OESTERREICHISCHE NATIONALBANK
EUROSYSTEM

USER MANUAL

Anhang E: Technische Anbindung

Clearing Service.International

Version: 6.0

Dokumentenrevisionsnummer: 1



Stand: November 2018

Inhaltsverzeichnis

1 Allgemeine Informationen 1
1.1 Änderungshistorie 1
2 Technische Anbindung allgemein 2
2.1 Dateinamenskonvention 2
2.2 Dateinamensgestaltung von CS 3
3 Anbindung per SWIFTNet FileAct 5
3.1 Kontaktadresse 5
4 Anbindung per SWIFTNet FIN 6
4.1 Kontaktadresse 6
5 Anbindung per Standleitung/Connect:Direct 7
5.1 Architektur 7
5.2 Verschlüsselung 7
5.3 Netzwerk-Schicht 7
5.4 Data Link-Schicht 8
6 Hardware 9
6.1 Adressen der Leitungsendstellen/Rechenzentren 9
7 Planung der Verbindung 10
8 Sonstiges 11
9 Kontaktadressen 12
10 Abkürzungsverzeichnis 13
11 Glossary 14

1 Allgemeine Informationen

Dieses Dokument beschreibt die technischen Voraussetzungen eines Teilnehmers am GSA Clearing Service.International, die für den Austausch von Nachrichten in den verschiedenen Formaten notwendig sind (z.B. Leitungsverschlüsselung, Dateinamenskonvention).

Die nachfolgenden Erläuterungen behandeln jedoch keine zeitlichen Abläufe von CS.I, diese sind dem User Manual bzw. den weiteren Anhängen zu entnehmen.

1.1 Änderungshistorie

Version	Datum	Änderungen	Bearbeiter
DR 1	2011-05-31	Initiale Erarbeitung	STEINDORFER, FLORIANI, ZENZ, SPATSCHIL, FATHI, FUSS, KUBICKI, BREUER, FIKAR
DR 2	2012-07-02	Layoutanpassungen	FIKAR
4.0	2013-07-08	Anpassung an Version 4.0 und Aktualisierung der Kontaktadressen	ZENZ
4.0 DR2	2014-01-15	Herausnahme Wunschcycle	FIKAR
4.2 DR1	2014-10-10	Anpassungen gemäß User Manual V4.2 DR1; Herausnahme, Verschlüsselung und Komprimierung, Aktualisierung des Aufbaus des Dateinamens, Überarbeitung des Hardwarekapitels sowie von Kapitel 5	KUBICKI
4.6 DR1	2016-09-20	Korrektur einzelner Formulierungen, Aktualisierung der Kontaktdaten	KUBICKI, WOTRUBA
4.8 DR1	2017-10-03	Korrektur einzelner Formulierungen und Formatierungen	WOTRUBA
6.0 DR1	2018-07-09	Aktualisierung der (Kontakt-)Adressen in Kapitel 3.1, 6.1 und 9, geringfügige Korrektur einzelner Formulierungen	WOTRUBA

2 Technische Anbindung allgemein

Grundsätzlich ist eine technische Anbindung an das Clearing Service.International über

- Standleitung/Sterling Commerce Connect:Direct,
- SWIFTNet FileAct sowie
- SWIFTNet FIN (eingeschränkt auf Einzelsatz-Nachrichten)

möglich. Die beiden erstgenannten Anbindungen können, sofern sie initial technisch eingerichtet wurden, in beliebiger Kombination für die Anlieferung von Files an das GSA Clearing Service genutzt werden. SWIFTNet FIN hingegen wird vom CS ausschließlich ausgangsseitig für den SRR-/MT940-Versand verwendet (siehe dazu Kapitel 4). Für die Auslieferung von CS.I ist die entsprechende Einmeldung der technischen Stammdaten zwecks Erfassung der Zielhosts sowie Dateinamen erforderlich.

Voraussetzung für eine technische Anbindung ist die Verschlüsselung auf zumindest einer der folgenden beiden Ebenen:

- Verschlüsselung auf Dateiübertragungsendpunktebene (Connect:Direct Secure Plus)
- Verschlüsselung auf Netzwerkübertragungsebene (Routerverschlüsselung)

Eine Kombination der obigen Verschlüsselungsvarianten ist ebenso möglich.

2.1 Dateinamenskonvention

Unabhängig vom Übertragungskanal ist der folgende Aufbau der Dateinamen für Dateian- und auslieferungen zu berücksichtigen:

CS{I|X}{bbbbbbbbccc}(BC|CB|SR){yyyymmdd}{nn}{x..x}.(XML|SWI)

Platzhalter	Werte	Länge
CS	Clearing Service	**2**
I|X	I für CS.I-Dateien X für MT940 aus gemeinsamen CS.A und CS.I Settlements (nur ausgangsseitig)	**1**
bbbbbbbb	8-stelliger BIC gemäß SWIFT-Standard	**8**
ccc	3-stelliger Branch Code gemäß SWIFT-Standard (entweder regulärer Branch Code oder „XXX“)	**3**
BC|CB|SR	BC für Bank an Clearing Service CB für Clearing Service an Bank SR für Settlement Reconciliation Report (nur ausgangsseitig)	**2**
yyyymmdd	8-stelliges ISO Datum	**8**
nn	optional Cut Off-Nummer/Stundenangabe (01-24, reine Informationsangabe ohne Auswirkung auf die konkrete Verarbeitung)	**2**
x..x	maximal 6-stelliger alphanumerischer Wert (0-9, A-Z)	**max. 6**
.XML|.SWI	.XML für SEPA-Dateien .SWI für MT940 (nur ausgangsseitig)	**4**

Folgend wird der Aufbau der Dateinamen für Routingtabellen des GSA Clearing Service dargestellt:

CSA{bbbbbbbbccc}RTO{yyyymmdd}{x..x}.(XML)

Platzhalter	Werte	Länge
CSA	Clearing Service	**3**
bbbbbbbb	8-stelliger BIC gemäß SWIFT-Standard	**8**
ccc	3-stelliger Branch Code gemäß SWIFT-Standard (entweder regulärer Branch Code oder „XXX“)	**3**
RTO	RTO für Routingtabelle im OeNB ROCS Format	**3**
yyyymmdd	8-stelliges ISO Datum	**8**
x..x	maximal 7-stelliger alphanumerischer Wert	**max. 7**
.XML	.XML für ROCS-Format	**4**

2.2 Dateinamensgestaltung von CS

Wahlweise kann die Auslieferung mit einem von GSA Clearing Service gesondert generierten Dateinamen genutzt werden, der sich aus folgenden dynamischen Bestandteilen zusammensetzt:

Datum und Uhrzeit	
#DATE-YYYYMMDD#	Datum in 8-stelliger Form (z.B. 20171231 für 31. Dez. 2017)
#DATE-YYMMDD#	Datum in 6-stelliger Form (z.B. 171231 für 31. Dez. 2017)
#DATE-MMDD#	Datum in 4-stelliger Form (z.B. 1712 für Dez. 2017)
#TIME-HHMMSS#	Uhrzeit in 6-stelliger Form (z.B. 235959 für 23:59:59)
#TIME-HHMM#	Uhrzeit in 4-stelliger Form (z.B. 2359 für 23:59)
Fortlaufende Nummer	
#ID-6#	6-stellige fortlaufende Nummer (z.B. 012345)
#ID-5#	5-stellige fortlaufende Nummer (z.B. 01234)
#ID-4#	4-stellige fortlaufende Nummer (z.B. 0123)
#ID-3#	3-stellige fortlaufende Nummer (z.B. 012)
#ID-2#	2-stellige fortlaufende Nummer (z.B. 01)
#ID-A6#	6-stelliger alphanumerischer Wert (z.B. 0123FZ)
#ID-A5#	5-stelliger alphanumerischer Wert (z.B. 012KB)
#ID-A4#	4-stelliger alphanumerischer Wert (z.B. 01BS)
#ID-A3#	3-stelliger alphanumerischer Wert (z.B. 0K2)
#ID-A2#	2-stelliger alphanumerischer Wert (z.B. 0Z)
Settlement/Weiterleitungs-Cut Off	
#CUTOFF-NR#	2-stellige Settlement- bzw. Weiterleitungs-Cut Off-Nummer (z.B. 12)

Als Zieldateinamen für Auslieferungen vom GSA Clearing Service sind auch Host-GDGs zulässig. Es werden nur Dateinamen als GDG akzeptiert, die entweder dem Original-dateinamen oder einem Dateinamen mit festem Aufbau und fortlaufender Nummer entsprechen.

Dateinamen, die einen festen Aufbau haben, jedoch nur eine Zeitangabe um die Eindeutigkeit zu bestimmen, werden für den Versand von CS.I nicht unterstützt. Grund dafür ist, dass durch parallelisierte Ausgabeprozesse nicht davon ausgegangen werden kann, dass diese nicht in derselben Sekunde zwei Ausgangsdateien erzeugen, wodurch die

Dateiangaben in identen Dateinamen resultieren würden und zu einem Konflikt auf der Empfängerseite führen könnten.

3 Anbindung per SWIFTNet FileAct

Der Austausch von Dateien mittels SWIFTNet FileAct ist lediglich im Push-Mode möglich und bedarf einer initialen Einrichtung. Zusätzlich zu den notwendigen Tests ist die Anmeldung zur CUG bei SWIFT erforderlich, selbst wenn dieser Weg nur als reine Ausfallsschiene im Contingency Fall benutzt wird.

Eine ad hoc-Nutzung von SWIFTNet FileAct ist im Rahmen des Generic Service bei SWIFT möglich. In diesem Fall kommt kein Bulkpricing zur Anwendung, die Verrechnung erfolgt nach Filegröße (kchar) zusätzlich zur Gebührenstaffelung (Tier) des jeweiligen Senders. Dies ist jedoch nur eine Übergangslösung während des Anmeldungsprozesses zur CUG für neue Teilnehmer. Grundsätzlich müssen alle Teilnehmer, die SWIFTNet FileAct verwenden möchten, bei der CUG eingemeldet sein.

Um SWIFTNet FileAct zu nutzen, ist der Requester DN der sendenden Stelle bekanntzugeben. Die nachstehenden Daten sind im Request zu verwenden:

Responder DN	Ist mit “cn=cs,o=nabaatwg,o=swift“ anzugeben.
Request Type*	Ist mit “pacs.xxx.cs.any“ anzugeben.
DelNotRequestType*	Ist mit “xsys.xxx.delnotif” anzugeben.
ServiceName*	Ist mit “oenb.csa.rt!p“ (Pilot) bzw. „oenb.csa.rt“ (Live) anzugeben.
NonRepudiation*	Ist mit “TRUE” anzugeben.
DeliveryNotification*	Ist mit “TRUE” anzugeben.
Number of Transactions*	Ist mit der Anzahl der Transaktionen zu befüllen.

Bei den mit * gekennzeichneten Feldern ist die exakte Befüllung für das Bulkpricing Service über die CUG erforderlich.

Die Information über die Transaktionen ist über folgende erweiterte FileAct-Headerstruktur möglich:

```
<Sw:HeaderInfo>
        <ApplSpcfc xmlns="urn:swift:xsd:ApplSpcfc.TxsCntr.01">
                <TxsCntr>
                        <TtlNbOfTxs>12345678</TtlNbOfTxs>
                </TxsCntr>
        </ApplSpcfc>
</Sw:HeaderInfo>
```

3.1 Kontaktadresse

Für weitere Fragen sowie die technische Einrichtung eines SWIFTNet FileAct-Zugangs wenden Sie sich bitte an:

Dipl.-Ing. (FH) Markus Göbl E-Mail: markus.goebl@oenb.at Telefon: +43-1-40420/2716

4 Anbindung per SWIFTNet FIN

Die Anbindung über SWIFTNet FIN erfordert ebenso eine initiale Einrichtung.

Über SWIFTNet FIN ist die Zusendung von Settlement Reconciliation Reports des Clearing Service im MT940-Format möglich. Diese kann mittels technischem Stammdatenformular angefordert werden.

4.1 Kontaktadresse

Für weitere Fragen sowie die technische Einrichtung eines SWIFTNet FIN-Zugangs wenden Sie sich bitte an:

Friedrich Levy E-Mail: friedrich.levy@oenb.at Telefon: +43-1-40420/4640

5 Anbindung per Standleitung/Connect:Direct

5.1 Architektur

Um für den Ausfall von Leitungen oder einzelnen Komponenten vorzusorgen, sind die Anschlüsse zumindest **doppelt über zwei getrennte Leitungswege** auszuführen. Die Nutzung von zwei Providern wird angeraten. Die Leitungswege oder die Applikation **müssen verschlüsselt** werden. Es wird empfohlen, Netzwerk (IPsec) und Applikations-Layer (sterling) zu verschlüsseln.

Die Betriebszustände der Router müssen lokal durch den jeweils Verantwortlichen überprüft, Bandbreitenauslastungen auf beiden Seiten überwacht werden.

Es ist sowohl eine zyklische, als auch im Bedarfsfall eine End-to-End-Prüfung des aktuellen Systems „Server-Router-Leitung-Router-Server“ und damit (automatisch) der dazwischen-liegenden transparenten Systeme, wie Switches und Firewalls, zuzulassen.

5.2 Verschlüsselung

Wie bereits erwähnt, müssen aus Sicherheitsgründen die Leitungen oder die Applikation verschlüsselt werden.

Die Leitungsverschlüsselung soll mit IPsec/ISAKMPerfolgen:

```
isakmp policy
encr aes 256
authentication rsa-encr
group 5
lifetime 3600

transformSet esp-aes 256 esp-sha-hmac
```

Als Schlüssel wird eine Public-Private Key-Verschlüsselung verwendet.

Bei Bedarf werden die Vorgaben an die nach neuestem Stand der Technik als sicher geltenden Werte angepasst.

Die Applikationsverschlüsselung soll mit Connect:Direct Secure Plus geschehen.

5.3 Netzwerk-Schicht

Als Linknetze werden zwei von der OeNB vorgegebene Subnetze verwendet. Sollte für die Applikation keine offizielle Adresse zur Verfügung stehen, wird eine Adresse von der OeNB vorgegeben, auf die die Serveradresse übersetzt wird.

Als Routing-Protokoll kommt BGP zum Einsatz, die Authentisierung der BGP-Sessions untereinander erfolgt via MD5-Passwort. Durch die Verwendung von BGP können gezielt Routen übergeben und die Priorisierung der Primary und Backup Links gesteuert werden. Durch das dynamische Routing kann bei Ausfall einer Leitung automatisch umgeschaltet werden.

5.4 Data Link-Schicht

Wie in Kapitel 11 dargestellt, sind SDH, VPLS, MPLS, ATM oder Ethernet denkbar. Nicht gemanagte Verbindungen wie SDH oder Ethernet bieten fixe Transferraten während QOS gesteuerte Netze wie VPLS, MPLS, ATM meist innerhalb der SLAs bleiben, dafür aber kostengünstiger sind.

Die Übergabe zu Systemen der OeNB erfolgt allerdings ausschließlich mit Ethernet. Als Schnittstellen können entweder Kupfer TP/RJ45 (10Mb/100Mb/1000Mb) oder SFP 1Gb, Multi- oder Singlemode, MTRJ 100Mb Multimode angenommen werden.

Layer 2 Verbindungen werden grundsätzlich bevorzugt, da sich der Einrichtungs- und Administrationsaufwand verringert.

6 Hardware

Für Primär- und Backupverbindungen muss jeweils eine eigene Hardware verwendet werden.

Auf Wunsch kann der Partner eigene Konverter oder einen eigenen Access Router in den jeweiligen Rechenzentren der OeNB betreiben, um die Übergabe auf Ethernet zu gewährleisten.

6.1 Adressen der Leitungsendstellen/Rechenzentren

- OeNB, Garnisongasse 15, 1090 Wien, Österreich
- T-Systems, Rennweg 97-99, 1030 Wien, Österreich

7 Planung der Verbindung

Die Auswahl der Art der Leitungsverbindung zwischen dem Clearing Service-Teilnehmer und den Rechenzentren der Oesterreichischen Nationalbank erfolgt in Absprache. Aufgrund von Faktoren wie Robustheit und garantierter Bandbreite sind Standleitungen zu bevorzugen. Die OeNB verfügt über Leitungen der Firmen Telekom, Colt, UPC und Wienstrom.

Eine Verbindung über Internet wird nicht unterstützt.

Die verwendeten Router müssen bei Leitungsverschlüsselung den Vorgaben für die Bandbreite entsprechen.

Die benötigte Hardware für die Leitungsverbindung wird vom Clearing Service-Teilnehmer bestellt und gewartet.

8 Sonstiges

Eventuell bereits bestehende Connect:Direct-Verbindungen können auf Wunsch ebenfalls über die CS-Verbindungen geschaltet werden.

9 Kontaktadressen

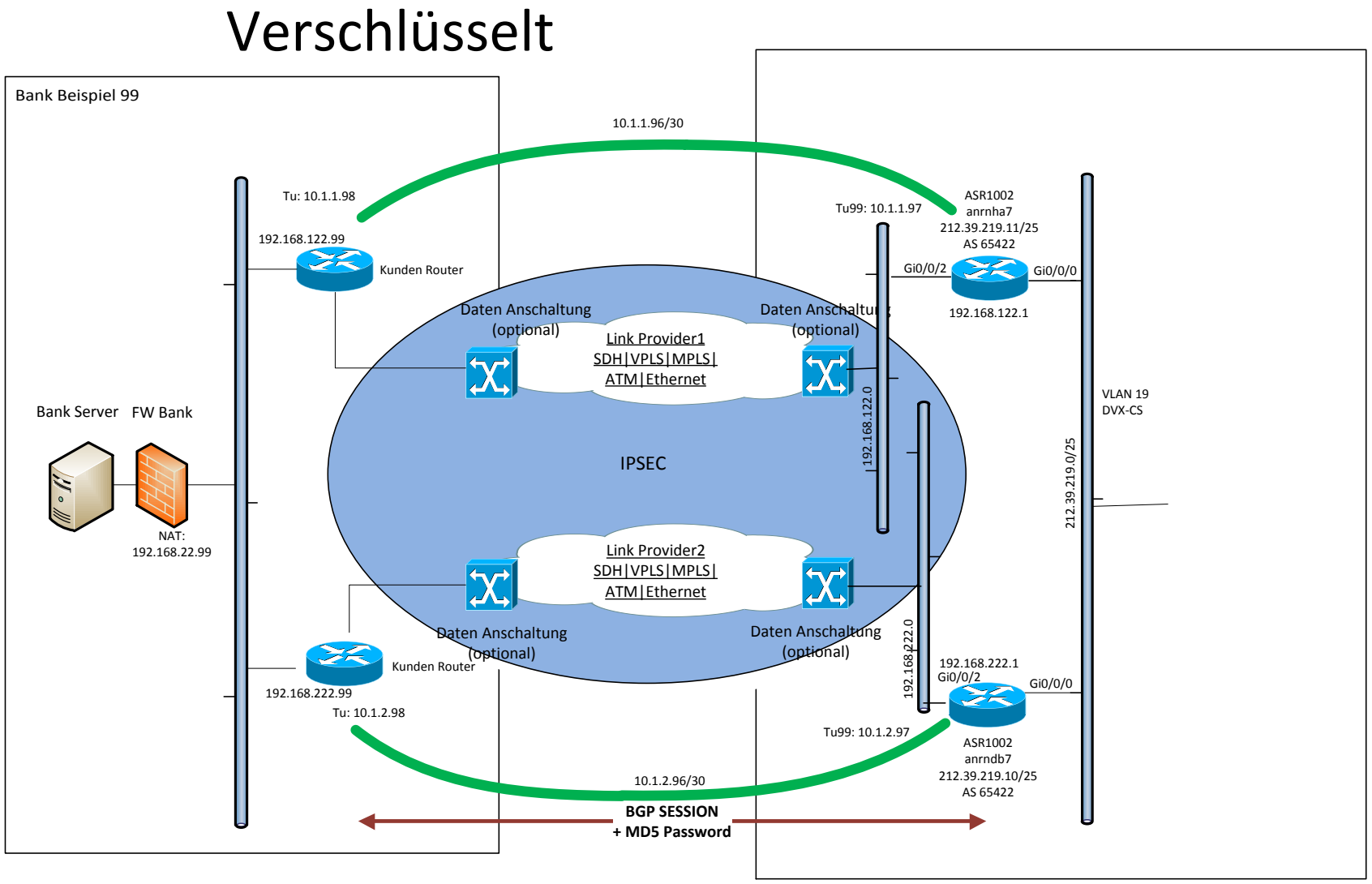
Oesterreichische Nationalbank, Abteilung ITO:

DI Michael Taurer, BSc	E-Mail: michael.taurer@oenb.at	Telefon: +43-1-40420/2746
Ing. Thomas Zenz	E-Mail: thomas.zenz@oenb.at	Telefon: +43-1-40420/2744

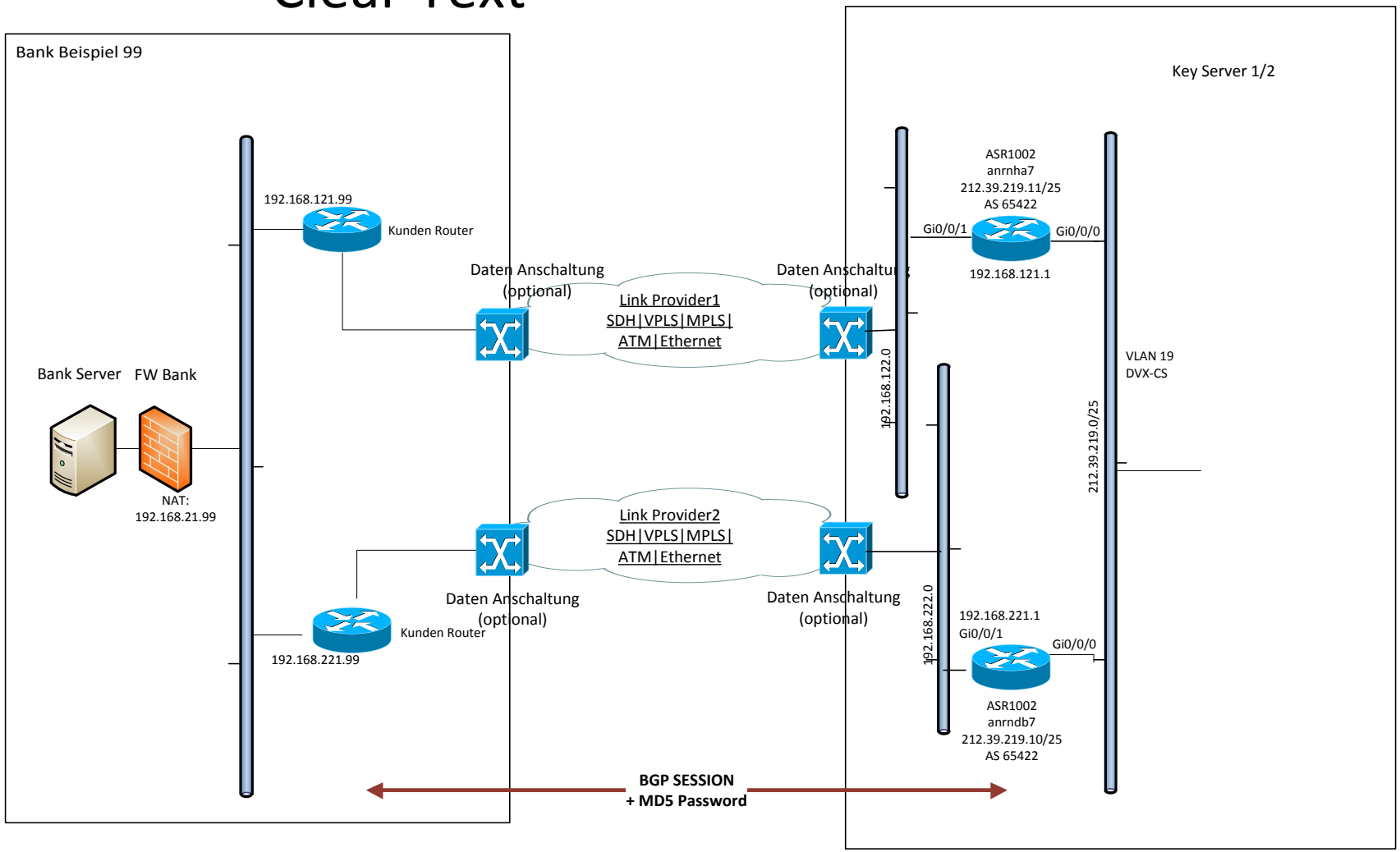
10 Abkürzungsverzeichnis

IPsec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
PSK	Preshared Key
GET VPN	Group Encrypted Transport VPN
VPLS	Virtual Private LAN Service (sieheKapitel 11)
BGP	Border Gateway Protokoll (Routing-Protokoll)
SA	Security Association
GDOI	Group Domain of Interpretation
DN	Distinguished Name

11 Glossary


Verschlüsselt
Bank Beispiel 99
10.1.1.96/30
Tu: 10.1.1.98
192.168.122.99
Kunden Router
Tu99: 10.1.1.97
ASR1002
anrnha7
212.39.219.11/25
AS 65422
Gi0/0/2
Gi0/0/0
192.168.122.1
Daten Anschaltung
(optional)
Link Provider1
SDH|VPLS|MPLS|
ATM|Ethernet
Daten Anschaltung
(optional)
192.168.122.0
VLAN 19
DVX-CS
212.39.219.0/25
Bank Server
FW Bank
IPSEC
NAT:
192.168.22.99
Link Provider2
SDH|VPLS|MPLS|
ATM|Ethernet
Daten Anschaltung
(optional)
Daten Anschaltung
(optional)
192.168.222.0
192.168.222.1
Gi0/0/2
Gi0/0/0
Kunden Router
192.168.222.99
Tu: 10.1.2.98
Tu99: 10.1.2.97
ASR1002
anrndb7
212.39.219.10/25
AS 65422
10.1.2.96/30
BGP SESSION
+ MD5 Password

Clear Text


Bank Beispiel 99
Key Server 1/2
192.168.121.99
Kunden Router
Daten Anschaltung
(optional)
Link Provider1
SDH|VPLS|MPLS|
ATM|Ethernet
Daten Anschaltung
(optional)
ASR1002
anrnha7
212.39.219.11/25
AS 65422
Gi0/0/1
Gi0/0/0
192.168.121.1
Bank Server
FW Bank
NAT:
192.168.21.99
192.168.122.0
VLAN 19
DVX-CS
212.39.219.0/25
Link Provider2
SDH|VPLS|MPLS|
ATM|Ethernet
Daten Anschaltung
(optional)
Daten Anschaltung
(optional)
192.168.221.99
Kunden Router
192.168.222.0
192.168.221.1
Gi0/0/1
Gi0/0/0
ASR1002
anrndb7
212.39.219.10/25
AS 65422
BGP SESSION
+ MD5 Password