Technischer Anhang

zum Vertrag

über die Zulassung als IP-Netz-Provider

im electronic cash-System der deutschen Kreditwirtschaft

Version 1.2

30.05.2011

Inhaltsverzeichnis

1 Einleitung

Im Folgenden werden die technischen Anforderungen beschrieben, die für die Zulassung als IP-Netz-Provider durch die Kreditwirtschaft zu erfüllen sind.

2 Anforderungen an IP-Netz-Provider

2.1 Grundsätzliche Anforderungen

Die Anbindung an die Kopf- und Übergabestellen und an die Netzbetreiber sind so zu gestalten, dass die Verfügbarkeit des Netzes gewährleistet ist.

Der Austausch von electronic cash-Daten darf **nur** zwischen den Kopf- und Übergabestellen und den Netzbetreibern als Anschlussnehmer möglich sein.

2.2 Technische Mindestanforderungen

Die folgende Übersicht legt die technischen Mindestanforderungen für die durch den IP-Netz-Provider zu erbringenden Servicemerkmale fest.

Zusätzliche Sicherheitsmerkmale wie Vertraulichkeit und Datenintegrität (bspw. Verschlüsselung) sind kein gefordertes Servicemerkmal, das der IP-Netz-Provider anbieten muss.

Ein IP-Netz-Provider muss die Einhaltung der folgenden Anforderungen für jeden an das VPN angeschlossenen Standort im Falle einer redundanten Anbindung garantieren:

Servicemerkmal	Anforderung	Bemerkung
Leistung		
Verfügbarkeit	> = 99.9 % p. a.	Abhängig von dieser Anforderung wird der Provider ein entsprechendes Lösungsangebot für die Anbindung der Netzbetreiber schaffen. _
MTTR	4 Stunden	Mittlere Zeitdauer für die Behebung einer gemeldeten produktiven Netzwerkstörung.
RTD	< 200 ms	Kurzform for *Round Trip Delay*. Die benötigte Laufzeit eines Signals innerhalb einer Datenverbindung des VPN circuit.
Bandbreite	Wert / Einheit:	Digitale Datenmenge die innerhalb einer Zeiteinheit über einen VPN Zugang übertragen werden kann (Wert pro Zeiteinheit ist einzutragen).
Quality of Services – QoS		*Quality of Service* (*QoS*) bezeichnet die Priorisierung von Datenpaketen anhand bestimmter Merkmalen und Eigenschaften.

Servicemerkmal	Anforderung	Bemerkung
Anzahl Classes of Service (CoS)	>= 2	Bezeichnet allgemein die Anzahl unterschiedlicher Dienstgüteklassen.
IP-Adressen		
Anzahl der IP Addressen pro VPN-Zugang	>= 8	Minimale Anzahl von IP-Adressen des VPN Providers für jeden Zugang
NAT	Unterstützung	Der Provider verpflichtet sich, NAT auf der Seite der CPE zu unterstützen und je nach Bedarf in Abstimmung mit dem jeweiligen Anschlussnehmer umzusetzen.

2.3 Technische Anforderungen an den Applikationsbetrieb

2.3.1 Verwendung eines Längenheaders

Für den Transaktionsaustausch zwischen den Partnern sind für die einzelnen Transaktionstypen entsprechende Längenheader vorzusehen. Dieses Verfahren dient der notwendigen Längenbestimmung der folgenden Nachricht im IP-Datenstrom durch die Applikation.

	Autorisierungs-TX	OPT-TX
Headerlänge	2 Byte binär	2 Byte binär
Inklusiv/exklusiv	inklusiv	inklusiv

Tabelle: Übersicht Längenheader

Beispiel: AutorisierungsTX mit Header 2 Byte länge binär inklusiv.
(wird in der Nachrichtenlänge mit berechnet)

2.3.2 Konfiguration der Session-Timeouts

Das Timeoutverhalten für geöffnete Applikationssessions ist so zu konfigurieren, dass ein mögliches Timeout immer zuerst durch die Applikation erfolgt. Es gilt zu verhindern, dass eine geöffnete Session durch ein Timeout beteiligter Netzwerkkomponenten unterbrochen wird und die beteiligten Applikationen dieses nicht erkennen.

Um mögliche Überlastungen von Firewall-Systemen auszuschließen, sind für genutzte TCP-Ports zwischen den Systemen die voreingestellten Session-Timeout-Parameter abzuschalten oder, falls dies je nach eingesetztem Produkt nicht möglich sein sollte, die beteiligten Anwendungen beim Abbau einer Session durch die Firewall (bspw. bei einem "Packet Out-of-State") darüber zu informieren. Hiermit (Stichwort: Reset an Client und Server) wird sichergestellt, dass die Session unmittelbar bei Bedarf von der Clientanwendung neu aufgebaut wird. Die beteiligten Kommunikations-

partner haben durch ein entsprechendes Vorgehen dafür Sorge zu tragen, dass die verwendeten Netzwerkkomponenten (Firewall etc.) entsprechend konfiguriert werden.

2.4 Ansprache der Kopfstellen

Die von der Kreditwirtschaft zugelassene Kopfstelle ist berechtigt, jedem IP-Netz-Provider für jeden Netzbetreiber eine feste Port-Adresse bzw. eine feste Port-Range vorzugeben. Der IP-Netz-Provider darf diese nicht einschränken.

2.5 Weitere Anforderungen

Die von der Kreditwirtschaft zugelassenen Kopf- und Übergabestellen sind von den IP-Netz-Providern redundant (das heißt über zwei Leitungen) anzuschließen.

Netzwerkprobleme mit einem Anschlussnehmer dürfen keinen Einfluss auf die technische Anbindung weiterer Anschlussnehmer haben (Zugangsisolierung).

Es sind integrierte Überwachungs- und Eskalationsprozesse einzurichten.

Der IP-Netz-Provider ist für den Betrieb seines VPN verantwortlich. Dies umfasst den Betrieb des VPN bis zum jeweiligen Netzwerkzugang auf Seiten des Anschlussnehmers.

Üblicherweise erfolgt der Zugang zum VPN am bereitgestellten Zugangsrouter des IP-Netz-Providers. Die hierbei verwendete Netzwerktechnologie kann vom IP-Netz-Provider frei gestaltet werden. Die eingesetzte Lösung darf die Flexibilität des Anschlussnehmers auf Seiten des lokalen Netzwerks (LAN) nicht beeinträchtigen.

Das IP-Netz des Providers muss dem aktuellen Stand der Technik genügen.

3 Glossar:

IP	Abkürzung für Internet Protocol. Das Internet Protocol (IP) ist ein in Computernetzen weit verbreitetes Netzwerkprotokoll und stellt die Grundlage des Internets dar. IP bildet die erste vom Übertragungsmedium unabhängige Schicht der Internetprotokoll-Familie. Das bedeutet, dass mittels IP-Adresse und Subnetzmaske (subnet mask) Computer innerhalb eines Netzwerkes in logische Einheiten, so genannte Subnetze, gruppiert werden können. Auf dieser Basis ist es möglich, Computer in größeren Netzwerken zu adressieren und Verbindungen zu ihnen aufzubauen, da logische Adressierung die Grundlage für Routing (Wegewahl und Weiterleitung von Netzwerkpaketen) ist.
MPLS	Abkürzung für Multiprotocol Label Switching, ermöglicht die verbindungsorientierte Übertragung von Datenpaketen in einem Netzwerk entlang eines zuvor aufgebauten („signalisierten“) Pfades. Dieses Vermittlungsverfahren wird überwiegend von Betreibern großer Transportnetze eingesetzt, die Sprach- und Datendienste auf Basis von IP anbieten.

MTTR	Kurzform für Mean Time to Repair. Die durchschnittliche Zeit für die Korrektur einer Störung, die im Netz auftritt. Ziel ist es, die Störung innerhalb einer im SLA definierten Zeit zu beheben, dies ist abhängig von der Priorität des Fehlers.
NAT	Kurzform für Network Address Translation. Es ermöglicht neben der Umsetzung von IP-Adressen auch eine Umsetzung von Ports. Oft wird es eingesetzt, um durch sogenanntes „Maskieren“ (masquerading) eine Reihe von (privaten) IP-Adressen und zugeordneten Port-Nummern zur Nutzung nur einer (öffentlichen) IP-Adresse zu verwenden.
QoS	Abkürzung für Quality of Service. QoS bezeichnet die Priorisierung von Datenpaketen anhand bestimmter Merkmalen und Eigenschaften. Mit diesen Mechanismen ist es möglich, z. B. Autorisierungsdaten, deren Übertragung in Echtzeit und Verzögerungsfrei erfolgen sollte, stärker zu bevorzugen als die Übertragung von Clearing Daten.
RTD	Kurzform for Round Trip Delay. Die benötigte Laufzeit eines Signals innerhalb einer Datenverbindung des IP VPN circuit.
VPN	Abkürzung für Virtuelles Privates Netzwerk. Ein VPN ist ein Computernetz, das zum Transport privater Daten ein vorhandenes Netz nutzt. Teilnehmer eines VPN können Daten wie in einem internen lokalen Netzwerk austauschen. Die einzelnen Teilnehmer selbst müssen hierzu nicht direkt verbunden sein. Das VPN ermöglicht die Kommunikation der VPN-Partner basierend auf einer Tunneltechnik und ist in sich geschlossen (daher „privat“). Durch die Verwendung von Passwörtern, öffentlichen Schlüsseln oder durch ein digitales Zertifikat kann die Authentifizierung der VPN-Partner gewährleistet werden. Der Begriff „Privat“ impliziert jedoch nicht, dass es sich um eine verschlüsselte Übertragung handelt, durch die Vertraulichkeit und Integrität der Daten sichergestellt wird. Zur Gewährleistung der Vertraulichkeit und Integrität der übertragenen Daten müssen die Teilnehmer angemessene Maßnahmen implementieren.