Hinweise für Administratoren zur Inbetriebnahme und zum Betrieb der Registerbox

Inhalt

1 Übersicht

Dieses Dokument gibt Informationen zur Integration der Registerbox in Netzwerke. Es richtet sich an Administratoren und technisch Verantwortliche.

Neben der in der Anleitung zur Inbetriebnahme der Registerbox beschriebenen Variante zur Einrichtung eines Zugangs zur IT-Plattform der Bundesnotarkammer bestehen vielfältige weitere Konfigurations-Möglichkeiten, zu denen nachstehend Anregungen zusammengefasst sind. Außerdem sind Hinweise für Firewall-Einstellungen und zur Problemlösung enthalten.

In jedem Fall ist auszuschließen, dass Personen, die selbst keine notarielle Tätigkeit bzw. einen Notar bei Ausübung einer notariellen Tätigkeit unterstützen, Zugriff auf die Registerbox und die IT-Plattform der Bundesnotarkammer erhalten. Es dürfen nur Workstations über das Notarnetz (Netz 77.76.214.0/23) geroutet werden, die dem Notariat zugehörig sind und die Bundesnotarkammer-Dienste wie z. B. das Zentrale Testamentsregister oder XNotar nutzen. Die Verantwortung für einen wirksamen Zugriffsschutz liegt beim Notar.

In kleineren Notariaten wird die in der technischen Anleitung beschriebene Vorgehensweise bevorzugt zu empfehlen sein. In mittleren Nur-Notariaten mit einer übersichtlichen Struktur werden einfache zentral zu administrierende Lösungen interessant. Während in größeren und insbesondere in großen überregional vernetzen (Anwalts-) Notariaten restriktive arbeitsplatz- und benutzerbezogene Zugangsmodelle eingesetzt werden und die Registerbox selbst physikalisch und netzwerktechnisch vor missbräuchlichem Zugriff bewahrt werden muss. Um den physischen Zugriff auf einen bestimmten Benutzerkreis wirksam einzuschränken, kann es notwendig sein, die Registerbox in einem verschließbaren Schrank unterzubringen. Netzwerk-technisch kann insbesondere in größeren Netzwerken ein unkontrollierter Zugriff durch Anschluss an einer DMZ (DMZ-Betrieb siehe Kapitel 2.2.2) eingeschränkt werden.

2 Anschluss der Registerbox

Wie in der technischen Anleitung beschrieben, wird die Registerbox mit nur einem Netzwerkanschluss (FE0 bis FE2) wie ein Arbeitsplatz oder ein Netzwerkdrucker im LAN angeschlossen. Der für die IT-Plattform der Bundesnotarkammer bestimmte Datenverkehr wird für das Netz 77.76.214.0/23 durch geeignete Routing-Maßnahmen im LAN von den betreffenden Arbeitsplätzen oder Terminalservern zur Registerbox geleitet, dort verschlüsselt und in einem VPN-Tunnel über dasselbe Netzwerk-Interface zum Internet-Gateway geleitet. WAN-seitig darf der Tunnel zwischen Registerbox und Gegenstelle bei der Bundenotarkammer nicht behindert werden. LAN-seitig ist die Registerbox in der Regel im Subnetz zusammen mit den betreffenden Arbeitsplatz-Rechnern angeschlossen. Andernfalls sind geeignete Maßnahmen erforderlich, damit Daten zwischen den Arbeitsplätzen und der Registerbox den Hin- und Rückweg finden. Im Folgenden wird unterschieden:

- Tunnelverbindung zwischen Registerbox und den VPN-Servern als Gegenstelle
- Datenverbindung und Routing zwischen den betreffenden Arbeitsplätzen und der Registerbox

2.1 Tunnel-Verbindung zwischen Registerbox und Bundesnotarkammer

Damit der Datenverkehr des Tunnels zwischen Registerbox und den VPN- / LN-Servern im Rechenzentrum der Bundesnotarkammer über das Internetgateway ungehindert passieren kann, sind die in den folgenden Kapiteln beschriebenen Punkte zu beachten. Eine aktive Tunnel-Verbindung wird an der Registerbox durch dauerhaftes Leuchten der PPP-LED angezeigt.

2.1.1 Port- und Protokollfreigaben

Das verwendete L2TP-Protokoll muss passieren können. Dazu muss ausgehend UDP 1701 für die IP-Adresse der Registerbox offen und L2TP-Passthrough möglich sein. In manchen Fällen hilft ein Port-Forwarding eingehend für UDP 1701 zur IP-Adresse der Registerbox bzw. ein Port-Triggering für UDP 1701 ein- und ausgehend. Die Tunnel-Gegenstellen (LN-Server) liegen im IP-Adressbereich 212.63.94.48/29 (212.63.94.48 .. 212.63.94.55). Bei Bedarf kann eine Portfreigabe auf diesen Adressbereich einerseits und auf die Registerbox andererseits eingegrenzt werden. Außerdem muss die MTU insbesondere auch WAN-seitig über die Internetverbindung ausreichend groß sein (1492).

Schalten Sie möglichst WAN-seitig ICMP frei. Sofern die Registerbox in der DMZ betrieben wird, bitte den Zugriff IP- oder Port-basierend einschränken.

2.1.2 Firewall - Ausnahme und Intrusion-Detection

Unter Umständen werden UDP-Datenpakete zwischen Registerbox und der Gegenstelle, den LN-Servern, von Firewall- / Router-Regeln blockiert oder als Angriff gewertet. Dies kann zu folgenden Effekten führen:

- Sehr langsame Verbindung durch Verzögern oder Blockieren eines Teils von Datenpaketen
- Zeitweise Unterbrechung und automatischer Wiederaufbau des Tunnels
- Verbindungsunterbrechung des Tunnels bis der Internet-Router / die Firewall neu gestartet wird. In einigen Fällen muss zusätzlich die Registerbox neu gestartet werden

In manchen Fällen treten Tunnelabbrüche regelmäßig auf, z.B. 24 h nach Neustart des Internet-Routers. Auslöser ist i. d. R die Zwangstrennung des Internetproviders. Internetprovider haben unterschiedliche Regelungen und Zeiten bezüglich der Zwangstrennung. Je nach Leitungsprodukt gibt es keine Zwangstrennung. Durch Neustart der Firewall / des Internet-Routers wird die Blockade häufig bis zur nächsten Zwangstrennung aufgehoben.

Wie im Kapitel Port- und Protokollfreigabe ausgeführt, kann ein explizites Port-Forwarding zur IP-Adresse der Registerbox oder ein Port-Trigger die Blockaden unterbinden. Bei hochwertigen Routern / Firewalls können explizit Ausnahmen in Firewall und Intrusion-Detection gesetzt werden.

Die Blockaden können auch beim Internet-Anschluss liegen. Bei einigen Providern gibt es beispielsweise für Produkte, die für den Privatgebrauch angeboten werden, Einschränkungen bei der Datenweiterleitung.

2.1.3 Konkurrierende VPN-Verbindungen

Wenn auf dem Router / der Firewall bereits L2TP-VPNs unter Verwendung von UDP 1701 terminieren, kann es zu Konflikten kommen, wenn der Router die für die Registerbox bestimmten Datenpakete nicht weiterleitet. Wenn weitere VPN-Clients im LAN hinter dem Router platziert sind, kann es ebenfalls zu Konflikten kommen. Nicht alle Router / Firewalls können mit den beschriebenen Szenarien umgehen. Erfahrungsgemäß liegt dies zum Teil an Fehlern in der Router-Software, die durch ein Update der Firmware oder Austausch des Internet-Routers behoben werden kann.

2.1.4 Vermeidung mehrfach verschachtelter Tunnel

Die Registerbox baut einen L2TP-Tunnel zur IT der Bundesnotarkammer auf. Es ist zu vermeiden, dass WAN-seitig dieser Tunnel über bereits per L2TP oder PPTP VPN getunnelte Verbindungen erfolgt. Bei einer Verschachtelung mehrerer gleichartiger VPNs wird oftmals die zulässige Netzwerk-Paketgröße überschritten. Neben Performance-Einschränkungen kommt es dann zu sporadisch auftretenden fehlerhaften Netzwerkpaketen. Um diese Problematik zu vermeiden, sollte darauf geachtet werden, dass die Registerbox in einem Subnetz / an einem Standort mit direktem Zugang zum Internet installiert wird – siehe auch Kapitel „Registerbox in einem anderen Subnetz“.

2.2 Datenroute vom Arbeitsplatz zur Registerbox

Die Registerbox wird normalerweise im Subnetz zusammen mit den Arbeitsplatzrechnern angeschlossen. Wenn die Registerbox in einem anderen Subnetz platziert werden muss, sind besondere Maßnahmen notwendig. Bei Einsatz von Proxy-Servern ist zu beachten, dass die Proxy-Konfiguration neben den Routen-Einstellungen an Rechnern und Routern den Weg des Datenflusses bestimmt.

2.2.1 Registerbox im Subnetz mit den Arbeitsplätzen

Über ein Routing des Netzes 77.76.214.0/23 im Subnetz werden die Daten zur Registerbox geleitet. Im Rückkanal finden die Datenpakete innerhalb des Subnetzes den betreffenden Arbeitsplatz-Rechner. Die Route zur Registerbox wird individuell am Arbeitsplatz gesetzt, per Gruppenrichtlinien, Logon- / Logoff-Skript oder andere Methoden an die betreffenden Arbeitsplätze verteilt oder am Gateway für die Arbeitsplätze des Subnetzes zentral eingestellt. Siehe hierzu auch das Kapitel Routen-Einstellungen an den Arbeitsplatz-Rechnern.

2.2.2 Registerbox in einem anderen Subnetz / DMZ

Da in der Registerbox nur das Gateway für ausgehenden Datenverkehr nicht aber das Gateway für die Rückroute zu den Arbeitsplätzen konfiguriert werden kann, muss die Registerbox entweder im Subnetz mit den Arbeitsplätzen platziert werden oder es muss über NATing gewährleistet werden, dass die Daten den Rückweg zu den betreffenden Arbeitsplatz-Rechnern in anderen Subnetzen über dazwischenliegende Gateways finden. Alternative Konfigurationen sind mit dem Notarnetz und dem darin enthaltenen Notarnetz-Router möglich. Beim Notarnetz-Router können beispielsweise individuelle Rückrouten gesetzt werden, und es ist bei Bedarf eine zweite Schnittstelle in ein Transfernetz möglich.
Für den Betrieb in einer DMZ muss die Registerbox mit einer IP-Adresse aus der DMZ konfiguriert sein/werden. Der Zugriff außerhalb der DMZ auf die Registerbox (fremdes Subnetz) muss via NATing erfolgen, da die Registerbox eine Firewall-ACL besitzt, die den Zugriff zum Register von den SRC-Adressen des LAN einschränkt.

2.2.3 Verwendete Protokolle

Die Registerbox nutzt für den Zugriff auf die Dienste der Bundesnotarkammer folgende Protokolle:

- Aufbau des Tunnels per L2TP (Layer 2 Tunneling Protocol) Port UDP 1701
- Zugriffe auf die Dienste per HTTPS (Hypertext Transfer Protocol over SSL/TLS) Port TCP 443

2.2.4 Proxy-Server im Einsatz – Proxy-Ausnahmen

Wenn Proxy-Server im Einsatz sind, müssen diese bei der Konfiguration der Daten-Routen vom Arbeitsplatz zur Registerbox und zurück berücksichtigt werden. Durch Setzen von Proxy-Ausnahmen an den betreffenden Arbeitsplätzen werden die betreffenden Datenpakete gemäß den Routen-Einstellungen am Arbeitsplatz zur Registerbox geleitet und nicht zum Proxy-Server und von dort in das Internet. Wenn der Proxy-Server nicht beim Provider sondern im eigenen Netzwerk betrieben wird, können alternativ Regeln am Proxy-Server gesetzt werden, die die betreffenden Daten über die Registerbox leiten.

Proxy- Ausnahmen für namensbasierte Adressierung (z.B. im Internet-Explorer unter Internetoptionen oder im Firefox-Browser unter Netzwerkeinstellungen):

**.bnotk.de;*.dnoti-online-plus.de;progov-osci.bnotk.de; sdv.bnotk.de*

Für die direkte IP-basierende Adressierung muss der IP-Netzbereich 77.76.214.0/23 (77.76.214.0 bis 77.76.215.255) über die Registerbox geleitet werden.

2.2.5 Registerbox als Standardgateway

Die Registerbox kann als Standard-Gateway genutzt werden. Die Registerbox routet die für die IT-Plattform der Bundesnotarkammer bestimmten Daten durch den VPN-Tunnel und alle anderen Daten zum allgemeinen Internet-Gateway. An den betreffenden Arbeitsplätzen wird die Registerbox als Standardgateway eingestellt. Zu beachten ist, dass alle externen Datenpakete zunächst über die Registerbox laufen, diese also eingeschaltet und funktionsfähig sein muss.

2.3 VLAN-Infrastruktur

Prinzipiell kann die Registerbox auch in VLAN-Infrastrukturen betrieben werden. Dabei sollten allerdings folgende Hinweise beachtet werden:

- Die Ports der Registerbox sind „untagged“.
- Die Registerbox verwendet intern das Native-VLAN VID 1.
- STP ist auf der Registerbox für Native-VLAN per Standardeinstellung aktiv.

Sofern auf dem Ihrem Switch die Registerbox in ein anderes VLAN gehängt wird, kann es vorkommen, dass der Switch den Port aufgrund eines VLAN-Missmatch blockiert. Dies sollte allerdings im Log des Switch ersichtlich sein bzw. lässt sich das Verhalten des Ports entsprechend einstellen.

3 Routen-Einstellungen an Arbeitsplatz-Rechnern

In den meisten Fällen ist es von Vorteil, Einstellungen an zentraler Stelle konfigurieren und kontrollieren zu können. Durch das Setzen der Route am Standard-Gateway wird der Zugang zur IT-Plattform für alle am lokalen Netzwerk angeschlossenen Arbeitsplätze und Server möglich.

Das Setzen einer Route am Standardgateway kann durch Konfiguration des Gateway Routers und/oder der Gateway Firewall erfolgen. Gegebenenfalls ist dies auch durch Serverkonfiguration in einer Windows-Domäne abgebildet, sodass dort entsprechende Änderungen erfolgen sollten.

3.1 Routen-Einstellung am Arbeitsplatz

Im Folgenden finden Sie Hinweise zum Einstellen einer Route vom Arbeitsplatz-Rechner zur Registerbox für die Betriebssysteme Linux, Microsoft Windows und Apple Macintosh.

Um unter Linux statische Routen zu konfigurieren, gibt es für die verschiedenen Distributionen unterschiedliche Wege. Nachfolgend werden zwei Klassen von Systemen betrachtet (Debian/Ubuntu und Suse/Redhat).

3.1.1 Windows-Arbeitsplatz

Am Windows-Arbeitsplatz können Routen mit dem route-Befehl in der Windows-Eingabeaufforderung verwaltet werden. Setzen der permanenten Route zur Registerbox unter Windows siehe Technische Anleitung. Eine zentrale Verteilung ist auch über Gruppenrichtlinien oder Logon- / Logoff-Scripts denkbar.

3.1.2 Linux Debian/Ubuntu

Die Konfiguration muss jeweils als Benutzer "root" erfolgen.

Fügen Sie für das Standard-Netzwerkinterface zwei Direktiven in die Datei */etc/network/interfaces* ein, die erste zum Hochfahren (up) und die zweite zum Herunterfahren (down) des Interfaces.

*up ip r a 77.76.214.0/23 via **[Gateway-Adresse Registerbox]***
*down ip r d 77.76.214.0/23 via **[Gateway-Adresse Registerbox]***

Beispiel:
auto eth0
iface eth0 inet static
address 192.168.0.100
netmask 255.255.255.0
network 192.168.0.0
broadcast 192.168.0.255
gateway 192.168.0.1
*up ip r a 77.76.214.0/23 via **[Gateway-Adresse Registerbox]***
*down ip r d 77.76.214.0/23 via **[Gateway-Adresse Registerbox]***

[Gateway-Adresse Registerbox] ist die IP-Adresse der Registerbox, die bei der Antragsstellung angegeben wurde. Sie wird in der Zuweisungsverfügung, die der Registerbox beiliegt, ebenfalls angegeben.

3.1.3 Suse/Redhat

Um eine statische Route unter Suse/Redhat einzurichten, wird eine zusätzliche Konfigurationsdatei für das Interface benötigt, über welches die statische Route führen soll. Im Beispiel wird als Interface-Name "eth0" verwendet.

Erstellen Sie eine Datei */etc/sysconfig/network-scripts/route-eth0* mit vim mit folgendem Inhalt:
*77.76.214.0/23 via **[Gateway-Adresse Registerbox]***

[Gateway-Adresse Registerbox] ist die IP-Adresse der Registerbox, die bei der Antragsstellung angegeben wurde. Sie wird in der Zuweisungsverfügung, die der Registerbox beiliegt, ebenfalls angegeben.

3.1.4 macOS

Führen Sie im Terminal für das Hinzufügen einer statischen Route folgenden Befehl aus:

```
networksetup -setadditionalroutes [Interface Name] [Destination Network]
[Subnet Mask] [Gatway IP Address]
```

Angenommen Ihre Registerbox hat die LAN-IP 191.168.100.150, dann geben Sie bitte die Route wie folgt ein:

```
networksetup -setadditionalroutes "Ethernet" 77.76.214.0 255.255.254.0
192.168.100.150
```

Für das Löschen einer statischen Route führen Sie bitten folgenden Befehl aus:

```
networksetup -setadditionalroutes [Interface Name]
```

3.2 Arbeitsplatz- oder benutzerspezifische Routen-Einstellung

Insbesondere in größeren (Anwalts-) Notariaten dürfte jedenfalls ein restriktiver arbeitsplatz- und benutzerbezogener Umgang mit der IP-Route gegenüber einer globalen Einstellung für das gesamte Netzwerk vorzugswürdig sein. Dadurch kann missbräuchlichen Zugriffen auf das ZTR entgegengewirkt werden.

3.2.1 Arbeitsplatz-Gruppe

Die Route kann spezifisch nur auf einer Gruppe von Arbeitsplätzen, an denen notarielle Tätigkeit verrichtet wird, gesetzt werden. Dies kann entsprechend der Installationsanleitung durch Nutzung des Route-Befehls oder durch zentrale Einstellung (s.u. Logon-Skript oder Gruppenrichtlinien) erreicht werden. Es ist sicherzustellen, dass diese Arbeitsplätze nur von berechtigten Personen verwendet werden, die Zugriff auf das Zentrale Testamentsregister in Ausübung notarieller Tätigkeit erhalten.

3.2.2 Benutzergruppe

Ergänzend könnten spezifische Arbeitsplätze (z.B. Windows AD Computerkonten) nur zur Benutzung durch eine bestimmte eingeschränkte Benutzergruppe freigegeben werden. Durch diese Windows AD-Server-Einstellung können wirksam Anmeldungen an diesen Computern durch nicht zum Notariat zugehörige Mitarbeiter unterbunden werden. Durch die Einbindung in den Active Directory Dienst wird dadurch darüber hinaus erreicht, dass durch zentrale ohnehin erforderliche Benutzerpflege automatisch die Anforderungen des § 18 BNotO eingehalten werden.

3.2.3 Steuerung über Windows Gruppenrichtlinien

In einem Windows-Server-Netzwerk kann mit Hilfe von Gruppenrichtlinien eine automatische zentrale Verteilung einer permanenten Route für bestimmte Computer bzw. Nutzer oder einer browserbasier-

ten Proxyeinstellung (z.B. Internet-Explorer) realisiert werden. Dies setzt voraus, dass eine Benutzer-Anmeldung an der Domäne auf jedem betroffenen Arbeitsplatz durchgeführt wird.

Zu beachten ist dabei das unterschiedliche Verhalten von Betriebssystemversionen z.B. in Bezug auf die seit Windows Vista und Windows 7 eingeführte Benutzerkontensteuerung (UAC). Ebenfalls sollte entsprechende Erfahrung bei der Nutzung von Gruppenrichtlinien vorliegen, um nicht gewünschte Seiteneffekte zu vermeiden.

3.2.4 Routen-Einstellung durch Anmelde-Skript (Logon-Skript)

Alternativ zur Steuerung über Windows Gruppenrichtlinien kann in einem Windows-Netzwerk die Einstellung einer nicht permanenten Route oder einer Proxy-Einstellung für Browser-Anwendungen für eine Benutzer-Sitzung an einem Netzwerkarbeitsplatz im Anmelde-Skript erfolgen. In einem solchen Skript kann bei Lösung über die Kommandozeile beispielsweise der Befehl „runas“ über „Ausführen als <Benutzer mit entsprechenden Rechten>“ erfolgen. Alternativ kann sich der Einsatz eines VB-Skripts als Anmeldeskript empfehlen. Für das erfolgreiche Erstellen von Skripten ist einschlägige Erfahrung erforderlich.

Die Route sollte so gesetzt werden, dass sie bei Neustart des Rechners oder durch ein Abmeldeskript mittels Gruppenrichtlinie wieder gelöscht wird. Dadurch ist die Route bei Neustart oder Benutzerwechsel entfernt, wenn sich nicht ein entsprechend privilegierter Nutzer wieder anmeldet.

Das Setzen einer permanenten Route durch Anmeldeskript kann in einem homogenen Berufsträger-Umfeld (z.B. im Nur-Notariat) zur Verteilung der Route auf alle Arbeitsplätze eingesetzt werden.

Bei einer Verteilung der Routen-Einstellung an Benutzer im Windows-Netzwerk sind wie bei der Einstellung direkt am Arbeitsplatz entsprechende Rechte an den betreffenden Arbeitsplätzen erforderlich. Zu diesem Zweck kann ggf. ein Benutzer-Account mit eingeschränkten Administrationsrechten (<Benutzer mit entsprechenden Rechten> = <Routen-Admin>) eingerichtet werden. Benutzername und Passwort müssen im Skript lesbar angegeben werden. Das Skript sollte deshalb ohne Echoprompt erstellt werden. Dies stellt ein abzuwägendes Sicherheitsrisiko dar. Beachten Sie dabei bitte das unterschiedliche Verhalten von Betriebssystemversionen z.B. in Bezug auf die seit Windows Vista und Windows 7 eingeführte Benutzerkontensteuerung (UAC).

3.3 Administration der Arbeitsplätz-Einstellungen von zentraler Stelle

Mit Administrations-Werkzeugen können Arbeitsplätze komfortabel von zentraler Stelle aus konfiguriert werden. In diesem Fall ersetzt ein solches Werkzeug ggf. Einstellungen in Gruppenrichtlinien oder in Anmeldeskripten. Für Windows-Netzwerke enthält beispielsweise die Tool-Sammlung „Windows Sysinternals“ geeignete Funktionalität.

4 Einsatz-Szenarien

4.1 Getrennter Internet-Einzelplatz

Bei getrennten Internet-Einzelplatzlösungen wird die Registerbox zusammen mit dem Internet-Arbeitsplatz an einem Internet-Router angeschlossen. Ist der Internet-Einzelplatz direkt über ein DSL-Modem angeschlossen und wird die Verbindung vom PC aus über ein Einwahlprogramm z.B. per PPPoE vorgenommen, kann die Registerbox nur angeschlossen werden, wenn die vorhandene Lösung auf Router-Betrieb umgestellt wird.

4.2 Windows Terminal Server Umgebung

Ein Windows Terminal Server (WTS) stellt über das RDP-Protokoll Windows-Client-Sitzungen an zentraler Stelle zur Verfügung. Die Registerbox wird idealerweise im Subnetz mit dem Terminalserver installiert. Die Route zur Registerbox wird in diesem Fall am Terminalserver gesetzt.

4.3 Kanzlei mit verteilten Standorten

Alternativ kann die Registerbox direkt an Standorten mit Internetzugang oder an zentraler Stelle installiert werden. Notare können gemeinsam eine Registerbox nutzen.

Wenn an zentraler Stelle ein Terminalserver zum Zugriff auf die Dienste der Bundesnotarkammer eingesetzt wird, sollte die Registerbox im Subnetz mit dem Terminal-Server installiert werden. Siehe auch die Kapitel Registerbox in einem anderen Subnetz und Tunnel-Verbindung zwischen Registerbox und Bundesnotarkammer.

Soll von Arbeitsplätzen aus verschiedenen Subnetzen aus zugegriffen werden, ist Kapitel Registerbox in einem anderen Subnetz.

Bei Registerboxen, die aus einem Subnetz WAN-seitig über ein VPN zum Internet gelangen ist Kapitel Vermeidung mehrfach verschachtelter Tunnel zu beachten.

Individuelle Konfigurationen sind mit dem Notarnetz und dem darin enthaltenen Notarnetz-Router möglich. Bei Einsatz des Notarnetz-Routers anstelle der Registerbox können beispielsweise Rückrouten gesetzt werden, und bei Bedarf ist eine zweite Schnittstelle in ein Transfernetz möglich.

4.4 Nutzung der Registerbox als zusätzlichen LAN Switch

Falls bei Inbetriebnahme festgestellt wird, dass im LAN-Switch kein weiterer Netzwerk-Port verfügbar ist, kann ein vorhandenes Gerät im LAN-Switch auf einen der 4 gelb markierten LAN-Ports der Registerbox umgesteckt werden und die Registerbox am LAN-Switch eingesteckt werden. Die Registerbox fungiert dann als zusätzlicher LAN-Switch und VPN-Router.

5 Besonderheit AnNoNet-Anschluss

AnNoText-Kunden (Wolters Kluwer Deutschland GmbH) haben einen speziellen Internetanschluss, der für die Registerbox vorkonfiguriert ist. Kontaktinformationen finden Sie unter Punkt 8.

5.1 IP-Adressen

Die Arbeitsplatzrechner der AnNoNet-Kunden befinden sich stets in einem Netz mit identischer IP-Adressierung. Für den Anschluss der Registerbox von AnNoNet-Kunden gelten deswegen immer folgende Angaben:

- Netzwerk-IP des lokalen Netzes: 192.168.10.0
- Subnetzmaske: 255.255.255.0
- IP-Adresse des AnNoNet-Routers (Standard-Gateway): 192.168.10.1
- IP-Adresse Registerbox: 192.168.10.10

5.2 Route für den Registerzugang setzen

Der in der Standardanleitung angegebene Route-Befehl (route –p ADD …) darf in der AnNoNet-Umgebungen NICHT eingegeben werden! Die Route wird in diesen Fällen zentral auf dem AnNoNet-Router gesetzt. Bitte nehmen Sie Kontakt zum AnNoText-Support auf, damit dieser die Route setzen kann. Dies passiert i.d.R. remote, d.h. das Support-Team wählt sich aus der Ferne auf dem Router ein. Eine Anwesenheit vor Ort ist also nicht notwendig. Sobald AnNoText die Route gesetzt hat, fahren Sie fort mit dem nächsten Schritt.

HINWEIS: Sofern Sie in früheren Verbindungsversuchen die Route zum Register bereits gesetzt haben, müssen Sie diese Route an der Arbeitsplatzrechner oder in der Firewall löschen.

5.3 Weitere Hinweise

Für weitere Informationen z. B. zur speziellen Verkabelung der Registerbox oder zur Nutzung von Proxy-Ausnahmen wenden Sie sich bitte an den Support von AnNoNet-Support. Kontaktinformationen finden Sie unter Punkt 8.

6 Besonderheit DATEVnet-Anschluss

DATEVnet-Kunden (DATEV e. G.) haben einen speziellen Internetanschluss, der für die Registerbox vorkonfiguriert ist. Informationen zur Einrichtung der Registerbox finden Sie im DATEVnet-Dokument 1070178 „Registerbox einrichten unter DATEVnet pro“ und unter folgendem Link http://www.datev.de/dnlexos/mobile/document.aspx?document=1070178&consumer=webApp Kontaktinformationen finden Sie unter Punkt 8.

7 Rekonfiguration der Registerbox

Wenn sich die IP-Netzwerkumgebung z. B. die Gateway-Adresse für die Registerbox ändert, muss diese rekonfiguriert werden. Für den Rekonfigurationsauftrag wenden Sie sich bitte an unseren Support registerbox@testamentsregister.de.
Die Rekonfiguration erfolgt über den LAN Port FE3. Die Registerbox wird somit per LAN-Kabel am FE3-Port mit einem Internetrouter verbunden, der der Registerbox per DHCP eine IP-Konfiguration zuweist. Diese IP-Konfiguration darf dabei aber NICHT dem aktuellen und künftigen Netz-Bereich der Registerbox entsprechen.

Beispiel:
Wenn die Registerbox auf den Adressbereich 192.168.1.0/24 konfiguriert werden soll und aktuell im Adressbereich 192.168.2.0/24 konfiguriert ist, darf der Internetrouter nicht diese beiden Adressbereiche nutzen sondern z. B. den Adressbereich 192.168.10.0/24.

Wenn sich dieses Verfahren im Notariat nicht abbilden lässt, kann die Registerbox nach Abstimmung zw. dem Systembetreuer und dem Notar auch außerhalb der Geschäftsstelle konfiguriert werden.
Für die Rekonfiguration wird ein Zeitfenster von ca. 90 Minuten benötigt. Ihre Anwesenheit oder telefonische Erreichbarkeit ist währenddessen nicht erforderlich.

7.1 Variante Einsendung der Registerbox

Falls sich das o. g. Standardverfahren zur Rekonfiguration nicht umsetzen lässt, können Sie die Registerbox zu diesem Zweck auch einsenden. Wenden Sie sich dazu bitte an unseren Support registerbox@testamentsregister.de.

8 Probleme und Lösungen

8.1 Probleme beim Netzwerkanschluss der Registerbox

Wichtiger Hinweis: Den LAN-Port FE3 können Sie nicht für den Netzwerkanschluss verwenden. Dieser ist für Wartungsarbeiten konfiguriert und stellt keine LAN-Verbindung zum Netzwerk her.

8.1.1 Netzwerkanschluss funktioniert nicht und keine der LEDs FE0..FE2 leuchtet

Obwohl die Registerbox mit einem Netzwerkkabel an einem der Anschlüsse FE0..FE2 mit einem Switch, Hub oder einem Router verbunden wurde, leuchtet die dem Anschluss entsprechende LED FE0..FE2 nicht und die Registerbox kann nicht von einem angeschlossenen Netzwerkgerät z.B. per Ping angesprochen werden. Prüfen Sie bitte Folgendes:

- Netzwerkkabel und Anschlüsse prüfen auf Wackler.
- Verwendung eines anderen LAN-Ports der Registerbox (FE0 …FE2).
- Testen Sie einen anderen Anschluss am Switch.
- Austausch des Netzwerkkabels und testweise Verwendung eines Kabels und eines Netzwerkanschlusses, die mit einem anderen Netzwerkgerät funktionieren.
- Auch wenn kein direkter Defekt vorliegt, kann es sein, dass eine automatische Protokollaushandlung per Auto-Sensing nicht funktioniert.
    - Registerbox testweise an einen anderen Switch oder einem anderen Netzwerkinterface, z.b. direkt am Router oder einem Notebook / Arbeitsplatzrechner einstecken und per Ping testen, ob die Registerbox antwortet.
    - Versuchen Sie am Switch / Netzwerkinterface eine feste Einstellung (z.B. duplex half speed 10).
- Sperrt der von Ihnen verwendete Switch den Port aus Sicherheitsgründen beim Anschluss unbekannter Geräte? Beispielsweise könnten spanning-tree BPDU's eine Portsperre am Switch verursachen.

Die Ports an der Registerbox verhalten sich wie folgt:

- Alle Ports haben eine gemeinsame IP Adresse und sind im gleichen VLAN.
- Jeder Port hat eine andere MAC Adresse.

8.1.2 Netzwerkanschluss funktioniert nicht bei leuchtender LED FE0...FE2

Leuchtet die zum Netzwerkanschluss entsprechende LED FE0..FE2 unregelmäßig, so sollte die Kabel-Verbindung funktionieren. Bei defekten Kabeln, Steckern oder Netzwerkanschlussdosen zwischen dem Switch und dem Netzwerkanschluss kann es jedoch vorkommen, dass die Datenverbindung nicht, nur unregelmäßig oder sehr langsam funktioniert, obwohl die LEDs an den Netzwerk-Ports des Switches und der Registerbox leuchten, siehe auch Netzwerkanschluss funktioniert nicht und keine der LEDs FE0..FE2 leuchtet.

8.2 Probleme mit der PPP-Tunnel-Verbindung

8.2.1 Keine PPP-Tunnel-Verbindung von Registerbox zur BNotK

Der PPP-Tunnel zwischen Registerbox und der Gegenstelle, den LN-Servern der Bundesnotarkammer, wird nicht aufgebaut. Die PPP-LED leuchtet nicht permanent und es kann von einem Arbeitsplatz mit eingestellter Route keine Verbindung zu *https://ztrdemo.bnotk.de* aufgebaut werden. Prüfen Sie bitte Folgendes:
Siehe hierzu auch die entsprechenden Kapitel unter Prüfungen der Tunnelverbindung.

- Ist die Registerbox in Betrieb und im LAN mit dem Internet-Gateway verbunden?
- Kann die Registerbox den Tunnel über Internet-Router / Firewall ungehindert aufbauen?
- Beeinträchtigt der Internet-Anschluss die Tunnelverbindung?

8.2.2 Keine PPP-Tunnel-Verbindung nach erfolgreicher Inbetriebnahme

Wenn die Registerbox nicht mehr online geht, hilft oft ein Neustart des Internet-Routers. Besteht die Verbindung für mindestens 24 Stunden, wird automatisch eine verbesserte Registerbox-Konfiguration geladen. Je nach Router-Typ kann es anschließend weiterhin zu Verbindungsabbrüchen kommen. Siehe hierzu Kapitel Verbindungsabbrüche und Unterbrechungen der PPP-Tunnel-Verbindung.

8.2.3 Verbindungsabbrüche und Unterbrechungen der PPP-Tunnel-Verbindung

Wird die Verbindung nach einer Unterbrechung einige Minuten später nicht wieder automatisch aufgebaut, kann ein Neustart des Internet-Routers / Firewall für eine gewisse Zeit wieder eine Verbindung der Registerbox ermöglichen. Wenn die Verbindungsabbrüche regelmäßig z.B. 24 h nach Neustart des Internet-Routers eintreten, ist der Auslöser i. d. R die Zwangstrennung des Internetproviders. Internetprovider haben unterschiedliche Regelungen und Zeiten bezüglich der Zwangstrennung. Je nach Leitungsprodukt gibt es keine Zwangstrennung.

Prüfen Sie bitte Folgendes:

- Gab es Veränderungen im Netzwerk und beim Internetanschluss?
- Bitte prüfen Sie die Firewall-Einstellungen. Siehe Kapitel Prüfung der Router- / Firewall-Einstellungen
- Ist die Netzwerkkabelverbindung zur Registerbox einwandfrei. Defekte Kabel- und Steckverbindungen können zu zeitweiligen Unterbrechungen oder verlangsamter Datenübertragung führen.
- Beeinträchtigt der Internet-Anschluss die Tunnelverbindung *(siehe gleichlautendes Kapitel)*
- Steht der Router auf der Kompatibilitätsliste. Siehe Kapitel Erfahrungen zur Kompatibilität von Routern.

8.2.4 Langsame Verbindung über die Registerbox

Obwohl die Internetverbindung gewohnt schnell ist, werden Aufrufe zu den Diensten der Bundesnotarkammer, beispielsweise zur ZTRDemo-Seite, sehr langsam aufgebaut. Unter Umständen bleibt die Seite minutenlang weiß oder es kommt zu Timeout-Fehlermeldungen.

Prüfen Sie bitte Folgendes:

- Ist die Internetverbindung weiterhin schnell?
- Zur Anzeige des Verlustes von Datenpaketen führen Sie ein *ping ztr.bnotk.de* aus.
- Ist die Datenpaketgröße / MTU WAN-seitig kleiner als 1492?
- Ist die Netzwerkkabelverbindung zur Registerbox einwandfrei. Defekte Kabel- und Steckverbindungen können zu zeitweiligen Unterbrechungen oder verlangsamter Datenübertragung führen.
- Prüfen Sie die Firewall-Einstellungen und die Internet-Verbindung.
  Oft verursachen Firewall-Einstellungen und konkurrierende VPN-Verbindungen eine Verzögerung oder den Verlust von Datenpaketen. Siehe hierzu Kapitel *Prüfung der Router- / Firewall-Einstellungen*.

8.2.5 PPP-LED leuchtet nicht, obwohl eine Verbindung besteht

In manchen Fällen leuchtet die PPP-LED nicht, obwohl eine Verbindung besteht. Falls ein Defekt der LED an der Registerbox vorliegt, kann diese vom Vorort-Austausch-Service ab Januar 2012 getauscht werden. Funktioniert von einem Arbeitsplatz mit eingestellter Route die ZTRdemo-Webseite, dann sollte auch der Tunnel funktionieren. Informieren Sie bitte den Support registerbox@testamentsregister.de.

8.2.6 PPP-LED leuchtet, obwohl keine Verbindung besteht

Dieser Effekt ist bisher nur bei QSC-Internetanschlüssen aufgefallen. Die Tunnelverbindung steht offensichtlich, aber der Datenverkehr funktioniert nicht. In diesem Fall wenden Sie sich bitte an unseren Support registerbox@testamentsregister.de.

8.3 Prüfungen der PPP-Tunnelverbindung

8.3.1 Ist die Registerbox in Betrieb und im LAN mit dem Internet-Gateway verbunden

- Die Registerbox ist mit Strom versorgt, die OK-LED leuchtet.
- Ein LAN-Kabel verbindet die Registerbox und die entsprechende LED FE0..FE2 zeigt eine aktive LAN-Verbindung zu Ihrem Netzwerk an. Schließen Sie testweise die Registerbox über ein an einem anderen Gerät funktionierendes Netzwerkkabel und dem damit funktionierenden Netzwerk-Anschluss an.
- Kann die Registerbox von einem Arbeitsplatz im Subnetz der Registerbox und vom Internet-Gateway aus mit PING <IP-Registerbox> angesprochen werden?
- Sind die auf der Zuweisungsverfügung angegebenen IP-Daten der Registerbox (Netzwerk-IP, Netzmaske, Gateway-IP und IP der Registerbox) passend?
  Hinweis: Nach einer Rekonfiguration können diese abweichend von der Zuweisungsverfügung sein.

8.3.2 Prüfung der Router- / Firewall-Einstellungen

Bei funktionierender Netzwerkverbindung prüfen Sie bitte, ob die benötigten Ports und das L2TP-Protokoll frei geschaltet sind, die Datenpakete durch Firewall-Regeln oder Intrusion-Detection-Funktionen blockiert werden, ob es konkurrierende Verbindungen gibt.

- Ist UDP 1701 ausgehend explizit freigeben, hilft ein Port-Forwarding UDP 1701 eingehend zur IP-Adresse der Registerbox oder alternativ ein entsprechender Port-Trigger?
- Gibt es eine Einstellung zum L2TP-Passthrough?
- Schalten Sie möglichst ICMP WAN-seitig frei.
- Kann die Registerbox-Verbindung testweise in einer DMZ-Einstellung ungehindert der allgemeinen Firewall-Einstellungen konfiguriert werden? Sofern die Registerbox in der DMZ betrieben wird, bitte den Zugriff IP- oder Port-basierend einschränken.
- Falls konkurrierende VPN-Verbindungen auf der Firewall terminieren, die das L2TP-Protokoll nutzen, kann es zu Konflikten kommen - insbesondere, wenn diese Port UDP 1701 nutzen.
- Kann der Router in der vorliegenden Firmware-Version nur eine VPN-Verbindung verwalten oder hat er Probleme mit mehreren gleichzeitigen VPNs, die am Router terminieren oder sich als Client aus dem LAN in entfernte Netze einwählen?
- Prüfen Sie, ob das Log des Routers / der Firewall Blockaden des Datenverkehrs von der Registerbox und zurück anzeigt. Adressen der LN-Server liegen im Bereich: 212.63.94.48/29 (212.63.94.48 .. 212.63.94.55).
- Informieren Sie sich bitte beim Hersteller oder bei Usergruppen zu Problemen mit dem Router und der verwendeten Firmware-Version.
- Versuchen Sie ein Update der Internet-Router-Firmware.
- Steht der Router auf der Kompatibilitätsliste (siehe Kapitel Erfahrungen zur Kompatibilität von Routern).
- Ist zwischen Internet-Router und Registerbox eine Firewall, Router oder ein Server mit 2 Schnittstellen (WAN- und LAN-Seitig)? Sind das Routing und die Firewall- / Zugriffregeln dort ebenfalls passend konfiguriert? Was sagen die Log-Einträge an dieser Stelle aus?

8.3.3 Beeinträchtigt der Internet-Anschluss die Tunnelverbindung

Nicht alle Internetverbindungen sind für alle Arten des Datenverkehrs geeignet. Bei einigen Produkten, die in erster Linie für die Privatnutzung konzipiert wurden, sind die Protokolle eingeschränkt, die Bandbreite zu bestimmten Diensten oder die Antwortzeiten (Latenz) sehr groß. Bei zunehmender Bedeutung des elektronischen Rechtsverkehrs für das Notariat wird ein solider Anschluss benötigt.

- Geht die Tunnelverbindung nicht über eine direkte LAN-Verbindung zum Internetanschluss und wird sie über eine Tunnelverbindung zu einem zentralen Internetanschluss geleitet, kann dies zu Problemen wegen Überschreitens der erlaubten Datenpaketgröße führen.
- Fragen Sie den Internetprovider, ob das angebotene Produkt für den Verwendungszweck geeignet ist.
- Informieren Sie sich in Anwenderforen.

- Wählen Sie möglichst ein Produkt, das für professionellen Einsatz (Geschäftskunden) konzipiert wurde, eine entsprechende Qualität hat in Bezug auf Bandbreite, Verfügbarkeit und Service sowie für L2TP-Datenverbindungen geeignet ist.

8.4 Erfahrungen zur Kompatibilität von Routern

Nicht alle Router sind für den professionellen Einsatz geeignet. Viele preisgünstige Router haben Firewall-Funktionalität, die bei privater Nutzung bestimmte Angriffsszenarien blockieren kann, jedoch bei professioneller Nutzung benötigte Datenkanäle oder Protokolle behindert. Die Einstell- und Log-Möglichkeiten dieser einfachen Geräte sind meistens sehr begrenzt. In vielen Fällen können Blockaden durch Kombination verschiedener Einstellungen, die nicht immer schlüssig sind, aufgehoben werden. In manchen Fällen ist die Firmware-Programmierung der Router fehlerhaft. Ein Blick ins Handbuch, Firmware-Update, Nachfragen beim Hersteller oder die Recherche im Internet sowie in Anwenderforen können oft weiterhelfen. Führt dies nicht zum Erfolg, empfehlen wir den Austausch des Routers.

8.4.1 Austausch des Routers

Wenn Firmware-Updates und Einstellungen des Routers nicht zum Erfolg führen oder der Router auf der Kompatibilitätsliste als nicht geeignet gelistet ist, muss der Internet-Router ausgetauscht werden. Bei zunehmender Bedeutung des elektronischen Rechtsverkehrs für das Notariat wird ein solider Anschluss benötigt. Router / Firewall sollten schon zum Erhalt der Datensicherheit auf dem aktuellen Stand der Technik sein und sich für den professionellen Einsatz eignen.

8.4.2 Inkompatible Router

Liste NICHT kompatibler Router, mit denen wir bei Supportanfragen Erfahrungen sammeln durften. Die Liste gibt also kein vollständiges Bild wieder.			
AVM	Fritz!Box 2030	alle	
D-Link	804	2.05B1	
Netgear	WPN 824	2.0.20_102.17	
Netgear	DG834GB	1.05.00	
Netgear	DG834GBv4	5.01.01, 5.01.05, 5.01.08, 5.01.09	V5.01.14 ist aktuell beim Hersteller abrufbar, derzeit unbekannt ob diese funktioniert
Netgear	FVS318 ProSafe	Rev. 1+2+3	NAT – Fehler nach der Zwangstrennung
Netgear	FVS336 ProSafe		Probleme mit Zwangstrennung
Netgear	FVS338 ProSafe		Probleme mit Zwangstrennung
O2	Homebox 6641		
Telekom	Speedport W303V TypB	alle	
Telekom	Speedport W502V	alle	
Telekom	Speedport W503V	vor 66.04.66	
Telekom	Speedport W503V Typ C	alle	
Telekom	Speedport W700V	nur 3.15 fehlerhaft s. WL	
Telekom	Speedport W720V	nur 1.34 fehlerhaft s. WL	
Telekom	Teledat 302 (Modem)		
Telekom	Speedport W724V		
Zyxel	P-660HW-T7C	Alle	Tunnel wird aufgebaut, kein RMS

8.4.3 Einstellungen bei Netgear-Routern

Die Router-Modelle von Netgear unterscheiden sich durch Funktionsumfang und bezüglich der Einstellmöglichkeiten. Soweit der Verbindungsaufbau nicht grundsätzlich durch Fehlfunktion der jeweiligen Software-Version gestört wird, wie es bei den Modellen auf der Liste nicht kompatibler Router der Fall ist, führten folgende Einstellungen zu einem erfolgreichen Verbindungsaufbau. Allerdings haben wir festgestellt, dass es grundsätzlich bei vielen Netgear-Produkten im Zusammenhang mit dem L2TP-Tunnel der Registerbox Schwierigkeiten bei der Zwangstrennung und mit dem IDS gibt. Bitte informieren Sie sich auch beim Netgear-Support bzw. den Netgear-Support-Webseiten (http://support.netgear.com/app/answers/detail/a_id/966/~/troubleshooting-vpn-passthrough-for-home-routers).

- Port 1701 UDP ausgehend frei geschaltet
- Port-Forwarding oder Triggering je nach Einstellmöglichkeiten
  - Port-Triggering ein- und ausgehend Port 1701 udp
  - Port-Forwarding 1701 udp zur IP-Adresse der Registerbox
- Block UDP-Flooding" deaktivieret
- Block non-Standard-Pakets" deaktiviert
- L2TP Passthrough aktiviert
- ICMP von WAN-Seite aktivieren: Respond to Ping on Internet Port

8.5 Probleme bei der Datenverbindung zwischen Arbeitsplatz und Servern

8.5.1 Problem bei ZTR-Webseiten-Zugriff trotz aktiver PPP-Verbindung

Wenn Aufrufe zu den Diensten der Bundesnotarkammer, beispielsweise zur Testamentsregister-Seite https://ztr.bnotk.de, nicht funktionieren, obwohl die PPP-Tunnelverbindung aktiv ist (PPP-LED an der Registerbox leuchtet), ist bitte Folgendes zu prüfen.

- Funktioniert das Routing vom betreffenden Arbeitsplatz über die Registerbox richtig? Siehe auch Kapitel Routenverfolgung vom Arbeitsplatz zum Server und zurück.
- Gibt es Proxy-Einstellungen und sind bei Einsatz eines Proxy-Servers die Ausnahmen richtig gesetzt? Siehe auch Kapitel Prüfung der Proxy-Ausnahmen.
- Ist die Registerbox in demselben Subnetz mit den betreffenden Arbeitsplätzen? Siehe Kapitel Ist die Registerbox in einem anderen Subnetz als der betreffende Arbeitsplatz.
- Sind die LAN-Ports

8.5.2 Zertifikatsfehler bei Aufruf der Diensten der Bundesnotarkammer

Ein Zertifikatsfehler wird typischerweise angezeigt, wenn der Aufruf der Dienste der Bundesnotarkammer über das Internet geleitet wird. Prüfen Sie bitte Folgendes:

- Funktioniert das Routing richtig. Zur Prüfung der Route siehe Kapitel Routenverfolgung vom Arbeitsplatz zum Server und zurück.
- Gibt es Proxy-Einstellungen und sind die Ausnahmen richtig gesetzt? Siehe Kapitel Prüfung der Proxy-Ausnahmen.

8.5.3 Andere Webseiten der BNotK können nicht erreicht werden

Wenn die Registerbox-Route für den betreffenden Arbeitsplatz gesetzt ist, werden auch andere Webseiten der Bundesnotarkammer durch die Route über die Registerbox geleitet. Ist die Registerbox ausgeschaltet oder gibt es keine aktive Verbindung, funktionieren also diese Webseiten ebenfalls nicht, z.B. www.bnotk.de, www.testamentsregister.de, www.notar-inter.de. Diesbezüglich ist eine Änderung geplant, die die öffentlichen von den nicht-öffentlichen Seiten trennt.

8.5.4 Keine Verbindung bei korrekt gesetzter Route oder langsame Verbindung

Wenn die Webseiten nicht aufgerufen werden können oder nur mit langer Ladezeit, obwohl, die PPP-LED und die Route für den betreffenden Arbeitsplatz richtig gesetzt ist, kann dies an einer schlechten PPP-Tunnel-Verbindung liegen.

Prüfen Sie bitte Folgendes:

- Tritt das Problem auch auf bei einem Arbeitsplatz, der direkt an der Registerbox angeschlossen ist?
- Zur Anzeige des Verlustes von Datenpaketen führen Sie ein *ping ztr.bnotk.de* aus.
- Prüfen Sie die Routenverfolgung, siehe Kapitel Routenverfolgung vom Arbeitsplatz zum Server und zurück.
- Ist die Datenpaketgröße / MTU WAN-seitig kleiner als 1492?
- Ist die Netzwerkkabelverbindung zur Registerbox einwandfrei. Defekte Kabel- und Steckverbindungen können zu zeitweiligen Unterbrechungen oder verlangsamter Datenübertragung führen.
- Prüfen Sie die Firewall-Einstellungen und die Internet-Verbindung.
  Oft verursachen Firewall-Einstellungen und konkurrierende VPN-Verbindungen eine Verzögerung, den Verlust von Datenpaketen oder Unterbrechung der Datenverbindung. Siehe hierzu Kapitel *Prüfung der Router- / Firewall-Einstellungen*.

8.6 Prüfung der Datenverbindung zwischen Arbeitsplatz und Servern

8.6.1 Routenverfolgung vom Arbeitsplatz zum Server und zurück

Verbindung von einem Arbeitsplatz mit gesetzter Route testen:

- Bei „Ping ztr.bnotk.de“ kommt eine Antwort.
- Routenverfolgung Beispiel Windows: Bei „tracert ztr.bnotk.de“ sollte die Registerbox antworten, danach der LN-Server und schließlich der adressierte Zielhost.
- Die Routenverfolgung muss eindeutig anzeigen, dass die Verbindung nicht über das Internet läuft.

Beispielsweise könnte eine Ausgabe von tracert wie folgt aussehen:
Routenverfolgung zu ztr.bnotk.de [77.76.215.98] über maximal 30 Abschnitte:

1 373 ms 323 ms 333 ms 192.168.11.1
2 11 ms 11 ms 10 ms lns3.notarnet.de [213.214.12.125]
3 11 ms 13 ms 10 ms 77.76.214.44
4 11 ms 10 ms 10 ms ztr.bnotk.de [77.76.215.98]

Ablaufverfolgung beendet.

Die Routenverfolgung geht nicht bis zur Registerbox. Die Registerbox antwortet nicht.
Obwohl die PPP-Verbindung der Registerbox steht und keine Verbindungsabbrüche zu verzeichnen sind, kann die ZTRDemo-Seite nicht erreicht werden. Prüfen Sie bitte Folgendes:

- Ist die Registerbox eingeschaltet und hat sie eine aktive Tunnel-Verbindung?
- Funktioniert die Netzwerkverbindung vom betreffenden Arbeitsplatz zur Registerbox? Kann die Registerbox vom betreffenden Arbeitsplatz per PING erreicht werden?
- Ist die auf der Zuweisungsverfügung angegebene IP-Adresse der Registerbox und die Netzwerkmaske passend? Hinweis: Nach einer Rekonfiguration können diese abweichend von der Zuweisungsverfügung sein.
- Bitte prüfen Sie die Routen-Einstellungen. Siehe Kapitel Prüfung der Route.

Routenverfolgung (tracert) geht nur bis zur Registerbox

Wenn das Ergebnis der Routenverfolgung nur bis zur Registerbox geht (die Registerbox ist die letzte Netzwerkschnittstelle in der Liste, die antwortet), bitte Folgendes prüfen:

- Ist der PPP-Tunnel aktiv (PPP-LED leuchtet)?
- Soweit der PPP-Tunnel aktiv ist, funktioniert in diesem Fall meist die Rückroute nicht oder die Tunnelverbindung ist teilweise gestört.
- Prüfen Sie die Routing-Einstellungen, insbesondere, wenn die Route nicht individuell am Arbeitsplatz, sondern an zentraler Stelle konfiguriert ist. Siehe Kapitel Prüfung der Route.
- Die Registerbox sollte in demselben Subnetz mit den Arbeitsplätzen sein, da in der Registerbox kein Gateway für die Rückroute gesetzt ist. Siehe auch Kapitel Ist die Registerbox in einem anderen Subnetz als der betreffende Arbeitsplatz.
- Prüfen Sie die Firewall-Einstellungen und die Internet-Verbindung.
  Oft verursachen Firewall-Einstellungen und konkurrierende VPN-Verbindungen eine Verzögerung, den Verlust von Datenpaketen oder eine Unterbrechung der Datenverbindung. Siehe hierzu Kapitel *Prüfung der Router- / Firewall-Einstellungen*.

Routenverfolgung (tracert) zeigt Route über das Internet an
Wenn am betreffenden Arbeitsplatz eine Routenverfolgung anzeigt, dass die Daten über das Internet laufen, bitte Folgendes prüfen:

- Siehe Kapitel Prüfung der Route.

8.6.2 Prüfung der Route

Bei Prüfung der Route bitte Folgendes beachten:

- Ist die IP-Route an den betreffenden Arbeitsplätzen gesetzt? Oft wurde bei der Inbetriebnahme die Route nur an einem Arbeitsplatz gesetzt.
- Bei Routeneinstellung am Arbeitsplatz:
  - Wurde die IP-Route korrekt eingegeben? (Anzeige der Routentabelle z.B. mit route print, Löschen mit route delete)
  - Wurde bei mehreren Netzwerkschnittstellen (z.B. WLAN und LAN-Anschluss) an einem Arbeitsplatz die Route für die passende Netzwerkschnittstelle gesetzt?
- Bei zentraler Routeneinstellung, diese bitte inklusive Rückrouten überprüfen.
- Ist die Metrik der Route im Vergleich zu konkurrierenden Routen passend gesetzt?
- Ist die Registerbox in demselben Subnetz mit dem betreffenden Arbeitsplatz / Terminalserver? Siehe Kapitel Ist die Registerbox in einem andere Subnetz als der betreffende Arbeitsplatz.

8.6.3 PPP-Tunnel-Verbindung ist teilweise gestört

Wenn bei korrekt gesetzter Route (hin und zurück) und leuchtender PPP-LED an der Registerbox Datenverluste angezeigt werden oder eine Routenverfolgung nur bis zur Registerbox geht, kann dies an einer nur teilweise funktionierenden Tunnelverbindung liegen.

- Prüfen Sie die Firewall-Einstellungen und die Internet-Verbindung.
  Oft verursachen Firewall-Einstellungen und konkurrierende VPN-Verbindungen eine Verzögerung, den Verlust von Datenpaketen oder eine Unterbrechung der Datenverbindung. Siehe hierzu Kapitel *Prüfung der Router- / Firewall-Einstellungen*.

8.6.4 Ist die Registerbox in einem anderen Subnetz als der betreffende Arbeitsplatz

Die Registerbox sollte im Subnetz mit Arbeitsplätzen / Terminalserver betrieben werden. Sind Router zwischen dem betreffenden Arbeitsplatz und der Registerbox geschaltet, können die Datenpakete den Rückweg nicht finden, da in der Registerbox die entsprechende Gateway-IP nicht gesetzt werden kann. Durch ein entsprechendes NATing der betreffenden Subnetze kann das Problem gelöst werden. Alternativ kann ein Notarnetz-Router eingesetzt werden, der auch für individuelle Rückrouten konfiguriert werden kann.

8.6.5 Prüfung der Proxy-Ausnahmen

Folgendes gilt nur, wenn ein Proxy-Server eingesetzt wird!

Wenn bei Aufruf von https://ztr.bnotk.de eine Fehler-Seite mit der Information erscheint, dass der Aufruf über Internet und nicht über die Registerbox erfolgt, kann dies an fehlenden oder nicht korrekten Proxy-Ausnahmen liegen. Prüfen Sie bitte Folgendes:

- Zeigt eine Routenverfolgung an, dass die Datenpakete bei IP-Adressierung tatsächlich den richtigen Weg über die Registerbox nehmen? Siehe auch Kapitel Routenverfolgung vom Arbeitsplatz zum Server und zurück.
- Sind die Proxy-Ausnahmen korrekt gesetzt? Siehe Kapitel Proxy-Server im Einsatz.

8.7 Fernwartungsmöglichkeit der Registerbox für Monitoring-Zwecke

Für die Registerbox kann auch aus der Fern ein Monitoring erfolgen. Dazu muss die Registerbox so angeschlossen werden, wie in Kapitel 7 Rekonfiguration beschrieben. Diese Monitoring-Möglichkeit wird durch den Support im Verlauf der Fehleranalyse ggf. zur Hilfe genommen.

8.8 Änderungen der Notarstelle

8.8.1 Die Notarstelle endet ohne Nachfolger

Der Notar erhält eine Widerruf-Zuweisungsverfügung mit Rücklieferschein. Die Registerbox geht zurück an den dort angegebenen Empfänger.

8.8.2 Die Notarstelle endet mit Nachfolger

Die Registerbox bleibt vor Ort. Sie wird an den Amtsnachfolger übertragen. Der Vorgänger erhält eine Widerruf-Zuweisungsverfügung. Der Nachfolger erhält eine Zuweisungsverfügung.

9 Support-Kontakt und weitere Informationen zur Problembehebung

Falls die angegebenen Hinweise zur Problemlösung nicht zu einem Ergebnis führen sollten, wenden Sie sich bitte unter Angabe des für die Registerbox verantwortlichen Notars mit einer möglichst konkreten Problembeschreibung an registerbox@testamentsregister.de. Beantworten Sie bitte auch fallbezogen folgende Fragen:

9.1.1 Keine PPP-Tunnelverbindung oder Verbindungsabbrüche

Internet-Anschluss

1. Provider und Produkt:
2. Internet-Router und Modellbezeichnung:
3. Firmware-Version des Internet-Routers:
4. Welche Bandbreite ist vor Ort geschaltet:
5. Wie viele User gibt es vor Ort, die auf das Internet zugreifen:
6. Ist zwischen der Registerbox und dem Internetanschluss eine VPN-Tunnelverbindung (ja/nein):

Ist die Registerbox pingbar?

1. Vom Router aus:
2. Vom Arbeitsplatz aus:

Wann kommt eine PPP-Verbindung zustande?

1. Nur nach Neustart der Registerbox notwendig (ja/nein):
2. Nur Neustart des Internet-Routers notwendig (ja/nein):
3. Neustart des Internet-Routers und anschließend der Registerbox notwendig (ja/nein)::
4. Ergänzende Informationen zu diesem Punkt:

Router-Einstellungen

1. UDP 1701 ausgehend frei (ja/nein):
2. UDP 1701-Forwarding auf Registerbox (ja/nein):
3. Port-Trigger UDP 1701 ausgehend und eingehend (ja/nein):
4. L2TP Passthrough gesetzt (ja/nein):
5. ICMP WAN-seitig aktiviert (ja/nein):
6. DMZ-Einstellung (ja/nein):
7. Sonstige Einstellungen:
8. Was sagen die Log-Einträge des Routers zum Zeitpunkt des Verbindungsabbruchs:

VPNs auf dem Router

1. Ist der Router für VPN eingerichtet (ja/nein):
2. Wenn ja welche:
3. Wird dabei L2TP über Port 1701 verwendet:
4. Andere VPN Clients / Server hinter dem Router:
5. Unterstützt der Router nur 1 VPN (ja/nein):

Paketverluste und Routenverfolgung

1. Angabe der MTU auf der WAN-Seite:
2. Ergebnis PING ztr.bnotk.de:
3. Ergebnis TRACERT ztr.bnotk.de:

Beschreibung des Netzwerkaufbaus

1. Internet-Router am Internetzugang. Auf der LAN-Seite des Internetzugangs sind die betreffenden Arbeitsplätze / Terminalserver zusammen mit der Registerbox in einem Subnetz (ja/nein):
2. Ist zwischen Internet-Router und Registerbox eine Firewall, Router oder ein Server mit 2 Schnittstellen WAN- und LAN-Seitig (ja/nein):
3. Eventuell weitere Beschreibung zum Aufbau:

9.1.2 Datenverbindung oder Routing zwischen Arbeitsplatz und Registerbox

Wie ist der Aufbau des LANs?

1. Ist die Registerbox in demselben Subnetz mit dem betreffenden Arbeitsplatz / Terminalserver (ja/nein):
2. Ist zwischen Arbeitsplatz / Terminalserver und der Registerbox ein Router oder eine Firewall geschaltet, z.B. bei einer Geschäftsstellen-Anbindung (ja/nein):

Routing-Einstellungen

1. IP-Adresse und Netzmaske des betreffenden Arbeitsplatzes:
2. Wenn die Route am Arbeitsplatz eingestellt ist, bitte die Routentabelle übermitteln (z.B. bei Windows über die Ausgabe von *route print*):
3. Bei zentraler Routen-Einstellung bitten wir um eine Beschreibung des Routings zwischen Arbeitsplatz und Registerbox sowie dem Rückkanal:

Proxy-Einstellungen

1. Sind am Arbeitsplatz Proxy-Einstellungen gesetzt, z.B. in den Internetoptionen (ja/nein):
2. Ist ein Proxy-Server im Einsatz (ja/nein):

Antiviren/Firewall-Software

1. Eingesetzte AV-Software o.ä. im LAN/PC:

10 Support-Adressen

Zentrales Testamentsregister	Telefon: 0800 – 35 50 600 E-Mail: registerbox@testamentsregister.de
EGVP	Telefon: 01805 – 348 778 E-Mail: egvp@westernacher.com
AnNoText – Wolters Kluwer	Telefon: 0221 – 94 373-16060 E-Mail: support@annotext.de
DATEVnet – DATEV	Telefon: 0911 – 319 4999 E-Mail: datevnet@service.datev.de