

**Bilateral and Multilateral Processing of  
International Transactions in Europe  
Minimum Requirements on IP based networks**

Version 2.0

Date: 02/02/2007

## Notice

This Specification has been prepared by the Participants of the Berlin Group. Permission is hereby granted to use the document solely for the purpose of implementing the Specification subject to the following conditions: (i) that none of the participants of the Berlin Group nor any contributor to the Specification shall have any responsibility or liability whatsoever to any other party from the use or publication of the Specification; (ii) that one cannot rely on the accuracy or finality of the Specification; and (iii) that the willingness of the participants of the Berlin Group to provide the Specification does not in any way convey or imply any responsibility for any product or service developed in accordance with the Specification and the participants of the Berlin Group as well as the contributors to the Specification specifically disclaim any such responsibility to any party.

Implementation of certain elements of this Specification may require licenses under third party intellectual property rights, including without limitation, patent rights. The Participants of the Berlin Group and any other contributors to the Specification are not, and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. **This Specification is provided "AS IS", "WHERE IS" and "WITH ALL FAULTS", and no participant in the Berlin Group makes any warranty of any kind, express or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights (whether or not the Participants of the Berlin Group have been advised, have reason to know, or are otherwise in fact aware of any information), and fitness for a particular purpose (including any errors and omissions in the Specification).**

To the extent permitted by applicable law, neither the Participants of the Berlin Group nor any contributor to the Specification shall be liable to any user of the Specification for any damages (other than direct actual out-of-pocket damages) under any theory of law, including, without limitation, any special, consequential, incidental, or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, nor any damages arising out of third party claims (including claims of intellectual property infringement) arising out of the use of or inability to use the Specification, even if advised of the possibility of such damages.

The Participants of the Berlin Group are: Banksys, Belgium; Ceca, Spain; Cetrel, Luxemburg; Co.Ge.Ban, Italy; EURO Kartensysteme, Germany; Europay, Austria; Equens, The Netherlands; SSB, Italy; Seceti, Italy; ServiRed, Spain; Sibs, Portugal; Sistema 4B, Spain; Zentraler Kreditausschuss, Germany; Visa Europe; Master Card; First Data Europe; Eufiserv, Belgium; Link, United Kingdom.

Participation in the Berlin Group does not imply either endorsement of any of the solutions identified in the Feasibility Study, carried out by the Berlin Group, or a commitment to implement them.

The Specification, including technical data, may be subject to export or import regulations in different countries. Any user of the Specification agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import the Specification.

**Contents**

**1 Introduction ..... 1**

**2 Definitions..... 2**

**3 Minimum IP VPN standard requirements..... 3**

**4 Minimum IP VPN Network objectives ..... 4**

**5 Minimum gateway architecture..... 5**

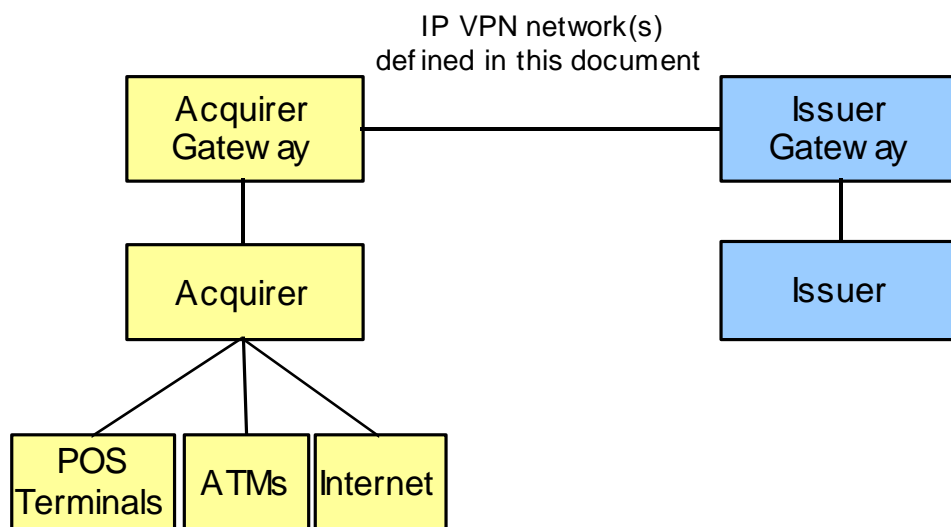
**6 Glossary ..... 7**

## 1 Introduction

This document describes the minimum requirements on IP based networks, which are used between international gateways in order to authorize, clear and settle international bank card originated debit transactions.

The acquirer gateways receive messages from acquirers that process card based transactions originating from ATMs, POS terminals or the internet. The acquirer gateways communicate with the issuer gateways to receive online authorization from the issuer of the card.

The acquirer gateways receive clearing information from acquirers that process card based transactions originating from ATMs, POS terminals or the internet. The acquirer gateway communicates with the issuer gateway sending and receiving batch files containing transaction messages like presentments, reversals and charge backs for defining the reconciliation amount to be settled between issuer and acquirer for a fixed clearing period.



**Figure 1: Infrastructure for bilateral and multilateral processing of international transactions**

The focus of this document is on the minimum requirements on IP based networks used to send the above mentioned ISO 8583 messages exchanged between acquirer gateways and issuer gateways.

## 2 Definitions

For the sake of clarification, some definitions are provided hereafter:

**Gateway:** platform used to exchange authorizations and clearing files with one or more other gateways.

**VPN:** a private communications network often used within a company, or by several companies or organizations, to communicate confidentially over a publicly accessible network. VPN message traffic can be carried over a public networking infrastructure (e.g. the Internet using encryption) on top of standard protocols, or over a service provider's private network with a defined Service Level Agreement (SLA) between the VPN customer and the VPN service provider.

**IPSEC:** an encryption method based upon IP-technology. It is a standardized framework for securing Internet Protocol (IP) communications by encrypting and/or authenticating each IP packet in a data stream.

Type of connections - in the context of the network Bilateral or Multilateral mean the following:

**Bilateral** connection: one to one connection

**Multilateral** connection: 1 to N connections (where N is > 1). Each gateway is connected to more than one other gateway:

For one gateway these are the only two possibilities.

When all members are participating, all gateways between themselves have 1 or more connections.

### 3 Minimum IP VPN standard requirements

The minimum service a network service provider has to provide is “connectivity”. Security services for confidentiality and integrity (e.g. encryption) is not a required service a network service provider has to provide. This decision was taken on the basis of a risk analysis, taking into account the current applications being processed via the Berlin Group specifications and the known threats.

A service provider must provide for the following attributes. Means for an adequate service level control must be defined in service level agreements:

Items	Requirements	Notes
<b>Performance</b>		<b>Connectivity/Performance is the main feature the network service provider has to provide.</b>
Availability	> 99.9	Approximate 8,5 hours of down-time per year. Depending on this requirement the service provider decides which solution is used to connect the members premises to the Berlin-Group VPN.
MTTR	4 hours	“Mean time to repair” means the average down-time per site.
RTD	< 200 ms	
<b>Quality of Services - QoS</b>		
# of classes	>2	For clearing and settlement files and for authorization requests.
<b>IP-Adresses</b>		
# of IP addresses per subnet	> 8	Minimum number of IP addresses the network provider has to provide for each gateway. The users of Berlin Group interfaces will agree on an IP network address range.
<b>Access points (POPs)</b>		
Locations	To be defined	Cities where access points must be present. Ability to provide for access for locations without PoPs.

#### **4 Minimum IP VPN Network objectives**

The VPN IP Network should be designed for secure and fast connections through Gateways.

The VPN IP network should at least cover the Single European Payment Area SEPA (Euro and Non Euro-countries).

The type of traffic IP VPNs must process according to Berlin Group specifications is at least as follows:

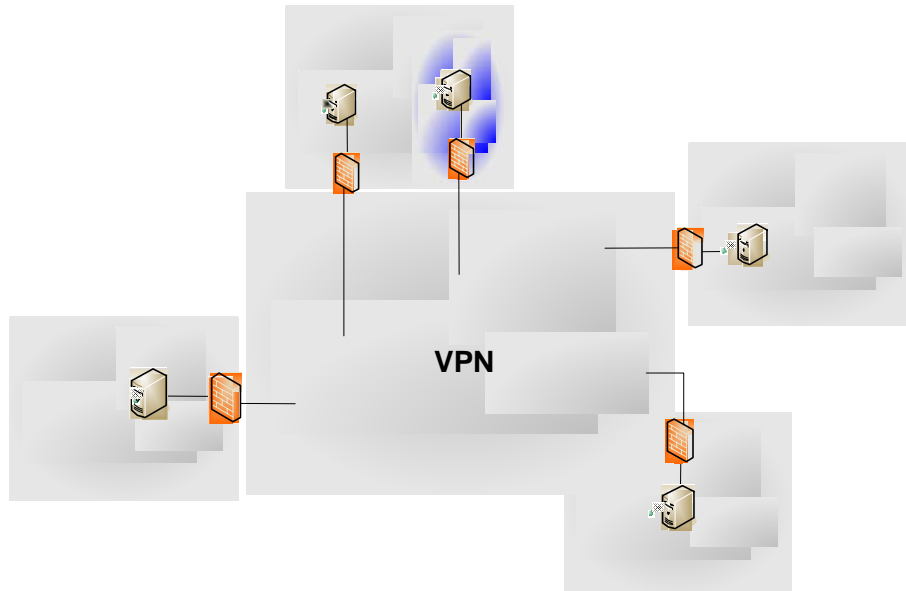
- Authorization traffic,
- File transfers for clearing and settlement.

Preconditions for the usage of an IP VPN network by gateways using Berlin Group Specifications should be:

- Rapid & Costless SEPA presence,
- Telecommunication independence,
- Gateway isolation,
- Network isolation : network problems at a Gateway site must not impact the traffic of other Gateways,
- Future proof technology,
- Network redundancy.

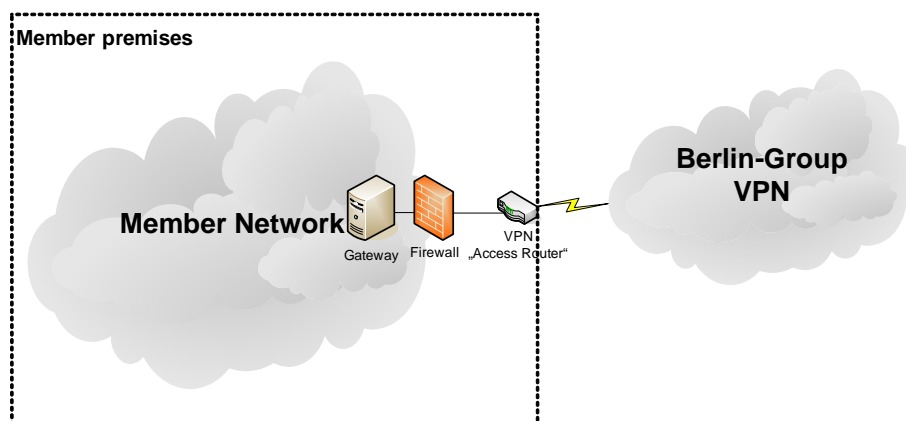
## 5 Minimum gateway architecture

The general structure of an IP VPN processing via Berlin Group interfaces is shown in the following picture. All gateways are connected directly to an IP VPN operated by a network service provider using firewall systems under control of the gateway. The service provider



recommends how to connect each member to the IP VPN to fulfill availability requirements.

The network service provider is responsible for the operation of the IP VPN and access to this network up to the network link located at the premises of each participating entity. The “Blue” network is a sample how to implement backup-sites.



The network structure at each gateway site is shown in more detail at the following picture:

Usually access to the IP VPN takes place using an access router operated by the network service provider. The gateway is normally free to design the network topology “behind” the access router (e.g. implementing network address translation [NAT] on the firewall). The

solution the network service provider offers must not limit the flexibility of each gateway within the parameters of the agreed service.

## 6 Glossary

Term	Definition
NAT	Short for <i>Network Address Translation</i> , an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations.
BGP	Short for <i>Border Gateway Protocol</i> , an exterior gateway routing protocol that enables groups of routers (called autonomous systems) to share routing information so that efficient, loop-free routes can be established. BGP is commonly used within and between Internet Service Providers (ISPs). The protocol is defined in RFC 1771.
VPN	Short for <i>Virtual Private Network</i> , a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.
MTTR	Short for <i>Mean Time To Repair</i> . The usual time taken to fix a problem that occurs on the network. Targets are normally set within an SLA and depends on the priority of the fault
RTD	Short for <i>Round Trip Delay</i> . The elapsed time for transit of a signal over a closed circuit.
ACL	Short for <i>access control list</i> , a set of data that informs a computer's operating system which permissions, or access rights, that each user or group has to a specific system object, such as a directory or file. Each object has a unique security attribute that identifies which users have access to it, and the ACL is a list of each object and user access privileges such as read, write or execute.
QoS	Short for <i>Quality of Service</i> , a networking term that specifies a guaranteed throughput level. One of the biggest advantages of ATM over competing technologies such as Frame Relay and Fast Ethernet, is that it supports QoS levels. This allows ATM providers to guarantee to their customers that end-to-end latency will not exceed a specified level.
IPSec	Short for IP Security, a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPSec has been deployed widely to implement Virtual Private Networks (VPNs).

Term	Definition
MPLS	<p data-bbox="386 392 1404 539">Short for Multiprotocol Label Switching, an IETF initiative that integrates Layer 2 information about network links (bandwidth, latency, utilization) into Layer 3 (IP) within a particular autonomous system--or ISP--in order to simplify and improve IP-packet exchange.</p> <p data-bbox="386 573 1404 645">MPLS gives network operators a great deal of flexibility to divert and route traffic around link failures, congestion, and bottlenecks.</p>