe weiterer SmartCards.



Vergeben Sie den Namen und fügen Sie bei Bedarf zusätzliche Informationen über den Benutzer hinzu.

Wenn Sie den Kommentar z.B. generell mit der Abteilung des jeweiligen Benutzers beginnen, können Sie diese später leicht anhand der Abteilungen sortieren.

3.5 Weitere Aufgaben

Übertragung einer SmartCard

Eine existierende, bereits mit Rechten versehene, Karte kann relativ einfach auf einen anderen Benutzer oder Administrator übertragen werden. Allerdings muss dazu die PIN des alten Benutzers oder Administrators bekannt sein:

Markieren Sie in der Benutzerverwaltung den bisherigen Benutzer und wählen Sie im Menü *Benutzer/Administrator bearbeiten*. Nun tragen Sie die neuen Benutzerinformationen ein. Vor der Ausgabe der Karte an den neuen Benutzer oder Administrator sollten Sie jedoch die PIN der Karte auf die Standard-PIN setzen oder eine neue PIN vergeben.
Der neue Benutzer oder Administrator erhält mit der SmartCard alle Rechte, die auch der vorherige Besitzer hatte.

Ändern des Benutzerart

Die Umwandlung der Benutzerart kann folgendermaßen durchgeführt werden:
Sie benötigen für diesen Vorgang die SmartCard des Benutzers oder Administrators und deren PIN. Löschen Sie in der Benutzerverwaltung diese SmartCard mit *Karte löschen*. Danach legen Sie über das Menü, je nach gewünschter Benutzerart, einen neuen Benutzer oder Administrator mit dieser Karte an. Dabei wird der alte Eintrag in der Datenbank mit den Daten des neuen Benutzers oder Administrators überschrieben. Die bisherigen Rechte dieser SmartCard an den Tresoren bleiben dabei erhalten.

Vergessene SmartCard

Sollte ein Mitarbeiter seine SmartCard vergessen haben, so besteht die Möglichkeit, ihm vorübergehend oder dauerhaft über die Funktion *Ersetzen* im Benutzermanager eine Ersatzkarte zu generieren.
Dazu öffnen Sie den Benutzermanager und legen für diesen Benutzer eine neue Karte, die Ersatzkarte, an. Nun markieren Sie die "vergessene" Karte und klicken auf *Ersetzen*. Sie erhalten eine Maske mit 2 Auswahlfeldern. Im Feld "Benutzer-ID" ist bereits die "vergessene" Karte eingetragen. In dem Feld "Ersetzen mit" wählen Sie die soeben angelegte Ersatzkarte aus und bestätigen mit <OK>.
Nach erfolgreicher Durchführung der Aktion erhalten Sie eine entsprechende Meldung mit der Information, bei wie vielen Tresoren die Rechte ersetzt wurden. Damit sind alle Rechte der "vergessenen" Karte des Benutzers auf die Ersatzkarte übertragen worden. Er kann mit dieser nun uneingeschränkt wie mit seiner alten Karte arbeiten. Seine alte Karte ist zwar noch in der Benutzerverwaltung vorhanden, verfügt nun aber über keinerlei Rechte mehr, da diese auf die neue Karte übertragen worden sind. Damit ist Sie für eine Identifizierung gegenüber *WinSafe.net* wertlos.
Der Benutzer verfügt nun **nicht** über 2 funktionstüchtige Karten!
Zu einem späteren Zeitpunkt, wenn wieder Zugriff auf die alte Karte besteht, kann bei Bedarf, z.B. bei personalisierten Karten mit Passfoto o.ä., dieser Vorgang in umgekehrter Richtung durchgeführt werden, um dem Benutzer wieder seine ursprüngliche Karte zur Verfügung zu stellen.
Ansonsten sollte die alte Karte vom Administrator eingezogen und aus dem System gelöscht werden.

Verlorene SmartCard

Sollte ein Mitarbeiter seine SmartCard verloren haben, so muss ihm zuerst wie in Vergessene SmartCard erläutert, eine Ersatzkarte ausgestellt werden.
Danach sollte jedoch die alte Karte aus dem System gelöscht werden, um jeglichen Missbrauch zu verhindern.

Gesperrte SmartCard

Beim ersten Zugriff auf die SmartCard nach deren Einstecken in den Card-Leser wird die PIN abgefragt. Der Benutzer hat lediglich 3 Versuche die PIN korrekt einzugeben. Die Zählung der Versuche erfolgt intern auf der SmartCard, d.h. es stehen in jedem Fall nur 3 Versuche zur Verfügung, auch wenn zwischendurch die Karte aus dem Leser entfernt und neu eingesteckt wurde.
Erfolgen jedoch 3 falsche Eingaben, so wird die Karte, ebenfalls intern, gesperrt und ist damit nicht mehr nutzbar.

Die SmartCard ist damit zerstört!

In solch einem Fall ist es nur noch möglich, dem Benutzer, wie in Vergessene SmartCard beschrieben, eine Ersatzkarte auszustellen. Die alte Karte sollte anschließend aus dem System entfernt werden.

Kapitel IV

4 Allg. Verwaltungsaufgaben

Im folgenden Kapitel werden weitere wichtige Verwaltungsaufgabenrund um *WinSafe.net*, die nicht direkt mit der Verwalten von SmartCards zusammenhängen, vorgestellt.

4.1 Backup verschlüsselter Daten

Die verschlüsselten und in *WinSafe.net* abgelegten Daten stellen voraussichtlich ein wichtiges und besonders zu schützendes Gut Ihrer Firma dar. Deshalb ist auch ein Backup dieser Daten besonders wichtig. Im Gegensatz zu den meisten anderen Verschlüsselungslösungen, erlaubt *WinSafe.net* eine Sicherung verschlüsselter Daten auch Benutzern, die keine Berechtigung für einen speziellen Tresor haben.
Ein Backup-System schreibt die Daten ohne jegliche Veränderungen auf das Sicherungsmedium, so dass auch über dieses kein unerlaubter Zugriff auf die geschützten Daten möglich ist, da sie nach wie vor verschlüsselt sind und diese auch zu keinem Zeitpunkt der Sicherung aufgehoben wird.

Das Backup von *WinSafe.net* geschützten Daten erfolgt exakt gleich wie das Backup anderer Daten!

Der Speicherort

Alle Daten die in einem *WinSafe.net*-Server als Tresor abgelegt sind, werden auf dem Server unter der Freigabe \\Servername\WinSafe$ gespeichert. Der konkrete Speicherort hängt davon ab, welcher Pfad bei der jeweiligen Installation des Servers gewählt wurde.

NTFS- und Freigabeberechtigungen

Nach der Installation von *WinSafe.net* sind weder die NTFS- noch die Freigabeberechtigungen der Freigabe Winsafe$ eingeschränkt. Wurden diese Berechtigungen wie im Kapitel Einstellen der Berechtigungen beschrieben modifiziert, so ist darauf zu achten, dass das Konto unter dem die Sicherung erfolgt über ausreichende Rechte verfügt.

4.2 Virenprüfung

Da *WinSafe.net* alle Dateien verschlüsselt ablegt, kann ein lokal auf dem Server installierter Virenscanner die Tresore nicht auf einen Virenbefall prüfen.
Daher ist es wichtig, dass jeder Client, der verschlüsselte Dateien liest oder erzeugt, über einen lokalen On-Access Scanner verfügt.

Dieser Nachteil ist jedoch gleichzeitig auch ein Vorteil:
Der Server selbst kann von den Viren auf einem verschlüsselten Laufwerk niemals infiziert werden, da der Programmcode lokal nicht ausgeführt werden kann und erst durch die Verwendung einer passenden SmartCard über das Netzwerk auf dem Client entschlüsselt wird.

Da die Freigabe, unter der die Datentresore liegen, lokal und über das Netzwerk erreichbar ist, sollte diese jedoch nicht vom lokalen Scanner ausgeschlossen werden.

4.3 Kombination mit NTFS Dateirechten

Für die Arbeit mit WinSafe.net und mit den Tresoren müssen die Benutzer über entsprechende Dateirechte auf dem Server verfügen. Dazu sollte der Ordner, unterhalb dessen alle Tresore angelegt werden, mit den benötigten Rechten ausgestattet werden, d.h. die Benutzer müssen i.d.R. in diesem Ordner Dateien lesen, schreiben und erstellen können.
Lesen Sie dazu auch das Kapitel Einstellen der Berechtigungen.
Andererseits ist somit über die NTFS-Rechtevergabe aber auch eine Einschränkung von Rechten möglich, so dass Benutzern z.B. zwar die Möglichkeit eingeräumt wird, Daten in Tresoren zu lesen, diese aber nicht ändern können.

Kapitel V

5 Die Arbeit mit WinSafe.net

Folgende Themen werden ausführlich im "Benutzerhandbuch zu WinSafe.net" behandelt:

- die Arbeit mit *WinSafe.net*
- der tägliche Umgang mit *WinSafe.net*
- Erstellung, Verwaltung, Einsatz und Löschen von Tresoren
- Bedienung von *WinSafe.net* aus der Sicht des Benutzers

Einen kurzen Überblick über die behandelten Kapitel erhalten Sie in der folgenden Aufstellung:

1. Einführung
2. Arbeit mit *WinSafe.net*
2.1. Allgemein
2.2. SmartCard
2.3. Tresore
2.3.1. Erstellen
2.3.2. Verwalten
2.3.3. Arbeit mit den Tresoren
2.3.4. Löschen
3. Problemlösungen
3.1. Häufige Fragen (FAQ)
3.2. Technischer Support

Das "Benutzerhandbuch zu WinSafe.net" finden sie auf Ihrer Installations-CD von *WinSafe.net* oder Sie können es sich von unserer WEB-Site www.datapol.de herunterladen.

Kapitel VI

6 Deinstallation von WinSafe.net

Führen Sie die Deinstallation der Server- sowie der Client-Komponente über das Icon Software in der Systemsteuerung durch.
Folgen Sie den jeweiligen Anweisungen der Deinstallationsroutine.
Den SmartCard-Leser am Client können Sie bei eingestecktem Leser über den Gerätemanager von Windows deinstallieren.

Kapitel VII

7 Problemlösungen

In diesem Kapitel versuchen wir einige Hinweise für die Beseitigung eventueller Probleme zu geben und informieren Sie darüber, wo und wie Sie im Bedarfsfall Unterstützung durch unsere Firma erhalten.

7.1 Häufige Fragen (FAQ)

SmartCard-Leser:

Welche SmartCards und SmartCard-Leser können mit WinSafe.net verwendet werden?

Die SmartCards und die Spezifikation der SmartCard-Leser, die mit *WinSafe.net* verwendet werden können, sind im Abschnitt Systemvorrausetzungen aufgeführt.

Nach dem Anschluss des SmartCard-Lesers an den USB-Port fordert Windows zum Einlegen einer CD auf. Wo finde ich den richtigen Treiber?
Verwenden Sie einen von Datapol mit *WinSafe.net* gelieferten SmartCard-Leser, so verweisen Sie auf die Freigabe "dpcryclnt" des *WinSafe.net*-Servers. Ansonsten legen Sie die zum Leser mitgelieferte CD ein oder schauen nach Treibern auf der WEB-Site des betreffenden Herstellers.

Trotz korrekter Installation funktioniert der SmartCard-Leser nicht. Wie kann ich vorgehen, um den Fehler zu finden?
Bitte überprüfen Sie, ob der SmartCard-Leser richtig am USB-Anschluss eingesteckt ist. Danach kontrollieren Sie im Gerätemanager ob das Gerät korrekt installiert wurde und die USB-Anschlüsse auch aktiviert sind.
Bei einigen SmartCard-Lesern, wie z.B. bei dem von Datapol zu *WinSafe.net* ausgelieferten, wird zusätzlich zum Treiber noch ein Diagnostik-Tool installiert. Dieses finden Sie in der Systemsteuerung und es bietet die Möglichkeit, ebenfalls die korrekte Installation und Funktionsfähigkeit des Gerätes sowie die Erkennung der SmartCard zu überprüfen. Beachten Sie bitte, dass nur die in Systemvorrausetzungen aufgeführten SmartCards und Leser unterstützt werden.

Warum dauert die Abfrage der SmartCard sehr lange?
Dieses Problem kommt nur in Verbindung mit langsamen SmartCard-Lesern vor. Bitte kontaktieren Sie den Hersteller des Lesers und fragen Sie nach einem Geräten bzw. Treibern, die mit 115200 Bits pro Sekunde (oder schneller) arbeiten.

***WinSafe.net*-Clients:**

Warum erscheint nach dem Neustart das Tray-Icon von WinSafe.net nicht?
Entweder ist kein SmartCard-Leser mit dem Computer verbunden, dieser ist nicht korrekt installiert oder der *WinSafe.net*-Client-Dienst ist nicht gestartet.

Können die für WinSafe.net verwendeten SmartCards auch für eine Anmeldung der Benutzer an Windows genutzt werden?
Ja, dies ist mit dem Produkt SmartLogOn möglich, welches optional zu *WinSafe.net* erworben werden kann.

Kann ein WinSafe.net Client auch auf dem gleichen Computer wie der Server ausgeführt werden, um z.B. einen lokalen Zugriff auf die Daten, eine Administration am Server oder einen kompletten Standalone-Betrieb auf einem Notebook zu ermöglichen?

Prinzipiell ist solch eine Konfiguration ohne Probleme möglich. Bei einem Notebook sollten Sie jedoch zusätzlich den "Microsoft Loopback-Adapter" installieren, um sicherzustellen, dass auch bei einem mobilen Betrieb ohne physische Netzwerkverbindung die Netzwerkkomponenten korrekt initialisiert werden.

***WinSafe.net*-Server:**

Ein Client findet den WinSafe.net-Server nicht automatisch. Was kann die Ursache sein und wie kann ich überprüfen, ob dieser wirklich arbeitet.

Folgende Ursachen kommen in Frage, wenn ein Client den Server nicht automatisch findet:

- der *WinSafe.net*-Server-Dienst ist nicht gestartet
- der Server befindet sich in einer anderen Domäne/Arbeitsgruppe als der Client
- es besteht keine Netzwerkverbindung zwischen dem Server und dem Client
- der Client besitzt keine ausreichenden Zugriffsberechtigungen auf dem Server

Überprüfen Sie zuerst auf dem *WinSafe.net*-Server, ob der Dienst "WinSafe.net Server Service" korrekt gestartet wurde. Wenn dies der Fall ist, sollten Sie nachsehen, ob der Server in der Netzwerkumgebung des Clients angezeigt wird und ob Sie sich auf die Freigabe "dpcryclnt" verbinden können. Eventuell fehlen dem am Client angemeldeten Benutzer lediglich die benötigten Rechte (Einstellen der Berechtigungen) auf dem Server.
Falls der Server sich in einer anderen Domäne bzw. Arbeitsgruppe als der Client befindet, haben Sie die Möglichkeit, bei der Auswahl des Servers diesen nicht automatisch suchen zu lassen, sondern dessen Namen oder IP-Adresse manuell einzugeben. Die prinzipielle Erreichbarkeit des Servers können Sie mit Hilfe des Dienstprogramms PING überprüfen.
Kontrollieren Sie außerdem die Netzwerkeinstellungen auf dem Client sowie dem Server und probieren Sie es gegebenenfalls mit einem anderen Client.

7.2 Technischer Support

Wir bieten Kunden einen **kostenlosen Support für 30 Tage** nach dem Kauf von *WinSafe.net*. Um diesen Support in Anspruch zu nehmen, fügen Sie bitte Ihrer E-Mail Anfrage an die Adresse support@datapol.de die Auftragsnummer oder eine Rechnungskopie des Kaufs bei.

Ihre Anfrage sollte von unserem Supportteam innerhalb von 3 Tagen beantwortet werden.

Außerdem können Sie auch unsere Hotline von Mo-Fr. jeweils von 09.00-18.00Uhr unter Telefon 0-900-1-328276 (kostenpflichtig, 1,85€/Min.) erreichen. Bitte halten Sie dabei ebenfalls Ihre Auftragnummer bereit.

Wartungsvertrag:

Wir bieten für Firmenkunden auch spezielle Wartungsverträge an. Für detaillierte Informationen über Wartungsverträge rufen Sie uns bitte unter Telefon +49 (0)7352 9222 0 an oder senden eine Anfrage an die Adresse sales@datapol.de

Kapitel VII

8 Anhang

8.1 Systemvorrausetzungen

Server

Betriebssystem: Microsoft® Windows™ Server 2000, 2003 bzw. deren NAS-Varianten.
Die Hardwareanforderungen werden dabei von Windows vorgegeben.
Des Weiteren ist keine spezifische Hardware für *WinSafe.net* notwendig.

Client

- Betriebssystem: Microsoft® Windows™ 2000 Professional, XP Professional
- die Hardwareanforderungen entsprechen denen der installierten Windowsversion
- Netzwerkverbindung per TCP/IP zum *WinSafe.net*-Server
- PC/SC kompatibler SmartCard-Leser (115.000 KBit)

SmartCards

Folgende SmartCards werden von *WinSafe.net* unterstützt:

- Deutsche Telekom E4NetKey
- Deutsche Telekom NetKey2000

Index

- A -

- B -

- C -

- D -

- E -

- F -

- G -

- H -

- I -

- K -

- L -

- M -

- N -

- O -

- P -

- R -

- S -

- T -

- U -

- V -

- W -