Sicherheitsvorgaben (Security Target)

zu Netviewer one2one^{TS} Version 5.1

der Netviewer AG, Karlsruhe

BSI-Zertifizierungs-ID:	BSI-DSZ-CC-0524
ST-Version:	1.8

Inhaltsverzeichnis

1 ST-Einführung

1.1 ST-Identifikation

Dieses Dokument stellt die Sicherheitsvorgaben (Security Target) für das Produkt Netviewer one2one^{TS} Version 5.1 der Netviewer AG, Erzbergerstr. 117, 76133 Karlsruhe dar. Das Produkt Netviewer one2one^{TS} besteht aus mehreren Programmen, die in Kapitel 2 aufgeführt sind.

Identifikationsdaten:

BSI-Zertifizierungs-ID:	BSI-DSZ-CC-0524
ST-Datum:	14.09.2008
ST-Version:	1.8
EVG-Name:	Netviewer one2one^{TS}
EVG-Version:	5.1 build-nummer 1208
ST-Dateiname:	ST_Netviewer_one2oneTS_v1.8.pdf
Verfasser:	Netviewer AG, Erzbergerstr. 117, 76133 Karlsruhe

Die vorliegenden Sicherheitsvorgaben basieren auf den „Common Criteria (CC)" [CC] in Version 2.3, die aus den folgenden drei Teilen bestehen:

- [CC_P1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 2.3, August 2005
- [CC_P2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 2.3, August 2005
- [CC_P3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 2.3, August 2005

1.2 ST-Übersicht

Dieses Dokument beschreibt die Sicherheitsvorgaben (Security Target, ST) des Evaluationsgegenstands (EVG, das Produkt Netviewer one2one^{TS} Version 5.1 der Netviewer AG). Die ST sind die Grundlage für die Übereinstimmung aller beteiligten Seiten hinsichtlich der von einem EVG gebotenen Sicherheit, sowie ihrer Prüfung und Bewertung.

Dieses Dokument besteht aus acht Kapiteln und vier Anhängen. Es ist inhaltlich nach den Vorgaben des Anhang B von Teil 1 der Common Criteria [CC_P1] aufgebaut.

Kapitel 1 enthält die ST-Einführung, Kapitel 2 die EVG-Beschreibung, Kapitel 3 beschreibt die EVG-Sicherheitsumgebung, Kapitel 4 identifiziert die Sicherheitsziele, Kapitel 5 spezifiziert die IT-Sicherheitsanforderungen, Kapitel 6 enthält die EVG-Übersichtsspezifikation, Kapitel 7 enthält die relevanten PP-Postulate und Kapitel 8 enthält die notwendigen Erklärungen.

Als Anhänge sind ein Glossar, ein Verzeichnis der Abkürzungen, ein Verzeichnis der Referenzen und Versionsinformationen über dieses Dokument angefügt.

1.3 Postulat der Übereinstimmung mit den CC

Der EVG ist konform zu den Common Criteria [CC] Version 2.3.

Der EVG ist konform zu Teil 2 der Common Criteria [CC_P2].

Der EVG ist konform zu Teil 3 der Common Criteria [CC_P3] und erfüllt die Anforderungen des Vertrauenswürdigkeitspaketes EAL2.

Die Stärke der verwendeten Mechanismen ist SoF-Basic.

2 EVG-Beschreibung

Der Evaluierungsgegenstand (EVG) ist ein auf einer Client-Server-Architektur basierendes Softwaresystem und umfasst die Anwendersoftware Netviewer one2one^{TS} (Clientprogramme) in Kombination mit den Serverkomponenten Netviewer Standard Server^{TS} und SSLswitch.

2.1 Übersicht über den EVG

Netviewer one2one^{TS} ist ein Client-Server-basiertes System zum Desktop-Sharing für zwei Anwender, die sich an entfernten Computern befinden. Im Rahmen einer one2one^{TS}-Sitzung können die Sitzungspartner sich gegenseitig ihren Bildschirm zeigen, sich gegenseitig Fernsteuerungsrechte einräumen und weitere Netviewer-Funktionen zur Kommunikation und Zusammenarbeit nutzen.

Der EVG umfasst die Netviewer one2one^{TS} Clients, die den Anwendern über eine grafische Benutzeroberfläche die Funktionalitäten von Netviewer one2one^{TS} zur Verfügung stellen, sowie die Serversoftware Netviewer Standard Server^{TS}, welche die Kommunikation der beiden entfernten Computer über das Internet oder ein Intranet ermöglicht.

Die Clientkomponenten von Netviewer one2one^{TS} sind für Anwender ohne besondere Sachkenntnis im Bereich EDV konzipiert und für den Einsatz in normaler Büroumgebung geeignet.

Netviewer one2one^{TS} ist für Einsatzbereiche mit niedrigem Schutzbedarf konzipiert. Der EVG bietet Schutz gegen Angreifer mit einem niedrigen Angriffspotential. Die Sicherheitsfunktionen des EVG verhindern, dass der Angreifer mit Lesen, Umleiten und Manipulieren der über das Netzwerk ausgetauschten Nachrichten die Sicherheit des Systems kompromittieren kann. Der Angreifer kann in Besitz der Clientprogrammen kommen und nicht-ausführbare Teile davon mit einem Binäreditor manipulieren, ohne dass dadurch die Sicherheit des one2one^{TS}-Systems gefährdet wäre.

2.2 Lieferumfang

Zum Lieferumfang bei Auslieferung des EVG gehören:

Lfd. Nr.	Typ	Bezeichnung	Version	EVG-Teil
1	Programm	Netviewer one2one^{TS} – Beraterprogramm	5.1	Ja
2	Programm	Netviewer one2one^{TS} – Teilnehmerprogramm	5.1	Ja
3	Programm	Netviewer one2one^{TS} – Standard Server	5.1	Ja
4	Programm	Netviewer SSLswitch	1.3.0.5	Ja
5	Programm	Netviewer Netplayer	offen	Nein
6	Textdatei	Benutzerdatei	individuell	Ja

	(Initial)	(NVServer_users.txt)		
7	Textdatei (Vorlage)	SSLswitch Konfigurationsdatei (SSLswitch.xml)	individuell	Ja
8	Textdatei (Vorlage)	Allgemeine Konfiguration für Standard Server[TS] (ServerSettings.ini)	individuell	Ja
9	Binärdatei	Kundenspezifische Konfiguration für Standard Server[TS] (ServerData.dat)	individuell	Ja
10	Binärdatei	Kundenspezifische Konfiguration der Clientprogramme (ContractData.dat)	individuell	Ja
11	PDF-Dokument	Netviewer one2one[TS] Benutzerhandbuch	1.4	Ja
12	PDF-Dokument	Netviewer Standard Server[TS] Administratorhandbuch	1.4	Ja

Tabelle 1: Auslieferungsbestandteile des EVG

Mit dem EVG wird die Anwendung Netviewer NetPlayer ausgeliefert, die das Abspielen von Sitzungsaufzeichnungen erlaubt. Der Netviewer NetPlayer stellt keine Sicherheitsfunktion des EVG dar.

2.3 Anordnung und Benennung der Teile des EVG

Die folgende Grafik zeigt die Anordnung der Programme des EVG im Wirkbetrieb. Insbesondere sind die in diesem Dokument verwendeten Bezeichnungen den EVG-Programmen und -Komponenten zugeordnet:

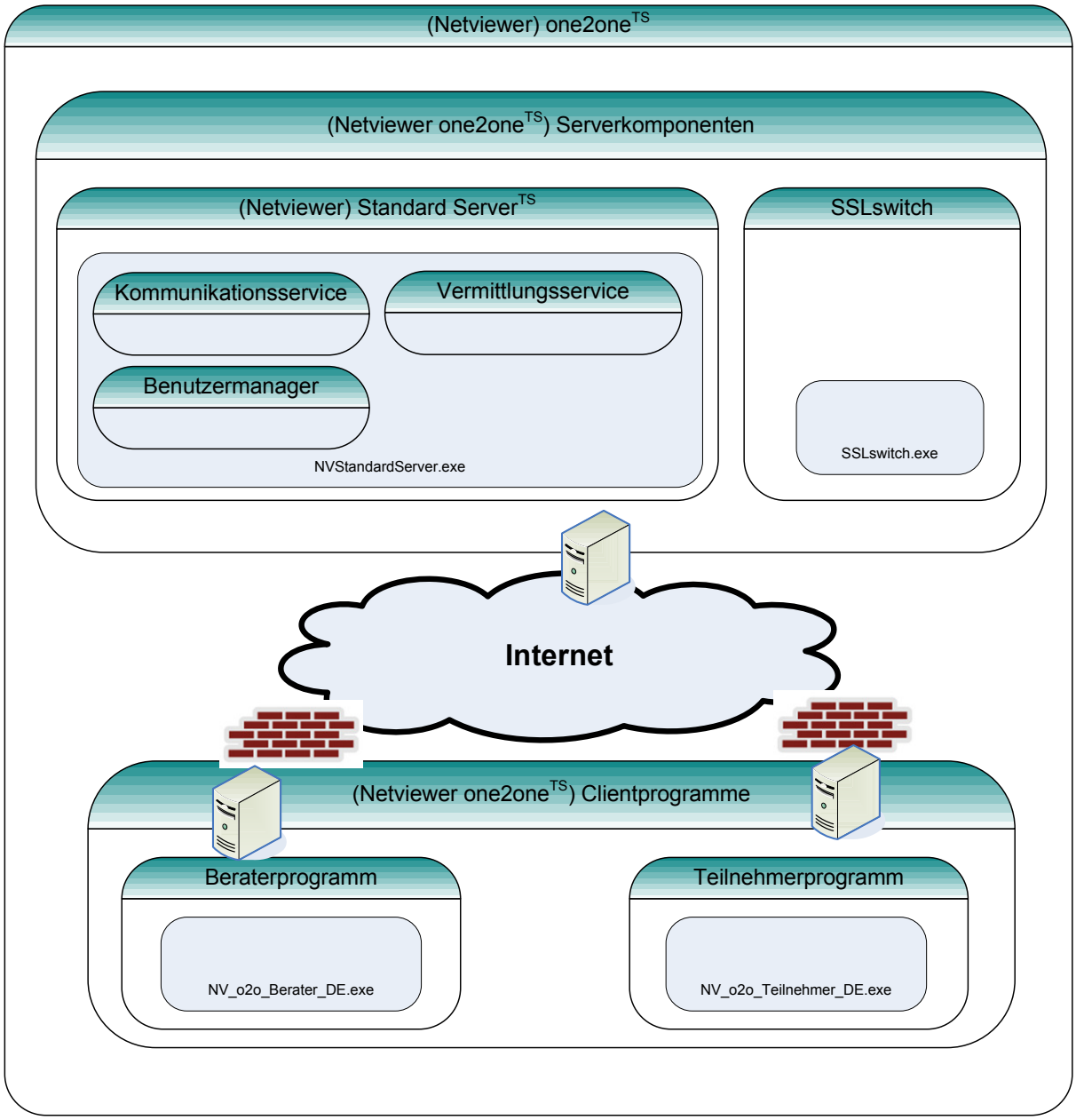

Abbildung 1: Bezeichnungen der Komponenten des EVGs (Netviewer one2one^{TS}) und deren Beziehungen.

Das Gesamtsystem Netviewer one2one^{TS} umfasst die Netviewer one2one^{TS} Serverkomponenten und die Netviewer one2one^{TS} Clientprogramme.

Die Serverkomponenten beinhalten die Serversoftware Netviewer Standard Server^{TS}, welche den Vermittlungsservice (Signalisierung und Verbindungsaufbau), den Kommunikationsservice (Übertragung der Sitzungsdaten) und den Benutzermanager (Benutzerverwaltung) in der Datei NVStandardServer.exe umfasst. Zu den Serverkomponenten gehört außerdem die SSLswitch.exe, welche den SSL-Handshake und die Weiterleitung der entschlüsselten Daten übernimmt.

Zu den Netviewer one2one^{TS} Clientprogrammen zählen das Beraterprogramm NV_o2o_Berater_DE.exe und das Teilnehmerprogramm NV_o2o_Teilnehmer_DE.exe.

Auf drei Rechnern (PC-Symbole) kommen demnach vier Programme zum Einsatz. Die Clientprogramme kommunizieren mit den Serverkomponenten über das Internet.

Im Kapitel 2.11.4 wird dargestellt, wie die EVG-Komponenten zusammenspielen, um Netviewer one2one^{TS} Sitzungen zwischen Beratern und Teilnehmern zu ermöglichen. Dort werden die Abläufe in der Signalisierung und auf Applikationsebene erläutert, die letztlich den Austausch des Sitzungsdatenstroms zwischen Beraterprogramm und Teilnehmerprogramm ermöglichen.

2.4 Systemanforderungen von Netviewer one2one^{TS}

Alle Komponenten des EVG sind auf dem Betriebssystem Microsoft Windows lauffähig. Die Clientprogramme können unter Microsoft Windows 2000 und Windows XP und die Serverkomponente unter Microsoft Windows Server 2000 und Server 2003 verwendet werden.

Für den erfolgreichen Betrieb des EVG ist auf allen beteiligten Systemen (Beraterrechner, Teilnehmerrechner und Serverrechner) eine geeignet schnelle Internetverbindung erforderlich. Weiterhin müssen das Berater- und das Teilnehmerprogramm eine TCP-Verbindung zum Netviewer Server aufbauen können.

Für den sicheren Betrieb des EVG ist es notwendig, dass das jeweilige Betriebssystem nicht korrumpiert ist, was u.a. durch gewissenhaftes einspielen von Aktualisierungen des Betriebssystemherstellers (Patches) und durch Betrieb von Programmen zur Abwehr von Schadsoftware geschieht (Virenscanner usw.). Insbesondere greift der EVG auf Kryptographiekomponenten des Betriebssystems zu, die SSL und die Zufallszahlengenerierung betreffen, die für einen sicheren Betrieb benötigt werden. Genaue Angaben zu diesbezüglichen Annahmen finden sich in Kapitel 3.2.

Detaillierte Systemanforderungen der Komponenten des EVG enthält das Kapitel 3.2.

2.5 Besonderheiten von Netviewer one2one^{TS}

Das Produkt Netviewer one2one^{TS} weist hinsichtlich der Erstellung, der Auslieferung und des Betriebs einige Besonderheiten auf, die im Folgenden näher erläutert werden:

- Die Clientprogramme des EVG müssen nicht installiert werden; sie bestehen aus einer direkt ausführbaren .exe-Datei, welche sofort einsatzbereit ist und keine Installation erfordert. Die Serverkomponenten müssen vom Betreiber installiert und konfiguriert werden.
- Der EVG wird vor der Auslieferung individuell für jeden einzelnen Kunden von der Netviewer AG konfiguriert und kompiliert. Die einzelnen Instanzen des EVG weisen daher in begrenztem Umfang unterschiedliche Eigenschaften auf. Diese variablen Eigenschaften der Software beeinflussen nicht die Sicherheitsfunktionen des EVG. Ebenso bleiben die EVG-Identifikationsmerkmale von der kundenindividuellen Konfiguration unberührt: Die Versionsnummer, der Hersteller (Netviewer AG) sowie der Signaturgeber (Netviewer AG) der digitalen Signaturen der ausführbaren Dateien sind bei allen ausgelieferten EVG-Instanzen dieselben. Genauer Beschreibungen dazu finden sich in Tabelle 3 in Kapitel 2.13 und dem Benutzerhandbuch (welches auch vor Sitzungsaufbau aus dem Startdialog der Clientprogramme zugänglich ist). Weitere Informationen zur Konfiguration von Netviewer one2one^{TS} enthält das Kapitel 2.13.
- Die Basis, aus der jede individuelle Instanz des EVG erstellt wird, ist stets dieselbe.
- Es können jeweils nur eine bestimmte Instanz der Clientsoftware und eine bestimmte Instanz der Serversoftware miteinander kommunizieren – Clientprogramme eines Kunden können nicht mit Clientprogrammen oder Serverkomponenten eines anderen Kunden zusammenarbeiten.

2.6 Clientprogramme von Netviewer one2one^{TS}

Bei den Clientprogrammen von Netviewer one2one^{TS} wird unterschieden zwischen dem Beraterprogramm, welches das Initiieren einer one2one^{TS} -Sitzung ermöglicht, und dem Teilnehmerprogramm, welches den Eintritt in eine initiierte Sitzung ermöglicht. Die Clientprogramme bestehen auf Berater- und Teilnehmerseite aus einer ausführbaren .exe-Datei.

2.6.1 Wichtige Einsatzszenarien Netviewer one2oneTS

Die wichtigsten Einsatzszenarien Netviewer one2one^{TS} sind Support und Fernwartung sowie der Vertrieb.

Support und Fernwartung

Die Stärken des Produkts Netviewer one2one^{TS} iegen in den Anwendungsbereichen Support und Fernwartung. Die Bandbreite reicht vom Anwenderfehler über Hilfe beim Ausfüllen von Formularen bis hin zur Neuinstallation eines bestimmten Programms.

Hilfe per Fernsteuerung: Gerade kleine, versteckte Fehler erfordern viele Rückfragen und Beschreibungen zwsichen Hifesuchendem und dem Supportmitarbeiter. Netviewer one2one^{TS} erlaubt dem Supportmitarbeiter den direkten Blick auf den Bildschirm des Hilfesuchenden, so dass der Supportmitarbeiter (der Berater) schnell erkennt, was das Problem ist und kann seinen internen oder externen Kunden zur richtigen Lösung lotsen oder per Fernsteuerung selbst aktiv werden.

Weniger Reisekosten im weltweiten Support: Insgesamt wird der Support mit Netviewer one2one^{TS} effizienter. Speziell bei weltweit agierenden Unternehmen, die Vor-Ort-Support anbieten müssen, kommen eingesparte Reise- und Zeitkosten als weitere Vorteile hinzu. So kann beispielsweise die zentrale IT-Abteilung eines Automobilherstellers auch in weit entfernten Werken schnelle Hilfe leisten. Der Maschinenbauer wiederum kann seine Anlage beim Kunden auf der anderen Seite des Globus warten, Einstellungen verändern oder zumindest eine Vordiagnose stellen, die die Reparatur vor Ort erleichtert.

Vertrieb

Ein weiteres wichtiges Einsatzgebiet von Netviewer one2one^{TS} ist der Vertrieb. Im persönlichen Vertriebsgespräch mit potenziellen Kunden können Berater auf dieselbe Weise Ihre Software individuell präsentieren oder interaktive Software-Schulungen für kleine Gruppen abhalten. Ebenso können Berater Produkte, die sich per Software präsentieren lassen (z. B. Finanzprodukte oder Versicherungen), mittels Netviewer one2one^{TS}, dem Kunden näherbringen.

2.6.2 Sitzungsaufbau aus Anwendersicht

Der Berater startet das Netviewer one2one^{TS} Beraterprogramm. Er muss sich im Login-Dialog mit seinem Benutzernamen und seinem Passwort authentifizieren. Der Berater kann daraufhin in einem weiteren Dialog die Sitzung initiieren. Auf dem Beraterbildschirm erscheint nun das Netviewer Control Panel und das Mini-Panel, welches die Sitzungsnummer anzeigt.

Der Berater übermittelt nun auf einem sicheren Weg die Sitzungsnummer an den Teilnehmer. Die Sitzungsnummer dient zur Authentifizierung des Teilnehmers. Der Berater darf die Sitzungsnummer nur der Person übermitteln, mit der er die Sitzung durchführen möchten. Das Netviewer one2one^{TS}-System schaltet den Teilnehmer, der eine Sitzungsnummer in das Teilnehmerprogramm eingibt, mit dem Berater zusammen, dessen Beraterprogramm ebendiese Sitzungsnummer angezeigt hat. Daher ist der Berater dafür verantwortlich, die Identität des Sitzungsteilnehmers, der die Sitzungsnummer erhält, festzustellen. Der Berater muss weiterhin gewährleisten, dass

die Sitzungsnummer auf einem sicheren Weg übertragen wird. Bei der Übertragung per E-Mail ist es notwendig, die E-Mails verschlüsselt zu versenden. Die Möglichkeiten zur Verschlüsselung können der Hilfe des E-Mail-Programms entnommen werden. In den in Kapitel 2.6.1 beschriebenen Einsatzszenarien sind Berater und Teilnehmer bereits in einem Telefonat über das Festnetz, so dass die Sitzungsnummer auch über diesen Weg übermittelt werden kann.

Der Teilnehmer startet nun das Teilnehmerprogramm, das er vom Berater erhalten hat, und gibt in einem Dialog die vom Berater übermittelte Sitzungsnummer ein. Nach der Bestätigung der Eingabe wird die Sitzung zwischen Berater und Teilnehmer hergestellt.

Spezielle Funktionen des Beraterprogramms

Das Beraterprogramm kann nur genutzt werden, wenn eine gültige Kombination aus Benutzername und Passwort eingegeben wird.

Das Beraterprogramm verfügt über administrative Funktionalitäten, die ihn bereits vor dem Starten einer one2one^{TS}-Sitzung bei der Organisation und der Durchführung von Sitzungen unterstützen:

- Sitzungsplaner: one2one^{TS}-Sitzungen mit Thema, Datum, Profil etc. planen und vor Sitzungsbeginn über den Standard-E-Mail-Client (z.B. Microsoft Outlook) Einladungen versenden. Im Sitzungsplaner kann der Berater weiterhin ein Sitzungspasswort definieren, welches der Teilnehmer beim Eintritt in die Sitzung zusätzlich zur Sitzungsnummer eingeben muss. Das Sitzungspasswort stellt keine Sicherheitsfunktion dar, da es nur bei geplanten one2one^{TS}-Sitzungen angewandt werden kann.
- Profilmanager: Sitzungsprofile anlegen, um das one2one^{TS} Berater- und Teilnehmerprogramm auf individuelle Bedürfnisse anzupassen.

Spezielle Funktionen des Teilnehmerprogramms

Das Teilnehmerprogramm kann an beliebig viele Anwender verteilt werden, z.B. indem es auf einer Webseite zum Download angeboten oder den Anwendern per E-Mail zugesandt wird.

Beim Starten des Teilnehmerprogramms ist keine Authentifizierung mit Benutzername und Passwort notwendig. Der Anwender des Teilnehmerprogramms authentifiziert sich durch die Eingabe der Sitzungsnummer (und ggf. des Sitzungspassworts), die er vom Berater erhält und mit welcher er in eine Sitzung eintreten kann. Das Initiieren einer one2one^{TS}-Sitzung ist mit dem Teilnehmerprogramm nicht möglich.

Im Folgenden wird kurz auf die Benutzeroberfläche und die Funktionen, die den Anwendern während der Sitzung zur Verfügung stehen, eingegangen.

2.6.3 Benutzeroberfläche

Die grafische Benutzeroberfläche von Netviewer one2one^{TS} nach dem Sitzungsstart ist bei Berater und Teilnehmer während einer bestehenden Sitzung unterschiedlich.

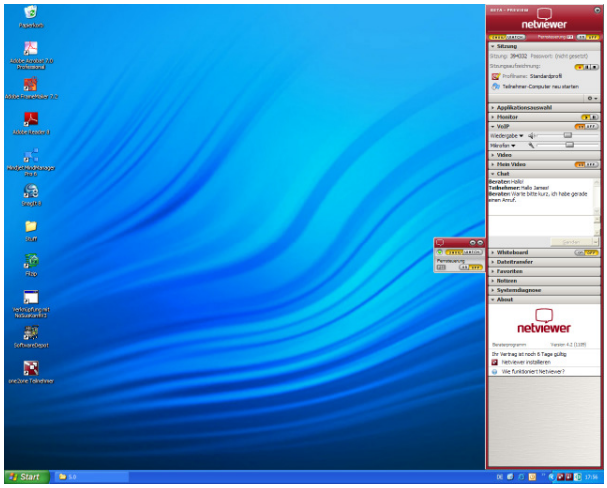

Abbildung 2: Bildschirmansicht beim Sitzungsstart beim Berater

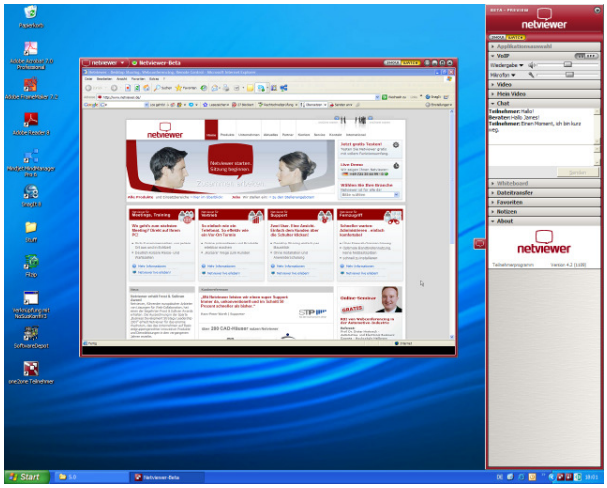

Abbildung 3: Bildschirmansicht beim Sitzungsstart beim Teilnehmer

Auf beiden Seiten ist das Netviewer Control Panel, ein seitlich am Bildschirmrand angedocktes Bedienfeld sichtbar. Es bietet Zugriff auf verschiedene Funktionen wie Applikationsauswahl, Dateitransfer etc. Der Anwender, der seinen Bildschirm zeigt, verfügt außerdem über das Mini-Panel, ein zusätzliches Bedienfeld mit zentralen Steuerungsfunktionen. Auf der Gegenseite ist das Netviewer-Fenster sichtbar, welches den übertragenen Bildschirminhalt des Sitzungspartners darstellt.

Abbildung 4: Das Netviewer one2one^{TS} Control Panel auf Beraterseite (im Show-Modus)

2.6.4 Funktionen

Die grafische Benutzeroberfläche bietet den Anwendern die Nutzung folgender Grundfunktionen während einer Sitzung:

Desktop-Sharing mit Blickrichtungswechsel

Die Bildschirmansicht eines Anwenders wird auf einen entfernten Computer übertragen, d.h. der Anwender befindet sich im so genannten Show-Modus (Zeigemodus). Der Sitzungspartner befindet sich im so genannten Watch-Modus (Betrachtermodus).

Die Blickrichtung (oder auch: Übertragungsrichtung) kann durch Benutzereingaben während der Sitzung jederzeit durch den Berater oder den Teilnehmer geändert werden, d.h. der Anwender im Show-Modus wechselt in den Watch-Modus und der Anwender im Watch-Modus wechselt in den Show-Modus.

Bevor der Bildschirm eines Anwenders an den Sitzungspartner übertragen wird und dieser Einsicht in geöffnete Dokumente und Anwendungen erhält, muss er der Übertragung in einem Bestätigungsdialog zustimmen.

Fernsteuerung

Befindet sich ein Anwender im Watch-Modus und betrachtet den Bildschirm des Sitzungspartners, kann der Sitzungspartner ihm die Fernsteuerung erteilen. Der Berater ist außerdem imstande, beim Teilnehmer die Fernsteuerung anzufordern.

Mithilfe der Fernsteuerung kann der Anwender Maus und Tastatur des Sitzungspartners steuern. Fernsteuernder und Ferngesteuerter haben gleichberechtigten Zugriff auf die Eingabegeräte.

Die Bedienlogik von Netviewer one2one gewährleistet, dass der Anwender im Watch-Modus sich nicht eigenmächtig das Fernsteuerungsrecht erteilen kann, sondern dies nur mit Zustimmung des Ferngesteuerten geschehen kann. Beim Anfordern der Fernsteuerung durch den Berater erscheint beim Teilnehmer ein Abfragedialog, bevor die Fernsteuerung freigegeben wird.

Der Entzug des Fernsteuerungsrechts ist jederzeit durch den Ferngesteuerten möglich durch Drücken der Taste F11.

Applikationsauswahl

Die Bildschirmübertragung und die Fernsteuerung sind beschränkt auf Anwendungen und Bildschirmelemente, die der Anwender im Show-Modus für diesen Zweck freigegeben hat. Nicht übertragene Anwendungen sind beim Sitzungspartner geschwärzt und per Fernsteuerung nicht bedienbar.

Weitere Funktionen

Die folgenden Funktionen stehen nur dem Berater zur Verfügung.

- Systemdiagnose: Mit Zustimmung des Teilnehmers kann der Berater Informationen über das System des Teilnehmers anfordern und einsehen.

Die folgenden Funktionen stehen beiden Sitzungspartnern zur Verfügung, sind jedoch zum Teil abhängig von der Blickrichtung (d.h. ob das jeweilige Clientprogramm im Show- oder Watch-Modus betreiben wird).

- Zeigepfeil: Ohne Fernsteuerung nutzbares Zeigeinstrument für den Anwender im Watch-Modus. Der Zeigepfeil ermöglicht keinerlei Manipulation des Computers des Sitzungspartners.

- Vorschau-Monitor: Eine verkleinerte Darstellung des eigenen Bildschirms erlaubt dem Anwender im Show-Modus zu prüfen, welche Anwendungen und Bildschirmelemente des eigenen Bildschirms im Netviewer-Fenster des Sitzungspartners sichtbar sind.
- Auswahl des Übertragungsmodus: Der Übertragungsmodus beeinflusst, in welcher Farbtiefe der übertragene Bildschirm beim Sitzungspartner im Watch-Modus dargestellt wird. Der Übertragungsmodus hat damit Einfluss auf die Übertragungsgeschwindigkeit und die Übertragungsqualität.
- VoIP: Die integrierte Sprachübertragung per Voice over IP kann von beiden Sitzungspartnern separat aktiviert und deaktiviert werden. Sie ersetzt das Telefonat parallel zur one2one^{TS}-Sitzung. Voraussetzung ist ein angeschlossenes Headset.
- Video: Die Video- oder Bildübertragung in beide Richtungen kann von beiden Sitzungspartnern separat aktiviert und deaktiviert werden. Voraussetzung ist eine korrekt installierte und angeschlossene Webcam.
- Chat: Austausch von Textnachrichten zwischen den Sitzungspartnern.
- Dateitransfer: Austausch von Dateien zwischen den Sitzungspartnern. Netviewer bietet zwei verschiedene Verfahren:
    - Dateien können über eine Container-Funktion im Netviewer Control Panel von beiden Seiten hoch- und heruntergeladen werden.
    - Dateien können vom Anwender im Watch-Modus bei aktivierter Fernsteuerung per Drag & Drop aus dem Netviewer Fenster heraus- und ins Netviewer Fenster hineingezogen werden. Der Anwender im Show-Modus muss der Übertragung von Dateien auf seinen Computer und von seinem Computer weg explizit zustimmen.
- Whiteboard: Der Anwender im Show-Modus kann die Whiteboard-Funktion aktivieren, welche einen Screenshot des derzeitigen Bildschirms erstellt, in welchem beide Sitzungspartner zeichnen können.
- Favoriten: Favoriten im Netviewer Control Panel sind Verknüpfungen zu Dateien, um auf diese während einer Sitzung schnell zugreifen zu können. Die erstellten Verknüpfungen sind nur für den lokalen Anwender und nicht für den Sitzungspartner zugänglich.
- Notizen: In einem Bereich des Netviewer Control Panels können Notizen festgehalten werden.
- Zoom/Autoscroll/Vollbild: Verschiedene Einstellungen zum Anpassen der Darstellung des übertragenen Bildschirms im Netviewer-Fenster
- Aufzeichnungsfunktion: Zusatzfunktionalität, die Sitzungen als Mitschnitt (im Dateiformat .nvl) aufzeichnet. Die Sitzungsmitschnitte können mit dem Netviewer NetPlayer abgespielt werden.

2.6.5 Beenden der Sitzung

Eine one2one^{TS}-Sitzung kann zu jedem Zeitpunkt während der Sitzung durch den Berater oder den Teilnehmer beendet werden.

Wird eine Sitzung beendet, senden Berater- und Teilnehmerprogramm Sitzungsdaten (z.B. Sitzungsdauer, übertragene Bytes) zur Protokollierung an den Vermittlungsservice.

Ein Dialog signalisiert auf Berater- und auf Teilnehmerseite das Ende der Sitzung.

2.6.6 Informationsbereitstellung für die Anwender der Clientprogramme

Die Netviewer AG stellt auf ihrer Webseite eine Informationsseite mit zentralen und aktuellen Informationen zu Netviewer one2one^{TS} zur Verfügung. Der Hyperlink auf die Informationsseite ist im Netviewer one2one^{TS} Benutzerhandbuch und in den Clientprogrammen einfach zugänglich angegeben.

Die Webseite dient der Information der Anwender der Netviewer one2one^{TS} Clientprogramme und dem Administrator von Netviewer Standard Server^{TS}.

Die Informationsseite enthält unter anderem folgende Informationen:

- Netviewer one2one^{TS} Benutzerhandbuch
- Aktuelle Informationen über eventuell aufgetretene Sicherheitslücken

2.7 Serverkomponente Standard Server^{TS}

Die Serversoftware Netviewer Standard Server^{TS} unterstützt den Verbindungsaufbau zwischen dem Netviewer Berater- und Teilnehmerprogramm und die Kommunikation während der Sitzung. Netviewer Standard Server^{TS} wird als Bestandteil des EVG auf einem physikalischen Serverrechner betrieben, der über das Internet oder Intranet für die Clientprogramme erreichbar ist. Netviewer Standard Server^{TS} umfasst die Komponenten Vermittlungsservice und Kommunikationsservice.

2.7.1 Vermittlungsservice

Der Vermittlungsservice übernimmt den sicheren Verbindungsaufbau zwischen Berater- und Teilnehmerprogramm auf zwei entfernten Rechnern. Die dazu benötigten Signalisierungsinformationen (z.B. zur Authentifizierung, zum Schlüsselaustausch und zur Schlüsselaushandlung) werden zwischen den Clients und dem Vermittlungsservice über sichere Kanäle übertragen und vom Vermittlungsservice verarbeitet. Der Vermittlungsservice übergibt weiterhin die Adresse des Kommunikationsservices für die Sitzung an das Berater- sowie das Teilnehmerprogramm.

2.7.2 Kommunikationsservice

Der Kommunikationsservice transportiert den Ende-zu-Ende verschlüsselten Datenstrom zwischen Berater- und Teilnehmerprogramm während einer laufenden Sitzung (Sitzungsdatenstrom). Der Sitzungsdatenstrom umfasst die Daten, die während einer bestehenden Sitzung ausgetauscht werden (z.B. Bildschirmdaten, Daten von Eingabegeräten, Video- und Audiodaten). Die beiden Clients bauen jeweils aktiv eine Verbindung zum Kommunikationsservice auf.

Der Vermittlungsservice ist weder am Aufbau der Client-Verbindungen zum Kommunikationsservice noch am darauf folgenden Austausch des Sitzungsdatenstromes beteiligt. Vermittlungsservice und Kommunikationsservice sind logisch voneinander getrennt, so dass kein Datenaustausch zwischen den beiden Services erfolgt. Der Kommunikationsservice verfügt somit auch nicht über den Schlüssel, mit dem die ausgetauschten Sitzungsdaten verschlüsselt sind.

Die Verwendung des Kommunikationsservices ermöglicht es, Netviewer one2one auch in Systemumgebungen mit Firewalls, welche üblicherweise die direkte Kommunikation zwischen Berater- und Teilnehmerprogramm verhindern, zu nutzen.

Wird der EVG in einem Intranet betrieben, ist der Aufbau einer Peer-to-peer-Verbindung zwischen den beiden Clientprogrammen möglich. Nach dem Verbindungsaufbau über den Vermittlungsservice erfolgt dann die Kommunikation während der Sitzung ausschließlich direkt zwischen den Clients (s. Abschnitt 2.11.2).

2.7.3 Benutzermanager

Der Netviewer Benutzermanager ist eine Komponente von Netviewer Standard Server^{TS} und ermöglicht das Anlegen, Verwalten und Entfernen von Benutzern, die berechtigt zur Nutzung der Netviewer one2one^{TS} Clientprogramme sind.

Ausführliche Informationen zur Benutzerverwaltung sind im Kapitel 2.12 enthalten.

2.7.4 Hilfsdateien des Standard Servers

Der Standard Server enthält die Module Vermittlungsservice, Benutzermanager und Kommunikationsservice, welche Dateien im Dateisystem zum Betrieb benötigen. Diese Dateien sind:

- NVStandardServer_<Datum>_logfile.txt
  Logging des Kommunikationsservice. Nicht sicherheitsrelevant.
- NVStandardServer_<Datum>_auditlog.txt
  Audit-Log der sicherheitsrelevanten Aktionen betreffend Benutzermanager und Sitzungen

- NVStandardServer_<Datum>_SessionLog.csv
  Sitzungsprotokolle zur statistischen Auswertung. Nicht sicherheitsrelevant.
- NVStandardServer_<Datum>_VMServerLog.csv
  Logging des Vermittlungsservice. Nicht sicherheitsrelevant.
- ContractData.dat
  Vom Konfigurator (siehe Kapitel 2.13) erzeugte Datei mit clientseitigen Einstellungen. Integrität gesichert mit TSF (HMAC).
- ServerData.dat
  Vom Konfigurator (siehe Kapitel 2.13) erzeugte Datei mit serverseitigen Einstellungen. Integrität gesichert mit TSF (HMAC).
- NVServer_users.txt
  Benutzerdaten von Beratern (Benutzername/Passwort, Profile, ...). Wird vom Benutzermanager gepflegt. Vertraulichkeit der Passwörter ist per TSF gewährleistet.

2.8 Serverkomponente SSLswitch

2.8.1 Funktionsweise des SSLswitches

Serverseitig kommt die EVG-Komponente SSLswitch zum Einsatz, um HTTPS zwischen den Clientprogrammen und dem Vermittlungsservice zu ermöglichen. Der SSLswitch läuft auf demselben Rechner wie Netviewer Standard Server^{TS}. Wenn ein Clientprogramm per SSL Daten an den Server sendet, wickelt der SSLswitch das SSL-Handshake ab und leitet entschlüsselte Daten an den Vermittlungsservice weiter. Dessen unverschlüsselte Antworten werden vom SSLswitch verschlüsselt per SSL an den Client gesandt. Der SSLswitch ist also der serverseitige Endpunkt des SSL-Tunnel zwischen den Clientprogrammen und dem Standard Server.

Beim SSLswitch wird in der Datei SSLswitch.xml das zu verwendende Serverzertifikat angegeben (siehe Kapitel 2.8.2). Der SSLswitch implementiert das SSL-Protokoll nicht selbst, vielmehr werden Windows-Bibliotheken dazu verwendet. Die von den Windows-Bibliotheken verwendbaren SSL Cipher Suites werden vom Server-Adminstrator so konfiguriert, so dass die kryptographische Stärke immer mindestens 128 Bit entspricht. Anweisungen dazu finden sich im Administratorhandbuch.

2.8.2 SSL-ServerZertifikat

Da die Clientprogramme im Rahmen der Signalisierung vertrauliche Informationen (z.B. das Beraterpasswort) an den Vermittlungsservice senden, muss sichergestellt werden, dass der Vermittlungsservice auch derjenige Vermittlungsservice ist, an den die Clientprogramme die Information senden wollen. Die URL (welche den DNS-Namen

enthält) des Vermittlungsservice ist fest in die Clientprogramme einkompiliert. Um zu verhindern, dass Clientprogramme mit einem unbeteiligten Vermittlungsservice kommunizieren, oder einer Man-In-the-Middle-Attack zum Opfer fallen, wird die Identität (Domain-Name) des Vermittlungsservice per SSL-Serverauthentifizierung geprüft.

Für die SSL-Serverauthentifizierung ist ein geeignetes X.509-Zertifkat notwendig. Dieses kann nicht von der Netviewer AG ausgestellt oder beschafft werden. Der Kunde muss es selbst beschaffen, installieren und warten. Die Beantragung eines SSL-Zertifikates erfolgt über eine unternehmenseigene Zertifizierungsstelle (beim Kunden), oder über eine Stammzertifizierungsstelle eines Anbieters, welche von einer unabhängigen und vertrauenswürdigen dritten Partei, der "Certification Authority (CA)", unterzeichnet wird. Die "CA" verbürgt sich mit ihrer Unterschrift für die Richtigkeit der im Zertifikat enthaltenen Daten (Domain-Name, Kontaktdaten, usw).

Das SSL-Zertifikat wird im Zertifikatsspeicher der Windows-Instanz installiert, auf dem die Serverkomponenten laufen.

Der Wert des ‚Common Name' des Eintrags ‚Subject' im SSL-Serverzertifikat muss mit dem DNS-Namen des Serverrechners, auf dem die Serverkomponenten betrieben werden, übereinstimmen.

Weitere Informationen zur Beschaffung, Installation und Wartung des SSL-Server-Zertifikats ist für den Server-Administrator im Netviewer Standard Server^{TS} Administratorhandbuch verfügbar.

2.9 Übersicht über die verwendeten Netzwerkprotokolle

Da es sich bei Netviewer one2one^{TS} um eine Client-Server-Applikation handelt, verfügt der EVG über verschiedene Schnittstellen. Wie bei Netzwerkprotokollstapeln üblich, ist die real genutzte Schnittstelle einer Schicht-N Protokollimplementierung die API der Schicht N-1. Es ergibt sich jedoch eine logische Verbindung und damit eine Schnittstelle zwischen zwei Schicht-N-Instanzen. Im Falle von Netviewer one2one^{TS} sind dies auf den unterschiedlichen Netzwerkebenen die folgenden Protokolle:

1. Protokoll für die **Signalisierung** zwischen den Clientprogrammen und dem Vermittlungsservice, welches aus Remote Procedure Calls (RPCs) besteht
2. **HttpsRpc** als sicheres Protokoll für die Signalisierung von den Clientprogrammen zum Vermittlungsservice (siehe Kapitel 2.10.1)
3. **PingPong**. Protokoll für den Sitzungsdatenstrom zwischen Beraterprogramm und Teilnehmerprogramm
4. **PingPongTransport (PPT)** für den Transport von PingPong-PDUs (ggf. über den Kommunikationsservice)
5. **HTTP** als Transport-/Darstellungsprotokoll für HttpsRpc und PingPongTransport
6. **SSL** als Sicherungsprotokoll für HttpsRpc

7. **TCP** als Transportprotokoll für SSL, HTTP und PingPongTransport

Dabei bilden 1. bis 4. die Schnittstelle der Komponenten untereinander. Die Protokolle 5. bis 7. (HTTP, SSL und TCP) werden von Windows-Bibliotheken zur Verfügung gestellt, die keine EVG-Bestandteile sind.

2.9.1 Protokollstapel

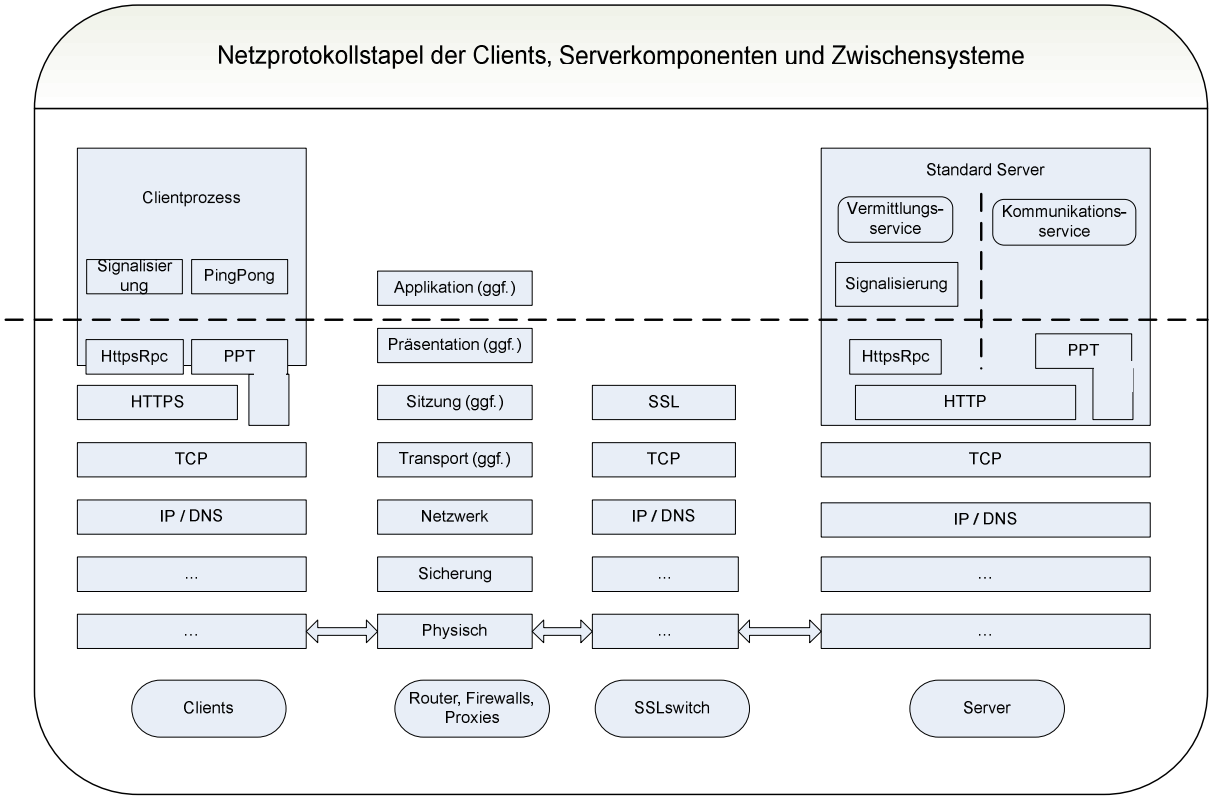

Abbildung 5: Protokollstapel bei Netviewer one2one^{TS}

Auf Applikationsebene (oberhalb der gestrichelten Linie) befinden sich Signalisierung und PingPong. In der Abbildung ist zu sehen, dass PingPong im Server nicht vorhanden ist, da dieses Protokoll ausschließlich zwischen Beraterprogramm und Teilnehmerprogramm zum Einsatz kommt, um den Sitzungsdatenstrom auszutauschen. PingPong-PDUs (Protocol Data Unit) werden zwischen den Clients über das PingPongTransport-Protokoll (PPT) über den Kommunikationsservice ausgetauscht. Das HTTP-Protokoll ist im Server selbst implementiert; clientseitig wird dies von einer Windows-Bibliothek übernommen. PingPongTransport kann sowohl auf TCP als auch auf HTTP aufsetzen. Signalisierung wird ausschließlich über das HttpRpc-Protokoll abgewickelt, welches auf HTTPS aufsetzt. Bei HttpsRpc sind Integrität, Vertraulichkeit und Authentizität der ausgetauschten PDUs

sichergestellt (durch SSL). Ebenso sind bei PingPong Integrität, Vertraulichkeit und Authentizität der ausgetauschten PDUs sichergestellt (durch Sicherheitsfunktionen in der PPT-Implementierung). Die dazu benötigten symmetrischen Schlüssel werden per Signalisierung vertraulich, integer und authentisch ausgetauscht.

2.9.2 Sicherungsmechanismen der Netzwerkprotokolle

Übersicht der Sicherungsmechanismen für die einzelnen Protokolle:

Protokoll	Integrität	Vertraulichkeit	Authentizität	TSF?
Signalisierung	-	-	Passwörter	ja
HttpsRpc	HMAC-SHA1-96 + SSL	SSL	HMAC-SHA1-96 + SSL	ja
PingPong	HMAC-SHA1-96	Blowfish/CBC oder AES/CBC	HMAC-SHA1-96	ja
PingPong-Transport	HMAC-SHA1-96	-	HMAC-SHA1-96	ja
SSL	verschiedene (konfigurierbar)	verschiedene (konfigurierbar)	verschiedene (konfigurierbar)	teilweise
http	-	-	-	nein
TCP	-	-	-	nein

Tabelle 2: Sicherungsmechanismen der verwendeten Netzwerkprotokolle

Die Protokolle und Protokollimplementierungen SSL, HTTP und TCP sind keine Bestandteile des EVG.

2.10 Client-Server-Kommunikation beim Verbindungsaufbau

Vermittlungsservice und Kommunikationsservice setzen aufgrund ihrer unterschiedlichen Aufgaben verschiedene Protokolle ein.

2.10.1 Das Protokoll HttpsRpc

Zur Kommunikation zwischen den Clientprogrammen und dem Vermittlungsservice wird das proprietäre Protokoll HttpsRpc auf Port 443 verwendet (setzt auf HTTP/1.1 über SSL auf). HttpsRpc etabliert einen sicheren Kanal, über welchen die integre, vertrauliche und authentische Übermittlung des Signalisierungsdatenstroms erfolgt.

Der Standard Server authentifiziert sich gegenüber einem Clientprogramm per SSL-Serverzertifikat. Das SSL-Protokoll wird serverseitig von der Serverkomponente SSLswitch unter Benutzung von Windows-Bibliotheken implementiert; clientseitig kommt die in Windows vorinstallierte Bibliothek WinInet.DLL zum Einsatz.

Ein Clientprogramm authentifiziert sich beim Server, indem es die Kenntnis eines fest eingebundenen Geheimnisses (Programmschlüssel) nachweist[1]. Dazu wird bei HttpsRpc zu Beginn eine Challenge-Response-Phase durchlaufen, in der mit der Server-Challenge (eine Pseudozufallszahl, generiert von einer Windows-Bibliothek außerhalb des EVGs) und dem beiderseitig bekannten Programmschlüssel Hashwerte gebildet werden. Der Programmschlüssel befindet sich serverseitig in der Datei ContractData.dat; clientseitig ist er fest eingebunden. Nach erfolgreich abgeschlossener Challenge-Response-Phase ist es dem Clientprogramm möglich, Requests (Signalisierungsanfragen, siehe Kapitel Ablauf der Signalisierung) an den Server zu stellen. Diese Requests (und die dazugehörigen Server-Responses) werden mit einem HMAC gesichert, um Integrität und Authentizität zu gewährleisten.

2.10.2 Ablauf der Signalisierung

Signalisierung wird mittels Remote Procedure Calls durchgeführt, welche per HttpsRpc transportiert werden. Signalisierung findet ausschließlich zwischen einem Clientprogramm und dem Vermittlungsservice statt. Die Argumente und Rückgabewerte werden serialisiert und per HTTPS zum Vermittlungsservice gesendet bzw. von diesem empfangen.

Die folgende Grafik zeigt den Ablauf des Sitzungsaufbaus einschließlich der Signalisierung:

[1] Die Asymmetrie ist darin begründet, dass auf Clientseite nicht die Möglichkeit besteht, ein SSL-Zertifikat zur Clientauthentifizierung zu installieren.

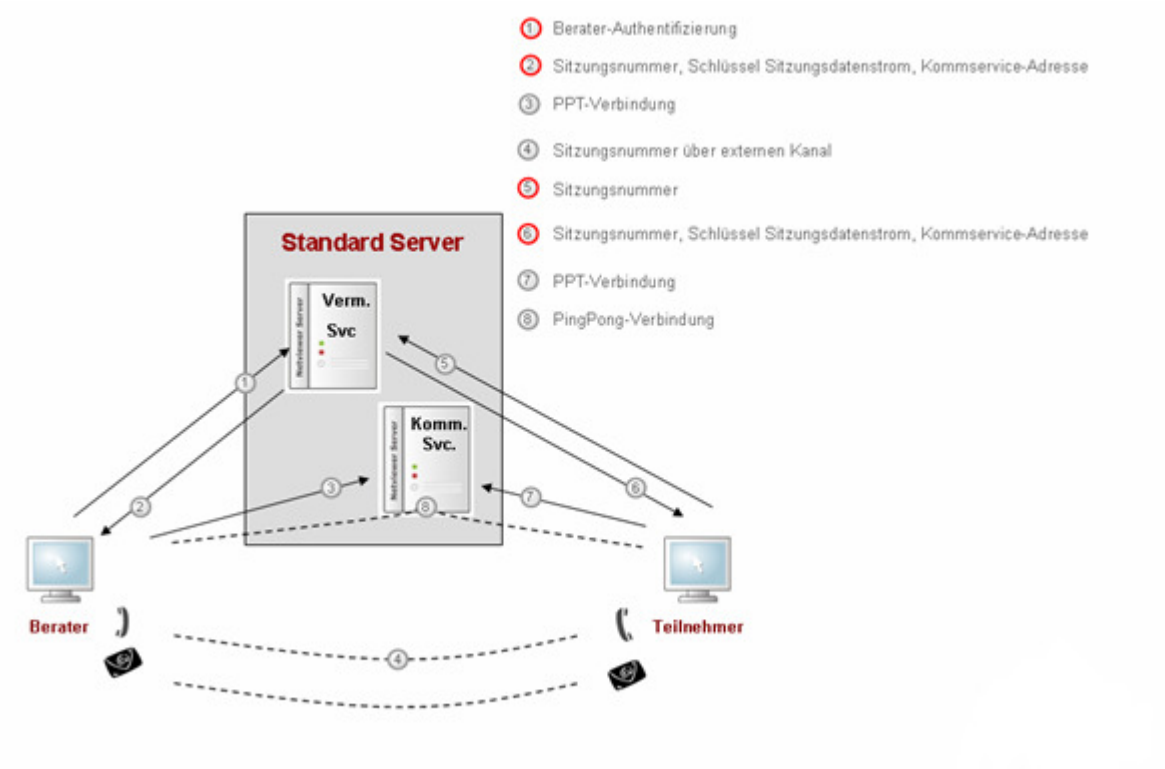

Abbildung 6: Signalisierung zwischen Clientprogrammen und Serverkomponenten beim Sitzungsaufbau

In obiger Abbildung sind die Schritte zur Signalisierung rot hervorgehoben.

Nach dem Aufbau des sicheren Kanals durch HttpsRpc übermittelt das Beraterprogramm die vom Berater eingegebenen Login-Daten an den Vermittlungsservice.

Der Vermittlungsservice generiert nach erfolgreicher Prüfung der Login-Daten die neunstellige Sitzungsnummer, einen symmetrischen Schlüssel zur Verschlüsselung des Sitzungsdatenstroms und einen Schlüssel zur Integritätssicherung des Sitzungsdatenstroms. Der Vermittlungsservice übermittelt die Sitzungsnummer, die Schlüssel zur späteren Sicherung des Sitzungsdatenstromes und die Adresse des Kommunikationsservices (DNS-Name/Port) zurück an das Beraterprogramm. Die Sitzungsnummer (und das Sitzungspasswort, falls dieses im Sitzungsplaner definiert wurde) wird dem Berater in der grafischen Benutzeroberfläche angezeigt.

Das Beraterprogramm wartet nun darauf, dass das Teilnehmerprogramm in die Sitzung eintritt und die Ende-zu-Ende verschlüsselte Verbindung für den Sitzungsdatenstrom zum Teilnehmerprogramm aufgebaut werden kann (Verbindung im PingPong-Protokoll).

Der Teilnehmer gibt die Sitzungsnummer (und ggf. das Sitzungspasswort) im gestarteten Teilnehmerprogramm ein. Das Teilnehmerprogramm übermittelt die Sitzungsnummer

(und ggf. das Sitzungspasswort) innerhalb einer Signalisierungsanfrage an den Vermittlungsservice und führt damit die Authentifizierung des Teilnehmers durch.

Anhand der übermittelten Sitzungsnummer identifiziert der Vermittlungsservice das zu der entsprechenden Sitzung wartende Beraterprogramm. Der Vermittlungsservice übermittelt dem Teilnehmerprogramm nun über den sicheren HttpsRpc-Kanal die Adresse des Kommunikationsservices, an dem das Beraterprogramm angemeldet ist, und das Schlüsselmaterial zur Sicherung des Sitzungsdatenstroms.

Das Teilnehmerprogramm meldet sich nun beim Kommunikationsservice an, welcher Berater- und Teilnehmerprogramm den Datenaustausch ermöglicht.

2.11 Kommunikation zum Austausch des Sitzungsdatenstroms

Die Kommunikation zwischen Beraterprogramm und Teilnehmerprogramm während einer laufenden Sitzung (Sitzungsdatenstrom) kann über zwei Modi erfolgen:

- Indirekte Kommunikation zwischen Berater- und Teilnehmerprogramm über den Kommunikationsservice
- Direkte Peer-to-peer-Kommunikation zwischen Berater- und Teilnehmerprogramm ohne zwischengeschalteten Server

Entscheidend für die Auswahl der Variante ist die Netzwerktopologie, innerhalb derer das Berater- und das Teilnehmerprogramm betrieben werden.

Für die Anwender des Berater- und des Teilnehmerprogramms erfolgt die Auswahl des Modus unbemerkt. Die folgenden beiden Unterkapitel erläutern die beiden unterschiedlichen Kommunikationsmodi.

Zur Kommunikation zwischen Beraterprogramm und Teilnehmerprogramm während einer laufenden Sitzung (Sitzungsdatenstrom) kommen zwei verschiedene Protokolle zum Einsatz: Das PPT-Protokoll und das darauf aufsetzende setzt das PingPong-Protokoll (siehe Abbildung Protokollstapel in Kapitel 2.9.1). Der wesentliche Unterschied ist: PingPong transportiert den Sitzungsdatenstrom zwischen Beraterprogramm und Teilnehmerprogramm; PPT transportiert PingPong *entweder* zwischen einem Clientprogramm und dem Kommunikationsservice *oder* direkt zwischen Beraterprogramm und Teilnehmerprogramm (Peer-to-peer-Modus). Im ersten Fall werden vom Kommunikationsservice genau zwei PPT-Verbindungen miteinander verbunden; im Peer-To-Peer-Modus existiert genau eine PPT-Verbindung. In beiden Fällen existiert genau eine PingPong-Verbindung.

2.11.1 Kommunikation über den Kommunikationsservice

Die Übermittlung des Sitzungsdatenstroms erfolgt über den Kommunikationsservice, falls ein direkter TCP-Verbindungsaufbau zwischen Berater- und das Teilnehmerprogramm (Peer-to-peer) nicht möglich ist. Dies kann z.B. folgende Gründe haben:

- Die Client-Komponenten befinden sich nicht im selben Intranet und können daher nur über das Internet eine Verbindung aufbauen.
- Die Client-Komponenten befinden sich im selben Intranet, die benötigten Ports für die direkte Verbindung sind jedoch gesperrt.

Das Teilnehmerprogramm sendet verschlüsselt das erste PPT-Datenpaket an den Kommunikationsservice, der dieses an das Beraterprogramm weiterleitet. Die verschlüsselte Verbindung zwischen Berater und Teilnehmer ist daraufhin aufgebaut. Daten können nun in beide Richtungen verschlüsselt über den Kommunikationsservice ausgetauscht werden.

Das Berater- und das Teilnehmerprogramm senden die auszutauschenden Daten als Anfrage an den Kommunikationsservice. Als Antwort gibt der Server die Daten mit, die der jeweils andere Client in seiner Anfrage geschickt hat. Auf diese Weise gelingt ein indirekter Datenaustausch.

Der Kommunikationsservice leitet die Datenpakete zwischen dem Berater- und Teilnehmerprogramm ausschließlich weiter. Aufgrund der Ende-zu-Ende-Verschlüsselung ist der Kommunikationsservice nicht in der Lage, die verschlüsselten Datenpakete zu lesen, da er nicht über den notwendigen Schlüssel verfügt.

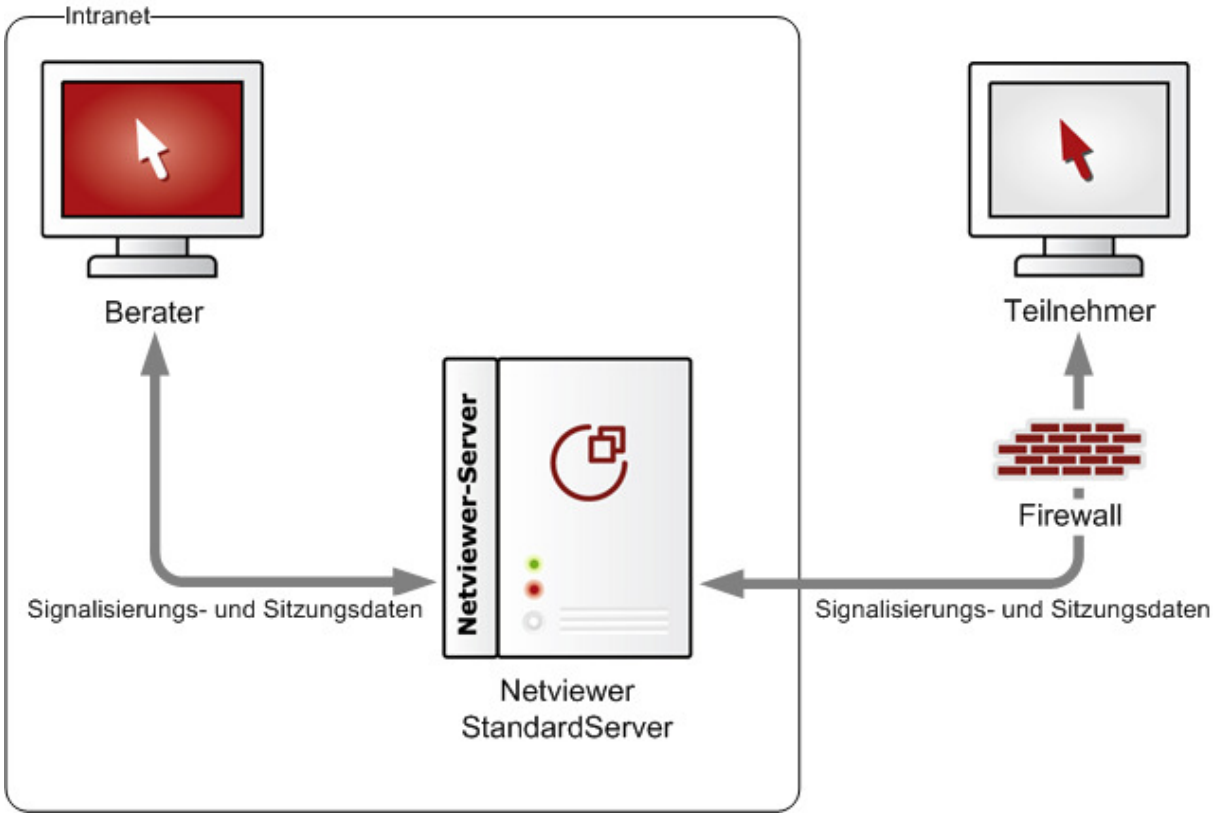

Abbildung 7: Kommunikation zwischen den EVG-Komponenten über den Kommunikationsservice (in der Abbildung Netviewer Server)

2.11.2 Kommunikation über eine Peer-to-peer-Verbindung

Voraussetzung für eine Peer-to-peer-Verbindung ist, dass das Berater- und das Teilnehmerprogramm innerhalb des gleichen Intranets betrieben werden. Auf dem System, auf dem das Beraterprogramm verwendet wird, können weiterhin die benötigten Ports geöffnet werden.

In diesem Fall kann der Austausch des Sitzungsdatenstroms über eine direkte Peer-to-peer-Verbindung erfolgen. Nach der Vermittlung der Verbindung zwischen Berater- und Teilnehmerprogramm, versucht das Teilnehmerprogramm eine TCP-Verbindung zum Beraterprogramm aufzubauen. Falls dies netzwerktopologisch möglich ist, wird auf die Nutzung eines Kommunikationsservices verzichtet und die direkte Verbindung (Peer-to-peer) verwendet. Verringerte Latenzzeiten und höhere Bandbreiten können die Sitzungsperformance erheblich steigern.

2.11.3 Sicherung des Sitzungsdatenstromes

Unabhängig davon, ob der Sitzungsdatenstrom zwischen Beraterprogramm und Teilnehmerprogramm über eine direkte TCP-Verbindung ausgetauscht wird oder über den Kommunikationsservice wird die Integrität, Authentizität und Vertraulichkeit des Sitzungsdatenstromes vom EVG gesichert.

In der Konfiguration des EVG kann eingestellt werden, welcher Algorithmus und welche Schlüssellänge verwendet werden soll. Die Clientprogramme unterstützen im Code verschiedene Verfahren und Schlüssellängen. Die zu benutzende Kombination erfahren die Clients vom Server im Rahmen der Signalisierung. Die zur Auswahl stehenden kryptographischen Algorithmen sind AES CBC und Blowfish CBC. Die Schlüssellänge beträgt mindestens 128 Bit.

2.11.4 Zusammenspiel der EVG-Komponenten

Im folgenden wird dargestellt, wie die EVG-Komponenten zusammenspielen, um Netviewer one2one^{TS} Sitzungen zwischen Beratern und Teilnehmern zu ermöglichen. Es wird eingegangen auf die Abläufe, die Protokolle und die jeweils verwendeten Dateien.

Die folgende Grafik gibt einen Überblick:

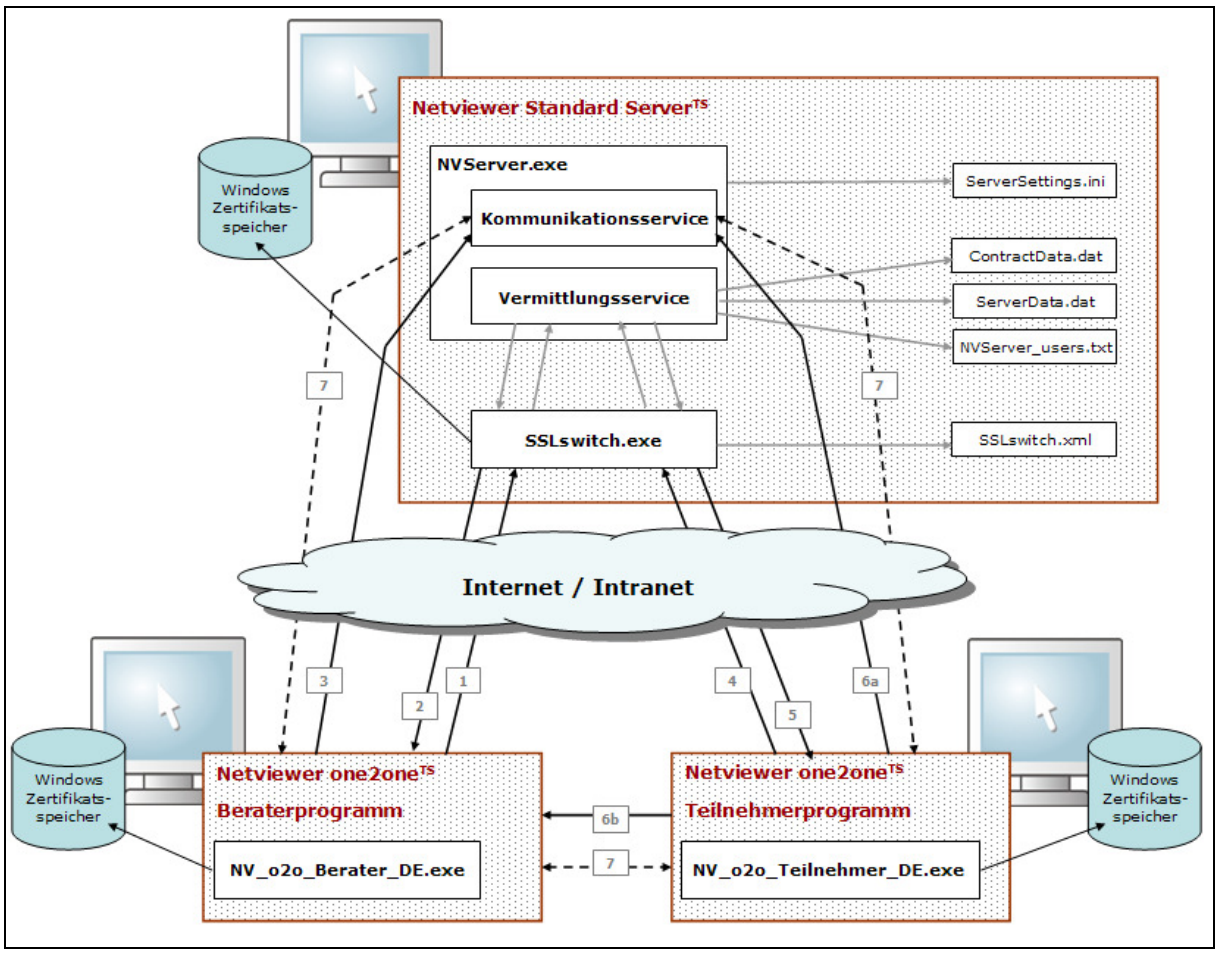

Abbildung 8: Zusammenspiel der EVG-Komponenten

Die in der Grafik nummerierten Schritte werden im folgenden erläutert und untergliedert:

1. Das Beraterprogramm sendet die Sitzungsanforderung und die Authentifizierungsdaten des Beraters an den Vermittlungsservice

   1.1. Das Clientprogramm initiiert eine HttpsRpc-Anfrage an die fest eingebundene Vermittlungsservice-URL des Netviewer Servers.

   1.2. Die HttpsRpc-Client-Implementierung kodiert die Anfrage und initiiert eine HTTPS-Anfrage über WinInet.DLL.

   1.3. Der SSLswitch nimmt die SSL-Verbindung entgegen und führt das SSL-Handshake durch. Um sich zu authentifizieren, entnimmt der SSLswitch dem Windows-Zertifikatsspeicher des Rechners, auf dem der Standard Server läuft, das SSL-Serverzertifikat. Die WinInet.DLL des Clientprogramms prüft die Gültigkeit des Zertifikats.

   1.4. Bei Erfolg nimmt der SSLswitch die HttpsRpc-Anfrage entgegen und leitet sie unverschlüsselt an den Vermittlungsservice.

1.5. Die HttpsRpc-Server-Implementierung entnimmt den Programmschlüssel der Datei ContractData.dat und prüft damit die Integrität und Authentizität der Anfragen.

1.6. Der Vermittlungsservice prüft die Authentifizierungsdaten gegen die Benutzerdatei (NVServer_users.txt). Der Vermittlungsservice prüft die Lizenzierung des Beraterprogramms (ContractData.dat). Der Vermittlungsservice generiert über einen Pseudozufallszahlengenerator aus einer Windows-Bibliothek eine neunstellige Sitzungsnummer

2. Der Vermittlungsservice sendet einen HttpsRPC-Aufruf mit der Sitzungsnummer, der Adresse des Kommunikationsservice (DNS-Name und Port konfiguriert in ServerData.dat), die symmetrischen Schlüssel zur Verschlüsselung und Integritätssicherung des Sitzungsdatenstroms und die PPT-Paarungsnummer (jeweils Pseudozufallszahlengenerator) an den SSLswitch. Der SSLswitch sendet diese HttpsRpc-Antwort verschlüsselt weiter an das Beraterprogramm. Das Beraterprogramm zeigt die Sitzungsnummer in der Benutzeroberfläche an

3. Das Beraterprogramm verbindet sich mit dem Kommunikationsservice

   3.7. Das Beraterprogramm sendet über das HttpsRpc-Protokoll eine PPT-Paarungsnummer an den Kommunikationsservice

   3.8. Das Beraterprogramm sendet über das PPT-Protokoll (PingPongTransport-Protokoll) Aufrufe an den Kommunikationsservice.

   3.9. Da das Teilnehmerprogramm noch keine PPT-Verbindung zum Kommunikationsservice hat, werden diese Aufrufe mit einer Wiederholungsbitte beantwortet.

   3.10. Der Berater übermittelt die Sitzungsnummer auf einem sicheren externen Kanal an den Teilnehmer. Der Teilnehmer startet das Teilnehmerprogramm. Der Teilnehmer gibt im Teilnehmerprogramm die Sitzungsnummer ein.

4. Das Teilnehmerprogramm sendet die Sitzungsnummer über HttpsRpc an den Vermittlungsservice

   4.11. wie 1.1

   4.12. wie 1.2

   4.13. wie 1.3

   4.14. wie 1.4

   4.15. wie 1.5

5. Der Vermittlungsservice prüft die Sitzungsnummer (Existenz, Sperre, ...) und liefert bei Erfolg in seiner Antwort die selben Daten, wie sie das Beraterprogramm in Schritt 2. erhalten hat (Sitzungsnummer, Adresse des Kommunikationsservice, symmetrische Schlüssel zur Verschlüsselung und Integritätssicherung des

Sitzungsdatenstroms und die PPT-Paarungsnummer). Der Vermittlungsservice zerstört seine Kopie der Schlüssel und sperrt die Sitzung(snummer).

6. Das Teilnehmerprogramm sendet über das PPT-Protokoll (6a) einen Aufruf an den Kommunikationsservice und gleichzeitig direkt an das Beraterprogramm (6b).
7. Etablieren der PingPong-Verbindung

   7.16. Kann eine direkte Peer-to-peer-Verbindung zwischen Berater- und Teilnehmerprogramm aufgebaut werden, wird diese zur Übermittlung der Sitzungsdaten über das PingPong-Protokoll verwendet.

   7.17. Ist dies aufgrund der Netzwerkumgebung nicht möglich, vermittelt der Kommunikationsservice die Daten der beiden PPT-Verbindungen anhand der PPT-Paarungsnummer.

   7.18. Damit ist die PingPong-Verbindung zwischen Beraterprogramm und Teilnehmerprogramm etabliert. Diese wird mit den Schlüsseln aus Schritt 2. bzw. 5. gesichert bzgl. Vertraulichkeit, Integrität und Authentizität.

2.12 Benutzerverwaltung

Der Benutzermanager ist eine Komponente des Netviewer Standard Server^{TS} und ermöglicht dem Berater-Administrator das Anlegen, Verwalten und Entfernen von Benutzern, die zur Benutzung des Netviewer one2one^{TS} Beraterprogramms berechtigt sind. Den Benutzern können verschiedene Rechte in Netviewer one2one^{TS} zugewiesen werden.

Der Benutzermanager kann nur auf dem Serverrechner, auf dem der Standard Server^{TS} läuft, verwendet werden. Beim Starten des Benutzermanagers muss sich der Berater-Administrator mit seinem Benutzernamen und seinem Passwort authentifizieren.

Die Informationen, die im Benutzermanager bearbeitet werden können, werden vom Standard Server in der Benutzerdatei NVServer_users.txt gespeichert. Passwörter werden nicht im Klartext in der Benutzerdatei abgelegt, sondern nur deren Hashwert (RIPEMD_256). So können die Passwörter vom Vermittlungsservice auf Gültigkeit geprüft werden, ohne im Klartext lesbar zu sein (vom Server-Administrator oder einem Einbrecher).

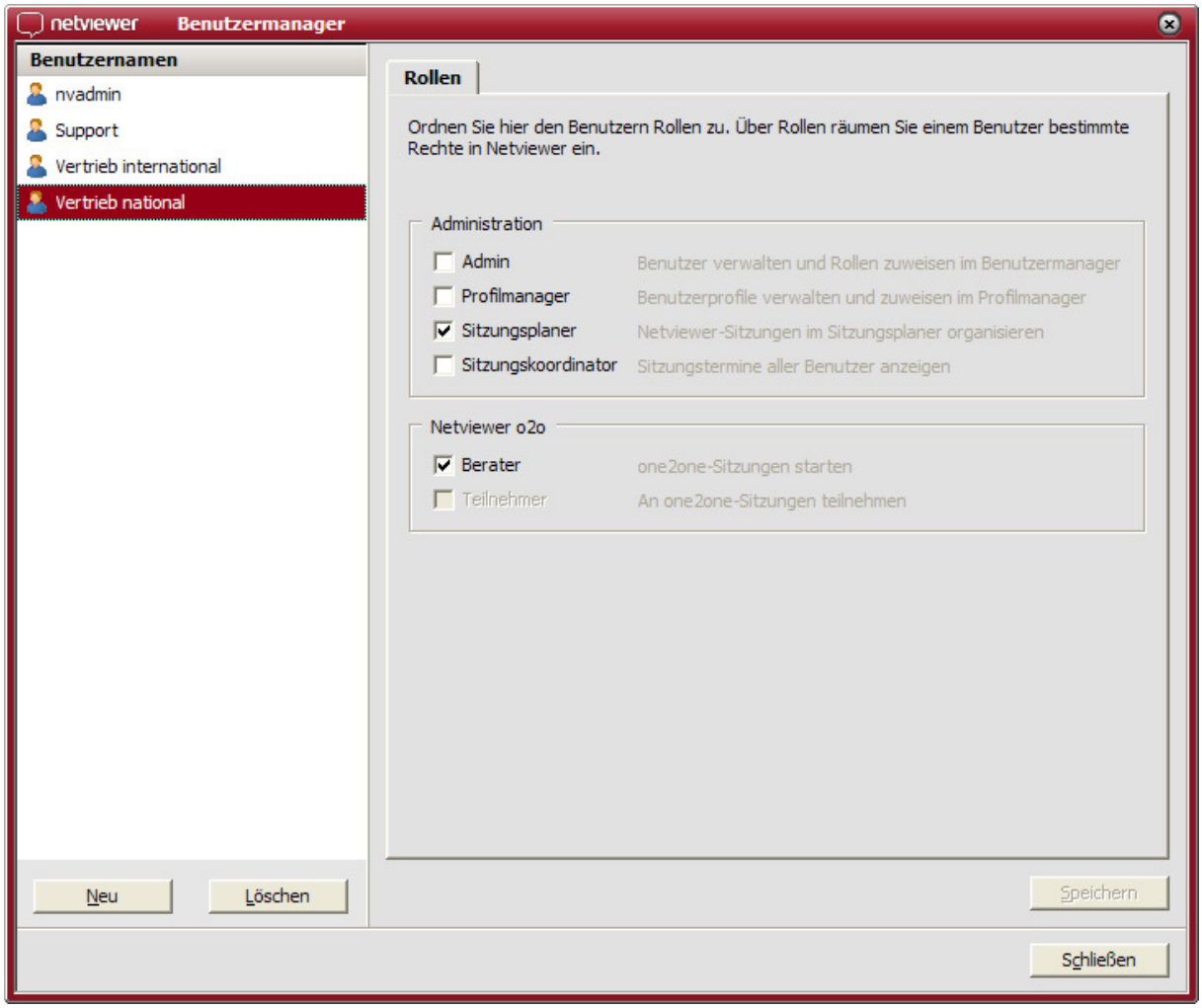

Abbildung 9: Beispielhafte Ansicht des Benutzermanagers

2.12.1 Initialer Berater-Administrator

Bei der Erstellung des EVGs durch die Netviewer AG mittels des Netviewer Konfigurators (siehe 2.13.1) definiert der verantwortliche Netviewer-Mitarbeiter der Abteilung Delivery die initialen kundenspezifischen Authentifizierungsmerkmale (Benutzername und Passwort) für den Berater-Administrator.

Die Authentifizierungsmerkmale für den Berater-Administrator werden getrennt vom EVG per Post ausgeliefert (siehe 2.13.3). Bei der Auslieferung erhält der Server-Administrator die EVG-Komponenten und nimmt sie in Betrieb. Der Berater-Administrator erhält im Rahmen der Auslieferung die Zugangsdaten für das initiale Berater-Administrator-Konto. Dieses Berater-Administrator-Konto muss zunächst aktiviert werden.

Beim ersten Starten des Benutzermanagers meldet sich der Berater-Administrator mit dem initialen Passwort an. Er wird daraufhin vom System aufgefordert, das initiale

Passwort durch ein persönliches zu ersetzen. Der Standard Server prüft das vom Berater-Administrator selbst gewählte Passwort auf hinreichende Qualität. Das Passwort muss eine Mindestlänge von acht Zeichen haben, jeweils mindestens einen Großbuchstaben, einen Kleinbuchstaben und eine Ziffer enthalten und unterschiedlich vom vorherigen Passwort sein. Erst wenn der Berater-Administrator das Passwort geändert hat, erhält er Zugriff auf die Funktionen des Benutzermanagers. Beim nächsten Starten des Benutzermanagers kann sich der Berater-Administrator nur noch mit den geänderten Zugangsdaten anmelden.

Alle Operationen, die der EVG zu oben genannten Administrator-Aktionen durchführt, werden im Audit-Protokoll der Serverkomponente festgehalten.

2.12.2 Funktionen für den Berater-Administrator

Der Berater-Administrator kann im Benutzermanager neue Benutzer anlegen. Dazu muss er lediglich den Benutzernamen des Beraters definieren. Benutzernamen müssen eindeutig sein, d.h. das Anlegen von Benutzern mit gleichem Benutzernamen ist unzulässig.

Das zu dem Benutzernamen gehörige initiale Passwort wird vom System generiert. Das generierte Passwort ist achtstellig und eine zufällige Kombination aus Großbuchstaben, Kleinbuchstaben und Ziffern, wobei jeweils mindestens ein Großbuchstabe, ein Kleinbuchstabe und eine Ziffer enthalten sein muss. Das Passwort wird dem Berater-Administrator im Benutzermanager angezeigt.

Die Authentifizierungsmerkmale (Benutzername und Passwort) muss der Berater-Administrator nun dem Benutzer vertraulich zukommen lassen. Geeignet ist hier eine persönliche Übermittlung, per verschlüsselter E-Mail oder per Post. Der Berater-Administrator wird im Netviewer Standard Server^{TS} Administratorhandbuch auf diese Notwendigkeit hingewiesen.

Wenn sich der Berater mit seinem Benutzernamen und seinem initialen Passwort zum ersten Mal beim Beraterprogramm anmeldet, muss er das neu erstellte Konto zunächst aktivieren. Dazu muss er im Beraterprogramm das initiale Passwort durch ein persönliches Passwort ersetzen. Das Beraterprogramm prüft das gewählte Passwort auf ausreichende Qualität. Das Passwort muss eine Mindestlänge von acht Zeichen haben, jeweils mindestens einen Großbuchstaben, einen Kleinbuchstaben und eine Ziffer enthalten und unterschiedlich vom vorherigen Passwort sein. Erst nach der Aktivierung erhält der Berater Zugriff auf das Beraterprogramm. Eine unzulässige Nutzung eines Kontos mittels des initialen Passwortes ist damit ausgeschlossen.

Der Berater kann sein Passwort jederzeit ändern, wenn er über das aktuelle Passwort verfügt. Auch bei einer späteren Änderung wird das Passwort auf die oben genannten Qualitätskriterien hin überprüft.

Der Berater-Administrator kann das personalisierte Passwort eines Beraters jederzeit auf ein neu generiertes initiales Passwort zurücksetzen, wodurch der Berater wieder

gezwungen wird dieses durch ein persönliches zu ersetzen. Weiterhin kann der Berater-Administrator Benutzer löschen. Gelöschte Benutzer haben keinen Zugriff auf das Beraterprogramm mehr.

Alle Operationen, die der EVG zu oben genannten Administrator-Aktionen durchführt, werden im Audit-Journal der Serverkomponente festgehalten.

2.13 Konfiguration und Auslieferung von Netviewer one2one^{TS}

2.13.1 Konfiguration

Das Produkt Netviewer one2one^{TS} ist an kundenspezifische Anforderungen anpassbar. Die Konfiguration des EVG erfolgt vor der Auslieferung durch die Netviewer AG an den Kunden. Im Zuge der Konfiguration werden unter anderem folgende Eigenschaften der Software angepasst:

- Funktionsumfang der Clientprogramme, z.B. Verfügbarkeit von Funktionen im Netviewer Control Panel
- Technische Einstellungen der Serverkomponenten, um die Client-Server-Kommunikation zu ermöglichen
- Authentifizierungsmerkmale für den Berater-Administrator

Dabei ist zu beachten, dass sicherheitsrelevante Eigenschaften und Funktionen von Netviewer one2one^{TS} nicht konfigurierbar sind. Jeder Netviewer-Kunde besitzt zwar eine individuelle Instanz des EVG. Essentielle Funktionen und Eigenschaften sind jedoch aufgrund des gleichen Codestamms immer gleich.

Die Konfiguration seitens der Netviewer AG erfolgt über die Netviewer-eigene Software Netviewer Konfigurator. Der Netviewer Konfigurator bietet über eine grafische Benutzeroberfläche folgende Funktionen:

- Konfiguration der Client- und Server-Software, z.B. Einstellungen der Client-Oberfläche und technische Einstellungen zur Client-Server-Kommunikation.
- Sichere Generierung der Programmschlüssel, die während des Erstellungsprozesses in die Client- und Server-Software integriert werden.
- Kompilierung der Client- und Server-Software
- Shrinken der Client- und Server-Software
- Signieren der Client- und Server-Software mit einem von der unabhängigen Zertifizierungsstelle VeriSign ausgegebenen Zertifikat
- Sichere Ablage der erstellten Software

Dieser Vorgang wird hier grafisch dargestellt:

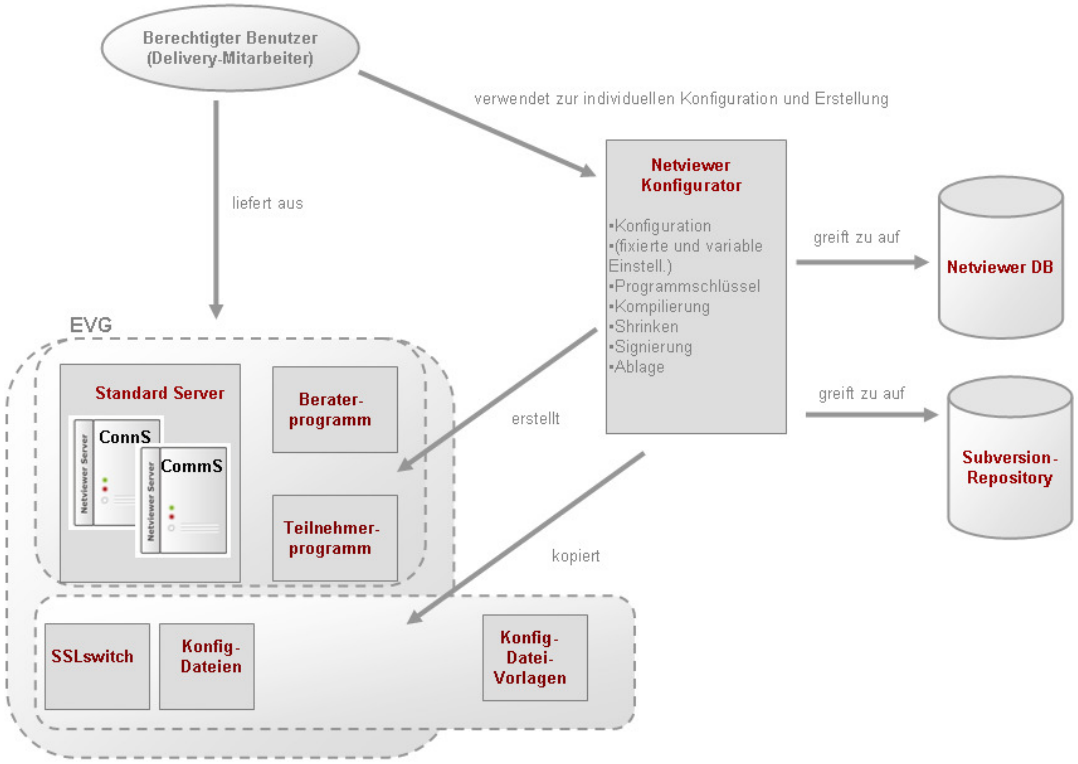

Abbildung 10: Erstellung des EVG mittels des Netviewer Konfigurators

Der für die Auslieferung verantwortliche Netviewer-Mitarbeiter verwendet den Netviewer Konfigurator zur Konfiguration und Erstellung der Software. Der Konfigurator greift auf das Codeverwaltungssystem Subversion zu und auf die Netviewer Datenbank, in der kundenspezifische Daten verwaltet werden. Der Netviewer Konfigurator erstellt die kundenindividuellen Clientprogramme und Serverkomponenten, kopiert die nicht kundenindividuellen Serverkomponenten sowie die Vorlagen für die adminstrierbaren Konfigurationsdateien und legt alle EVG-Komponenten im Auslieferungsverzeichnis ab. Von dort liefert der Netviewer-Mitarbeiter den EVG aus.

In der folgenden Grafik ist zu sehen, wie der unveränderliche Code-Stand aus dem Subversion-Repository mit über den Konfigurator festgelegten Einstellungen zum EVG zusammengebunden wird:

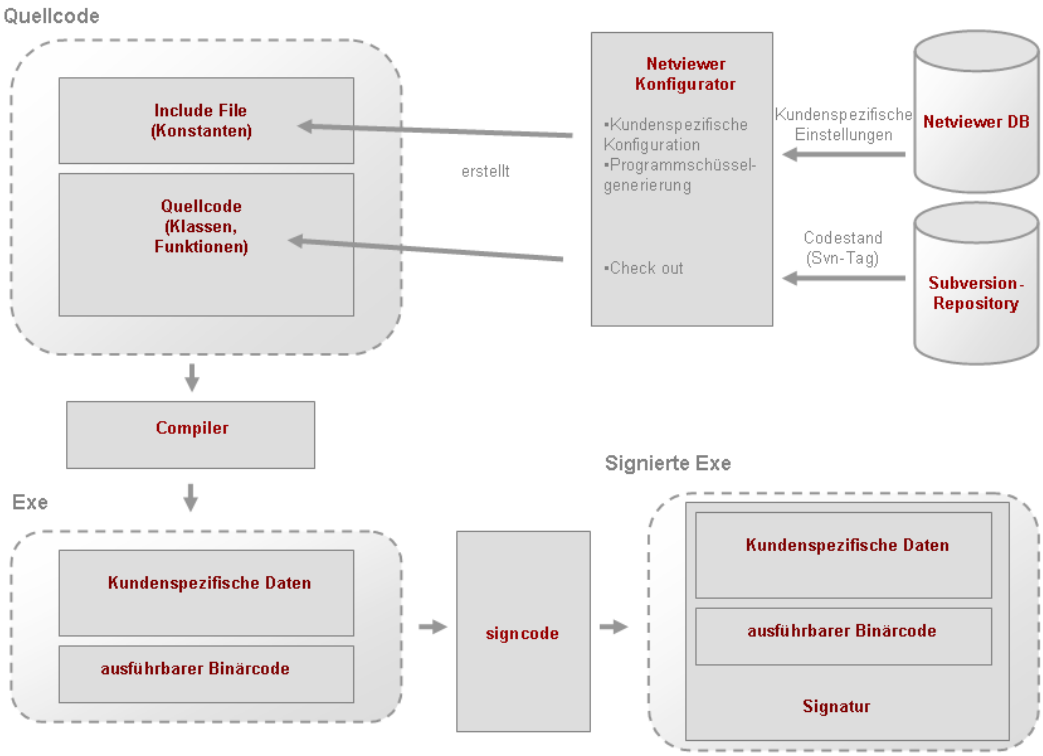

Abbildung 11 Kompilieren von statischem Code und kundenspezifischen Konstanten und anschließende Signierung

Nach dem Compilieren und Signieren sind die Konfigurationsparameter ein unveränderlicher Bestandteil des jeweiligen Programms.

2.13.2 Konfigurationsdaten nach der Erstellung

Nach der Erstellung fallen die Konfigurationsparameter hinsichtlich der Änderbarkeit in drei verschieden Kategorien:

- Änderbar: Die Konfigurationsdateien `ServerSettings.ini` und `SSLswitch.xml` sind vom Server-Administrator änderbar und werden beim Programmstart eingelesen.
- Austauschbar: Die Konfigurationsdateien `ContractData.dat` und `ServerData.dat` können durch vom Konfigurator neu erstellte Dateien ausgetauscht werden.
- Unveränderlich: Die Konfigurationsparameter, die in den signierten ausführbaren Dateien des EVGs (Beraterprogramm, Teilnehmerprogramm, Standard Server) enthalten sind, sind nur durch Austausch der umschließenden ausführbaren

Dateien veränderbar. Bezogen auf ein bestimmtes Exemplar einer ausführbaren Datei sind diese Konfigurationsparameter also unveränderlich.

2.13.3 Auslieferung

Auslieferung des Gesamtsystems an den Kunden

Die Auslieferung des kompletten EVGs (s. Kapitel 2) durch die Netviewer AG an den Kunden, der das Produkt bestellt und erworben hat, erfolgt per Postsendung. Der Delivery-Mitarbeiter, der für die Auslieferung zuständig ist, prüft dabei, ob die für einen bestimmten Kunden erstellten Programme auch an den entsprechenden Kunden gesendet werden. Die Postsendung wird direkt an den vom Kunden zuvor namentlich genannten Netviewer Server-Administrator gesendet.

Sämtliche Komponenten (exe-, Text-, Binär- und PDF-Dateien) werden auf einer CD-ROM ausgeliefert, die der Delivery-Mitarbeiter im Anschluss an die Erstellung des EVGs erzeugt hat.

Eine Ausnahme bilden die initialen Authentifizierungsdaten (Benutzername und Passwort) für den Berater-Administrator. Diese werden in einer separaten Postsendung direkt an den vom Kunden benannten Berater-Administrator verschickt.

Anhand der mit ausgelieferten Dokumentation sind der Server- und der Berater-Administrator imstande, das Netviewer one2one^{TS}-System eigenständig aufzusetzen und in Betrieb zu nehmen.

Der Prozess einer Nach- oder Neuauslieferung entspricht dem oben beschriebenen Prozess, da immer eine Komplettauslieferung des EVGs notwendig ist.

Auslieferung an den Berater

Die Auslieferung des Netviewer one2one^{TS} Beraterprogramms an die berechtigten Berater kann über verschiedene Wege erfolgen. Der Besitz des Beraterprogramms allein (ohne im Besitz einer gültigen Benutzername-Passwort-Kombination zu sein) stellt keine Bedrohung da.

Im Netviewer Standard Server^{TS} Administratorhandbuch werden folgende Auslieferungsmethoden für das Beraterprogramm empfohlen:

- Per E-Mail
- Per automatischer Software-Verteilung
- Per Ablage auf einem Netzlaufwerk

Die Verteilung der Benutzerdaten (Benutzername und Passwort) muss vertraulich durch den Berater-Administrator an den Empfänger erfolgen (s. Kapitel 2.12.2).

Der Server-Administrator hat weiterhin dafür Sorge zu tragen, dass der Berater Zugriff auf das Netviewer one2one^{TS} Benutzerhandbuch erhält. Zusätzlich ist das Benutzerhandbuch auch auf einer von der Netviewer AG gehosteten Webseite zu Netviewer one2one^{TS} verfügbar. Ein Link auf die Informationsseite ist im Login-Dialog des Beraterprogramms zu finden. Weitere Informationen zum Inhalt der Informationsseite bietet Kapitel 2.6.6.

Auslieferung an den Teilnehmer

Die Auslieferung des Netviewer one2one^{TS} Teilnehmerprogramms an den Teilnehmer, mit dem der Berater eine Sitzung durchführen möchte, kann über verschiedene Wege erfolgen. Der Besitz des Teilnehmerprogramms allein (ohne im Besitz einer gültigen Sitzungsnummer zu sein) stellt keine Bedrohung da.

Im Netviewer one2one^{TS} Benutzerhandbuch werden folgende Auslieferungsmethoden für das Teilnehmerprogramm empfohlen:

- Per E-Mail
- Per Download von der Webseite des Kunden
- Per Ablage auf einem Netzlaufwerk bei interner Nutzung

Das Benutzerhandbuch ist für den Teilnehmer auf der von der Netviewer AG gehosteten Informationsseite (s. Kapitel 2.6.6) zu Netviewer one2one^{TS} verfügbar. Ein Link auf die Informationsseite ist im Eingabedialog für die Sitzungsnummer im Teilnehmerprogramm zu finden. Das Netviewer one2one^{TS} Benutzerhandbuch informiert den Berater über die Notwendigkeit, den Teilnehmer auf diese Webseite hinzuweisen.

Auf der Informationsseite wird der Teilnehmer auch darauf hingewiesen, dass er prüfen sollte, ob er das Teilnehmerprogramm von dem Unternehmen erhalten hat, das in den Eigenschaften der exe-Datei bzw. im Splashscreen (Anzeige beim Starten des Programms) angegeben ist.

2.13.4 Identifizierung einer Instanz von Netviewer one2one^{TS}

Alle ausführbaren Dateien des EVG verfügen über die folgenden Identifikationsinformationen. Diese umfassen

- den Herstellernamen
- den Produktnamen,
- die Versionsnummer,
- die Buildnummer und
- den Kundennamen.

Bei den Clientprogrammen finden sich die Identifikationsinformationen im Splashscreen, der beim Programmstart erscheint, und in der About-Schublade. Beim Serverprogramm finden sich die Identifikationsinformationen im Serverfenster.

Weiterhin sind folgende Identifikationsinformationen bei allen Programmen als Eigenschaften der EXE-Dateien abrufbar.

Dateiversion	5.1.0.1208
Firma	Netviewer AG
Interner Name	<Kundenname, für den die exe-Datei durch die Netviewer AG erstellt wurde>
Originaldateiname	<Dateiname, z.B. NV_o2o_Teilnehmer_DE.exe>
Produktname	<Produktname, z.B. Netviewer one2one^{TS} Teilnehmerprogramm>
Produktversion	5.1.0.1208
Sprache	Deutsch

Tabelle 3: Angaben in den Dateieigenschaften der exe-Dateien

Darüber hinaus können der Berater und der Teilnehmer vor dem Gebrauch der Clientsoftware prüfen, ob es sich bei der vorliegenden .exe-Datei um ein Originalprogramm der Netviewer AG handelt und es unmodifiziert ist. Die Clientprogramme und der Standard Server sind mit einem VeriSign-Zertifikat, das auf die Netviewer AG ausgestellt ist, signiert. Damit werden die Authentizität und die Integrität der Programme sichergestellt. Hinweise zur manuellen Prüfung[2] der Codesignatur sind im Benutzerhandbuch und im Administratorhandbuch zu finden.

2.14 Übersicht über die Sicherheitsfunktionalität des EVG

In diesem Abschnitt wird eine Übersicht über die Sicherheitsfunktionalität des EVG gegeben. Der EVG bietet Schutz gegen Angreifer mit einem niedrigen Angriffspotential.

Die übertragenen Daten zwischen Berater und Teilnehmer werden symmetrisch verschlüsselt und mit Keyed Message Authentication Codes versehen. Mit diesen

[2] Die Clientprogramme und der Standard Server prüfen beim Start mittels Windows-API-Funktionen die Gültigkeit der Codesignatur und beenden sich mit einer Fehlermeldung, falls die Prüfung fehlschlägt. Dadurch ist sichergestellt, dass manipulierte und nicht authentische Programme nicht zum Einsatz kommen können, auch wenn eine manuelle Prüfung unterlassen wird

Maßnahmen wird die Vertraulichkeit **(Data Protection)** und die Integrität **(Integrity)** der Daten gewährleistet.

Die Daten, die Beraterprogramm und Teilnehmerprogramm mit dem Standard Server austauschen werden ebenfalls mit Keyed Message Authentication Codes versehen. Mit dieser Maßnahme ist die Integrität **(Integrity)** der Daten gewährleistet.

Die Sitzungspartner und die Clientkomponenten des EVGs authentifizieren sich gegenüber dem Vermittlungsservice. Der Berater authentifiziert sich gegenüber dem Vermittlungsservice mit einem Benutzernamen und einem Passwort. Der Teilnehmer authentifiziert sich mit der vom Berater erhaltenen Sitzungsnummer gegenüber dem Server. Der Berater-Administrator authentifiziert sich gegenüber dem Vermittlungsservice mit einem Benutzernamen und einem Passwort **(Identification & Authentification).**

Durch eine implementierte Zugriffsmethodik wird sichergestellt, dass

- nur Rechte für die Applikationen gewährt werden, die der einräumende Sitzungspartner in der Applikationsauswahl definiert hat. Auf alle anderen Daten hat der berechtigte Sitzungspartner keinen Zugriff;
- die Änderung der Blickrichtung nur mit ausdrücklicher Zustimmung des einräumenden Sitzungspartners erfolgt;
- durch die Fernsteuerungsrechte keine weiteren Rechte erworben werden können;
- während einer Sitzung die Fernsteuerung nur mit ausdrücklicher Zustimmung des einräumenden Sitzungspartners erfolgen kann;
- die Fernsteuerung einem Sitzungspartner nur eingeräumt werden kann, wenn dieser sich im Watch-Modus befindet. Die Fernsteuerung kann nur auf Applikationen erfolgen, die im Rahmen der Blickrichtungsänderung über die Applikationswahl definiert wurden;
- die Fernsteuerungsrechte jederzeit durch Betätigen einer Taste von dem einräumenden Sitzungspartner entzogen werden können (F11-Taste);
- während einer Sitzung die Funktion ‚Dateitransfer per Drag & Drop' nur mit ausdrücklicher Zustimmung des Sitzungspartners, der die Fernsteuerungsrechte für seinen Bildschirm eingeräumt hat, benutzt werden kann;
- nur zwei Sitzungspartner an einer Sitzung teilnehmen können **(Access Control)**.

Die Konfigurationsdateien ServerData.dat und ContractData.dat werden von dem Vermittlungsservice nur dann eingelesen, wenn sie nicht verändert wurden. **(Config Data Protection)**.

3 EVG-Sicherheitsumgebung

Das Kapitel ist unterteilt in die Unterkapitel:

- Definition von Objekten, Subjekten und Zugriffspolitiken;
- Annahmen, insbesondere
  - Annahmen über die Verwendung,
  - Materielle Annahmen,
  - Personelle Annahmen,
  - Annahmen über die Vernetzung;
- Bedrohungen;
- Organisatorische Sicherheitspolitiken.

3.1 Definition von Objekten, Subjekten und Zugriffspolitiken

In dem nachfolgenden Tabelle 5 werden folgende Bezeichnungen für Objekte definiert.

Objekt	Beschreibung
Daten	Sitzungsdaten oder Signalisierungsdaten
Sitzungsdaten	Daten, die zwischen den Clients ausgetauscht werden. Dies sind: - Daten zur Ausgabe (z.B. visualisierbare Daten wie Bildschirminhalte und Videodaten) - Daten von Eingabegeräten (z.B. Maus und Tastatur) Die Sitzungsdaten werden als ein zu schützendes Objekt definiert. <u>Informative Bemerkung:</u> Bei Sitzungsdaten ist zu unterscheiden zwischen - **Sitzungsdaten im Show-Modus** (ohne Fernsteuerung) des einräumenden Sitzungspartners (entspricht dem Watch-Modus des berechtigten Sitzungspartners), hier hat der berechtigte Sitzungspartner **Lese-Rechte** und **Zur Fernsteuerung freigegebene Sitzungsdaten** des einräumenden Sitzungspartners, hier hat der berechtigte Sitzungspartner **Lese- und Schreib-Rechte**.

Objekt	Beschreibung
Konfigurationsdateien	Die sicherheitsrelevanten Konfigurationsdateien `ServerData.dat` und `ContractData.dat` sind bei den Serverkomponenten lokalisiert.
Signalisierungsdaten	Signalisierungsdaten sind die zur Signalisierung zwischen den Clients und dem Vermittlungsservice ausgetauschten Daten. Signalisierung ist die Übermittlung von Information zu Steuerungszwecken. Hauptzweck beim Austausch von Signalisierungsinformationen ist es, die Verbindung zwischen den Clients herzustellen, aufrecht zu halten und schließlich wieder abzubauen. Zur Kommunikation zwischen Clients und dem Vermittlungsservice wird das Signalisierungsprotokoll HttpsRpc eingesetzt. Die Signalisierungsdaten werden als ein zu schützendes Objekt definiert.
Steuerungsdaten	Teil des Sitzungsdatenstroms. Beinhalten Steuerinformationen um die Modi des Sitzungsdatenaustauschs auszuhandeln (z.B. Initiierung eines Blickrichtungswechsels).
Sitzungsdatenstrom	Besteht aus Sitzungsdaten und Steuerungsdaten. Gesamtheit der Daten, die zwischen den Clientkomponenten des EVG (optional über den Kommunikationsservice) ausgetauscht werden.
Beraterkontendaten	Die Daten zu den Beraterkonten werden in der Benutzerdatei NVServer_users.txt bei der Server-Komponente gespeichert. Der Inhalt dieser Datei wird von dem Servermodul Benutzermanager gepflegt.
Verbindungsdaten	Log-Dateien, Protokolle

Tabelle 4: Definition der Objekte

In der nachfolgenden Tabelle 4 werden Bezeichnungen für Subjekte definiert. Subjekte sind Personen, aber auch Programme.

Subjekt / Rolle	**Beschreibung**
Autorisierter Berater	Der Berater verfügt über das Netviewer one2one^{TS} Beraterprogramm und gültige Zugangsdaten. Das Beraterprogramm befähigt den Berater, eine one2one^{TS}-Sitzung zu initiieren. Der Berater hat Zugriff auf die Funktionen des Netviewer-Programms zur Kommunikation

Subjekt / Rolle	Beschreibung
	und zum Datenaustausch mit dem Teilnehmer. Weiterhin stellt das Beraterprogramm dem Berater einen, im Vergleich zum Teilnehmerprogramm, erweiterten Funktionsumfang zur Organisation und Leitung der one2one^{TS}-Sitzung zur Verfügung. Der autorisierte Berater hat sich mittels Eingabe der Zugangsdaten autorisiert.
Autorisierter Teilnehmer	Der Teilnehmer muss Zugriff auf das Netviewer one2one^{TS} Teilnehmerprogramm erhalten. Das Teilnehmerprogramm befähigt den Teilnehmer, durch die Eingabe eines Identifikationsmerkmales in eine durch den Berater initiierte Sitzung einzutreten. Der Teilnehmer hat Zugriff auf die Funktionen des Netviewer-Programms zur Kommunikation und zum Datenaustausch mit dem Berater. Ein autorisierter Teilnehmer ist zur Nutzung des Teilnehmerprogramms durch die Eingabe einer gültigen Sitzungsnummer (die der autorisierte Berater ihm mitgeteilt hat) autorisiert.
Autorisierter Benutzer oder Sitzungspartner	Autorisierter Teilnehmer oder autorisierter Berater, die den EVG nutzen. Es wird unterschieden zwischen - einräumenden Sitzungspartner und - berechtigtem Sitzungspartner.
Einräumender Sitzungspartner	Einräumender Sitzungspartner räumt seinem Sitzungspartner gegenüber Rechte ein. Rechte können sein: - Show-Modus (Leserechte) - Freigabe der Fernsteuerung (Lese- und Schreibrechte)
Berechtigter Sitzungspartner	Besitzt Rechte, die der einräumende Sitzungspartner definiert hat.
Unautorisierte Person	Person, die kein autorisierter Benutzer ist
Angreifer	Angreifer können sein: - Unautorisierte Personen, die versuchen, die Verfügbarkeit des EVGs oder die Vertraulichkeit, Integrität und Authentizität der Daten des EVGs zu

Subjekt / Rolle	Beschreibung
	kompromittieren; - Autorisierte Benutzer, die Zugriff auf nicht für sie freigegebene Daten erlangen möchten. Angreifer werden als Verursacher von Bedrohungen definiert.
Server-Administrator	Der Administrator installiert und wartet den Rechner, das Betriebssystem, den Standard Server, den SSLswitch und das SSL-Serverzertifikat.
Server-Komponenten	Teil des EVGs, wird durch die beiden Rollen Vermittlungsservice und Kommunikationsservice repräsentiert.
Vermittlungsservice	Rolle auf der Server-Komponente des EVG
Kommunikationsservice	Rolle auf der Server-Komponente des EVG, der Kommunikationsservice wird optional eingesetzt, wenn kein Austausch des Datenstroms über eine Peer-to-Peer Verbindung zwischen den Clientkomponenten möglich ist.
Berater-Administrator	Der Berater-Administrator kann Beraterkonten anlegen und zurücksetzen. Dazu benutzt er das Modul „Benutzermanager" der Serverkomponente von one2one^{TS}.

Tabelle 5: Definition der Subjekte

Der EVG ist für Daten mit niedrigem Schutzbedarf geeignet. Es wird daher davon ausgegangen, dass der Angreifer über ein niedriges Angriffspotenzial verfügt.

Es wird davon ausgegangen, dass ein Angreifer begrenzte technische und zeitliche Möglichkeiten besitzt und über allgemein verfügbare Kenntnisse der Informationstechnik, des Betriebssystems und des EVG verfügt.

Der Sitzungsdatenstrom unterliegt folgender Zugriffspolitik **„ACCESS Session Data"**, die der EVG durchzusetzen hat:

Rolle	Zugriffsrecht
Einräumender Sitzungspartner	Sitzungsdaten im Showmodus: Read / Write Zur Fernsteuerung freigegebene Sitzungsdaten: Read / Write

Berechtigter Sitzungspartner	Sitzungsdaten im Watchmodus: Read Freigegebene Sitzungsdaten: Read Zur Fernsteuerung freigegebene Sitzungsdaten: Read / Write Es gelten hierbei folgende Bedingungen: - Es werden nur Rechte für die Applikationen gewährt, die der einräumende Sitzungspartner in der Applikationsauswahl definiert hat. Auf alle anderen Daten hat der berechtigte Sitzungspartner keinen Zugriff. - Die Änderung der Blickrichtung erfolgt nur mit ausdrücklicher Zustimmung des einräumenden Sitzungspartners. - Durch die Fernsteuerungsrechte können keine weiteren Rechte erworben werden. - Während einer Sitzung kann die Fernsteuerung nur mit ausdrücklicher Zustimmung des einräumenden Sitzungspartners erfolgen. - Die Fernsteuerung kann nur eingeräumt werden, wenn zuvor die Blickrichtung entsprechend der einräumenden Fernsteuerungsrechte geändert wurde. Die Fernsteuerung kann nur auf Applikationen erfolgen, die im Rahmen der Blickrichtungsänderung über die Applikationswahl definiert wurden. - Die Fernsteuerungsrechte können jederzeit durch Betätigen einer Taste von dem einräumenden Sitzungspartner entzogen werden (F11-Taste). - Während einer Sitzung kann die Funktion ‚Dateitransfer per Drag & Drop' nur mit ausdrücklicher Zustimmung des Sitzungspartners benutzt werden kann, der die Funktion nicht initiiert hat. - Es können nur zwei Sitzungspartner an einer Sitzung teilnehmen. - Die eingeräumten Fernsteuerungsrechte beziehen sich nur auf Fenster von Applikationen, die der Einräumende Sitzungspartner in der Applikationswahl-Schublade freigegeben hat. - Der EVG bietet dem Benutzer folgende Funktionalität an: Die Fernsteuerungsrechte können vom Berater im

	Watch-Modus angefordert werden. Der einräumende Sitzungspartner muss die Fernsteuerungsrechte darauf hin explizit erteilen (Zustimmungsdialog). - Fordert der Berater eine Systemdiagnose des Systems des Teilnehmers durchzuführen, so geschieht dies nur mit Zustimmung seines Sitzungspartners.

Tabelle 6: ACCESS Session Data

Die beiden bei den Serverkomponenten lokalisierten sicherheitsrelevanten Konfigurationsdateien `ServerData.dat` und `ContractData.dat` unterliegen folgender Zugriffspolitik **„ACCESS Secure Config Data"**, die der EVG durchzusetzen hat:

Rolle	Zugriffsrecht
Vermittlungsservice	Der Vermittlungsservice liest die Konfigurationsdateien `ServerData.dat` und `ContractData.dat` nur ein, wenn sie nicht verändert wurden. Er hat keine Schreibrechte.

Tabelle 7: ACCESS Secure Config Data

Die bei den Serverkomponenten lokalisierte sicherheitsrelevante Konfigurationsdatei `NVServer_users.txt` (auch als „Benutzerdatei" bezeichnet) unterliegt folgender Zugriffspolitik **„ACCESS Config User Data"**, die der EVG durchzusetzen hat:

Rolle	Zugriffsrecht
Vermittlungsservice	Benutzerdatei bei der Serverkomponente des EVG (Vermittlungsservice): Read.
Berater-Administrator	Benutzermanager: Read (teilweise[3]), write Mittels des Moduls „Benutzermanager" der Serverkomponente kann der Berater-Administrator die Beraterkontendatei lesen und verändern.

Tabelle 8:ACCESS Config User Data

[3] Der Berater-Administrator kann die individualisierten Passwörter der Berater nicht lesen oder verändern, diese werden gehasht in der Benutzerdatei abgelegt. Er kann Passwörter auf einen Initialwert zurücksetzen.

Bei der Definition von Passwörtern des Beraters und des Berater-Administrators werden folgende Regeln **(Passwort Policy)** beachtet:

- Länge mindestens 8 Zeichen;
- Es müssen mindestens ein Kleinbuchstabe, mindestens ein Großbuchstabe und mindestens eine Ziffer enthalten sein.

3.2 Annahmen

3.2.1 Annahmen über die Verwendung

Für die Verwendung des EVG werden folgende Annahmen getroffen:

A.USE.1	Die mit dem EVG zu verarbeitenden Daten besitzen einen niedrigen Schutzbedarf.

3.2.2 Materielle Annahmen

Für den Betrieb des EVG wird folgende materielle Annahme getroffen:

A.PHY.Server.1	Die Serverkomponente des EVG wird in einem Serverraum einer Behörde oder eines Unternehmens betrieben. Dabei wird davon ausgegangen, dass es durch geeignete technische und organisatorische Maßnahmen sichergestellt ist, - dass nur Administratoren der Serverkomponente des EVG kontrollierten Zugang zum Serverraum haben, - dass nur Administratoren der Serverkomponente Zugriff auf andere Repräsentationen der Daten (z. B. Backup) des EVG erhalten, - dass die verwendeten Hardwarekomponenten durch geeignete bauliche oder andere physische Sicherungsmaßnahmen vor Entwendung geschützt sind.
A.PHY.Client.1	Die Clientkomponente des EVG wird in einer normalen Büroumgebung einer Behörde oder eines Unternehmens betrieben. Dabei wird davon ausgegangen, dass es durch geeignete technische und organisatorische Maßnahmen sichergestellt ist, - dass unautorisierte Personen keinen Zugang zum Büro bzw. Arbeitsplatz haben,

	- dass unautorisierte Personen keinen Zugriff auf andere Repräsentationen der Daten des EVG erhalten.
A.Plattform.Server	Die Serverkomponente des EVG wird auf einer Plattform mit den nachfolgenden Anforderungen betrieben: - Betriebssystem Microsoft Windows Server 2000 oder Windows Server 2003 - Intel Pentium Prozessor mit mindestens 2 GHz (oder vergleichbar) - mindestens 1 GB RAM - mindestens 2 GB freien Festplattenplatz - mindestens 100 MBit Netzwerkkarte sowie Internet- oder Intranetanbindung - Microsoft .NET-Framework 2.0
A.Plattform.Client	Die Clientkomponenten des EVG werden auf einer Plattform mit den nachfolgenden Anforderungen betrieben: - PC mit Microsoft Windows 2000 oder Windows XP - Internet-/Intranetzugang mit beliebigem Browser - Prozessor mit mind. 300 MHz - mind. 64 MB RAM
A.PRNG.Server	Der Pseudozufallszahlengenerator (PRNG) des Betriebssystems, auf dem die Serverkomponenten und die Clientprogramme ausgeführt werden, liefert kryptographisch sichere Zufallszahlen.

3.2.3 Personelle Annahmen

Für den Betrieb des EVG werden folgende personelle Annahmen getroffen:

A.PER.1	Die Administration der Clientkomponente des EVG und der zugrunde liegende Systemumgebung wird durch den autorisierten Benutzer oder einer anderen vertrauenswürdigen Person (Administrator der Clientumgebung) gewissenhaft, umsichtig und verantwortungsbewusst durchgeführt und damit den sicheren Betrieb des EVG gewährleistet. Durch die Administration ist insbesondere sicher gestellt:

	- eine gesicherte Konfiguration der PCs und der Netzinfrastruktur. Dazu zählen der Einsatz von aktuellen Virenscannern, sowie die sichere Konfiguration von Firewalls auf den PCs bzw. innerhalb der jeweiligen Netzinfrastruktur.
A.PER.2	Die Administration der Serverkomponente des EVG und der zugrunde liegende Systemumgebung wird durch mindestens eine kompetente und vertrauenswürdige Person durchgeführt. Systemadministratoren nehmen ihre Aufgaben gewissenhaft, umsichtig und verantwortungsbewusst wahr. Durch die Administration ist insbesondere sicher gestellt: - eine gesicherte Konfiguration der PCs und der Netzinfrastruktur. Dazu zählen der Einsatz von aktuellen Virenscannern, sowie die sichere Konfiguration von Firewalls auf den PCs bzw. innerhalb der jeweiligen Netzinfrastruktur; - eine regelmäßige Aktualisierung der eingesetzten Software und des Betriebssystems zur Behebung von Sicherheitslücken; - eine regelmäßige Sicherung der Daten der EVG-Komponente Standard Server. Über diese Sicherungen können die Daten wieder hergestellt werden.
A.PER.3	Die Sitzungsnummer wird von dem Berater sicher an den Teilnehmer weiter gegeben, da sie ein Authentisierungsmerkmal darstellt. Der Berater ist verantwortlich, die Identität des Sitzungsteilnehmers, der die Sitzungsnummer erhält, festzustellen.
A.PER.4	Der autorisierte Benutzer geht mit dem Produkt gewissenhaft um, insbesondere ist der Benutzer dafür verantwortlich, das die Applikationsauswahl auf das Notwendigste beschränkt ist (Bildschirmbereiche die für den Fernsteuernden frei gegeben werden).
A.PER.5	Die Beraterkontendaten (Benutzername und Initialpasswort) werden von dem Berater-Administrator sicher an die autorisierten Berater weiter gegeben.

3.2.4 Annahmen über die Vernetzung

Für den Betrieb des EVG werden die folgenden Annahmen über die Vernetzung getroffen:

A.NET.1	Alle vier Komponenten des EVGs müssen in einem TCP/IP-Netz betrieben werden. Dessen Endsysteme sowie die dazwischen liegenden Transitsysteme (und ggf. vorhandene Gateways) müssen derart konfiguriert sein, dass es den Clientprogrammen möglich ist, eine TCP-Verbindung zum Standard Server aufzubauen. Als Mindestvoraussetzung muss es den Clientprogrammen möglich sein, http- und https-Requests an den Standard Server abzusetzen.
A.NET.2	Das SSL-Server-Zertifikat ist im Zertifikatsspeicher der Windows-Instanz, auf dem die Server-Komponenten laufen, installiert. Das SSL-Server-Zertifikat ist auf einen Domainnamen ausgestellt, der nachvollziehbar dem Betreiber zugeordnet ist.
A.NET.3	Die Zertifizierungsstelle, die das SSL-Serverzertifikat und das Exe-Signatur-Zertifikat ausgestellt hat, ist bei Clients vertrauenswürdig eingestuft.
A.NET.4	Die SSL-Zertifikatsspeicher der Windows-Instanzen, auf dem die Clientprogramme bzw. der Standard Server ausgeführt werden, enthalten ausschließlich Zertifikate von vertrauenswürdigen Zertifizierungsstellen.
A.NET.5	Die SSL-Implementierung der Windows-Instanz auf dem der SSlswitch ausgeführt wird, ist so konfiguriert, dass ausschließlich Kombinationen von Verschlüsselungsverfahren und Schlüssellängen verwendet werden, die eine Stärke von mindestens 128 Bit aufweisen.

3.3 Bedrohungen

Name	**T.Client.Auth.1**
Angriff	Eine unautorisierte Person tritt als Teilnehmer in eine Sitzung ein und erlangt so unberechtigten Zugriff auf Daten des Sitzungspartners.
Erläuterung	Technischer Angriff, gibt vor, jemand anderes zu sein. Umgehung der Zugriffspolitik **ACCESS Session Data**.
Wert	Daten
Angreifer	Unautorisierte Person

Name	**T.Client.Auth.2**
Angriff	Eine unautorisierte Person eröffnet als Berater eine Sitzung und erlangt so unberechtigten Zugriff auf Daten des Sitzungspartners.
Erläuterung	Umgehung der Zugriffspolitik **ACCESS Session Data**.
Wert	Daten
Angreifer	Unautorisierte Person

Name	**T.Berater.Log.1**
Angriff	Ein Angreifer liest oder manipuliert unberechtigterweise Aufzeichnungen von Sitzungen beim Beraterprogramm.
Erläuterung	Folgende Szenarien kommen in Betracht: Ein Angreifer kann versuchen, dass Auditaufzeichnungen verloren gehen oder dass zukünftige Auditaufzeichnungen umgangen werden, da die Audit-Speicherkapazität überschritten wird. Ein Angreifer manipuliert Sitzungsaufzeichnungen. Einem autorisierten Berater wird vorgeworfen, in einer vergangenen Sitzung unerwünschte Aktionen durchgeführt zu haben. Eine Sitzung sollte durch den Berater stets nachzuvollziehen sein.
Wert	Verbindungsdaten
Angreifer	Angreifer

Name	**T.Server.Log.1**
Angriff	Ein Angreifer liest oder manipuliert unberechtigterweise Aufzeichnungen von Sitzungen bei der Serverkomponente des EVG.
Erläuterung	Folgende Szenarien kommen in Betracht: Die Aufzeichnung der Sitzungsprotokolle bei der Server-Komponente des EVGs werden gestört oder manipuliert. Ein Angreifer kann versuchen, dass Auditaufzeichnungen verloren gehen oder dass zukünftige Auditaufzeichnungen umgangen werden, da die Audit-Speicherkapazität überschritten wird. Bei der Serverkomponente des EVG erfolgt unerkannter Verlust der Integrität der Protokolldaten und Zugangsdaten. Als Ursache kommen auch unbeabsichtigte äußere Einflüsse (z. B. Hardwarefehler) in Betracht.
Wert	Verbindungsdaten
Angreifer	Angreifer

Name	**T.Privacy.1**
Angriff	Eine unautorisierte Person erhält unberechtigterweise Kenntnis von Daten der Sitzungspartner.
Erläuterung	Folgende Szenarien kommen in Betracht: Der Angreifer belauscht eine Sitzung. Umgehung der Zugriffspolitik **ACCESS Session Data**.
Wert	Sitzungsdatenstrom
Angreifer	Unautorisierte Person

Name	**T.Client.Privacy.2**
Angriff	Eine unautorisierte Person gerät in den Besitz eines symmetrischen Schlüssels und kann damit kodierte Nachrichten entschlüsseln.
Erläuterung	Folgende Szenarien kommen in Betracht: Z. B kann eine unautorisierte Person versuchen, den Schlüssel bei

	der Übermittlung an die Clients zu belauschen. Umgehung der Zugriffspolitik **ACCESS Secure Config Data**.
Wert	Daten
Angreifer	Unautorisierte Person

Name	**T.Privacy.3**
Angriff	Ein Angreifer erhält unberechtigterweise Kenntnis von Daten, die die Sitzungspartner über die Clientkomponenten mit der Vermittlungsservice-Rolle austauschen (Signalisierungsdaten).
Erläuterung	Folgende Szenarien kommen in Betracht: Der Angreifer belauscht die Signalisierung und erhält vertrauliche Daten, wie z. B. das Beraterpasswort.
Wert	Daten Signalisierungsdaten
Angreifer	Angreifer

Name	**T.Integrity.1**
Angriff	Ein Angreifer manipuliert unbemerkt eine Sitzung durch Veränderung des Sitzungsdatenstroms[4] oder ersetzt diesen und übermittelt dem empfangenden Sitzungspartner falsche Daten.
Erläuterung	Folgende Szenarien kommen in Betracht: Es wird davon ausgegangen, dass der Angreifer so genannte man–in-the-middle Attacken oder session hijacking Attacken einsetzt, um dem Sitzungspartner falsche Daten zu übermitteln. Umgehung der Zugriffspolitik **ACCESS Session Data**.
Wert	Sitzungsdaten
Angreifer	Angreifer

Name	**T.Integrity.2**
Angriff	Ein Angreifer modifiziert das Netviewer Server-, Teilnehmer- oder Beraterprogramm unbemerkt, um z.B. die Sicherheitsfunktionen

[4] Der Austausch des Sitzungsdatenstroms kann optional über den Kommunikationsserver erfolgen.

	des EVG zu umgehen.
Erläuterung	Hierunter fällt unter anderem auch das Modifizieren der EVG-Komponenten vor Auslieferung an den Kunden, z.B. der Abänderung der sicherheitsrelevanten Konfigurationsparameter wie der eingebundenen Schlüssel.
Wert	Daten
Angreifer	Unautorisierte Person

Name	**T.Integrity.3**
Angriff	Ein Angreifer manipuliert unbemerkt Signalisierungsdaten, die zwischen den EVG-Clientkomponenten und der Serverkomponente ausgetauscht werden. Durch diese Manipulation erhalten die Clientkomponenten und/oder die Serverkomponente falsche Daten.
Erläuterung	Folgende Szenarien kommen in Betracht: Es wird davon ausgegangen, dass der Angreifer sogenannte man–in-the-middle Attacken oder session hijacking Attacken einsetzt, um dem Sitzungspartner falsche Daten zu übermitteln.
Wert	Signalisierungsdaten
Angreifer	Angreifer

Name	**T.Integrity.4**
Angriff	Eine unautorisierte Person verwendet den Benutzermanager, um die Benutzerdatei zu editieren.
Erläuterung	--
Wert	Benutzerdaten
Angreifer	Angreifer

Name	**T.Client.Rights.1**
Angriff	Der autorisierte Benutzer erlangt Rechte, die der einräumende Sitzungspartner nicht in diesem Umfang definiert hat oder ohne dass der einräumende Sitzungspartner Wissen hiervon erlangt hat. Dieser Angriff findet während einer laufenden Sitzung statt. Der

	autorisierte Benutzer ist der Angreifer. Der Angreifer versucht mittels der vom Clientprogramm zur Verfügung gestellten Funktionalität, maximalen Zugriff auf den Rechner seines Sitzungspartners zu erlangen. Beispielsweise aktiviert er die Fernsteuerung, versucht die Applikationswahl-Schublade in der GUI seines Sitzungspartners zu manipulieren oder versucht Dateien vom oder zum Rechner des Sitzungspartners zu übertragen.
Erläuterung	Insbesondere können folgende Rechte bedroht werden: z.B. Kann die Änderung der Blickrichtung während einer Sitzung erfolgen, ohne dass der andere Sitzungspartners zugestimmt oder hiervon Wissen erlangt hat. z.B. können einem Sitzungspartner mehr Applikationen angezeigt werden, als dies der einräumende Sitzungspartner definiert hat. z.B. Erlangt ein autorisierter Benutzer die Möglichkeit Programme auf dem Computer des Sitzungspartners auszuführen, ohne dass der Sitzungspartner seine Zustimmung erteilt oder hiervon Wissen erlangt hat. Dies wäre z.B. Der Fall, wenn der autorisierte Benutzer die Fernsteuerung für die Eingabegeräte seines Sitzungspartners erhält, obwohl der einräumende Sitzungspartner dies nicht in dem genutzten Umfang definiert hat. z.B. Ändert ein autorisierter Benutzer die EVG-Programmeinstellungen des Sitzungspartners, um weitergehende Rechte zu erlangen (privilege escalation). z.B. Kann ein autorisierter Benutzer ohne die Zustimmung seines Sitzungspartners einen Dateitransfer von/zu seinem Sitzungspartner durchführen. z.B. können mehr als zwei Sitzungspartner an einer Sitzung teilnehmen. z.B. kann ein Berater ohne die Zustimmung seines Sitzungspartners eine Systemdiagnose des Systems des Teilnehmers durchführen. Umgehung der Zugriffspolitik **ACCESS Session Data**.
Wert	Daten
Angreifer	Autorisierter Benutzer

Name	**T.Server.Cfg.1**

Angriff	Ein Angreifer, der Zugriff auf den Server erlangt, liest oder manipuliert Konfigurationsdaten.
Erläuterung	Folgende Szenarien kommen in Betracht: Bei der Serverkomponente des EVG erfolgt unerkannter Verlust der Integrität der Konfigurationsdaten. Als Ursache werden unbeabsichtigte äußere Einflüsse (z. B. Hardwarefehler) oder Manipulationsversuche autorisierter Benutzer angenommen. Umgehung der Zugriffspolitik **ACCESS Secure Config Data und ACCESS Config User Data**.
Wert	Daten
Angreifer	Unautorisierte Person

Name	**T.Server.Cfg.2**
Angriff	Ein Angreifer täuscht die Identität der Serverkomponenten vor, z.B. indem er Zugriff auf den privaten Key des SSL-Serverzertifikats erlangt. Das Vortäuschen der Identität der Serverkomponenten erlaubt es dem Angreifer, Sitzungen unter falscher Identität zu initiieren und sich dadurch das Vertrauen von Teilnehmern zu erschleichen.
Erläuterung	Folgende Szenarien kommen in Betracht: z.B. indem er Zugriff auf den privaten Key des SSL-Serverzertifikats erlangt.
Wert	Daten
Angreifer	Unautorisierte Person

3.4 Organisatorische Sicherheitspolitik

P.Datenschutz

Auf dem Server werden datenschutzrechtliche Bestimmungen eingehalten. Dies bedeutet, dass alle Dateien, die personenbezogene Daten enthalten, gemäß den Vorgaben des Bundesdatenschutzgesetzes[5] geschützt werden. Personenbezogene Daten fallen bei den Serverkomponenten des one2one^{TS}-Systems u.a. in Form von Nutzungsprotokollen (Benutzerkennungen, IP-Adressen) an und sind in den Dateien `NVStandardServer_<Datum>_logfile.txt`, `NVStandardServer_<Datum>_auditlog.txt`, `NVStandardServer_<Datum>_VMServerLog.csv`, `NVServer_users.txt` enthalten.

[5] Abhängig von der Organisation, in der der EVG zum Einsatz kommt, können weitere Gesetze, Verordnungen und Weisungen greifen (z.B. das jeweilige Landesdatenschutzgesetz).

4 Sicherheitsziele

Dieses Kapitel Sicherheitsziele ist unterteilt in die Unterkapitel:

- Sicherheitsziele für den EVG.
- Sicherheitsziele für die Umgebung,

4.1 Sicherheitsziele für den EVG

Name	**O.Auth.1**
Ziel	Nur autorisierte Benutzer können eine Sitzung eröffnen bzw. in eine Sitzung eintreten.

Name	**O.Auth.2**
Ziel	Ausschließlich authentifizierte Clientprogramme können die Serverkomponenten benutzen.

Name	**O.Auth.3**
Ziel	Ausschließlich authentifizierte Berater-Administratoren können mit Hilfe des Benutzermanagers Berater verwalten.

Name	**O.Privacy.1**
Ziel	Der zwischen den Sitzungspartnern übermittelte Sitzungsdatenstrom ist vertraulich und von Dritten[6] nicht einsehbar.

Name	**O.Privacy.2**
Ziel	Die Anzahl der Sitzungspartner wird auf zwei beschränkt.

Name	**O.Integrity.1**

[6] Auch nicht von dem Kommunikationsservice, über den der Austausch des Sitzungsdatenstroms optional erfolgt.

Ziel	Der zwischen den beiden Clientprogrammen der Sitzungspartner ausgetauschte Sitzungsdatenstrom[7] ist integer.

Name	**O.Integrity.2**
Ziel	Die zwischen den EVG-Komponenten übermittelten Signalisierungsdaten sind integer.

Name	**O.Rights.1**
Ziel	Während einer Sitzung kann die Änderung der Blickrichtung nur mit ausdrücklicher Zustimmung des einräumenden Sitzungspartners erfolgen.

Name	**O.Rights.2**
Ziel	Während einer Sitzung wird dem Sitzungspartner nur die Applikationen angezeigt, die der einräumende Sitzungspartner in der Applikationsauswahl definiert hat.

Name	**O.Rights.3**
Ziel	Während einer Sitzung kann die Fernsteuerung nur mit ausdrücklicher Zustimmung des einräumenden Sitzungspartners erfolgen. Die Fernsteuerung kann nur eingeräumt werden, wenn zuvor die Blickrichtung entsprechend der einräumenden Fernsteuerungsrechte geändert wurde. Die Fernsteuerung kann nur auf Applikationen erfolgen, die im Rahmen der Blickrichtungsänderung über die Applikationswahl definiert wurden. Während einer Sitzung kann der einräumende Sitzungspartner seinem Kommunikationspartner die Fernsteuerungsrechte jederzeit durch Betätigen der Sicherheitstaste (Taste F11) entziehen. Werden vom Berater im Watch-Modus die Fernsteuerungsrechte angefordert, muss der einräumende Sitzungspartner (Teilnehmer)

[7] Der Austausch des Sitzungsdatenstroms kann optional über den Kommunikationsserver erfolgen.

	die Fernsteuerungsrechte im Rahmen eines Zustimmungsdialoges explizit erteilen. Fordert der Berater eine Systemdiagnose des Systems des Teilnehmers durchzuführen, so geschieht dies nur mit Zustimmung seines Sitzungspartners.

Name	**O.Rights.4**
Ziel	Während einer Sitzung kann sich der Kommunikationspartner des einräumenden Sitzungspartners mittels der Fernsteuerungsrechte keine weitere Rechte selbst einräumen.

Name	**O.Rights.5**
Ziel	Während einer Sitzung kann die Funktion ‚Dateitransfer per Drag & Drop' nur mit ausdrücklicher Zustimmung des Sitzungspartners benutzt werden kann, der die Funktion nicht initiiert hat.

Name	**O.Server.Cfg.1**
Ziel	Die Konfigurationsdateien auf der Serverkomponente werden nur dann eingelesen, wenn sie integer sind.

4.2 Sicherheitsziele für die Umgebung

4.2.1 Sicherheitsziele für die IT-Umgebung

Name	**OE-IT.1**
Ziel	Die SSL-Implementierung des Betriebssystems, auf dem die Serverkomponenten und die Clientprogramme ausgeführt werden, arbeitet spezifikationsgemäß (TLS 1.0 [RFC2246] oder SSL 3.0 [SSL3]).

Name	**OE-IT.2**
Ziel	Der Pseudozufallszahlengenerator (PRNG) des Betriebssystems, auf dem die Serverkomponenten und die Clientprogramme

	ausgeführt werden, liefert kryptographisch sichere Zufallszahlen.

Name	**OE-IT.3**
Ziel	Die zwischen den EVG-Komponenten übermittelten Signalisierungsdaten sind vertraulich und von Dritten nicht einsehbar.

4.2.2 Sicherheitsziele für die Nicht IT-Umgebung

Name	**OE.1**
Ziel	Die Serverkomponente des EVG wird in einem Serverraum einer Behörde oder eines Unternehmens betrieben. Durch geeignete technische und organisatorische Maßnahmen ist sichergestellt, - dass unautorisierte Personen keinen Zugang zum Serverraum haben, - dass unautorisierte Personen keinen Zugriff auf andere Repräsentationen der Daten (z.B. Backup) des EVG erhalten, - dass die verwendeten Hardwarekomponenten durch geeignete bauliche oder andere physische Sicherungsmaßnahmen vor Entwendung geschützt sind.

Name	**OE.2**
Ziel	Auf dem Server werden datenschutzrechtliche Bestimmungen eingehalten. Da die vom Standard Server erzeugten Dateien (insbesondere `NVStandardServer_<Datum>_logfile.txt`, `NVStandardServer_<Datum>_auditlog.txt`, `NVStandardServer_<Datum>_VMServerLog.csv`, `NVServer_users.txt`) personenbeziehbare Angaben (wie z.B. Kennungen und IP-Adressen) enthalten, fallen sie unter das Bundesdatenschutzgesetz und sind demnach besonders zu Schützen.

Name	**OE.3**
Ziel	Die Clientkomponente des EVG wird in einer normalen Büroumgebung einer Behörde oder eines Unternehmens

	betrieben. Durch geeignete technische und organisatorische Maßnahmen ist sichergestellt, - dass unautorisierte Personen keinen Zugang zum Büro bzw. Arbeitsplatz haben, - dass unautorisierte Personen keinen Zugriff auf andere Repräsentationen der Daten des EVG erhalten.
Name	**OE.4**
Ziel	Die Administration der Clientkomponente des EVG und der zugrunde liegende Systemumgebung wird durch den autorisierten Benutzer oder einer anderen vertrauenswürdigen Person (Administrator der Clientumgebung) gewissenhaft, umsichtig und verantwortungsbewusst durchgeführt und damit den sicheren Betrieb des EVG gewährleistet. Durch die Administration ist insbesondere sicher gestellt: - eine gesicherte Konfiguration der PCs und der Netzinfrastruktur ausgegangen. Dazu zählen der Einsatz von aktuellen Virenscannern, sowie die sichere Konfiguration von Firewalls auf den PCs bzw. innerhalb der jeweiligen Netzinfrastruktur.

Name	**OE.5**
Ziel	Die Administration der Serverkomponente des EVG und der zugrunde liegende Systemumgebung wird durch mindestens eine kompetente und vertrauenswürdige Person durchgeführt. Systemadministratoren nehmen ihre Aufgaben gewissenhaft, umsichtig und verantwortungsbewusst wahr. Durch die Administration ist insbesondere sicher gestellt: - eine gesicherte Konfiguration der PCs und der Netzinfrastruktur ausgegangen. Dazu zählen der Einsatz von aktuellen Virenscannern, sowie die sichere Konfiguration von Firewalls auf den PCs bzw. innerhalb der jeweiligen Netzinfrastruktur; - eine regelmäßige Aktualisierung der eingesetzten Software und des Betriebssystems zur Behebung von Sicherheitslücken; - eine regelmäßige Sicherung der (Konfigurations)Daten der EVG-Komponente Standard Server. Über diese Sicherungen können die Daten wieder hergestellt werden.

Name	OE.6
Ziel	Nur autorisierte Personen erhalten ein Authentisierungsmerkmal. Sitzungsnummern stellen ein Authentisierungsmerkmal dar. Sitzungsnummern werden sicher ausgetauscht. Der Berater ist verantwortlich, die Identität des Sitzungsteilnehmers, der die Sitzungsnummer erhält, festzustellen. Berater erhalten Benutzername und Initialpasswort als Authentisierungsmerkmal von dem Berater-Administrator des EVG auf gesichertem Wege. Berater geben ihren Benutzernamen und ihr Passwort nicht weiter.

Name	OE.7
Ziel	Der Benutzer geht mit dem Produkt gewissenhaft um, insbesondere ist der Benutzer dafür verantwortlich, dass die Applikationsauswahl auf das Notwendigste beschränkt ist. (Bildschirmbereiche die für den Fernsteuernden frei gegeben werden)

Name	OE.8
Ziel	Die mit dem EVG zu verarbeitenden Daten besitzen einen niedrigen Schutzbedarf.

Name	OE.9
Ziel	Die Aufzeichnungen auf der Berater-Clientkomponente des EVG (Verbindungsdaten) sind integer und vertraulich.

Name	OE.10
Ziel	Die Aufzeichnungen auf der Server-Komponente des EVG (Verbindungsdaten) sind integer und vertraulich.

Name	OE.11
Ziel	Die Komponenten des EVG (Client- und Serverkomponente) sind integer und können nicht ausgetauscht werden.

Name	OE.12
Ziel	Die Konfigurationsdaten und Verbindungsdaten auf der Serverkomponente des EVG sind vertraulich verwaltet.

Name	OE.13
Ziel	Alle vier Programme des EVGs müssen in einem TCP/IP-Netz betrieben werden. Dessen Endsysteme sowie die dazwischen liegenden Transitsysteme (und ggf. vorhandene Gateways) müssen derart konfiguriert sein, dass es den Clientprogrammen möglich ist, eine TCP-Verbindung zu dem Rechner aufzubauen, auf dem die Serverkomponenten betrieben werden, aufzubauen. Als Mindestvoraussetzung muss es den Clientprogrammen möglich sein, http- und https-Requests an den Standard Server abzusetzen.

Name	OE.14
Ziel	Die Serverkomponente des EVG wird auf einer Plattform mit den nachfolgenden Anforderungen betrieben: - Betriebssystem Microsoft Windows Server 2000 oder Windows Server 2003 - Intel Pentium Prozessor mit mindestens 2 GHz (oder vergleichbar) - mindestens 1 GB RAM - mindestens 2 GB freien Festplattenplatz - Microsoft .NET-Framework 2.0 - mindestens 100 Mbit Netzwerkkarte sowie Internet- oder Intranetanbindung

Name	OE.15
Ziel	Die Clientprogramme des EVG werden auf einer Plattform mit den nachfolgenden Anforderungen betrieben: - PC mit Microsoft Windows 2000 oder Windows XP - Internet-/Intranetzugang mit beliebigem Browser - Prozessor mit mind. 300 MHz

	- mind. 64 MB RAM

Name	**OE.16**
Ziel	Die SSL-Zertifikatsspeicher der Windows-Instanzen, auf dem die Clientprogramme bzw. der Standard Server ausgeführt werden, enthalten ausschließlich Zertifikate von vertrauenswürdigen Zertifizierungsstellen.

Name	**OE.17**
Ziel	Das SSL-Server-Zertifikat ist im Zertifikatsspeicher der Windows-Instanz, auf dem die Server-Komponenten laufen, installiert. Das SSL-Server-Zertifikat ist auf einen Domainnamen ausgestellt, der nachvollziehbar dem Betreiber zugeordnet ist.

Name	**OE.18**
Ziel	Die Zertifizierungsstelle, die das SSL-Serverzertifikat und das Exe-Signatur-Zertifikat ausgestellt hat, ist bei Clients vertrauenswürdig eingestuft.

Name	**OE.19**
Ziel	Die Clientprogramme und der Standard Server sind integer.

Name	**OE.20**
Ziel	Das SSL-Serverzertifikat wird vertraulich und integer gespeichert.

Name	**OE.21**
Ziel	In der SSL-Implementierung der Windows-Instanz, auf der der SSLswitch ausgeführt wird, werden ausschließlich Kombinationen

	von Verschlüsselungsverfahren und Schlüssellängen verwendet, die eine kryptographische Stärke[8] von mindestens 128 Bit aufweisen.

[8] Bei symmetrischen Verfahren entspricht die Schlüssellänge i.d.R. der kryptographischen Stärke. Bei assymetrischen Verfahren müssen deutlich längere Schlüssel eingesetzt werden, um eine äquivalente Stärke zu erreichen.

5 IT-Sicherheitsanforderungen

Dieses Kapitel IT-Sicherheitsanforderungen ist unterteilt in die Unterkapitel:

- Funktionale Sicherheitsanforderungen an den EVG,
- Anforderungen an die Mindeststärke der EVG-Sicherheitsfunktionen,
- Anforderungen an die Vertrauenswürdigkeit des EVG,
- Sicherheitsanforderungen an die IT-Umgebung,
- Sicherheitsanforderungen an die Nicht-IT-Umgebung.

5.1 Funktionale Sicherheitsanforderungen an den EVG

Editorale Bemerkung: In der Ausführung der Operationen in den funktionalen Sicherheitsanforderungen werden die deutschen Bezeichnungen für Objekte etc. verwendet. Dies erfolgt aus Gründen der Zuordnung zu den Bezeichnungen im restlichen Dokument. Auch in der Ausführung der Operation in der Komponente FDP_ACF.1.2 in der Iteration für Session Data, wurde sich entschlossen, diese in der deutschen Sprache zu verfassen.

Bemerkung zur Notation: Die im folgenden benutzten CC-Komponenten (aus [CC]) sind wie folgt benannt: Es wird an vielen Stellen der in [CC_P2] angegebene Name um einen Iterationsbezeichner erweitert, der in Klammern angegeben ist. Die Bedeutung der Iterationsbezeichner ist:

- (COM) Sitzungsdatenstrom
- (SigMac) Message Authentication Code bei der Signalisierung
- (ComMac) Message Authentication Code beim Sitzungsdatenstrom
- (SessData) Inhalt des Sitzungsdatenstroms
- (CfgData) serverseitige Konfigurationsdaten
- (UserData) Daten auf dem Rechner eines Benutzers
- (Berater) Berater
- (Teilnehmer) Teilnehmer
- (TN) Teilnehmer
- (BaraterAdmin) Berater-Administrator
- (Berater Passwort) Berater Passwort
- (Berater-Administrator Passwort) Berater-Administrator Passwort
- (Berater-VS) Anmeldung des Beraters

- (TN-VS) Anmeldung des Teilnehmers
- (BeraterAdmin-Benutzermanager) Anmeldung des Berater-Administrators

FCS_CKM.1 (Com)	**Cryptographic key generation** (symmetric key communication)
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *AES or blowfish*[9] and specified cryptographic key sizes *of at least 128 bit*[10] that meet the following: *[AES] or [BLOWFISH]*[11].

Application Notes: Es wird der symmetrische Schlüssel betrachtet, der beim Datenstromaustausch zwischen Berater und Teilnehmer verwendet wird. Der Schlüssel wird vom Vermittlungsservice generiert und während der Signalisierung an die Clients übermittelt. Die verwendeten Algorithmen mit der dazugehörigen Schlüssellänge sind in den Konfigurationsdateien[12] der Serverkomponente ServerData.dat und ContractData.dat definiert.

FCS_CKM.2 (Com)	**Cryptographic key distribution** (iteration symmetric key communication)
FCS_CKM.2.1	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *negotiate the symmetric key*[13] that meets the following: uses *httpsRpc and ssl*[14].

Application Notes: Der symmetrische Schlüssel für den Datenaustausch zwischen Berater und Teilnehmer wird während der Signalisierung von dem Vermittlungsservice an den Berater und den Teilnehmer im Rahmen des proprietären httpsRpc Protokolls integer (durch httpsRpc) und vertraulich (durch SSL-Tunnel) ausgeliefert.

[9] assignment: cryptographic key generation algorithm

[10] assignment: cryptographic key size

[11] assignment: list of standards

[12] Die Konfigurationsdateien der Serverkomponente liegen in Binärformat vor und können von den Anwendern nicht geändert werden. Die Integrität der Konfigurationsdateien wird durch HMAC-Sicherung sicher gestellt.

[13] assignment: cryptographic key generation method

[14] assignment: list of standards

FCS_COP.1 (Com)	**Cryptographic operation** (iteration symmetric key communication)
FCS_COP.1.1	The TSF shall perform *encrypt user data*[15] in accordance with a specified cryptographic algorithm *AES or blowfish*[16] and specified cryptographic key sizes *at least 128 bit*[17] that meet the following standards: *[AES] or [BLOWFISH]*[18].

Application Notes: Der symmetrische Schlüssel wird für den vertraulichen Datenaustausch zwischen Berater und Teilnehmer verwendet.

FCS_COP.1 (SigMac)	**Cryptographic operation** (iteration mac signalization)
FCS_COP.1.1	The TSF shall perform *MAC generation and verification*[19] in accordance with a specified cryptographic algorithm *HMAC-SHA-1-96*[20] and specified cryptographic key sizes *160 bit*[21] that meet the following: *[RFC2104] and [RFC2404]*[22].

Application Notes: Der hier aufgeführte Algorithmus kommt im Rahmen des proprietären Protokolls httpsRpc zur Anwendung.

FCS_COP.1 (ComMac)	**Cryptographic operation** (iteration mac communication)
FCS_COP.1.1	The TSF shall perform *MAC generation and verification*[23] in accordance with a specified cryptographic algorithm *HMAC-SHA-1-96*[24] and specified cryptographic key sizes *160 bit*[25] that meet the following: *[RFC2104] and [RFC2404]*[26].

[15] assignment: list of cryptographic operations

[16] assignment: cryptographic algorithm

[17] assignment: cryptographic key sizes

[18] assignment: list of standards

[19] assignment: list of cryptographic operations

[20] assignment: cryptographic algorithm

[21] assignment: cryptographic key sizes

[22] assignment: list of standards

[23] assignment: list of cryptographic operations

[24] assignment: cryptographic algorithm

[25] assignment: cryptographic key sizes

[26] assignment: list of standards

Application Notes: Der hier aufgeführte Algorithmus kommt im Rahmen Datenstromaustauschs zwischen Berater und Teilnehmer zur Anwendung.

FDP_ACC.1 (SessData)	**Subset access control** (iteration Session Data)
FDP_ACC.1.1	The TSF shall enforce the *ACCESS Session Data*[27] on *subjects: Einräumender Sitzungspartner, Berechtigter Sitzungspartner, object: Session Data, and operation: read data, and write data*[28].

FDP_ACC.1 (CfgData)	**Subset access control** (iteration Secure Config Data)
FDP_ACC.1.1	The TSF shall enforce the *ACCESS Secure Config Data*[29] on *subjects: Vermittlungsservice, object: files* `ServerData.dat`, *and* `ContractData.dat`, *and operation: read*[30].

FDP_ACC.1 (UserData)	**Subset access control** (iteration Config User Data)
FDP_ACC.1.1	The TSF shall enforce the *ACCESS Config User Data*[31] on *subjects: Benutzermanager, and Vermittlungsservice, object: Benutzerdatei, and operation: read and write data, and read data*[32].

Application Notes: Das Modul Benutzermanager wird ausschließlich von dem Berater-Administrator bedient.

FDP_ACF.1 (SessData)	**Security attribute based access control** (iteration Session Data)

[27] assignment: access control SFP

[28] assigment: list of subjects, objects, and operations among subjects and objects covered by the SFP

[29] assignment: access control SFP

[30] assigment: list of subjects, objects, and operations among subjects and objects covered by the SFP

[31] assignment: access control SFP

[32] assigment: list of subjects, objects, and operations among subjects and objects covered by the SFP

FDP_ACF.1.1 The TSF shall enforce *ACCESS Session Data*[33] to objects based on the following: *subjects: Einräumender Sitzungspartner, Berechtigter Sitzungspartner and objects: session data, the SFP-relevant security attributes: eingeräumte Rechte*[34].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed[35]:

1. *Es werden nur Rechte für die Applikationen gewährt, die der einräumende Sitzungspartner in der Applikationsauswahl definiert hat. Auf alle anderen Daten hat der berechtigte Sitzungspartner keinen Zugriff.*
2. *Die Änderung der Blickrichtung erfolgt nur mit ausdrücklicher Zustimmung des einräumenden Sitzungspartners.*
3. *Durch die Fernsteuerungsrechte können keine weiteren Rechte erworben werden.*
4. *Die Fernsteuerungsrechte können jederzeit durch Betätigen eines Buttons von dem einräumenden Sitzungspartner beendet werden (F11-Taste).*
5. *Die Anzahl der Sitzungspartner wird auf zwei beschränkt. Dies geschieht durch Einrichten einer Sitzungssperre bei dem Vermittlungsservice, sobald zwei Sitzungspartner in eine Sitzung eingetreten sind.*
6. *Die eingeräumten Fernsteuerungsrechte beziehen sich nur auf Fenster von Applikationen, die der Einräumende Sitzungspartner in der Applikationswahl-Schublade freigegeben hat.*
7. *Der EVG bietet dem Benutzer folgende Funktionalität an: Die Fernsteuerungsrechte können vom Sitzungspartner im Watch-Modus angefordert werden. Der einräumende*

[33] assignment: access control SFP

[34] assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes

[35] assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects

Sitzungspartner muss die Fernsteuerungsrechte darauf hin explizit erteilen (Zustimmungsdialog).

8. *Fordert der Berater eine Systemdiagnose des Systems des Teilnehmers durchzuführen, so geschieht dies nur mit Zustimmung seines Sitzungspartners.*

FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[36].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the *none*[37].

FDP_ACF.1 (CfgData)	**Security attribute based access control** (iteration Secure Config Data)
FDP_ACF.1.1	The TSF shall enforce *ACCESS Secure Config Data*[38] to objects based on the following: *subjects: Vermittlungsservice, objects: files* `ServerData.dat`, *and* `ContractData.dat`, *SFP-relevant security attrinbutes: none*[39].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *Eigene sicherheitsrelevanten Konfigurationsdaten: Read*[40].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[41].

[36] assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects

[37] assignment: rules, based on security attributes, that explicitly deny access of subjects to objects

[38] assignment: access control SFP

[39] assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes

[40] assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects

[41] assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects

FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the *none*[42].

FDP_ACF.1 (UserData)	**Security attribute based access control** (iteration Config User Data)
FDP_ACF.1.1	The TSF shall enforce *ACCESS Config User Data*[43] to objects based on the following: *subjects: Berater-Administrator, and Vermittlungsservice, object: Benutzerdatei, and operation: read and write data, and read data, SFP-relevant security attrinbutes: none*[44].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *Benutzerdatei: Read and Write*[45].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[46].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the *none*[47].

FDP_ITT.1	**Basic internal transfer protection**
FDP_ITT.1.1	The TSF shall enforce the *ACCESS Session Data*[48] to prevent the *disclosure, modification*[49] of user data when it is transmitted between physically-separated parts of the TOE.

[42] assignment: rules, based on security attributes, that explicitly deny access of subjects to objects

[43] assignment: access control SFP

[44] assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes

[45] assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects

[46] assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects

[47] assignment: rules, based on security attributes, that explicitly deny access of subjects to objects

[48] assignment: access control SFP(s) and/or information flow control SFP(s)

[49] selection: disclosure, modification, loss of use -> *disclosure, modification*

FIA_AFL.1	**Authentication failure handling**
FIA_AFL.1.1	The TSF shall detect when *three*[50] unsuccessful authentication attempts occur related to *the number of entries of wrong Beraterpasswörter, the number of entries of wrong Sitzungsnummern*[51].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall *deactivate the machine from which the attempts originate for ten minutes*[52].

FIA_ATD.1 (Berater)	**User attribute definition** (iteration Berater)
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: *Beraterpasswort*[53].

FIA_ATD.1 (Teilnehmer)	**User attribute definition** (iteration Teilnehmer)
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: *Sitzungsnummer*[54].

FIA_ATD.1 (BeraterAdmin)	
	User attribute definition (iteration Berater-Administrator)
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: *Passwort des Berater-Administrator*[55].

FIA_SOS.1 (Berater Passwort)

---

[50] selection: [assignment: positive integer number], an administrator configurable positive integer within[assignment: range of acceptable values] -> assignment: positive integer number

[51] assignment: list of authentication events

[52] assignment: list of actions

[53] assignment: list of security attributes

[54] assignment: list of security attributes

[55] assignment: list of security attributes

	Verification of secrets (iteration Berater Passwort)
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet *Passwort Policy*[56].

FIA_SOS.1 (Berater-Administrator Passwort)

	Verification of secrets (iteration Berater-Administrator Passwort)
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet *Passwort Policy*[57].

FIA_UAU.1 (Berater-VS)	**Timing of authentication** (Berater-VS)
FIA_UAU.1.1	The TSF shall allow *to negotiate the authentification method*[58] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Notes: Der Berater (Benutzer) authentifiziert sich mittels Login und Passwort mit Hilfe des Beraterprogramms (Subjekt) bei dem Vermittlungsservice. Die Benutzer-Subjekt-Bindung und damit mittelbar die Authentisierung der Clientkomponente wird mit FIA_USB.1 formuliert. Die Eingabe des Passwortes erfolgt maskiert mit Sternen, dies ist mit FIA_UAU.7 formuliert.

FIA_UAU.1 (TN-VS)	**Timing of authentication** (iteration TN-VS)
FIA_UAU.1.1	The TSF shall allow *to negotiate the authentification method*[59] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

[56] assignment: a defined quality metric

[57] assignment: a defined quality metric

[58] assignment: list of TSF mediated actions

[59] assignment: list of TSF mediated actions

Application Notes: Der Teilnehmer (Benutzer) authentifiziert sich mittels der Sitzungsnummer mit Hilfe des Teilnehmerprogramms (Subjekt) bei dem Vermittlungsservice. Die Benutzer-Subjekt-Bindung und damit mittelbar die Authentisierung der Clientkomponente wird mit FIA_USB.1 formuliert. Für jede Sitzung wird eine neue Sitzungsnummer verwendet, dies wird mit FIA_UAU.4 formuliert.

FIA_UAU.1 (BeraterAdmin-Benutzermanager)

	Timing of authentication (iteration BeraterAdmin-Benutzermanager)
FIA_UAU.1.1	The TSF shall allow *to negotiate the authentification method*[60] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Notes: Der Berater-Administrotor (Benutzer) authentifiziert sich mittels Login und Passwort mit Hilfe des Benutzermanagers (Subjekt) bei dem Vermittlungsservice. Die Eingabe des Passwortes erfolgt maskiert mit Sternen, dies ist mit FIA_UAU.7 formuliert.

FIA_UAU.4	**Single-use authentication mechanisms** (TN-VS)
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to *authentificate Teilnehmer with Sitzungsnummer*[61].

FIA_UAU.7 (Berater)	**Protected authentication feedback** (Berater-VS)
FIA_UAU.7.1	The TSF shall provide only *obscured feedback*[62] to the user while the authentication is in progress.

FIA_UAU.7 (BeraterAdmin)

[60] assignment: list of TSF mediated actions

[61] assignment: identified authentication mechanism(s)

[62] assignment: list of feedback

	Protected authentication feedback (BeraterAdministrator-Benutzermanager)
FIA_UAU.7.1	The TSF shall provide only *obscured feedback*[63] to the user while the authentication is in progress.

FIA_UID.1 (Berater-VS)	**Timing of identification** (iteration Berater-VS)
FIA_UID.1.1	The TSF shall allow *to negotiate the identification method*[64] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.1 (TN-VS)	**Timing of identification** (iteration TN-VS)
FIA_UID.1.1	The TSF shall allow *to negotiate the identification method*[65] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.1 (BeraterAdmin-Benutzermanager)	
	Timing of identification (iteration BeraterAdmin-Benutzermanager)
FIA_UID.1.1	The TSF shall allow *to negotiate the identification method*[66] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

[63] assignment: list of feedback

[64] assignment: list of TSF-mediated actions

[65] assignment: list of TSF-mediated actions

[66] assignment: list of TSF-mediated actions

FIA_USB.1 (Berater)	**User-subject binding** (iteration Beraterkomponente)
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: *Beraterpasswort*[67].
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: *the Berater-Administrator defines the initial password*[68].
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: *first time of use: the Berater has to change the password*[69].

FIA_USB.1 (TN)	**User-subject binding** (iteration Teilnehmerkomponente)
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: *Sitzungsnummer*[70].
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: *none*[71].
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: *none*[72].

FIA_USB.1 (BeraterAdmin)

User-subject binding (iteration Benutzermanager)

[67] [assignment: list of user security attributes

[68] assignment: rules for the initial association of attributes

[69] assignment: rules for the changing of attributes

[70] [assignment: list of user security attributes

[71] assignment: rules for the initial association of attributes

[72] assignment: rules for the changing of attributes

FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: *Passwort des Berater-Administrators*[73].
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: *during the delivery procedure the initial password is defined*[74].
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: *first time of use: the Berater-Administrator has to change the password*[75].

FMT_MSA.1	**Management of security attributes**
FMT_MSA.1.1	The TSF shall enforce the *ACCESS Config User Data*[76] to restrict the ability to *modify, delete*[77] the security attributes *login and password Berater*[78] to *Berater-Administrator*[79].

FMT_SMF.1	**Specification of Management Functions**
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: *Bearbeiten der Benutzerdatei*[80].

FMT_SMR.1	**Security roles** (Berater-Administrator)
FMT_SMR.1.1	The TSF shall maintain the roles *Berater-Administrator*[81].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

[73] [assignment: list of user security attributes

[74] assignment: rules for the initial association of attributes

[75] assignment: rules for the changing of attributes

[76] assignment: access control SFP, information flow control SFP

[77] selection: change_default, query, modify, delete,[assignment: other operations] -> modify, delete

[78] assignment: list of security attributes

[79] assignment: the authorised identified roles

[80] assignment: list of security management functions to be provided by the TSF

[81] assignment: the authorised identified roles

FPT_ITT.1	**Basic internal TSF data transfer protection**
FPT_ITT.1.1	The TSF shall protect TSF data from *modification*[82] when it is transmitted between separate parts of the TOE.

5.2 Anforderungen an die Mindeststärke der EVG-Sicherheitsfunktionen

Der Authentisierungsmechanismus der in der Sicherheitsfunktion SF.I&A (Identification & Authentification) Anwendung findet, beruht auf einem Wahrscheinlichkeits- oder Permutationsmechanismus. Die Stärke dieser Funktionen wird mit SOF-Basic der Common Criteria [CC] angegeben.

5.3 Anforderungen an die Vertrauenswürdigkeit des EVG

Der EVG soll die Anforderungen der Vertrauenswürdigkeitsstufe EAL2 gemäß Teil 3 [CC_P3] der Common Criteria [CC] erfüllen.

5.4 Sicherheitsanforderungen an die IT-Umgebung

Die folgenden Sicherheitsanforderungen an die IT-Umgebung sind Komponenten aus Teil 2 [CC_P2] der der Common Criteria [CC].

FCS_CKM.1 (Env)	**Cryptographic key generation** (IT-environment)
FCS_CKM.1.1	The *IT-environment*[83] shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *as defined in the SSLv3 and TLSv1 standards [SSL3] and [RFC2246]*[84] and specified cryptographic key sizes *128 or 256*[85] that meet the following: *[AES] or [BLOWFISH]*[86].

[82] selection: disclose, modification -> modification

[83] Verfeinerung: TSF -> IT-environment

[84] assignment: cryptographic key generation algorithm

[85] assignment: cryptographic key sizes

[86] assignment: list of standards

Application Notes: Die Verschlüsselung der Daten im Rahmen der Signalisierung erfolgt unterstützt über die IT-Umgebung über SSL.

FPT_ITT.1	**Basic internal TSF data transfer protection**
FPT_ITT.1.1	The *IT-environment*[87] shall protect TSF data from *disclosure, modification*[88] when it is transmitted between separate parts of the TOE.

FCS_COP.1 (PRNG)	**Cryptographic operation** (pseudo number generation)
FCS_COP.1.1	The *IT-environment*[89] shall perform *random number generation*[90] in accordance with a specified cryptographic algorithm *given in [DSS] appendix 3.1 with SHA-1 as function G*[91] and cryptographic key sizes *160 bit*[92] that meet the following: *requirements given in [DSS]*[93].

Application Notes: Der EVG nutzt eine von dem Betriebssystem des Servers zur Verfügung gestellte Funktionalität zur Erzeugung von Zufallszahlen.

5.5 Sicherheitsanforderungen an die Nicht-IT-Umgebung

Es werden die folgenden Sicherheitsanforderungen an die Nicht-IT-Umgebung formuliert:

ANF1	Die Serverkomponente des EVG wird in einem Serverraum einer Behörde oder eines Unternehmens betrieben. Durch geeignete technische und organisatorische Maßnahmen ist sichergestellt, - dass nur Administratoren der Serverkomponente kontrollierten Zugang zum Büro bzw. Arbeitsplatz haben, - dass nur Administratoren der Serverkomponente Zugriff auf andere

[87] Verfeinerung: TSF -> IT-environment

[88] selection: disclosure, modification -> disclosure, modification

[89] Verfeinerung: TSF -> IT-environment

[90] assignment: list of cryptographic operations

[91] assignment: cryptographic algorithm

[92] assignment: cryptographic key sizes

[93] assignment: list of standards

	Repräsentationen der Daten des EVG erhalten, - dass die verwendeten Hardwarekomponenten durch geeignete bauliche oder andere physische Sicherungsmaßnahmen vor Entwendung geschützt sind.
ANF2	Auf dem Server werden datenschutzrechtliche Bestimmungen eingehalten.
ANF3	Die Clientkomponente des EVG wird in einer normalen Büroumgebung einer Behörde oder eines Unternehmens betrieben. Durch geeignete technische und organisatorische Maßnahmen ist sichergestellt, - dass unautorisierte Personen keinen unkontrollierten Zugang zum Büro bzw. Arbeitsplatz haben, - dass unautorisierte Personen keinen Zugriff auf andere Repräsentationen der Daten des EVG erhalten.
ANF4	Die Administration der Clientkomponente des EVG und der zugrunde liegende Systemumgebung wird durch den autorisierten Benutzer oder einer anderen vertrauenswürdigen Person (Administrator der Clientumgebung) gewissenhaft, umsichtig und verantwortungsbewusst durchgeführt und damit den sicheren Betrieb des EVG gewährleistet. Durch die Administration ist insbesondere sicher gestellt: - eine gesicherte Konfiguration der PCs und der Netzinfrastruktur. Dazu zählen der Einsatz von aktuellen Virenscannern, sowie die sichere Konfiguration von Firewalls auf den PCs bzw. innerhalb der jeweiligen Netzinfrastruktur.
ANF5	Die Administration der Serverkomponente des EVG und der zugrunde liegende Systemumgebung wird durch mindestens eine kompetente und vertrauenswürdige Person durchgeführt. Systemadministratoren nehmen ihre Aufgaben gewissenhaft, umsichtig und verantwortungsbewusst wahr. Durch die Administration ist insbesondere sicher gestellt: - eine gesicherte Konfiguration der PCs und der Netzinfrastruktur. Dazu zählen der Einsatz von aktuellen Virenscannern, sowie die sichere Konfiguration von Firewalls auf den PCs bzw. innerhalb der jeweiligen Netzinfrastruktur; - eine regelmäßige Aktualisierung der eingesetzten Software und des Betriebssystems zur Behebung von Sicherheitslücken; - eine regelmäßige Sicherung der (Konfigurations)Daten der EVG-Komponente Standard Server. Über diese Sicherungen können die Daten wieder hergestellt werden.
ANF6	Nur autorisierte Personen erhalten ein Authentisierungsmerkmal.

	Sitzungsnummern werden sicher ausgetauscht. Der Berater ist verantwortlich, die Identität des Sitzungsteilnehmers, der die Sitzungsnummer erhält, festzustellen. Berater erhalten Login und Passwort als Authentisierungsmerkmal.
ANF7	Der Benutzer geht mit dem Produkt gewissenhaft um, insbesondere ist der Benutzer dafür verantwortlich, das die Applikationsauswahl auf das Notwendigste beschränkt ist. (Bildschirmbereiche die für den Fernsteuernden frei gegeben werden)
ANF8	Die mit dem EVG zu verarbeitenden Daten besitzen einen niedrigen Schutzbedarf.
ANF9	Die Aufzeichnungen auf der Berater-Clientkomponente des EVG (Verbindungsdaten) sind integer und vertraulich.
ANF10	Die Aufzeichnungen auf der Server-Komponente des EVG (Verbindungsdaten) sind integer und vertraulich.
ANF11	Die Komponenten des EVG (Client- und Serverkomponente) sind integer und können nicht ausgetauscht werden.
ANF12	Die Konfigurationsdaten, Verbindungsdaten und die Login- und Passwortparameter der Berater werden auf der Serverkomponente des EVG vertraulich und integer verwaltet.
ANF13	Alle vier Programme des EVGs müssen in einem TCP/IP-Netz betrieben werden. Dessen Endsysteme sowie die dazwischen liegenden Transitsysteme (und ggf. vorhandene Gateways) müssen derart konfiguriert sein, dass es den Clientprogrammen möglich ist, eine TCP-Verbindung zu dem Rechner aufzubauen, auf dem die Serverkomponenten betrieben werden, aufzubauen. Als Mindestvoraussetzung muss es den Clientprogrammen möglich sein, http- und https-Requests an den Standard Server abzusetzen.
ANF14	Die Serverkomponente des EVG wird auf einer Plattform mit den nachfolgenden Anforderungen betrieben: - Betriebssystem Microsoft Windows Server 2000 oder Windows Server 2003 - Intel Pentium Prozessor mit mindestens 2 GHz (oder vergleichbar) - mindestens 1 GB RAM - mindestens 2 GB freien Festplattenplatz - Microsoft .NET-Framework 2.0 mindestens 100 Mbit Netzwerkkarte sowie Internet- oder

	Intranetanbindung
ANF15	Die Clientprogramme des EVG werden auf einer Plattform mit den nachfolgenden Anforderungen betrieben: - PC mit Microsoft Windows 2000 oder Windows XP - Internet-/Intranetzugang mit beliebigem Browser - Prozessor mit mind. 300 MHz mind. 64 MB RAM
ANF16	Die SSL-Zertifikatsspeicher der Windows-Instanzen, auf dem die Clientprogramme bzw. der Standard Server ausgeführt werden, enthalten ausschließlich Zertifikate von vertrauenswürdigen Zertifizierungsstellen.
ANF17	Das SSL-Server-Zertifikat ist im Zertifikatsspeicher der Windows-Instanz, auf dem die Server-Komponenten laufen, installiert. Das SSL-Server-Zertifikat ist auf einen Domainnamen ausgestellt, der nachvollziehbar dem Betreiber zugeordnet ist.
ANF18	Die Zertifizierungsstelle, die das SSL-Serverzertifikat und das Exe-Signatur-Zertifikat ausgestellt hat, ist bei Clients vertrauenswürdig eingestuft.
ANF19	Die Clientprogramme und der Standard Server sind integer.
ANF20	Das SSL-Serverzertifikat wird vertraulich und integer gespeichert.
ANF21	Die SSL-Implementierung der Windows-Instanz auf dem der SSlswitch ausgeführt wird, ist so konfiguriert, dass ausschließlich Kombinationen von Verschlüsselungsverfahren und Schlüssellängen verwendet werden, die eine Stärke von mindestens 128 Bit aufweisen.

6 EVG-Übersichtsspezifikation

Dieses Kapitel EVG-Übersichtsspezifikation ist unterteilt in die Unterkapitel:

- EVG-Sicherheitsfunktionen,
- Sicherheitsfunktionen, die auf Wahrscheinlichkeits- oder Permutationsverfahren beruhen und
- Maßnahmen zur Vertrauenswürdigkeit.

6.1 EVG-Sicherheitsfunktionen

zu Netviewer one2one^{TS} Version 5.1 der Netviewer AG bietet dem Betreiber die Sicherheitsfunktionen:

- Data Protection (SF.DP)
- Identification & Authentification (SF.I&A)
- Config Data Protection (SF.CD)
- Access Control (SF.AC)
- Integrity (SF.I)

Die Realisierung der einzelnen Sicherheitsfunktionen wird in den folgenden Unterkapiteln beschrieben. Für alle Sicherheitsfunktionen, für die eine Betrachtung der Stärke der Mechanismen relevant ist, wird in Einklang mit den Sicherheitsanforderungen (siehe Kapitel 5.2) eine Stärke von SOF-Basic erreicht.

6.1.1 SF.DP (DataProtection)

SF.DP.1 Die Daten, die zwischen Beraterprogramm und Teilnehmerprogramm (und umgekehrt) ausgetauscht[94] werden (Sitzungsdatenstrom), sind mit einem symmetrischen Schlüssel `sym_communication` verschlüsselt. Die Verschlüsselung findet im Protokoll PingPong (Zeile 3 in Tabelle 2 in Kapitel 2.9.2) statt. Dabei kommt entweder das Blowfish-Verschlüsselungsverfahren [BLOWFISH] oder das AES-Verschlüsselungsverfahren [AES] zum Einsatz.

[94] Der Austausch des Sitzungsdatenstroms kann optional über den Kommunikationsservice erfolgen.

SF.DP.2 Der Schlüssel `sym_communication` wird vom Vermittlungsservice für jede Sitzung neu generiert und vertraulich und integer an die Clientprogramme der berechtigten Sitzungspartner übermittelt. Dies gilt auch für alle anderen Signalisierungsdaten.

SF.DP.3 Der Austausch des Sitzungsdatenstromes zwischen Berater und Teilnehmer erfolgt optional über einen Kommunikationsservice. Der Kommunikationsservice leitet den Sitzungsdatenstrom ausschließlich weiter und hat keinen Zugriff auf die zur Sicherung eingesetzten Schlüssel. Daher kann er die Inhalte der Kommunikation nicht lesen und nicht verändern.

Die Sicherheitsfunktion SF.DP erfüllt die folgenden funktionalen Sicherheitsanforderungen:

	SF.DP
FCS_CKM.1 (Com)	1
FCS_CKM.2 (Com)	2,3
FCS_COP.1 (Com)	1
FDP_ITT.1	1

6.1.2 SF.I&A (Identification & Authentification)

SF.I&A.1 Der Berater authentifiziert sich mit Benutzername / Passwort bei dem Vermittlungsservice. Die Eingabe des Passwortes erfolgt maskiert, in dem Eingabefeld werden Sternchen anstatt des Passwortes angezeigt. Wird das Beraterpasswort von einem Rechner aus dreimal hintereinander falsch eingegeben, wird dieser Rechner für zehn Minuten für Berater-Authentifizierungen gesperrt.

SF.I&A.2 Der Teilnehmer authentifiziert sich mit der Sitzungsnummer an dem Vermittlungsservice. Die Sitzungsnummer wird pro Sitzung zur Authentifizierung nur einmal verwendet. Wird die Sitzungsnummer von einem Rechner aus dreimal hintereinander falsch eingegeben, wird dieser Rechner für zehn Minuten für Teilnehmer-Authentifizierungen gesperrt.

SF.I&A.3 Die Clientprogramme authentifizieren sich gegenseitig anhand des gleichen Schlüssels `hmac_communication`, den sie jeweils von dem Vermittlungsservice mitgeteilt bekommen haben. Die HMAC-Bildung findet im Protokoll PingPong (Zeile 3 in Tabelle 2 in Kapitel 2.9.2) statt.

SF.I&A.4 Vor der Authentifizierung der Beraters, des Teilnehmers und des Berater-Administrators sind keine anderen Aktionen möglich.

SF.I&A.5 Das Modul „Benutzermanager" des Standard Servers verwaltet Benutzername/Passwort der Berater in einer Benutzerdatei. Dabei werden die persönlichen Passwörter nicht im Klartext gespeichert, sondern als RipneMD-256-Hashwerte [RIPEMD].

SF.I&A.6 Die Clientprogramme authentifizieren sich gegenüber dem Vermittlungsservice anhand des programmindividuellen Programmschlüssels im Rahmen des Protokolls HttpsRpc (Zeile 2 in Tabelle 2 in Kapitel 2.9.2). Dieser Programmschlüssel ist Teil der in die Clientprogramme fest eingebundenen sicherheitsrelevanten Konfigurationsdaten.

SF.I&A.7 Der Berater-Administrator authentifiziert sich mit Benutzername / Passwort bei dem Vermittlungsservice, bevor er das Modul „Benutzermanager" verwenden kann. Die Eingabe des Passwortes erfolgt maskiert, in dem Eingabefeld werden Sternchen anstatt des Passwortes angezeigt.

SF.I&A.8 Wählen Berater oder Berater-Administrator neue Passworte, so werden diese auf ihre Güte verifiziert.

Die Sicherheitsfunktion SF.I&A erfüllt die folgenden funktionalen Sicherheitsanforderungen:

	SF.I&A
FCS_CKM.1 (Com)	3
FCS_COP.1 (Com)	3
FDP_ACC.1 (UserData)	1,4,5,7
FDP_ACF.1 (UserData)	1,4,5,7
FIA_AFL.1	1,2
FIA_ATD.1 (Berater)	1,6
FIA_ATD.1 (Teilnehmer)	2,6
FIA_ATD.1 (BeraterAdmin)	7
FIA_SOS.1 (Berater Passwort)	8
FIA_SOS.1 (Berater-Administrator Passwort)	8
FIA_UAU.1 (Berater-VS)	4
FIA_UAU.1 (TN-VS)	4
FIA_UAU.1 (BeraterAdmin-Benutzermanager)	4
FIA_UAU.4	2
FIA_UAU.7 (Berater)	1
FIA_UAU.7 (BeraterAdmin)	7
FIA_UID.1 (Berater-VS)	4
FIA_UID.1 (TN-VS)	4
FIA_UID.1 (BeraterAdmin-Benutzermanager)	4

FIA_USB.1 (Berater)	1,6
FIA_USB.1 (TN)	2,6
FIA_USB.1 (BeraterAdmin)	7
FMT_MSA.1	5,7
FMT_SMF.1	7
FMT_SMR.1	7

6.1.3 SF.CD (Config Data Protection)

SF.CD.1 Der Vermittlungsservice liest die Konfigurationsdateien `ServerData.dat` und `ContractData.dat` nur dann ein, wenn sie nicht verändert wurden.

Die Sicherheitsfunktion SF.CD erfüllt die folgenden funktionalen Sicherheitsanforderungen:

	SF.CD
FCS_COP.1 (ComMac)	1
FDP_ACC.1 (CfgData)	1
FDP_ACF.1 (CfgData)	1

6.1.4 SF.AC (Access Control)

SF.AC.1 Der EVG bietet dem Benutzer folgende Funktionalität an: In der Applikationsauswahl kann der einräumende Sitzungspartner definieren, welche Applikationen dem Sitzungspartner angezeigt werden.

SF.AC.2 Der EVG bietet dem Benutzer folgende Funktionalität an: Die Änderung der Blickrichtung erfolgt nur mit ausdrücklicher Zustimmung des einräumenden Sitzungspartners. Hierzu wird dem Benutzer ein Pop-Up Fenster angezeigt, welches er entsprechend bestätigen muss.

SF.AC.3 Der EVG bietet dem Benutzer folgende Funktionalität an: Die eingeräumten Fernsteuerungsrechte können jederzeit durch Betätigen der Sicherheitstaste (F11-Taste) oder der Schaltfläche „off" in der Benutzeroberfläche von dem einräumenden Sitzungspartner beendet werden.

SF.AC.4 Der EVG gewährleistet, dass durch die Fernsteuerungsrechte keine weiteren Rechte erworben werden können.

SF.AC.5 Die Anzahl der Sitzungspartner wird auf zwei beschränkt: In einer Sitzung befinden sich maximal ein Berater und ein Teilnehmer.

SF.AC.6 Der Berater initiiert die Sitzung. Der EVG startet im Show-Modus für den Berater.

SF.AC.7 Der EVG bietet dem Benutzer folgende Funktionalität an: Die Übertragung einer Datei von oder zu dem Sitzungspartner im Show-Modus erfolgt zum fernsteuernden Sitzungspartner nur mit ausdrücklicher Zustimmung des einräumenden Sitzungspartners. Hierzu wird dem Benutzer ein Pop-Up Fenster angezeigt, welches er entsprechend bestätigen muss.

SF.AC.8 Der EVG bietet dem Benutzer folgende Funktionalität an: Die eingeräumten Fernsteuerungsrechte beziehen sich nur auf Fenster von Applikationen, die der Einräumende Sitzungspartner in der Applikationsauswahl-Schublade freigegeben hat.

SF.AC.9 Der EVG bietet dem Benutzer folgende Funktionalität an: Die Fernsteuerungsrechte können vom Sitzungspartner im Watch-Modus angefordert werden. Der einräumende Sitzungspartner muss die Fernsteuerungsrechte darauf hin explizit erteilen (Zustimmungsdialog).

Die Sicherheitsfunktion SF.AC erfüllt die folgenden funktionalen Sicherheitsanforderungen:

	SF.AC
FDP_ACC.1 (SessData)	1 bis 9
FDP_ACF.1 (SessData)	1 bis 9

6.1.5 SF.I (Integrity)

SF.I.1 Die Unverletztheit der Integrität des Sitzungsdatenstroms wird bei dem Empfangenden Clientprogramm geprüft. Liegt eine Manipulation der verschlüsselten Daten vor, so wird die Sitzung mit einem Fehler abgebrochen. Dazu wird ein Message-Authentication-Code HMAC (siehe [RFC2104] und [RFC2404]) mit dem Schlüssel `hmac_communication` verwendet. Diese Integritätsprüfung findet in den Protokollen PingPong (Zeile 3 in Tabelle 2 in Kapitel 2.9.2) und PingPong-Transport (Zeile 4 in Tabelle 2 in Kapitel 2.9.2) statt.

SF.I.2 Die Daten, die zur Signalisierung mit dem von dem Beraterprogramm oder dem Teilnehmerprogramm an den Vermittlungsservice übertragen werden (und umgekehrt), sind mit einem Message-Authentication-Code HMAC (siehe [RFC2104] und [RFC2404]) zur Integritätssicherung ausgestattet. Diese Integritätsprüfung findet im Protokolle HttpsRpc (Zeile 2 in Tabelle 2 in Kapitel 2.9.2) statt. Das zur Integritätsprüfung verwendete Shared Secret wird integer und vertraulich über das Protokoll HttpsRpc (über SSL; Zeile 2 und Zeile 5 in Tabelle 2 in Kapitel 2.9.2)) ausgehandelt.

Die Sicherheitsfunktion SF.I erfüllt die folgenden funktionalen Sicherheitsanforderungen:

	SF.I
FCS_COP.1 (SigMac)	2
FCS_COP.1 (ComMac)	1,2
FDP_ITT.1	1
FPT_ITT.1	2

6.2 Sicherheitsfunktionen, die auf Wahrscheinlichkeits- oder Permutationsverfahren beruhen

Die folgende Tabelle führt die Sicherheitsfunktionen auf, welche auf Wahrscheinlichkeits- oder Permutationsverfahren beruhen:

Sicherheitsfunktionen	Verfahren	Algorithmus	Stärke
SF.DP.1	Blockchiffre/CBC	AES, [AES]	128 bis 256 Bit
siehe AES-Algorithmus	Blockchiffre/CBC	Blowfish, [BLOWFISH]	128 bis 256 Bit
SF.CD.1, SF.I.1, SF.I.2	HMAC	HMAC-SHA1-96, [RFC2104] [RFC2404]	96 Bit
siehe HMAC-Verfahren	Kryptographischer Hash	SHA-1 [RFC3174]	160 Bit
SF.I&A.5	Kryptographischer Hash	RipeMD-256 [RIPEMD]	256 Bit
SF.I&A.1, SF.I&A.2, SF.I&A.3	Shared Secret		Beraterpasswort: 47 Bit [ln(62^8)/ln2] Sitzungsnummer: 30 Bit [ln(10^9)/ln2] Programm-schlüssel: 128 Bit

SF.I.2	KDF	PKCS#12, [PKCS12]	>128 Bit
SF.DP.2, SF.I.2	HttpsRpc/SSL	[SSL3]	>=128 Bit

Tabelle 9 Gegenüberstellung der von den Sicherheitsfunktionen verwendeten Verfahren, Algorithmen sowie der effektiven Stärke.

6.3 Maßnahmen zur Vertrauenswürdigkeit

Im Folgenden wird aufgezeigt, welche Maßnahmen zur Sicherung der Vertrauenswürdigkeit in der Entwicklung getroffen wurden, um die in den Common Criteria [CC] EAL2 spezifizierten Anforderungen an die Vertrauenswürdigkeit zu erfüllen.

KOMPONENTEN	BEZEICHNUNGEN
Vertrauenswürdigkeitsklasse Konfigurationsmanagement	
ACM_CAP.2	Konfigurationsteile
Vertrauenswürdigkeitsklasse Auslieferung und Betrieb	
ADO_DEL.1	Auslieferungsprozeduren
ADO_IGS.1	Installations-, Generierungs- und Anlaufprozeduren
Vertrauenswürdigkeitsklasse Entwicklung	
ADV_FSP.1	Informelle funktionale Spezifikation
ADV_HLD.1	Beschreibender Entwurf auf hoher Ebene
ADV_RCR.1	Informeller Nachweis der Übereinstimmung
Vertrauenswürdigkeitsklasse Handbücher	
AGD_ADM.1	Administratorhandbuch
AGD_USR.1	Benutzerhandbuch
Vertrauenswürdigkeitsklasse Testen	
ATE_COV.1	Nachweis der Testabdeckung
ATE_FUN.1	Funktionales Testen
ATE_IND.2	Unabhängiges Testen – Stichprobenartig
Vertrauenswürdigkeitsklasse Schwachstellenbewertung	
AVA_SOF.1	Stärke der EVG-Sicherheitsfunktionen
AVA_VLA.1	Schwachstellenanalyse des Entwicklers

7 PP-Postulate

Der EVG stützt sich nicht auf ein Schutzprofil (Protection Profile, PP). Daher wird für den EVG kein PP-Postulat abgegeben.

7.1 PP-Verweis

Nicht zutreffend.

7.2 PP-Anpassung

Nicht zutreffend.

7.3 PP-Ergänzungen

Nicht zutreffend.

8 Erklärung

Dieses Kapitel Erklärung ist unterteilt in die Unterkapitel:

- Erklärung der Sicherheitsziele (aus Kapitel 4),
- Erklärung der Sicherheitsanforderungen (aus Kapitel 5),
- Erklärung der EVG-Übersichtsspezifikation (aus Kapitel 6),
- Erklärung der PP-Postulate (aus Kapitel 7).

8.1 Erklärung der Sicherheitsziele

8.1.1 Zuordnung der Sicherheitsziele zur EVG-Sicherheitsumgebung

In der folgenden Tabelle wird für jedes Sicherheitsziel für den EVG und für jedes Sicherheitsziel für die Umgebung angegeben, welche Bedrohungen abgewehrt werden sollen, welche Sicherheitspolitiken erfüllt werden sollen und welche Annahmen berücksichtigt werden sollen.

Sicherheitsziel	Bedrohung	OSP	Annahme
O.Auth.1	T.Client.Auth.1, T.Client.Auth.2		
O.Auth.2	T.Integrity.2		
O.Auth.3	T.Integrity.4		
O.Privacy.1	T.Privacy.1		
O.Privacy.2	T.Privacy.1		
O.Integrity.1	T.Integrity.1		
O.Integrity.2	T.Integrity.3		
O.Rights.1	T.Client.Rights.1		
O.Rights.2	T.Client.Rights.1		
O.Rights.3	T.Client.Rights.1		
O.Rights.4	T.Client.Rights.1		
O.Rights.5	T.Client.Rights.1		
O.Server.Cfg.1	T.Server.Cfg.1		
OE.1			A.PHY.Server.1
OE.2		P.Datenschutz	
OE.3			A.PHY.Client.1
OE.4			A.PER.1
OE.5			A.PER.2
OE.6			A.PER.3 und A.PER.5
OE.7			A.PER.4

Sicherheitsziel	Bedrohung	OSP	Annahme
OE.8			A.USE.1
OE.9	T.Berater.Log.1		
OE.10	T.Server.Log.1		
OE.11	T.Integrity.2		
OE.12	T.Server.Cfg.1		
OE.13			A.NET.1
OE.14			A.Plattform.Server
OE.15			A.Plattform.Client
OE.20	T.Server.Cfg.2		
OE.16			A.NET.4
OE-IT.1	T.Server.Cfg.2		
OE-IT.2			A.PRNG.Server
OE.17			A.NET.2
OE.18			A.NET.3
OE-IT.3	T.Privacy.3, T.Client.Privacy.2		
OE.19	T.Integrity.2		
OE.21			A.NET.5

Tabelle 10: Zuordnung der Sicherheitsziele zur EVG-Sicherheitsumgebung

8.1.2 Notwendigkeit der Sicherheitsziele

Aus der Tabelle 10 ist ersichtlich, dass jedes Sicherheitsziel mindestens eine Bedrohung, eine Politik oder eine Annahme adressiert.

8.1.3 Abwehr der Bedrohungen

Aus der Tabelle 10 ist ersichtlich, dass jede Bedrohung von mindestens einem Sicherheitsziel adressiert wird.

(Die Gesamtheit der Bedrohungen ist also vollständig abgedeckt.)

Nachweis für jede Bedrohung im Einzelnen:

Die Bedrohung **T.Cient.Auth.1** behandelt Angriffe, bei denen unautorisierte Personen in eine Sitzung eintreten und so unberechtigten Zugriff auf Daten der Sitzungspartner haben.

In dem Sicherheitsziel O.Auth.1 wird definiert, dass nur autorisierte Benutzer als Teilnehmer in eine Sitzung eintreten. Dieses Sicherheitsziel ist also hinreichend für T.Client.Auth.1.

Die Bedrohung **T.Cient.Auth.2** behandelt Szenarien, in denen unautorisierte Personen die Sitzung als Berater eröffnet und so unberechtigten Zugriff auf Daten des Sitzungspartners erlangt.

In dem Sicherheitsziel O.Auth.1 wird definiert, dass nur autorisierte Benutzer als Teilnehmer in eine Sitzung eintreten. Dieses Sicherheitsziel ist also hinreichend für T.Client.Auth.2.

Die Bedrohung **T.Berater.Log.1** behandelt Angriffe, bei denen ein Angreifer unberechtigt Verbindungsdaten bei der Clientkomponente des EVG liest oder manipuliert.

In dem Sicherheitsziel OE.9 wird definiert, dass die Verbindungsdaten der Clientkomponente des EVG integer und vertraulich sind. Dieses Sicherheitsziel ist also hinreichend für T.Berater.Log.1.

Die Bedrohung **T.Server.Log.1** behandelt Angriffe, bei denen ein Angreifer unberechtigt Verbindungsdaten bei der Serverkomponente des EVG liest oder manipuliert.

In dem Sicherheitsziel OE.10 wird definiert, dass die Verbindungsdaten der Serverkomponente des EVG integer und vertraulich sind. Dieses Sicherheitsziel ist also hinreichend für T.Server.Log.1.

Die Bedrohung **T.Privacy.1** behandelt Angriffe, bei denen eine unautorisierte Person unberechtigterweise Kenntnis von Daten der Sitzungspartner erhält.

In dem Sicherheitsziel O.Privacy.1 wird definiert, dass der zwischen den Sitzungspartnern übermittelte Sitzungsdatenstrom vertraulich und von Dritten nicht einsehbar ist. Als Dritter wird in diesem Zusammenhang auch der optional eingesetzte Kommunikationsservice interpretiert, der keine Kenntnis des Sitzungsdatenstroms erlangt.

In dem Sicherheitsziel O.Privacy.2 wird definiert, dass nicht mehr als zwei Sitzungspartner an einer Sitzung teilnehmen können.

Die Sicherheitsziele O.Privacy.1 und O.Privacy.2 sind also hinreichend für T.Privacy.1.

Die Bedrohung **T.Client.Privacy.2** behandelt Angriffe, bei denen eine unautorisierte Person in den Besitz eines kryptographischen Schlüssels gerät und damit kodierte Nachrichten entschlüsseln kann.

In dem Sicherheitsziel OE-IT.3 ist definiert, dass die zwischen den EVG-Komponenten übermittelten Signalisierungsdaten vertraulich und von Dritten nicht einsehbar sind. Kryptographische Schlüssel sind Teil der Signalisierungsdaten.

Dieses Sicherheitsziel ist also hinreichend für T.Client.Privacy.2.

Die Bedrohung **T.Privacy.3** behandelt Angriffe, bei denen ein Angreifer unberechtigterweise Kenntnis von Daten erhält, die die Sitzungspartner über die Clientkomponenten mit der Vermittlungsservice-Rolle austauschen (Signalisierungsdaten).

In dem Sicherheitsziel OE-IT.3 ist definiert, dass die zwischen den EVG-Komponenten übermittelten Signalisierungsdaten vertraulich und von Dritten nicht einsehbar sind.

Dieses Sicherheitsziel ist also hinreichend für T.Privacy.3.

Die Bedrohung **T.Integrity.1** behandelt Angriffe, bei denen ein Angreifer die Sitzung durch Veränderung des Sitzungsdatenstroms modifiziert oder ersetzt. Dem Sitzungspartner werden falsche Daten übermittelt.

In dem Sicherheitsziel O.Integrity.1 ist definiert, dass der zwischen den Sitzungspartnern übermittelte Sitzungsdatenstrom integer ist.

Dieses Sicherheitsziel ist hinreichend für T.Integrity.1.

Die Bedrohung **T.Integrity.2** behandelt Angriffe, bei denen ein Angreifer eine EVG-Komponente unbemerkt modifiziert.

In dem Sicherheitsziel O.Auth.2 wird definiert, dass ausschließlich authentifizierte Clientprogramme Serverkomponenten nutzen können.

In dem Sicherheitsziel OE.11 wird definiert, dass die Komponenten des EVG (Client- und Serverkomponente) integer sind und nicht ausgetauscht werden können.

In dem Sicherheitsziel OE.19 wird definiert, dass die Komponenten integer sind und nicht ausgetauscht werden können. Das Sicherheitsziel ist damit hinreichend für T.Integrity.2.

Die Sicherheitsziele O.Auth.2, OE.11 und OE.19 sind damit geeignet der Bedrohung für T.Integrity.2 zu entgegnen.

Die Bedrohung **T.Integrity.3** behandelt Angriffe, bei denen ein Angreifer unbemerkt Signalisierungsdaten manipuliert, die zwischen den EVG-Clientkomponenten und der Serverkomponente ausgetauscht werden.

In dem Sicherheitsziel O.Integrity.2 ist definiert, dass die zwischen den EVG-Komponenten übermittelten Signalisierungsdaten integer sind.

Dieses Sicherheitsziel ist also hinreichend für T.Integrity.3.

Die Bedrohung **T.Integrity.4** behandelt Angriffe, bei denen ein Angreifer unautorisiert den Benutzermanager bedient um die Benutzerdatei zu editieren.

In dem Sicherheitsziel O.AUTH.3 ist definiert, dass ausschließlich authentifizierte Berater-Administratoren mit Hilfe des Benutzermanagers die Benutzerdatei verwalten können.

Dieses Sicherheitsziel ist also hinreichend für T.Integrity.4.

Die Bedrohung **T.Client.Rights.1** behandelt Angriffe, in denen der autorisierte Benutzer Rechte erlangt, die der einräumende Sitzungspartner nicht in diesem Umfang definiert hat oder ohne dass der einräumende Sitzungspartner Wissen hiervon erlangt hat.

In dem Sicherheitsziel O.Rights.1 wird definiert, dass die Änderung der Blickrichtung während einer Sitzung nur mit ausdrücklicher Zustimmung des einräumenden Sitzungspartners erfolgen kann.

In dem Sicherheitsziel O.Rights.2 wird definiert, dass dem Sitzungspartner nur die Applikationen angezeigt werden, die der einräumende Sitzungspartner in der Applikationsauswahl definiert hat.

In dem Sicherheitsziel O.Rights.3 wird definiert, dass die Fernsteuerung nur mit ausdrücklicher Zustimmung des einräumenden Sitzungspartners erfolgen kann. Die Fernsteuerung kann nur eingeräumt werden, wenn zuvor die Blickrichtung entsprechend der einräumenden Fernsteuerungsrechte geändert wurde. Die Fernsteuerung kann nur auf Applikationen erfolgen, die im Rahmen der Blickrichtungsänderung über die Applikationswahl definiert wurden. Während einer Sitzung kann der einräumende Sitzungspartner seinem Kommunikationspartner die Fernsteuerungsrechte jederzeit durch Betätigen der Sicherheitstaste (Taste F11) entziehen. Werden vom Sitzungspartner im Watch-Modus die Fernsteuerungsrechte angefordert, muss der einräumende Sitzungspartner die Fernsteuerungsrechte im Rahmen eines Zustimmungsdialoges explizit erteilen. Fordert der Berater eine Systemdiagnose des Systems des Teilnehmers durchzuführen, so geschieht dies nur mit Zustimmung seines Sitzungspartners.

In dem Sicherheitsziel O.Rights.4 wird definiert, dass sich der Kommunikationspartner des einräumenden Sitzungspartners mittels der Fernsteuerungsrechte keine weitere Rechte selbst einräumen kann.

In dem Sicherheitsziel O.Rights.5 wird definiert, dass die Funktion ‚Dateitransfer per Drag & Drop' nur mit ausdrücklicher Zustimmung des Sitzungspartners benutzt werden kann, der die Funktion nicht initiiert hat.

Alle Sicherheitsziele O.Rights.1 bis O.Rights.5 dienen dazu, dass der Benutzer nur Rechte erlangt, die der einräumende Sitzungspartner in diesem Umfang definiert hat und dass der einräumende Sitzungspartner Wissen hiervon erlangt hat.

In O.Privacy.2 wird definiert, dass die Anzahl der Sitzungspartner auf zwei beschränkt ist.

Die Sicherheitsziele O.Rights.1 bis O.Rights.5 und O.Privacy.2 sind damit hinreichend für T.Client.Rights.1.

Die Bedrohung **T.Server.Cfg.1** behandelt Angriffe, bei denen ein Angreifer Konfigurations- oder Verbindungsdaten liest oder manipuliert, nachdem er Zugriff auf den Serverrechner erlangt hat.

In dem Sicherheitsziel O.Server.Cfg.1 ist definiert, dass die Konfigurationsdateien auf der Serverkomponente nur dann eingelesen werden, wenn sie integer sind.

In dem Sicherheitsziel OE.12 ist definiert, dass die Konfigurationsdaten und Verbindungsdaten auf der Serverkomponente des EVG vertraulich verwaltet sind.

Die Sicherheitsziele sind damit hinreichend für T.Server.Cfg.1.

Die Bedrohung **T.Server.Cfg.2** betrachtet das Szenario, dass ein Angreifer die Identität der Serverkomponenten vortäuscht.

Im Sicherheitsziel OE.20 ist definiert, dass das SSL-Serverzertifikat vertraulich und integer gespeichert wird.

Im Sicherheitsziel OE-IT.1 ist definiert, dass die SSL-Implementierung des Betriebssystems, auf dem die Serverkomponenten und die Clientprogramme ausgeführt werden, spezifikationsgemäß (TLS 1.0 [RFC2246] oder SSL 3.0 [SSL3]) arbeitet.

Die Sicherheitsziele OE.20 und OE-IT.1 sind damit geeignet der Bedrohung für T.Server.Cfg.2 zu entgegnen.

8.1.4 Erfüllung der Sicherheitspolitiken

Aus der Tabelle 10 ist ersichtlich, dass jede Sicherheitspolitik von mindestens einem Sicherheitsziel adressiert wird.

(Die Gesamtheit der Sicherheitspolitiken ist also vollständig abgedeckt.)

Nachweis für jede Sicherheitspolitik im Einzelnen:

Die Politik **P.Datenschutz** (Einhaltung der datenschutzrechtlichen Bestimmungen) legt fest, dass auf dem Server datenschutzrechtliche Bestimmungen eingehalten werden.

Dies entspricht dem Sicherheitsziel OE.2. Dieses Sicherheitsziel ist also hinreichend für P.Datenschutz.

8.1.5 Berücksichtigung der Annahmen

Aus der Tabelle 10 ist ersichtlich, dass jede Annahme von mindestens einem Sicherheitsziel adressiert wird.

(Die Gesamtheit der Annahmen ist also vollständig abgedeckt.)

Nachweis für jede Annahme im Einzelnen:

Die Annahme **A.USE.1** behandelt eine Vorgabe, bei der zugrunde gelegt wird, dass die mit dem EVG zu verarbeitenden Daten einen niedrigen Schutzbedarf besitzen.

Dies entspricht exakt dem Ziel OE.8.

Die Annahme **A.PHY.Server.1** behandelt eine Vorgabe, bei der zugrunde gelegt wird, dass die Serverkomponente des EVG in einem Serverraum einer Behörde oder eines Unternehmens betrieben wird. Dabei wird davon ausgegangen, dass es durch geeignete technische und organisatorische Maßnahmen sichergestellt ist,

- dass unautorisierte Personen keinen unkontrollierten Zugang zum Serverraum haben,
- dass unautorisierte Personen keinen Zugriff auf andere Repräsentationen der Daten des EVG erhalten,
- dass die verwendeten Hardwarekomponenten durch geeignete bauliche oder andere physische Sicherungsmaßnahmen vor Entwendung geschützt sind.

Dies entspricht exakt dem Ziel OE.1.

Die Annahme **A.PHY.Client.1** behandelt eine Vorgabe, bei der zugrunde gelegt wird, dass die Clientkomponente des EVG in einer normalen Büroumgebung einer Behörde oder eines Unternehmens betrieben wird. Dabei wird davon ausgegangen, dass es durch geeignete technische und organisatorische Maßnahmen sichergestellt ist,

- dass unautorisierte Personen keinen unkontrollierten Zugang zum Büro bzw. Arbeitsplatz haben,
- dass unautorisierte Personen keinen Zugriff auf andere Repräsentationen der Daten des EVG erhalten.

Dies entspricht exakt dem Ziel OE.3.

Die Annahme **A.PER.1** behandelt eine Vorgabe, bei der zugrunde gelegt wird, dass die Administration der Clientkomponente des EVG und der zugrunde liegende Systemumgebung durch den autorisierten Benutzer oder einer anderen vertrauenswürdigen Person (Administrator der Clientumgebung) gewissenhaft, umsichtig und verantwortungsbewusst durchgeführt wird und damit den sicheren Betrieb des EVG gewährleistet.

Durch die Administration ist insbesondere sicher gestellt:

- eine gesicherte Konfiguration der PCs und der Netzinfrastruktur ausgegangen. Dazu zählen der Einsatz von aktuellen Virenscannern, sowie die sichere Konfiguration von Firewalls auf den PCs bzw. innerhalb der jeweiligen Netzinfrastruktur.

Dies entspricht exakt dem Ziel OE.4.

Die Annahme **A.PER.2** behandelt eine Vorgabe, bei der zugrunde gelegt wird, dass die Administration der Serverkomponente des EVG und der zugrunde liegende Systemumgebung durch mindestens eine kompetente und vertrauenswürdige Person durchgeführt wird. Systemadministratoren nehmen ihre Aufgaben gewissenhaft, umsichtig und verantwortungsbewusst wahr.

Durch die Administration ist insbesondere sicher gestellt:

- eine gesicherte Konfiguration der PCs und der Netzinfrastruktur ausgegangen. Dazu zählen der Einsatz von aktuellen Virenscannern, sowie die sichere Konfiguration von Firewalls auf den PCs bzw. innerhalb der jeweiligen Netzinfrastruktur;
- eine regelmäßige Aktualisierung der eingesetzten Software und des Betriebssystems zur Behebung von Sicherheitslücken;
- eine regelmäßige Sicherung der (Konfigurations)Daten der EVG-Komponente Standard Server. Über diese Sicherungen können die Daten wieder hergestellt werden.

Dies entspricht exakt dem Ziel OE.5.

Die Annahme **A.PER.3** behandelt eine Vorgabe, bei der zugrunde gelegt wird, dass die Sitzungsnummern von dem Berater sicher an den Teilnehmer weiter gegeben werden.

Der Berater ist verantwortlich, die Identität des Sitzungsteilnehmers, der die Sitzungsnummer erhält, festzustellen.

Dies entspricht dem Ziel OE.6.

Die Annahme **A.PER.4** behandelt eine Vorgabe, bei der zugrunde gelegt wird, dass der Benutzer mit dem Produkt gewissenhaft umgeht, insbesondere ist der Benutzer dafür verantwortlich, dass die Applikationsauswahl auf das Notwendigste beschränkt ist. (Bildschirmbereiche die für den Fernsteuernden frei gegeben werden)

Dies entspricht exakt dem Ziel OE.7.

Die Annahme **A.PER.5** behandelt eine Vorgabe, bei der zugrunde gelegt wird, dass der Berater-Administrator den EVG im Rahmen ihrer Aufgabenerfüllung nutzt. Er gibt die Beraterkontendaten (Benutzername und Passwort) sicher an due autorisierten Berater weiter.

Dies entspricht dem Ziel OE.6.

Die Annahme **A.NET.1** behandelt eine Vorgabe, wonach alle vier Komponenten des EVGs in einem TCP/IP-Netz betrieben werden müssen. Dessen Endsysteme sowie die

dazwischen liegenden Transitsysteme (und ggf. vorhandene Gateways) müssen derart konfiguriert sein, dass es den Clientprogrammen möglich ist, eine TCP-Verbindung zum Standard Server aufzubauen. Als Mindestvoraussetzung muss es den Clientprogrammen möglich sein, http- und https-Requests an den Standard Server abzusetzen.

Dies entspricht exakt dem Ziel OE.13.

Die Annahme **A.NET.2** behandelt die Vorgabe, dass das SSL-Server-Zertifikat im Zertifikatsspeicher der Windows-Instanz, auf dem die Server-Komponenten laufen, installiert ist. Das SSL-Server-Zertifikat ist auf einen Domainnamen ausgestellt, der nachvollziehbar dem Betreiber zugeordnet ist.

Dies entspricht exakt dem Ziel OE.17.

Die Annahme **A.NET.3** behandelt die Vorgabe, dass die Zertifizierungsstelle, die das SSL-Serverzertifikat und das Exe-Signatur-Zertifikat ausgestellt hat, bei Clients vertrauenswürdig eingestuft ist.

Dies entspricht exakt dem Ziel OE.18.

Die Annahme **A.NET.4** behandelt die Vorgabe, dass die SSL-Zertifikatsspeicher der Windows-Instanzen, auf dem die Clientprogramme bzw. der Standard Server ausgeführt werden, ausschließlich Zertifikate von vertrauenswürdigen Zertifizierungsstellen enthalten.

Dies entspricht exakt dem Ziel OE.16.

Die Annahme **A.NET.5** behandelt die Vorgabe, dass die SSL-Implementierung der Windows-Instanz auf dem der SSlswitch ausgeführt wird, so konfiguriert ist, dass ausschließlich Kombinationen von Verschlüsselungsverfahren und Schlüssellängen verwendet werden, die eine Stärke von mindestens 128 Bit aufweisen.

Dies entspricht exakt dem Ziel OE.21.

Die Annahme **A.Plattform.Server** behandelt eine Vorgabe, wonach die Server-Komponente des EVG auf einer Plattform mit den nachfolgenden Anforderungen betrieben wird:

- Betriebssystem Microsoft Windows Server 2000 oder Windows Server 2003
- Intel Pentium Prozessor mit mindestens 2 GHz (oder vergleichbar)
- mindestens 1 GB RAM
- mindestens 2 GB freien Festplattenplatz

- Microsoft .NET-Franework2.0
- mindestens 100 Mbit Netzwerkkarte sowie Internet- oder Intranetanbindung

Dies entspricht exakt dem Ziel OE.14.

Die Annahme **A.Plattform.Client** behandelt eine Vorgabe, wonach die Clientkomponenten des EVG auf einer Plattform mit den nachfolgenden Anforderungen betrieben werden:

- PC mit Microsoft Windows 2000 oder Windows XP
- Internet-/Intranetzugang mit beliebigem Browser
- Prozessor mit mind. 300 MHz
- mind. 64 MB RAM

Dies entspricht exakt dem Ziel OE.15.

Die Annahme **A.PRNG.Server** fordert, dass der Pseudozufallszahlengenerator (PRNG) des Betriebssystems, auf dem die Serverkomponenten und die Clientprogramme ausgeführt werden, kryptographisch sichere Zufallszahlen liefert.

Dies entspricht exakt dem Ziel OE-IT.2.

8.2 Erklärung der Sicherheitsanforderungen

Dieses Kapitel Erklärung der Sicherheitsanforderungen ist unterteilt in die Unterkapitel:

- Erklärung der funktionalen Sicherheitsanforderungen an den EVG,
- Erklärung der Anforderungen an die Mindeststärke der EVG-Sicherheitsfunktionen,
- Erklärung der Anforderungen an die Vertrauenswürdigkeit des EVG,
- Erklärung der Sicherheitsanforderungen an die IT-Umgebung,
- Erklärung der Sicherheitsanforderungen an die Nicht-IT-Umgebung.

8.2.1 Erklärung der funktionalen Sicherheitsanforderungen an den EVG

8.2.1.1 Zuordnung der funktionalen Sicherheitsanforderungen zu den Sicherheitszielen

In der folgenden Tabelle 11 wird für jede identifizierte funktionale Sicherheitsanforderung aufgezeigt, zu welchen Sicherheitszielen sie beiträgt.

Sicherheitsziele / Funktionale Sicherheitsanforderungen	O.Auth.1	O.Auth.2	O.Auth.3	O.Privacy.1	O.Privacy.2	O.Integrity.1	O.Integrity.2	O.Rights.1	O.Rights.2	O.Rights.3	O.Rights.4	O.Rights.5	O.Server.Cfg.1
FCS_CKM.1 (Com)				x									
FCS_CKM.2 (Com)				x									
FCS_COP.1 (Com)				x									
FCS_COP.1 (SigMac)							x						
FCS_COP.1 (ComMac)						x							
FDP_ACC.1 (SessData)					x			x	x	x	x	X	
FDP_ACC.1 (CfgData)													x
FDP_ACC.1 (UserData)			x										
FDP_ACF.1 (SessData)					x			x	x	x	x	X	
FDP_ACF.1 (CfgData)													x
FDP_ACF.1 (UserData)			x										
FDP_ITT.1				x		x							
FIA_AFL.1	x												
FIA_ATD.1 (Berater)	x	x											
FIA_ATD.1 (Teilnehmer)	x	x											
FIA_ATD.1 (BeraterAdmin)			x										
FIA_SOS.1 (Berater Passwort)	x												
FIA_SOS.1 (Berater-Administrator Passwort)			x										
FIA_UAU.1 (Berater-VS)	x												
FIA_UAU.1 (TN-VS)	x												
FIA_UAU.1 (BeraterAdmin-Benutzermanager)			x										
FIA_UAU.4	x												
FIA_UAU.7 (Berater)	x												
FIA_UAU.7 (BeraterAdmin)			x										
FIA_UID.1 (Berater-VS)	x												
FIA_UID.1 (TN-VS)	x												
FIA_UID.1 (BeraterAdmin-Benutzermanager)			x										
FIA_USB.1 (Berater)		x											
FIA_USB.1 (TN)		x											
FIA_USB.1 (BeraterAdmin)			x										
FMT_MSA.1			x										
FMT_SMF.1			x										
FMT_SMR.1			x										
FPT_ITT.1							x						

Tabelle 11: Zuordnung der funktionalen Sicherheitsanforderungen zu den Sicherheitszielen

Das Sicherheitsziel **O.Auth.1** definiert, dass nur autorisierte Benutzer in eine Sitzung eintreten.

FIA_UAU.1 (Berater-VS) und FIA_UAU.1 (TN-VS) fordern, dass vor der Authentifizierung keine Methode möglich ist. Die funktionale Sicherheitsanforderung wird einmal für die Authentifizierung des Beraters und des Vermittlungsservices und einmal für die Authentifizierung des Teilnehmers und des Vermittlungsservices definiert.

FIA_UAU.4 fordert, dass eine Einweg-Autoriserung mittels Sitzungsnummer notwendig ist. Dies ist bei der die Authentifizierung des Teilnehmers gegenüber dem Vermittlungsservice der Fall.

FIA_UAU.7 fordert, dass die Eingabe des Passwortes verdeckt erfolgt (maskiert mit Sternen). Dies ist bei der Authentifizierung des Beraters gegenüber dem Vermittlungsservice der Fall.

FIA_AFL.1 fordert, dass nach dreimaliger falscher Eingabe des Beraterpasswortes oder der Sitzungsnummer der Rechner, auf dem die Eingabe gemacht wurde, für 10 Minuten gesperrt wird. Dies ist bei der Authentifizierung des Beraters und des Teilnehmers gegenüber dem Vermittlungsservice der Fall.

FIA_UID.1 (Berater-VS) und FIA_UID.1 (TN-VS) fordern, dass vor der Identifizierung keine Methode möglich ist. Die funktionale Sicherheitsanforderung wird einmal für die gegenseitige Authentifizierung des Beraters und des Vermittlungsservices und einmal für die gegenseitige Authentifizierung des Teilnehmers und des Vermittlungsservices definiert.

FIA_SOS.1 (Berater Passwort) fordert, dass das Beraterpasswort einer bestimmten Policy folgt.

FIA_ATD.1 (Berater) fordert, dass ein Beraterpasswort zu einem individuellen Nutzer, nämlich einem Berater zuzuordnen ist. Ein Beraterpasswort wird zusammen mit der Beraterkennung vom Berater-Adminstrator vergeben. Durch diese Vergabe wird der Berater autorisiert.

FIA_ATD.1 (Teilnehmer) fordert, dass eine Sitzungsnummer zu einem Teilnehmer zuzuordnen ist. Der Berater autorisiert den Teilnehmer, indem er ihm die Sitzungsnummer übermittelt.

Das Sicherheitsziel **O.Auth.2** definiert, dass nur authentifizierte Clientprogramme die Serverkomponenten benutzen können.

FIA_ATD.1 (Berater) fordert, dass ein Beraterpasswort zu einem individuellen Nutzer, nämlich einem Berater zuzuordnen ist. Jeder Berater erhält eine ihm eindeutig zuzuordnendes Beraterpasswort.

FIA_ATD.1 (Teilnehmer) fordert, dass eine Sitzungsnummer zu einem Teilnehmer zuzuordnen ist. Durch die Umgebung wird sicher gestellt, dass der Berater nur dem Teilnehmer die Sitzungsnummer mitteilt, mit dem er die Sitzung führen möchte. Jede Sitzungsnummer ist daher genau einem Teilnehmer zuzuordnen.

FIA_USB.1 (Berater) fordert, dass mit dem Sicherheitsattribut Beraterpasswort der Benutzer *Berater* assoziiert wird. Der Berater muss sich mittels des Beraterprogramms an der Serverkomponente authentifizieren, bevor er das System benutzen kann. Vor erfolgreicher Authentifizierung ist keine Nutzung möglich. Somit sind ausschließlich Beraterprogramme von authentifizierten Beratern in der Lage, die Serverkomponente zu nutzen.

FIA_USB.1 (TN) fordert, dass mit dem Sicherheitsattribut Sitzungsnummer mit der Benutzer *Teilnehmer* assoziiert wird. Der Teilnehmer muss sich mittels des Teilnehmerprogramms an der Serverkomponente authentifizieren, bevor er das System benutzen kann. Vor erfolgreicher Authentifizierung ist keine Nutzung möglich. Somit sind ausschließlich Teilnehmerprogramme von authentifizierten Teilnehmer in der Lage, die Serverkomponente zu nutzen.

Das Sicherheitsziel **O.Auth.3** definiert, dass nur authentifizierte Berater-Administratoren mit Hilfe des Benutzermanagers Berater verwalten können.

Die Authentifizierung des Berater-Administrators unterstützen folgende funktionale Sicherheitsanforderungen:

FIA_UAU.1 (BeraterAdmin-Benutzermanager) fordert, dass vor der Authentifizierung keine Methode möglich ist.

FIA_UAU.7 (BeraterAdmin) fordert, dass die Eingabe des Passwortes verdeckt erfolgt (maskiert mit Sternen). Dies ist bei der Authentifizierung des Berater-Administrators gegenüber dem Vermittlungsservice der Fall.

FIA_UID.1 (BeraterAdmin-Benutzermanager) fordert, dass vor der Identifizierung keine Methode möglich ist.

FIA_SOS.1 (Berater-Administrator Passwort) fordert, dass das Berater-Administrator Passwort einer bestimmten Policy folgt.

FMT_SMF.1 spezifiziert die Management Funktionen der Benutzerdatei durch den Benutzermanager.

FMT_SMR.1 spezifiziert die Rolle Berater-Administrator der Serverkomponente.

Die Authentifizierung des Benutzerverwalters unterstützen folgende funktionale Sicherheitsanforderungen:

FIA_USB.1 (BeraterAdmin) fordert, dass mit dem Sicherheitsattribut Berater-Administrator-Passwort der Benutzer *Berater-Administrator* assoziiert wird. Der authentifizierte Nutzer Berater-Administrator aktiviert den Benutzermanager. Das Sicherheitsattribut Berater-Administrator-Passwort wird vollständig mit dem Benutzermanager assoziiert.

FIA_ATD.1 (BeraterAdmin) fordert, dass ein Berater-Administrator Passwort zu einem individuellen Nutzer, nämlich dem Berater-Administrator zuzuordnen ist. Der Berater-Administrator erhält eine ihm eindeutig zuzuordnendes Berater-Administrator Passwort.

Die Verwaltung der Berater unterstützen folgende funktionale Sicherheitsanforderungen:

FDP_ACC.1 (UserData) und FDP_ACF.1 (UserData) in der Iteration für die sicherheitsrelevanten Konfigurationsparameter setzt die Zugriffspolitik ACCESS Config User Data durch. In der Benutzerdatei werden die Passwörter für den Berater verwaltet. Das Passwort dient dazu, dass nur autorisierte Berater als Teilnehmer in eine Sitzung eintreten können.

FMT_MSA.1 fordert die geregelte Verwaltung von Sicherheitsattributen. Sicherheitsattribut ist in diesem Fall der Login und das Passwort des Beraters, das in der Benutzerdatei mit Hilfe des Benutzermanagers von dem Berater-Administrator verwaltet wird.

Das Sicherheitsziel **O.Privacy.1** definiert, dass der zwischen den Sitzungspartnern übermittelte Sitzungsdatenstrom vertraulich und von Dritten nicht einsehbar ist.

FCS_CKM.1 (Com) fordert die Generierung des symmetrischen Schlüssels, der für die Verschlüsselung des Sitzungsdatenstroms verwendet wird.

FCS_CKM.2 (Com) fordert bei der Distribution der symmetrischen Schlüssel, dass diese ausgehandelt werden gemäß HttpsRpc.

FCS_COP.1 (Com) behandelt die kryptographische Operation des symmetrischen Verschlüsselns beim Austausch des Sitzungsdatenstroms.

FDP_ITT.1 fordert, dass die Vertraulichkeit der Benutzerdaten bei der Übermittlung zwischen den verschiedenen Komponenten erhalten bleibt.

Das Sicherheitsziel **O.Privacy.2** definiert, dass die Anzahl der Sitzungspartner auf zwei beschränkt ist.

FDP_ACC.1 (SessData) legt die Zugriffsrechte der Subjekte Einräumender Sitzungspartner und Berechtigter Sitzungspartner fest. Dies sind genau zwei Sitzungspartner.

FDP_ACF.1 (SessData) legt die Zugriffsrechte der Subjekte Einräumender Sitzungspartner und Berechtigter Sitzungspartner fest. Dies sind genau zwei Sitzungspartner.

Das Sicherheitsziel **O.Integrity.1** definiert, dass der zwischen den Sitzungspartnern ausgetauschte Sitzungsdatenstrom integer ist – unabhängig davon, ob zum Austausch ein Kommunikationsservice benutzt wird oder nicht.

FCS_COP.1 (ComMac) behandelt die kryptographische Operation der Hashwertberechnung beim Austausch des Sitzungsdatenstroms.

FDP_ITT.1 fordert, dass die Integrität der Benutzerdaten bei der Übermittlung zwischen den verschiedenen Komponenten erhalten bleibt.

Das Sicherheitsziel **O.Integrity.2** definiert, dass der zwischen den EVG-Komponenten übermittelte Signalisierungsdaten integer ist. Signalisierungsdaten werden zwischen einem Clientprogramm und einem Serverprogramm ausgetauscht.

FCS_COP.1 (SigMac) behandelt die kryptographische Operation der Hashwertberechnung im Rahmen des proprietären Protokolls httpsRpc, das zum Austausch der Signalisierungsdaten zur Anwendung kommt.

FPT_ITT.1 fordert die Integrität von TSF-Daten bei der Übermittlung.

Die Sicherheitsziele **O.Rights.1 bis O.Rights.5** definieren, dass die Rechte auf dem Rechner des Kommunikationspartners genau in dem Umfang ausgeführt werden, die der einräumende Sitzungspartner definiert hat.

Dies bedeutet insbesondere,

- Es werden nur Rechte für die Applikationen gewährt, die der einräumende Sitzungspartner in der Applikationsauswahl definiert hat. Auf alle anderen Daten hat der berechtigte Sitzungspartner keinen Zugriff.
- Die Änderung der Blickrichtung erfolgt nur mit ausdrücklicher Zustimmung des einräumenden Sitzungspartners.
- Durch die Fernsteuerungsrechte können keine weiteren Rechte erworben werden.
- Während einer Sitzung kann die Fernsteuerung nur mit ausdrücklicher Zustimmung des einräumenden Sitzungspartners erfolgen.

- Die Fernsteuerung kann nur eingeräumt werden, wenn zuvor die Blickrichtung entsprechend der einräumenden Fernsteuerungsrechte geändert wurde. Die Fernsteuerung kann nur auf Applikationen erfolgen, die im Rahmen der Blickrichtungsänderung über die Applikationswahl definiert wurden.
- Die Fernsteuerungsrechte können jederzeit durch Betätigen einer Taste von dem einräumenden Sitzungspartner entzogen werden (F11-Taste).
- Während einer Sitzung kann die Funktion ‚Dateitransfer per Drag & Drop' nur mit ausdrücklicher Zustimmung des Sitzungspartners benutzt werden kann, der die Funktion nicht initiiert hat.
- Die eingeräumten Fernsteuerungsrechte beziehen sich nur auf Fenster von Applikationen, die der Einräumende Sitzungspartner in der Applikationswahl-Schublade freigegeben hat.
- Der EVG bietet dem Benutzer folgende Funktionalität an: Die Fernsteuerungsrechte können vom Sitzungspartner im Watch-Modus angefordert werden. Der einräumende Sitzungspartner muss die Fernsteuerungsrechte darauf hin explizit erteilen (Zustimmungsdialog).
- Fordert der Berater eine Systemdiagnose des Systems des Teilnehmers durchzuführen, so geschieht dies nur mit Zustimmung seines Sitzungspartners.

FDP_ACC.1 (SessData) und FDP_ACF.1 (SessData) setzen die Zugriffspolitiken ACCESS Session Data durch. Diese Zugriffspolitiken setzen das zuvor aufgeführte Sicherheitsziel um.

Das Sicherheitsziel **O.Server.Cfg.1** definiert, dass die Konfigurationsdateien auf der Serverkomponente nur dann eingelesen werden, wenn sie integer sind.

FDP_ACC.1 (CfgData) und FDP_ACF.1 (CfgData) in der Iteration für die Konfigurationsdateien `ServerData.dat` und `ContractData.dat` setzt die Zugriffspolitik ACCESS Secure Config Data durch.

8.2.1.2 Notwendigkeit der funktionalen Sicherheitsanforderungen

Aus der Tabelle 8 ist ersichtlich, dass jede funktionale Sicherheitsanforderung (Komponente) mindestens ein Sicherheitsziel adressiert.

(Es gibt also zu einer Komponente keine leere Zeile.)

8.2.1.3 Berücksichtigung der Sicherheitsziele

Aus der Tabelle 8 ist ersichtlich, dass jedes der identifizierten Sicherheitsziele von mindestens einer funktionalen Sicherheitsanforderung (Komponente) zumindest teilweise abgedeckt wird.

8.2.1.4 Erfüllung der Abhängigkeiten

In der folgenden Tabelle 12 werden alle in den CC aufgeführten Abhängigkeiten zwischen den ausgewählten funktionalen Sicherheitsanforderungen (Komponenten) und anderen funktionalen Komponenten aufgeführt.

	SFR	**Abhängigkeit**	**Kommentar**
1.	FCS_CKM.1 (Com)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4 FMT_MSA.2	Erfüllt in 2 Nicht erfüllt Nicht erfüllt
2.	FCS_CKM.2 (Com)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	Erfüllt in 1 Nicht erfüllt Nicht erfüllt
3.	FCS_COP.1 (Com)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	Erfüllt in 1 Nicht erfüllt Nicht erfüllt
4.	FCS_COP.1 (SigMac)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	Nicht erfüllt Nicht erfüllt Nicht erfüllt
5.	FCS_COP.1 (ComMac)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	Nicht erfüllt Nicht erfüllt Nicht erfüllt
6.	FDP_ACC.1 (SessData)	FDP_ACF.1	Erfüllt in 9
7.	FDP_ACC.1 (CfgData)	FDP_ACF.1	Erfüllt in 10
8.	FDP_ACC.1 (UserData)	FDP_ACF.1	Erfüllt in 11
9.	FDP_ACF.1 (SessData)	FDP_ACC.1 FMT_MSA.3	Erfüllt in 6 Nicht erfüllt
10.	FDP_ACF.1 (CfgData)	FDP_ACC.1 FMT_MSA.3	Erfüllt in 7 Nicht erfüllt
11.	FDP_ACF.1 (UserData)	FDP_ACC.1 FMT_MSA.3	Erfüllt in 8 Nicht erfüllt
12.	FDP_ITT.1	[FDP_ACC.1 or FDP_IFC.1]	Erfüllt in 6
13.	FIA_AFL.1	FIA_UAU.1	19 und 20
14.	FIA_ATD.1 (Berater)	None	
15.	FIA_ATD.1 (Teilnehmer)	None	

	SFR	Abhängigkeit	Kommentar
16.	FIA_ATD.1 (BeraterAdmin)	None	
17.	FIA_SOS.1 (Berater Passwort)	None	
18.	FIA_SOS.1 (Berater-Administrator Passwort)	None	
19.	FIA_UAU.1 (Berater-VS)	FIA_UID.1	Erfüllt in 25
20.	FIA_UAU.1 (TN-VS)	FIA_UID.1	Erfüllt in 26
21.	FIA_UAU.1 (BeraterAdmin-Benutzermanager)	FIA_UID.1	Erfüllt in 27
22.	FIA_UAU.4	None	
23.	FIA_UAU.7 (Berater)	FIA_UAU.1	Erfüllt in 19
24.	FIA_UAU.7 (BeraterAdmin)	FIA_UAU.1	Erfüllt in 21
25.	FIA_UID.1 (Berater-VS)	None	
26.	FIA_UID.1 (TN-VS)	None	
27.	FIA_UID.1 (BeraterAdmin-Benutzermanager)	None	
28.	FIA_USB.1 (Berater)	FIA_ATD.1	Erfüllt in 14
29.	FIA_USB.1 (TN)	FIA_ATD.1	Erfüllt in 15
30.	FIA_USB.1 (BeraterAdmin)	FIA_ATD.1	Erfüllt in 16
31.	FMT_MSA.1	[FDP_ACC.1, or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	Erfüllt in 8 Erfüllt in 33 Erfüllt in 32
32.	FMT_SMF.1	None	
33.	FMT_SMR.1	FIA_UID.1	Erfüllt in 27
34.	FPT_ITT.1	None	

Tabelle 12: Abhängigkeiten der ausgewählten funktionalen Komponenten nach CC

Die Tabelle 12 zeigt, dass die von den CC als abhängig bezeichneten Komponenten ausgewählt wurden oder die Abhängigkeit nicht erfüllt wurde. Nachfolgend wird für jede nicht erfüllte Abhängigkeit aufgeführt, warum diese nicht erfüllt wird.

Nicht erfüllte Abhängigkeiten zur laufenden Nummer 1 der Tabelle 12:

Die Abhängigkeiten der funktionalen Sicherheitsanforderung **FCS_CKM.1** zu **FCS_CKM.4** und zu **FMT_MSA.2** werden nicht erfüllt. FCS_CKM.1 (Com) behandelt die Erzeugung des symmetrischen Schlüssels (der beim Austausch des Datenstroms verwendet wird), FCS_CKM.4 die Zerstörung des Schlüssels und FMT_MSA.2 beinhaltet Anforderungen an sichere Sicherheitsattribute.

Der Austausch der symmetrischen Schlüssel wird mittels des proprietären Protokolls HttpsRpc ausgehandelt, der Schlüssel wird jeweils nur temporär für eine Session verwendet. Nach Beendigung der Session ist der symmetrische Schlüssel nicht mehr gültig.

Da der Schlüssel nur temporär verwendet wird, ist eine Zerstörung des Schlüssels wie sie bei der funktionalen Sicherheitsanforderung FCS_CKM.4 gefordert wird, nicht notwendig.

Da der Schlüssel nur temporär verwendet wird, sind Anforderungen an den sicheren Zustand des Schlüssels nicht notwendig.

Nicht erfüllte Abhängigkeiten zur laufenden Nummer 2 der Tabelle 12:

Die Abhängigkeit der funktionalen Sicherheitsanforderung **FCS_CKM.2** zu **FCS_CKM.4** und **FMT_MSA.2** wird nicht erfüllt. FCS_CKM.2 (Com) behandelt die Erzeugung des symmetrischen Schlüssels, der der beim Austausch des Datenstroms verwendet wird.

Der Austausch der symmetrischen Schlüssel wird mittels des proprietären Protokolls HttpsRpc ausgehandelt, der Schlüssel wird jeweils nur temporär für eine Sitzung verwendet.

Nach Beendigung der Session ist der symmetrische Schlüssel nicht mehr gültig, eine Zerstörung des Schlüssels wie sie bei der funktionalen Sicherheitsanforderung FCS_CKM.4 gefordert wird, ist nicht notwendig.

Da der Schlüssel nur temporär verwendet wird, sind Anforderungen an den sicheren Zustand des Schlüssels nicht notwendig. Nach Beendigung der Session ist der symmetrische Schlüssel nicht mehr gültig, ein Management des Schlüssels ist nicht notwendig.

Nicht erfüllte Abhängigkeiten zur laufenden Nummer 3 der Tabelle 12:

Die Abhängigkeit der funktionalen Sicherheitsanforderung **FCS_COP.1** (symmetrischer Schlüssel beim Austausch des Datenstroms) zu **FCS_CKM.4** und **FMT_MSA.2** wird nicht erfüllt.

FCS_COP.1 (Com) behandelt den kryptographischen Betrieb für den symmetrischen Schlüssel, der im Rahmen der Signalisierung ausgehandelt und beim Austausch des Datenstroms verwendet wird.

Nach Beendigung der Session ist der symmetrische Schlüssel nicht mehr gültig, eine Zerstörung des Schlüssels wie sie bei der funktionalen Sicherheitsanforderung FCS_CKM.4 gefordert wird, ist nicht notwendig.

Da der Schlüssel nur temporär verwendet wird, sind Anforderungen an den sicheren Zustand des Schlüssels nicht notwendig. Nach Beendigung der Session ist der symmetrische Schlüssel nicht mehr gültig, ein Management des Schlüssels ist nicht notwendig.

Nicht erfüllte Abhängigkeiten zur laufenden Nummer 4 der Tabelle 12:

Die Abhängigkeit der funktionalen Sicherheitsanforderung **FCS_COP.1.**

FCS_COP.1 (SigMac) behandelt den kryptographischen Betrieb für die Berechnung des HMAC (keyed-hash message authentication code) zur Integritätssicherung während der Signalisierung. HMAC ist eine Hashfunktion, die den Hashwert mit Hilfe eines Schlüssels berechnet. Der Schlüssel wird im Rahmen der Signalisierung ausgehandelt.

Nach Beendigung der Session ist der Schlüssel nicht mehr gültig, eine Zerstörung des Schlüssels wie sie bei der funktionalen Sicherheitsanforderung FCS_CKM.4 gefordert wird, ist nicht notwendig. Da der Schlüssel nur temporär verwendet wird, sind Anforderungen an den sicheren Zustand des Schlüssels nicht notwendig. Nach Beendigung der Session ist der symmetrische Schlüssel nicht mehr gültig, ein Management des Schlüssels ist nicht notwendig.

Nicht erfüllte Abhängigkeiten zur laufenden Nummer 5 der Tabelle 12:

Die Abhängigkeit der funktionalen Sicherheitsanforderung **FCS_COP.1.**

FCS_COP.1 (ComMac) behandelt den kryptographischen Betrieb für die Berechnung des HMAC (keyed-hash message authentication code) zur Integritätssicherung des Datenstromsaustauschs zwischen Berater und Teilnehmer. HMAC ist eine Hashfunktion, die den Hashwert mit Hilfe eines Schlüssels berechnet. Der Schlüssel wird im Rahmen der Signalisierung ausgehandelt.

Nach Beendigung der Session ist der Schlüssel nicht mehr gültig, eine Zerstörung des Schlüssels wie sie bei der funktionalen Sicherheitsanforderung FCS_CKM.4 gefordert wird, ist nicht notwendig. Da der Schlüssel nur temporär verwendet wird, sind Anforderungen an den sicheren Zustand des Schlüssels nicht notwendig. Nach

Beendigung der Session ist der symmetrische Schlüssel nicht mehr gültig, ein Management des Schlüssels ist nicht notwendig.

Nicht erfüllte Abhängigkeiten zur laufenden Nummer 9 der Tabelle 12:

Die Abhängigkeit der funktionalen Sicherheitsanforderung **FDP_ACF.1 (SessData)** zu **FMT_MSA.3** wird nicht erfüllt.

FMT_MSA.3 fordert, dass die Initialisierung mit Standardwerten von Sicherheitsattributen sicherstellt, dass diese angemessen einschränkend oder zulassend sind. Die in FDP_ACF.1 (SessData) genannten Sicherheitsattribute sind aber nicht durch (autorisierte) Benutzer verwaltbar. Daher gibt es keine Initialisierung mit Standardwerten.

Nicht erfüllte Abhängigkeiten zur laufenden Nummer 10 der Tabelle 12:

Die Abhängigkeit der funktionalen Sicherheitsanforderung **FDP_ACF.1 (CfgData)** zu **FMT_MSA.3** wird nicht erfüllt.

FMT_MSA.3 fordert, dass die Initialisierung mit Standardwerten von Sicherheitsattributen sicherstellt, dass diese angemessen einschränkend oder zulassend sind. Die in FDP_ACF.1 (CfgData) genannten Sicherheitsattribute sind aber nicht durch (autorisierte) Benutzer verwaltbar. Daher gibt es keine Initialisierung mit Standardwerten.

Nicht erfüllte Abhängigkeiten zur laufenden Nummer 11 der Tabelle 12:

Die Abhängigkeit der funktionalen Sicherheitsanforderung **FDP_ACF.1 (UserData)** zu **FMT_MSA.3** wird nicht erfüllt.

FMT_MSA.3 fordert, dass die Initialisierung mit Standardwerten von Sicherheitsattributen sicherstellt, dass diese angemessen einschränkend oder zulassend sind. Bezogen auf die Benutzerdatei gibt es keinen Standardwert, der sich verwalten lässt. Die initiale Benutzerdatei gehört zum Lieferumfang und muss vom Berater-Administrator bei Inbetriebnahme geändert werden. Bezogen auf den Inhalt der Benutzerdatei, stellt der EVG sicher, dass sichere Passwörter verwendet werden. Initiale Passwörter sind keine Standardwerte, sondern werden jeweils neu generiert, daher braucht die Abhängigkeit zu FMT_MSA.3 nicht erfüllt zu werden.

8.2.2 Erklärung der Anforderungen an die Mindeststärke der EVG-Sicherheitsfunktionen

Die Mechanismen, die auf einem Wahrscheinlichkeits- oder Permutationsmechanismus beruhen, erreichen die Mindeststärke SOF-Basic. Es wird darauf hingewiesen, dass mit dem SoF Claim keine Beurteilung der algorithmischen Strenge vorgenommen wird.

Als Angreifer wurden Personen mit begrenzten technischen und zeitlichen Möglichkeiten und mit allgemein verfügbaren Kenntnissen der Informationstechnik, des Betriebssystems und des EVG angenommen.

Die Mindeststärke SOF-Basic bietet entsprechend Sicherheitsziel OE.9 einen hinreichenden Schutz gegenüber einem solchen Angriffspotential.

8.2.3 Erklärung der Anforderungen an die Vertrauenswürdigkeit des EVG

Der EVG soll die Anforderungen der Vertrauenswürdigkeitsstufe EAL2 gemäß Teil 3 der CC erfüllen.

Die mit dem EVG zu verarbeitenden Daten besitzen einen niedrigen Schutzbedarf. Der EVG soll eine dem Schutzbedarf der Informationen angemessene Vertrauenswürdigkeit bieten.

Als Angreifer wurden Personen mit begrenzten technischen und zeitlichen Möglichkeiten und mit allgemein verfügbaren Kenntnissen der Informationstechnik, des Betriebssystems und des EVG angenommen.

Da die Komponenten des EVGs über das ungeschützte Internet miteinander kommunizieren (müssen), sind der EVG und die mit im verarbeiteten Daten Gefahren ausgesetzt.

Die Vertrauenswürdigkeitsstufe EAL2 bietet entsprechend Sicherheitsziel OE.9 für diesen Schutzbedarf ein angemessenes Maß von Vertrauenswürdigkeit.

8.2.4 Erklärung der Sicherheitsanforderungen an die IT-Umgebung

8.2.4.1 Zuordnung der Sicherheitsanforderungen an die IT-Umgebung zu den Sicherheitszielen

In der folgenden Tabelle 13 wird für jede identifizierte Sicherheitsanforderung an die IT-Umgebung aufgezeigt, zu welchen Sicherheitszielen sie beiträgt.

Sicherheitsanforderung an die IT-Umgebung	Sicherheitsziel
FCS_CKM.1 (Env)	Erreichung von OE-IT.1, OE-IT.2
FPT_ITT.1	Erreichung von OE-IT.1, OE-IT.3
FCS_COP.1 (PRNG)	Erreichung von OE-IT.2

Tabelle 13: Zuordnung der Sicherheitsanforderungen an die IT-Umgebung zu den Sicherheitszielen

Die Ziele OE-IT.1 und OE-IT.2 werden durch die Anforderung FCS_CKM.1 (Env) erreicht, weil dieses die Generierung kryptographisch sicherer Zufallszahlen (OE-IT.2), und zwar gemäß [SSL] und [RFC2246] fordert (OE-IT.1).

Die Ziele OE-IT.1 und OE-IT.3 werden durch die Anforderung FPT_ITT.1 erreicht, weil das in [SSL] und [RFC2246] spezifizierte Verfahren die Integrität, Authentizität und Vertraulichkeit der transportierten durch Verschlüsselung Daten sicherstellt.

Das Ziel OE-IT.2 wird durch die Anforderung FCS_COP.1 (PRNG) erreicht, diese die Erzeugung kryptographisch sicherer Zufallszahlen nach [DSS] fordert.

8.2.4.2 Notwendigkeit der Sicherheitsanforderung an die IT-Umgebung

Aus der Tabelle 13 ist ersichtlich, dass jede Sicherheitsanforderungen an die Nicht-IT-Umgebung mindestens ein Sicherheitsziel adressiert.

(Es gibt also zu einer Sicherheitsanforderung keine leere Zeile.)

8.2.4.3 Berücksichtigung der Sicherheitsziele

Aus der Tabelle 13 ist ersichtlich, dass jedes der identifizierten Sicherheitsziele von mindestens einer Sicherheitsanforderung an die IT-Umgebung zumindest teilweise abgedeckt wird.

8.2.4.4 Erfüllung der Abhängigkeiten

In der folgenden Tabelle 14 werden alle in den [CC] aufgeführten Abhängigkeiten zwischen den ausgewählten funktionalen Sicherheitsanforderungen (Komponenten) und anderen funktionalen Komponenten aufgeführt.

Sicherheitsanforderung an die die IT-Umgebung	**Abschnitt in Teil 2 [CC]**	**Abhängigkeit**	**Erfüllung**
FCS_CKM.1.1 (ENV)	10.1	[FCS_CKM.2 oder FCS_COP.1] FCS_CKM.4 FMT_MSA.2	`FCS_CKM.2` erfüllt in [SSL] `FCS_CKM.4` erfüllt in [SSL] `FCS_MSA.2` erfüllt in [SSL]
FCS_COP.1.1 (PRNG)	10.2	[FDP_ITC.1 oder FDP_ITC.2 oder FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	`FCS_CKM.1` erfüllt in [SSL] erfüllt in [SSL] erfüllt in [SSL]

Sicherheitsanforderung an die die IT-Umgebung	Abschnitt in Teil 2 [CC]	Abhängigkeit	Erfüllung
FPT_ITT.1.1	15.6	keine	erfüllt

Tabelle 14: Abhängigkeiten der ausgewählten funktionalen Komponenten nach [CC]

Die Tabelle 14 zeigt, dass alle von den [CC] als abhängig bezeichneten Komponenten ausgewählt wurden.

8.2.5 Erklärung der Sicherheitsanforderungen an die Nicht-IT-Umgebung

8.2.5.1 Zuordnung der Sicherheitsanforderungen an die Nicht-IT-Umgebung zu den Sicherheitszielen

In der folgenden Tabelle 15 wird für jede im Kapitel 5.4 identifizierte Sicherheitsanforderung an die Nicht-IT-Umgebung aufgezeigt, zu welchen Sicherheitszielen sie beiträgt.

Sicherheitsanforderung an die Nicht-IT-Umgebung	Sicherheitsziel
ANF1	Erreichung von OE.1
ANF2	Erreichung von OE.2
ANF3	Erreichung von OE.3
ANF4	Erreichung von OE.4
ANF5	Erreichung von OE.5
ANF6	Erreichung von OE.6
ANF7	Erreichung von OE.7
ANF8	Erreichung von OE.8
ANF9	Erreichung von OE.9
ANF10	Erreichung von OE.10
ANF11	Erreichung von OE.11
ANF12	Erreichung von OE.12
ANF13	Erreichung von OE.13

ANF14	Erreichung von OE.14
ANF15	Erreichung von OE.15
ANF16	Erreichung von OE.16
ANF17	Erreichung von OE.17
ANF18	Erreichung von OE.18
ANF19	Erreichung von OE.19
ANF20	Erreichung von OE.20
ANF21	Erreichung von OE.21

Tabelle 15: Zuordnung der Sicherheitsanforderungen an die Nicht-IT-Umgebung zu den Sicherheitszielen

8.2.5.2 Notwendigkeit der Sicherheitsanforderungen an die Nicht-IT-Umgebung

Aus der Tabelle 15 ist ersichtlich, dass jede Sicherheitsanforderungen an die Nicht-IT-Umgebung mindestens ein Sicherheitsziel adressiert.

(Es gibt also zu einer Sicherheitsanforderung keine leere Zeile.)

8.2.5.3 Berücksichtigung der Sicherheitsziele der Nicht-IT-Umgebung

Aus der Tabelle 10 ist ersichtlich, dass jedes der identifizierten Sicherheitsziele von mindestens einer Sicherheitsanforderung an die Nicht-IT-Umgebung zumindest teilweise abgedeckt wird.

8.3 Erklärung der EVG-Übersichtsspezifikation

8.3.1 Zuordnung der funktionalen Sicherheitsanforderungen zu den Sicherheitsfunktionen

In der folgenden Tabelle 16 wird für jede im Kapitel 6 identifizierte funktionale Sicherheitsanforderung aufgezeigt, von welchen Sicherheitsfunktionen sie erfüllt wird.

	SF.DP	SF.I&A	SF.CD	SF.AC	SF.I
FCS_CKM.1 (Com)	1	3			
FCS_CKM.2 (Com)	2,3				
FCS_COP.1 (Com)	1	3			
FCS_COP.1 (SigMac)					2
FCS_COP.1 (ComMac)			1		1
FDP_ACC.1 (SessData)				1 bis 9	
FDP_ACC.1 (CfgData)			1		
FDP_ACC.1 (UserData)		1,4,5,7			
FDP_ACF.1 (SessData)				1 bis 9	

	SF.DP	SF.I&A	SF.CD	SF.AC	SF.I
FDP_ACF.1 (CfgData)			1		
FDP_ACF.1 (UserData)		1,4,5,7			
FDP_ITT.1	1				1
FIA_AFL.1		1,2			
FIA_ATD.1 (Berater)		1,6			
FIA_ATD.1 (Teilnehmer)		2,6			
FIA_ATD.1 (BeraterAdmin)		7			
FIA_SOS.1 (Berater Passwort)		8			
FIA_SOS.1 (Berater-Administrator Passwort)		8			
FIA_UAU.1 (Berater-VS)		4			
FIA_UAU.1 (TN-VS)		4			
FIA_UAU.1 (BeraterAdmin-Benutzermanager)		4			
FIA_UAU.4		2			
FIA_UAU.7 (Berater)		1			
FIA_UAU.7 (BeraterAdmin)		7			
FIA_UID.1 (Berater-VS)		4			
FIA_UID.1 (TN-VS)		4			
FIA_UID.1 (BeraterAdmin-Benutzermanager)		4			
FIA_USB.1 (Berater)		1,6			
FIA_USB.1 (TN)		2,6			
FIA_USB.1 (BeraterAdmin)		7			
FMT_MSA.1		5,7			
FMT_SMF.1		7			
FMT_SMR.1		7			
FPT_ITT.1					2

Tabelle 16: Zuordnung der funktionalen Sicherheitsanforderungen zu den Sicherheitsfunktionen

8.3.2 Notwendigkeit der Sicherheitsanforderung

Aus der Tabelle 16 ist ersichtlich, dass jede der identifizierten Sicherheitsfunktionen von mindestens einer funktionalen Sicherheitsanforderung zumindest teilweise abgedeckt wird.

Nachweis für jede Sicherheitsfunktion im Einzelnen:

SF.DP

FCS_CKM.1 (Com) behandelt die kryptographische Schlüsselgenerierung. Der Vermittlungsservice erzeugt im Rahmen der Signalisierung einen symmetrischen Schlüssel. Der Schlüssel wird in der weiteren Kommunikation zur Verschlüsselung des Sitzungsdatenstroms in der Kommunikationsphase zwischen den Sitzungspartner verwendet. Die funktionalen Sicherheitsanforderungen unterstützen daher die Sicherheitsfunktion SF.DP.1.

FCS_CKM.2 (Com) fordert für den symmetrischen Schlüssel, dass dieser mittels HttpsRpc zwischen den EVG-Komponenten ausgehandelt werden. Die funktionale Sicherheitsanforderung unterstützt daher die Sicherheitsfunktion SF.DP.2 und SF.DP.3.

FCS_COP.1 (Com) behandelt den kryptographischen Betrieb. Der kryptographische Betrieb realisiert die Verschlüsselung und damit unterstützt FCS_COP.1 die Sicherheitsfunktion SF.DP.1.

FDP_ITT.1 fordert, dass die Vertraulichkeit der Benutzerdaten bei der Übermittlung zwischen den verschiedenen Komponenten erhalten bleibt. Benutzerdaten ist der Sitzungsdatenstrom, der in der Kommunikationsphase zwischen den Benutzern ausgetauscht wird. Die Sicherheitsanforderung unterstützt daher die Sicherheitsfunktion SF.DP.1.

SF.I&A

FDP_ACC.1 (UserData) und FDP_ACF.1 (UserData) fordert den geregelten Zugriff auf die Daten in der Benutzerdatei gemäß der Zugriffspolitik ACCESS Config User Data. In der Benutzerdatei werden Login und Passwort des Beraters verwaltet, daher unterstützen diese Sicherheitsanforderungen die Sicherheitsfunktion SF.I&A (insbesondere SF.I&A.1, SF.I&A.4, SF.I&A.5 und SF.I&A.7).

FIA_AFL.1 fordert, dass nach dreimaliger falscher Eingabe des Beraterpasswortes oder der Sitzungsnummer der Rechner, auf dem die Eingabe gemacht wurde, für 10 Minuten gesperrt wird. FIA_AFL.1 unterstützt daher SF.I&A.1 und SF.I&A.2.

FIA_UAU.1 (Berater-VS), FIA_UAU.1 (TN-VS) und FIA_UAU.1 (BeraterAdmin-Benutzermanager) fordern, dass vor der Authentifizierung nur das Aushandeln der Authentifizierungsart möglich ist. Diese funktionalen Sicherheitsanforderungen unterstützen daher die Sicherheitsfunktion SF.I&A.4.

FIA_UAU.4 fordert, dass der Autorisierungsmechanismus nur einmal erbracht wird. Die ist bei der Authentifizierung des Teilnehmers gegenüber dem Vermittlungsservice der Fall. Jede Sitzungsnummer wird nur einmal verwendet (SF.I&A.2).

FIA_UAU.7 (Berater) und FIA_UAU.7 (BeraterAdmin) fordern, dass eine geschützte Authentisierungsrückmeldung bereitgestellt wird. Diese funktionale Sicherheitsanforderung unterstützt die Sicherheitsfunktion SF.I&A.1 und SF.I&A.7.

FIA_UID.1 (Berater-VS), FIA_UID.1 (TN-VS) und FIA_UID.1 (BeraterAdmin-Benutzermanager fordern, dass vor der Identifizierung keine Aktion möglich ist. Diese funktionalen Sicherheitsanforderungen unterstützen daher die Sicherheitsfunktion SF.I&A.4.

FMT_MSA.1 fordert die geregelte Verwaltung von Sicherheitsattributen. Sicherheitsattribut ist in diesem Fall der Login und das Passwort des Beraters, das in der Benutzerdatei verwaltet wird. Durch die Verwaltung der Login-Daten wird die Sicherheitsfunktion SF.I&A (insbesondere SF.I&A.5 und SF.I&A.7) unterstützt.

FMT_SMF.1 fordert das Management von Benutzername und Passwort des Beraters durch Bearbeiten der Benutzerdatei. Dies entspricht der Sicherheitsfunktion Identification & Authentification (SF.I&A.7).

FMT_SMR.1 fordert die Rolle Berater-Administrator. Diese ist in der Sicherheitsfunktion Identification & Authentification (SF.I&A.7) aufgeführt.

FCS_CKM.1 (Com) und FCS_COP.1 (Com) behandeln die Erzeugung und die Operation des symmetrischen Schlüssels, der zur Verschlüsselung des Datenaustausches verwendet wird. Gleichzeitig dient der Schlüssel zur gegenseitig Authentifizierung. Dies entspricht der Sicherheitsfunktion SF.I&A.3.

FIA_SOS.1 (Berater Passwort) und FIA_SOS.1 (Berater-Administrator Passwort) erfordert die Verifikation des Passwortes nach einer bestimmten Metrik. Dies entspricht der Sicherheitsfunktion SF.I&A.8.

FIA_USB.1 (Berater) und FIA_USB.1 (TN) erfordern jeweils die Bindung zwischen dem Benutzer und den Clientkomponenten. FIA_USB.1 (BeraterAdmin) erfordert die Bindung zwischen Berater-Administrator und Benutzermanager. FIA_ATD.1 (Berater), FIA_ATD.1 (Teilnehmer) und FIA_ATD.1 (BeraterAdmin) erfordern die Zuordnung der Sicherheitsattribute Beraterpasswort, Sitzungsnummer und Berater-Administrator Passwort zu den jeweiligen Benutzern. Durch die funktionalen Sicherheitsanforderungen wird die Authentisierung der Clientkomponenten und des Benutzermanagers gewährleistet wie sie in der Sicherheitsfunktion unter SF.I&A.1 und SF.I&A.6 für die Beraterkomponente und unter SF.I&A.2 und SF.I&A.6 für die Teilnehmerkomponente und unter SF.I&A.7 für den Benutzermanager gefordert ist.

SF.CD

FDP_ACC.1 (CfgData) und FDP_ACF.1 (CfgData) fordern den geregelten Zugriff auf die Konfigurationsdateien `ServerData.dat` und `ContractData.dat` gemäß der Zugriffspolitik ACCESS Secure Config Data. Dies entspricht SF.CD.1.

SF.AC

FDP_ACC.1 (SessData) und FDP_ACF.1 (SessData) fordert den geregelten Zugriff auf die Sitzungsdaten gemäß der Zugriffspolitik ACCESS Session Data. Dies entspricht der Sicherheitsfunktion Access Control (SF.AC).

SF.I

FDP_ITT.1 fordert, dass die Integrität der Benutzerdaten bei der Übermittlung zwischen den verschiedenen Komponenten erhalten bleibt. Benutzerdaten sind im Sitzungsdatenstrom enthalten, der in der Kommunikationsphase zwischen den Benutzern ausgetauscht wird. Die Sicherheitsanforderung unterstützt daher die Sicherheitsfunktion

Integrity (SF.I.1). Benutzerdaten sind ebenso in den Signalisierungsdaten enthalten. Die Sicherheitsanforderung unterstützt daher die Sicherheitsfunktion Integrity (SF.I.2).

FCS_COP.1 (SigMac) behandelt die MAC Generierung und Verifikation des Schlüssels der zur Integritätssicherung während der Signalisierung verwendet wird. Die Sicherheitsanforderung unterstützt daher die Sicherheitsfunktion Integrity (SF.I.2).

FCS_COP.1 (ComMac) behandelt die MAC Generierung und Verifikation des Schlüssels der zur Integritätssicherung des Sitzungsdatenstroms verwendet wird. Die Sicherheitsanforderung unterstützt daher die Sicherheitsfunktion Integrity (SF.I.1).

8.3.3 Mindeststärke der Sicherheitsfunktionen

Die Tabelle 9 in der EVG-Übersichtsspezifikation in Kapitel 6.2 führt die Sicherheitsfunktionen auf, welche auf Wahrscheinlichkeits- oder Permutationsverfahren beruhen. In der Tabelle sind die effektiven Mindeststärken der jeweiligen Sicherheitsfunktionen angegeben. Diese entsprechen Mindeststärken alle mindestens der in Kapitel 5.2 geforderten Stärke SoF-Basic gemäß [CC].

8.3.4 Nachweis der Maßnahmen zur Vertrauenswürdigkeit des EVG

Der Nachweis der Wirksamkeit der Maßnahmen zur Vertrauenswürdigkeit wird durch eine Evaluierung des EVGs mitsamt der Dokumentation gemäß der Stufe EAL2 in [CC_P3] erbracht. Die dabei zu erfüllenden Anforderungen an die Vertrauenswürdigkeit sind in Kapitel 5.3 gegeben. Die Erklärung der getroffenen Maßnahmen bei der Entwicklung des EVGs sind in Kapitel 6.3 gegeben.

8.4 Erklärung der PP-Postulate

Es wurden keine PP-Postulate abgegeben.

Anhang A: Glossar

Berater

Anwender des Netviewer one2one Beraterprogramms.

Beraterprogramm

Das Netviewer one2one Beraterprogramm, mit dem ein Anwender eine Netviewer-Sitzung initiieren kann. Das Beraterprogramm verfügt im Vergleich zum Teilnehmerprogramm über zusätzliche administrative Funktionen.

Blickrichtung

Richtung der Bildschirmübertragung (Desktop-Sharing) während einer Netviewer-Sitzung. Die Bildschirmübertragung ist in beide Richtungen möglich (entweder der Berater zeigt seinen Bildschirm oder der Teilnehmer zeigt seinen Bildschirm) und kann während der Sitzung geändert werden.

Client

Sammelbegriff für das Netviewer one2one Berater- und/oder Teilnehmerprogramm.

Client-Konfiguration

Eine Menge von Parametern (Schlüssel-Wert-Paare), welche das Verhalten eines Client-Programms (und damit auch dessen Leistungsumfang) vorgeben. Die Konfiguration erfolgt vor der Auslieferung der Clients an den Kunden durch die Netviewer GmbH.

Desktop-Sharing

Übertragung des Bildschirminhalts eines Rechners auf den Bildschirm eines entfernten Rechners mit der Möglichkeit der Fernsteuerung. Bei Netviewer one2one ist die Übertragung beschränkt auf freigegebene Applikationen und Bildschirmelemente.

Ferngesteuerter

Sitzungspartner im Show-Modus, der seinem Sitzungspartner die Fernsteuerung für den eigenen Bildschirm erteilt hat.

Fernsteuernder

Sitzungspartner im Watch-Modus, der den Bildschirm des Sitzungspartners mithilfe der Fernsteuerung bedienen kann.

Fernsteuerung

Bedienung eines entfernten Rechners mithilfe von Tastatureingaben und Mausbefehlen vom lokalen Rechner aus. Bei Netviewer one2one ist die Fernsteuerung beschränkt auf freigegebenen Applikationen und Bildschirmelemente.

Kommunikationsservice

Der Kommunikationsservice ermöglicht es den Clients, ihren Sitzungsdatenstrom auszutauschen.

Peer-to-peer

Bezieht sich bei Netviewer one2one nur auf den Sitzungsdatenstrom und meint, dass zu dessen Austausch kein Kommunikationsservice benötigt wird, da die Netzwerktopologie eine direkte Verbindung zwischen Beraterprogramm und Teilnehmerprogramm ermöglicht.

Schlüssel, Symmetrischer/Asymmetrischer

Zeichenkette, mit der Nachrichten anhand eines bestimmten Algorithmus so umkodiert werden, dass sich die Originalnachricht nur mit Hilfe eines Schlüssels wiedergewinnen lässt.

Sind die Schlüssel zur Kodierung und zur Dekodierung dieselben, spricht man von Symmetrischer Verschlüsselung. Bei Asymmetrischer Verschlüsselung kommen unterschiedliche Schlüssel zum Einsatz.

Serverrechner

Auf dem Serverrechner ist die Serversoftware Netviewer Standard Server eingerichtet.

Show-Modus

Modus während einer Netviewer-Sitzung, in dem der Anwender von Netviewer one2one seinen Bildschirminhalt an den Sitzungspartner überträgt.

Prozess

Programm, das gerade ausgeführt wird.

Signalisierung

Signalisierung ist die Übermittlung von Information zu Steuerungszwecken. Hauptzweck beim Austausch von Signalisierungsinformationen bei Netviewer ist es, die Verbindung zwischen den Clients herzustellen, aufrecht zu halten und schließlich wieder abzubauen.

Sitzung

Eine Sitzung bezeichnet die bestehende visuelle Verbindung (Desktop-Sharing) zwischen dem Netviewer one2one Berater- und Teilnehmerprogramm.

Sitzungsdatenstrom

Daten, die zwischen den Clients ausgetauscht werden. Dies sind:

- visualisierbare Daten (z.B. Bildschirminhalte und Videodaten)
- Daten von Eingabegeräten (z.B. Maus und Tastatur)
- Steuerungsdaten (z.B. Initiierung eines Blickrichtungswechsels)

Sitzungsnummer

Zufällig generierte, neunstellige Nummer, die eine Netviewer-Sitzung bis zum Sitzungsende eindeutig identifiziert. Die Sitzungsnummer wird insbesondere zur korrekten Vermittlung der beiden Sitzungspartner verwendet.

Sitzungspartner

Sammelbegriff für Berater und/oder Teilnehmer.

Teilnehmer

Anwender des Netviewer one2one Teilnehmerprogramms.

Teilnehmerprogramm

Das Netviewer one2one Teilnehmerprogramm, mit dem ein Anwender in eine gestartete Netviewer-Sitzung eintreten kann.

Vermittlungsservice

Die Hauptaufgabe des Vermittlungsservices ist es, Berater und Teilnehmer zusammenzuführen, so dass diese eine Sitzung durchführen können. Des Weiteren führt der Vermittlungsservice Authentifizierung, Autorisierung, Lizenzprüfung, Protokollierung, u.a. durch. Zur Kommunikation zwischen Clients und dem Vermittlungsservice wird das Netviewer-eigene Protokoll HttpsRpc-Protokoll eingesetzt.

Watch-Modus

Modus während einer Netviewer-Sitzung, in dem der Anwender von Netviewer one2one den Bildschirminhalt des Sitzungspartners betrachtet.

Anhang B: Abkürzungen

Die folgenden Abkürzungen werden in diesem Dokument benutzt:

CC	Common Criteria for Information Technology Security Evaluation (Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik)
EAL	Evaluation Assurance Level (Vertrauenswürdigkeitsstufe)
ECC	elliptic curve cryptosystem, asymmetrisches Verschlüsselungsverfahren
EVG	Evaluationsgegenstand (Target Of Evaluation, TOE)
HMAC	keyed-hash message authentication code; Der HMAC wird aus der Nachricht und einem geheimen Schlüssel mittels einer Hash-Funktion berechnet
IT	Informationstechnik
PP	Protection Profile (Schutzprofil)
SOF	Strength Of Function (Stärke der Funktionen)
SFR	Security Functional Requirements
ST	Security Target (Sicherheitsvorgaben)
TOE	Target Of Evaluation (Evaluationsgegenstand, EVG)
TSF	TOE Security Functions (EVG-Sicherheitsfunktionen)

Anhang C: Referenzen

Die folgenden Dokumente enthalten weitere Informationen:

[AES] U.S. Government Federal Information Processing Standards (FIPS), FIPS PUB 197, Advanced Encryption Standard (AES), 2001

[BLOWFISH] B. Schneier; "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)"; Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204.

[CC] Common Criteria, consists of [CC_P1], [CC_P2], and [CC_P3]

[CC_P1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 2.3, August 2005

[CC_P2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 2.3, August 2005

[CC_P3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 2.3, August 2005

[DSS] National Institute of Standards and Technology: Digital signature standard (DSS), Federal Information Processing Standard 186-2, National Institute of Standards and Technology, Washington, 2000

[PKCS12] PKCS #12: Personal Information Exchange Syntax Standard, version 1.0; RSA Laboratories; June 24, 1999

[RFC2246] RFC 2246 - The TLS Protocol Version 1.0

[RIPEMD] H. Dobbertin, A. Bosselaers, B. Preneel, ``RIPEMD-160, a strengthened version of RIPEMD,'' (ps, pdf). Fast Software Encryption, LNCS 1039, D. Gollmann, Ed., Springer-Verlag, 1996, pp. 71-82

[RFC2104] RFC2104: HMAC: Keyed-Hashing for Message Authentication

[RFC2404] RFC2404: The Use of HMAC-SHA-1-96 within ESP and AH

[RFC3174] RFC 3174: US Secure Hash Algorithm 1 (SHA1)

[SSL3] A. Frier, P. Karlton, and P. Kocher, "The SSL 3.0 Protocol", Netscape Communications Corp., Nov 18, 1996, Internet Draft <draft-freier-ssl-version3-02.txt>

Anhang D: Versionsinformationen

Version	Datum	Autor	Korrektor	Bemerkungen (Autor/Korrektor)
0.1	2006-08-17	IS, RS		Grundlage Dokument CC-NETV-102 in Version 1.2; Kapitel 1-2 überarbeitet und ergänzt, Gesamtes Dokument auf Netviewer CI angepasst, Bedrohungen sortiert, EVG-Beschreibung überarbeitet, Glossar eingefügt
0.1.1	2006-08-29	SF		Überarbeitung EVG-Beschreibung: Bedrohungen, Sicherheitsziele, Kapitel 1-2 Sicherheitsfunktionalität
0.1.2	2006-09-10	SF		Erarbeitung Sicherheitsfunktionen, Teile der Erklärung
0.1.3	2006-09-13	SF	GG	Einarbeitung Reviewbemerkungen, Überarbeitung der Sicherheitsfunktionen und der EVG-Umgebung
0.2	2006-09-18	SF		Vorlage Netviewer zur Feinabstimmung der Sicherheitsfunktionen
0.3	2006-10-04	SF	GG	Vollständige Fassung zur Vorlage Netviewer
0.3.1	2006-10-26	SF		Vorlage zum internen Review
0.3.2	2006-11-02	SF		Einarbeitung Reviewbemerkung Netviewer
0.4	2006-11-07	IS		Einarbeitung Reviewbemerkungen mtG in Kapitel 1-2
0.4.1	2006-11-13	IS	CL, RS	Einarbeitung Korrekturen aus internem Review
0.5	2006-11-16	IS		Vorlage zum abschließenden Review bei mtG
0.6	2007-05-08	SF		Einarbeitung der Reviewbemerkungen Netviewer; Einarbeitung der Änderungen gemäß Herstellerdokumentation; Überarbeitung der Sicherheitsfunktionen.
0.6.1	2007-06-01	IS		Einarbeitung von Korrekturen von mtG und Netviewer-intern
0.7	2007-07-11	IS		Einarbeitung verschiedener Korrekturen, finaler Stand für Evaluierungsphase
0.7.1a	2007-07-13	SF		Einarbeitung der Ergebnisse aus dem Gespräch mit Herrn Dr. Schöller, BSI vom

				12.07.2007. In der vorliegenden Version handelt es sich um einen Vorschlag, wie der Konfigurator Teil des Auslieferungsverfahrens betrachtet wird. Der Konfigurator findet daher in diesem Dokument keine weitergehende Berücksichtigung.
0.7.2a		IS		Überarbeitung und Vorlage BSI zur Abnahme
0.7.3	2007-10-22	SF		Überarbeitung der ST gemäß Anforderungen des BSI
0.8	2008-02-29	SF		Überarbeitung gemäß dem von Netviewer beim BSI vorgelegtem Konzeptpapier vom 01.02.2008
0.8.1	2008-03-03	SF		Einpflegen der von Netviewer AG bereit gestellten überarbeiteten EVG-Beschreibung und weitere Überarbietung gemäß dem Konzeptpapier.
0.9	2008-03-03	IS		Korrektur der von mtG gelieferten Überarbeitung des ST, Version wird beim BSI zur Vorprüfung eingereicht
0.9.1.0	2008-03-17	IS		Überarbeitung hinsichtlich der vom BSI am 18.01.2008 gelieferten Kommentare
0.9.1.0.1	2008-03-20	SF		Review auf Teilbereich, Überarbeitung bzgl. Unstimmigkeit zu ANF 20, Einpflegen von FIA_AFL.1
1.0	2008-03-20	CL		Änderungen von SF überarbeitet, versandfertig gemacht.
1.0 -> pre1.5	2008-07-10	CL		Beginn der Überarbeitung wg. Reviewbericht v0.80 von 2008-06-25 (0524_ASE_080625_v0.80.pdf, basierte auf ST_Netviewer_one2oneTS_v1.0.doc/.pdf vom 20.03.2008)
1.5	2008-07-28	CL		Fertigstellung Version 1.5. Änderungen mit Kommentaren versehen.
1.6	2008-07-28	CL		Alle Kommentare aus 1.5 gelöscht. Sonst nichts geändert.
pre1.7	2009-02-02	CL		Beginn der Überarbeitung wg. Reviewbericht 0524_ASE_090129_v0.90.pdf

1.7	2009-03-30	CL		Fertigstellung Überarbeitung wg. Reviewbericht 0524_ASE_090129_v0.90.pdf
1.8	2009-09-14	CL		jetzt ‚niedriger Schutzbedarf', Version 5.1.0.1208, Neues Kapitel vor 2.6.1: Wichtige Einsatzszenarien Netviewer one2oneTS, Kapitel 2.5 Zusatz zum zweiten Spiegelstrich, Kapitel 2.4 ein neuer Abschnitt, ADM und USR jetzt v1.4 (wg. Schutzbedarf)

Version: Bitte verwenden Sie das Format "x.x.x oder x.x".

Datum : Bitte verwenden Sie das Format "Jahr-Monat-Tag".