

White Paper Sicherheit: Netviewer Support 6.0

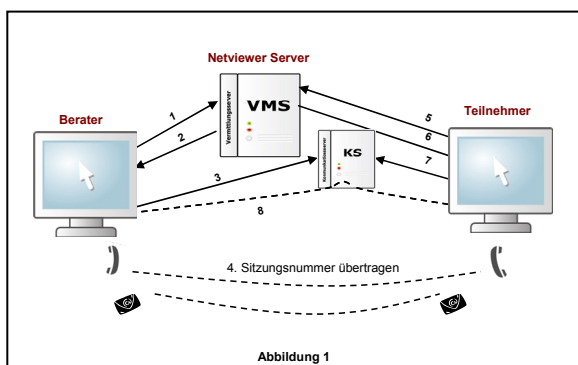
Dieses White Paper beschreibt die Sicherheitsmechanismen von Netviewer Support. Im ersten Teil des Dokuments liegt der Fokus auf der Netzwerktransportschicht. Der zweite Teil beschreibt die Sicherheitsmechanismen auf der Applikationsschicht.

Sicherheit auf der Netzwerktransportschicht

Die Sicherheitsmechanismen der Transportschicht stellen die Grundlage einer sicheren Kommunikation dar. Im Folgenden wird erläutert, wie Netviewer die verwendeten Kommunikationskanäle durch gegenseitige Authentifizierung und Verschlüsselung schützt.

Aufbau einer Sitzung

Der Sitzungsaufbau ist in Abbildung 1 dargestellt und wird im Folgenden beschrieben. Der Berater startet das Beraterprogramm, welches den Vermittlungsserver (VMS) mit der Sitzungsanforderung kontaktiert (1). Nachdem der Berater mittels E-Mail-Adresse und Passwort erfolgreich authentifiziert wurde, sendet der Vermittlungsserver die neunstellige Sitzungsnummer und die Adresse des Kommunikationsservers an den Berater zurück (2). Das Beraterprogramm kontaktiert den Kommunikationsserver und wartet, bis der Teilnehmer in die Sitzung eintritt (3).



Im nächsten Schritt übermittelt der Berater dem Teilnehmer die neunstellige Sitzungsnummer per Telefon oder Einladungs-E-Mail (4). Der Teilnehmer startet das Teilnehmerprogramm und gibt die Sitzungsnummer im entsprechenden Feld ein. Das Teilnehmerprogramm sendet daraufhin eine Anfrage zum Vermittlungsserver (5). Der Vermittlungsserver sendet die Adresse des Kommunikationsservers, auf dem das Beraterprogramm wartet, zurück (6). Das Teilnehmerprogramm kontaktiert den Kommunikationsserver (7). Die Sitzung ist damit als Ende-zu-Ende-Verbindung zwischen dem Berater- und dem Teilnehmerprogramm über den Kommunikationsserver hergestellt (8).

Die Integrität und die Vertraulichkeit der Daten während der Sitzung sind gewährleistet. Da Netviewer Support eine Ende-zu-Ende-Verschlüsselung verwendet, kann der Kommunikationsserver die übermittelten Daten nicht entschlüsseln. Weiterhin kann kein Dritter in die Sitzung eintreten, da sie auf zwei Sitzungspartner beschränkt ist.

Der Vermittlungsserver und der Kommunikationsserver sind unabhängige Entitäten. Der Signalisierungsdatenstrom (z.B. Authentifizierung, Schlüsselaustausch) und der Sitzungsdatenstrom sind logisch voneinander getrennt.

Verschlüsselungsmethoden

Da der Vermittlungsserver und der Kommunikationsserver verschiedene Aufgaben erfüllen, werden bei der Kommunikation unterschiedliche Methoden zur Sicherung der Kommunikation verwendet.

Die Kommunikation zwischen den Clients und dem Vermittlungsserver ist durch TLS (Standard RFC

2246) gesichert¹. Dabei kommt ein 2048-Bit RSA-Serverzertifikat zum Einsatz. Client-Programme authentifizieren sich auf dieser Ebene per HTTP Digest Access Authentication (Standard RFC 2617).

Die Kommunikation der Clients mit dem Kommunikationsserver wird mit AES im CBC-Modus und 256-Bit langen Session Keys abgesichert. Die Integrität der Daten wird mit Authentication Headers gesichert (nach Standard RFC 2404).

Abbildung 2 zeigt den Verbindungsaufbau im Detail.

Beim Sitzungsaufbau

Vor dem Sitzungsaufbau kann der Anwender die Authentizität der Netviewer Software prüfen. Die Software ist mit einem von der unabhängigen Zertifizierungsstelle VeriSign ausgestellten Zertifikat signiert.

Beim Starten des Beraterprogramms muss sich der Berater mit seiner E-Mail-Adresse und einem selbstgewählten Passwort authentifizieren. Nach der erfolgreichen Authentifizierung wird eine einmalige neunstellige Sitzungsnummer durch den

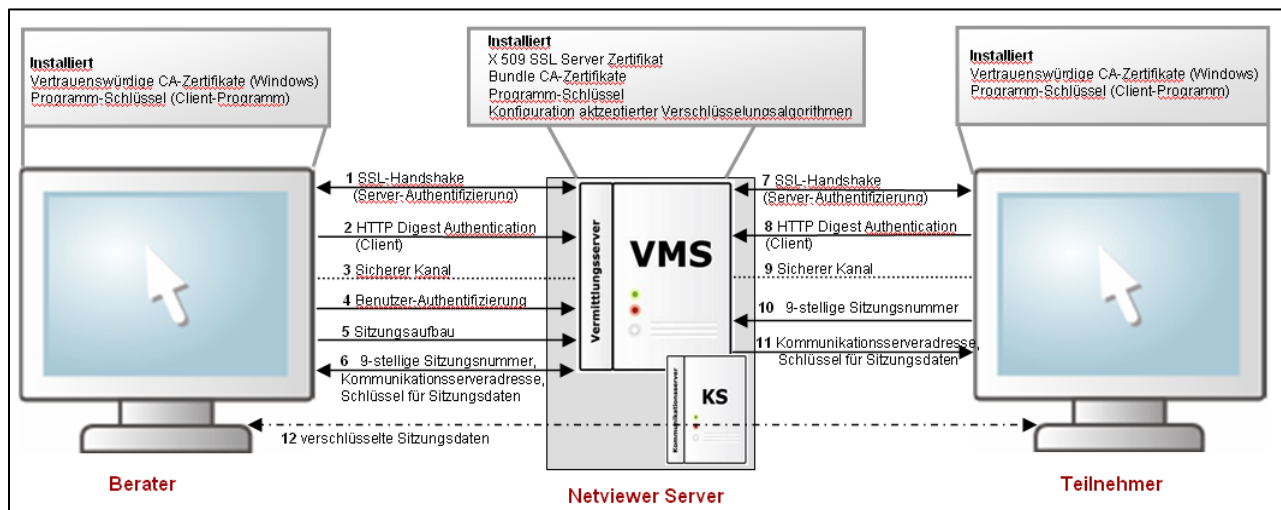


Abbildung 2

Sicherheit auf der Applikationsschicht

Auf der Applikationsschicht bietet Netviewer verschiedene technologie- und prozessgestützte Sicherheitsmechanismen, anhand welcher der Sicherheitsgrad der Software an unterschiedliche Anforderungen anpassbar ist.

Viele der folgenden Funktionen lassen sich individuell konfigurieren.

Vermittlungsserver generiert und zum Beraterprogramm übermittelt. Diese Nummer wird telefonisch oder per E-Mail an den Teilnehmer übermittelt (siehe Abbildung 1).

Ein Sitzungspasswort und eine zweite Bestätigungs-PIN, die vom Teilnehmer zum Berater übermittelt wird, können zusätzlich verwendet werden.

Während der Sitzung

Die Privatsphäre der Sitzungspartner und der Schutz persönlicher Daten ist während einer Netviewer-Sitzung durch verschiedene Funktionen und Einstellungen geschützt.

¹ Für Umgebungen, in denen TLS nicht möglich ist, kann eine Alternative konfiguriert werden.

Weder der Berater noch der Teilnehmer sind in der Lage, das Fernsteuerungsrecht für den Computer des Sitzungspartners ohne dessen Zustimmung zu erlangen.

Beide Sitzungspartner müssen jegliche Veränderung des Status ihres Computers (Wechsel der Blickrichtung, Fernsteuerung, Dateitransfer, Abfrage der Systeminformationen des Computers) explizit erlauben. Erst nach der Freigabe ist der Sitzungspartner imstande, den Computer fernzusteuern oder andere Aktionen durchzuführen.

Applikationen oder Dateien, die nicht an den Sitzungspartner übertragen werden sollen, können explizit ausgewählt werden. So ist es beispielsweise möglich, den Desktop oder die Taskleiste zu verbergen. Nicht freigegebene Applikationen und Bildelemente können nicht über die Fernsteuerung bedient werden.

Der Sitzungspartner, der seinen Bildschirm zeigt, kann die Bildschirmübertragung unterbrechen und ein Standbild übertragen, um während der Sitzung vertrauliche Daten oder Applikationen zu bearbeiten (Pause-Funktion der Monitor-Schublade).

Mit der Sicherheitstaste (standardmäßig F11) wird dem Sitzungspartner mit sofortiger Wirkung das Fernsteuerungsrecht entzogen.

Protokollierung und Aufzeichnung

Das Beraterprogramm erzeugt eine TXT-Datei am Ende der Sitzung, welche unter anderem die Sitzungsdauer und die Anzahl der übertragenen Bytes protokolliert. Die Sitzungsdaten können alternativ als CSV-Datei, z.B. zur weiteren Verwendung zur Abrechnung, auf Berater- oder auf Teilnehmerseite protokolliert werden. Zusätzlich können serverseitig Logdateien erzeugt werden.

Alle Sitzungsdaten inklusive Video- und Audiodaten können aufgezeichnet und im Netviewer-eigenen Format NVL gespeichert werden. NVL-Dateien können manuell in das Dateiformat ASF konvertiert werden.

Zusammenfassung

Die Sicherheit von Netviewer Support und die Integrität der übertragenen Daten wird durch die Verwendung verschiedener Sicherheitsmechanismen garantiert:

- Netviewer Support ist mit dem Netviewer Zertifikat signiert, welches durch eine unabhängige Zertifizierungsstelle (VeriSign) ausgestellt wurde.
- SSL/TLS wird zur gegenseitigen Authentifizierung und zur Verschlüsselung zwischen Client und Vermittlungsserver verwendet.
- Client-Programme authentifizieren sich per HTTP Digest Access Authentication (RFC 2617).
- Ein 256-Bit AES Key wird zur Verschlüsselung der Sitzungsdaten verwendet.
- Der Vermittlungsserver und der Kommunikationsserver sind unabhängige Entitäten.
- Der Austausch der Sitzungsnummer erfolgt über ein anderes Medium (Telefon oder E-Mail).
- Nach dem Sitzungsstart kann kein Dritter in die Sitzung eintreten.
- Die Sitzung ist Ende- zu-Ende verschlüsselt.
- Jede Sitzung kann beim Berater, beim Teilnehmer oder auf dem Server protokolliert werden.
- Alle Sitzungsdaten können zur späteren Revision aufgezeichnet werden.
- Für jede Sitzung wird eine neue Sitzungsnummer generiert.
- Auf dem Computer des Sitzungspartners können keine Aktionen ohne explizite Zustimmung durchgeführt werden. Dies gilt für den Berater und den Teilnehmer.
- Beim Verbindungsaufbau können optional ein Sitzungspasswort und eine zusätzliche Bestätigungs-PIN verwendet werden.

Version 1.0 Januar 2010

© 2010 Netviewer AG. Netviewer Support, Meet, Admin, Server und das Netviewer Logo sind eingetragene Marken der Netviewer AG. Alle Rechte vorbehalten. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.