Remote Service

Connectivity Information
SAP/DVS ID 10373979 GSS 000 07

Table of contents

1 Document History

Version	Date	Name	Reason
V00 GRIPS v1	19-Nov-2010	Thomas Maly	Added information for Roche Vanilla Agent and connect 2 Minor changes throughout the document. Changed PAP to GSS document → Digital Signature in DVS
V01 GRIPS v2	19-May-2011	Thomas Maly	Updated complete document to reflect new Axeda infrastructure hosted by Axeda in the On Demand Center.
V02 GRIPS v3	23-Oct-2011	Thomas Maly	Corrected B2BVPN hostnames. Added more connectivity details (e.g. Proxy information).
V03 GRIPS v4	25-Apr-2013	R. Gwerder, C. Schindler	Changed 'TeleService' to 'Remote Service'. Changed 'cobas IT firewall' to 'FortiGate 40C'. Added more details for the Virus Definition deployment. Glossary aligned with Remote Service Glossary 10013271 PJM 000 03.
V04 GRIPS v5	03-Jun-2014	Roland Gwerder	• Changed 'Out of Scope' as the UK is now on the global DMZ. • Removed a duplicate table under 'Basic connectivity requirements' under '6.1.3 Connectivity requirements'. • Updated information regarding 'Client Hello packets' under chapter '6.1.3 Connectivity requirements'. • Removed references regarding 'UK exceptions' as the UK has joined the global DMZ. • Updated information regarding communication protocols under chapter '6.2.1 Roche Connectivity Layer Tunnel'.
V05 GRIPS v6	12-Aug-2015	S. Rosu R. Gwerder	• Updated connectivity diagrams • Updated glossary with 'WiFi' and '3G' • Team email address updated • Changed title of the documentation set under chapter Scope • Added additional chapter (8) for the test environment URLs and IP addresses • Updated B2B VPN chapter with new contact details
V06 GRIPS v7	20-Jan-2016	C. Schindler	• Document History corrected, release dates and GRIPS version number added • Document references updated in chapter Scope • Corrected IP address for teleservice2.roche.com from 196.3.50.101 to 196.3.50.51
V07 GRIPSv8	Date of Approval	F.Merk	• Corrected IP address for teleservice4.roche.com from 196.21.20.150 to 198.21.20.150

Disclaimer: Working copy if printed.

2 Purpose

The purpose of this document is to describe the ***technical connectivity*** of the Roche Remote Service Platform. This document should also give answers to potential questions arising from the laboratory IT-personnel. The target audiences of this document are Roche Affiliates world-wide.

The document describes main aspects of the Remote Service Platform infrastructure related to ***connectivity***. Regulatory agencies *may require more detailed documentation from Roche*.

Organizational solutions for regulatory compliance are here only suggested – local country organizations consulted by Remote Service are responsible for the implementation.

3 Scope

This document is part of the Remote Service Privacy, Security and Connectivity documentation. The complete set is outlined below:

- Remote Service Privacy Information (SAP/DVS ID 10373982)
- Remote Service Security Information (SAP/DVS ID 10373981)
- Remote Service Connectivity Information (SAP/DVS ID 10373979 / this document)

3.1 In scope

The described solutions apply to the **Remote Service Platform** infrastructure and hardware:

- Remote Service Platform
  - Axeda Enterprise
  - Axeda Global Access Servers
  - Axeda (Gateway) Agent
  - TeleService-Net
- **cobas®** link (including Roche Connectivity Layer Software)
- connect 2

3.2 Out of scope

Other Roche products besides the Remote Service Platform are out of scope.

4 Introduction

Remote Service offers a secure communication platform and service for Roche Diagnostics: The “Remote Service Platform”.

Primary objective is to increase the quality of service and additional cost containment for both sides (Customer, Roche).

Connectivity on the laboratory side is always established by the Axeda Agent or the Roche Connectivity Layer software.

The Axeda Agent is available for:

- connect 2 (hardware gateway), integrated part
- Standalone installation (software gateway) for direct installation on specific systems. The software gateway is further referenced as the “Roche Vanilla Agent”.
- **cobas**® link (hardware gateway), integrated part

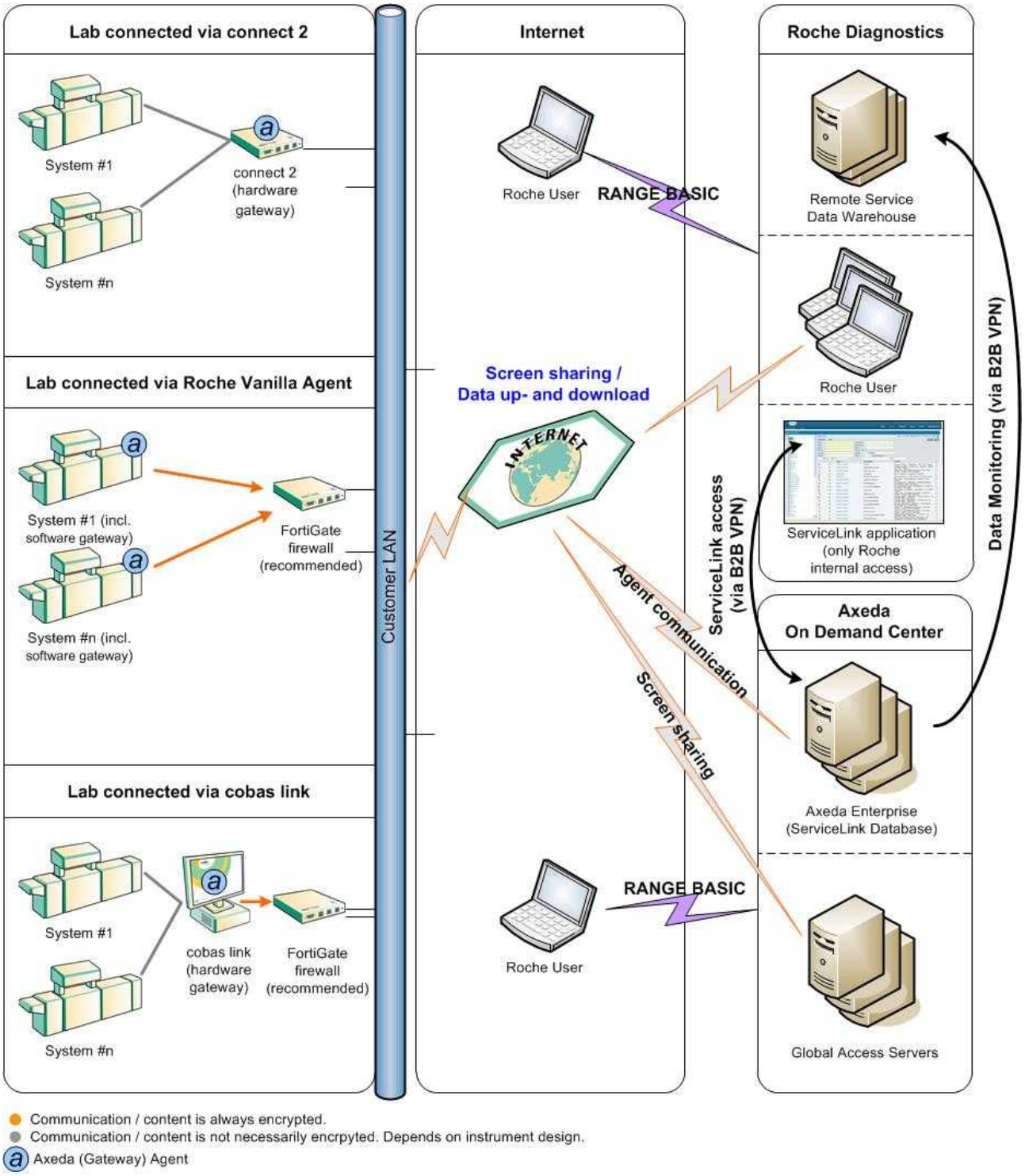
The Roche Connectivity Layer (RCL) is available for:

- **cobas**® link (hardware gateway), integrated part

Generally, the following use cases are implemented:

(Depending on the system type, one or more services may be available.)

1. **Remote sessions** incl. manual **data transfer** (on response to user‘s reported problems). These services are offered by the Axeda Agent only.
    - From Roche User PC to remote system (e.g. cobas 6000 or Integra 400) (files can be transferred in both directions).
    - From Roche User PC to remote gateway (e.g. **cobas**® link or connect 2) (files can be transferred in both directions).
2. Scheduled **data transfer** from remote host to Roche: These services are offered by the Axeda Agent and the RCL.
    - upload of monitoring information
    - on-line monitoring of systems (e.g. alarm data)
    - performance evaluation
3. Scheduled **data transfer** from Roche to remote host: These services are offered by the Axeda Agent and the RCL.
    - Download of system parameters, chemistry lot data of reagent / calibrators / controls (e-BC → electronic Barcode)
    - Download of Human Readable Data (e-PI → electronic Package Insert – regulatory relevant information similar to package insert or other information for customer)
    - Download of software patches / upgrades / security hot fixes and virus definitions.



Schematic overview outlining the basic connectivity involved for the Remote Service Platform (Axeda services only).

Details are described in the following chapter: “5 - Infrastructure characteristics”

5 Infrastructure characteristics

The **Remote Service Platform** is the infrastructure and the software used for transfer, storage, evaluation and presentation of information. The Remote Service Platform hardware & software is mainly outsourced to the Axeda Corporation and is subject to regular security related procedures of Roche IT organization (e.g. penetration tests by independent consultants).

The connect 2, Roche Vanilla Agent and the **cobas®** link are communication gateways. Where the connect 2 and **cobas®** link contain Roche provided hardware including communication software, the Roche Vanilla Agent is pure software only. The gateways are located at the customer site and function primarily as a secure communication gateway between the system network and the Axeda Enterprise (ServiceLink & Global Access Servers).

Axeda ServiceLink is a 3rd party software providing a communication and data exchange solution comparable to the Remote Connectivity Layer, which is a Roche developed solution. The **Axeda (Gateway) Agent** is pre-installed on the connect 2 and the **cobas®** link hardware gateway.

Global Access Servers are required by the Axeda ServiceLink application to provide efficient screen sharing sessions world-wide.

The **Remote Service Data Warehouse** (RSDW) is a temporary data storage (XML) for uploaded instrument data (e.g. monitoring information). This data is then made available for other Roche business applications.

5.1 Hosting / access details

Axeda Solution

All services (hardware & software) are outsourced to the Axeda Corporation.

- The Axeda Enterprise system is physically located in a Datacenter in Europe (Germany). The disaster recovery infrastructure is physically located in the United States.
- The Global Access Servers are physically located at three different sites: Europe (Germany), North America and Asia.

The Axeda ServiceLink application is accessible Roche internally only. It is not available directly via the internet. Users accessing the application from a Roche internal computer are always authenticated using their active directory credentials. User accessing the application via the internet using the Roche service “**RANGE BASIC**”, are authenticated by a 2-factor authentication mechanism. RANGE is a service offered by Roche Global Informatics.

Roche Connectivity Layer Solution

All services (hardware & software) are hosted Roche internally. The system is used for data distribution only. The enterprise infrastructure is called “TSN or TeleService-Net”

6 Communication pathways

As described in chapter 4 - Introduction, the Axeda agent is an integrated part of the connect 2 and **cobas®** link hardware gateway. In addition, the Axeda agent is available as pure software: Roche Vanilla Agent (RVA). The communication pathways are similar

In addition to the Axeda agent, the Roche Communication Layer (RCL) is offered as a gateway software on the **cobas®** link only. The **cobas®** link is equipped with the Axeda (Gateway) Agent and the RCL.

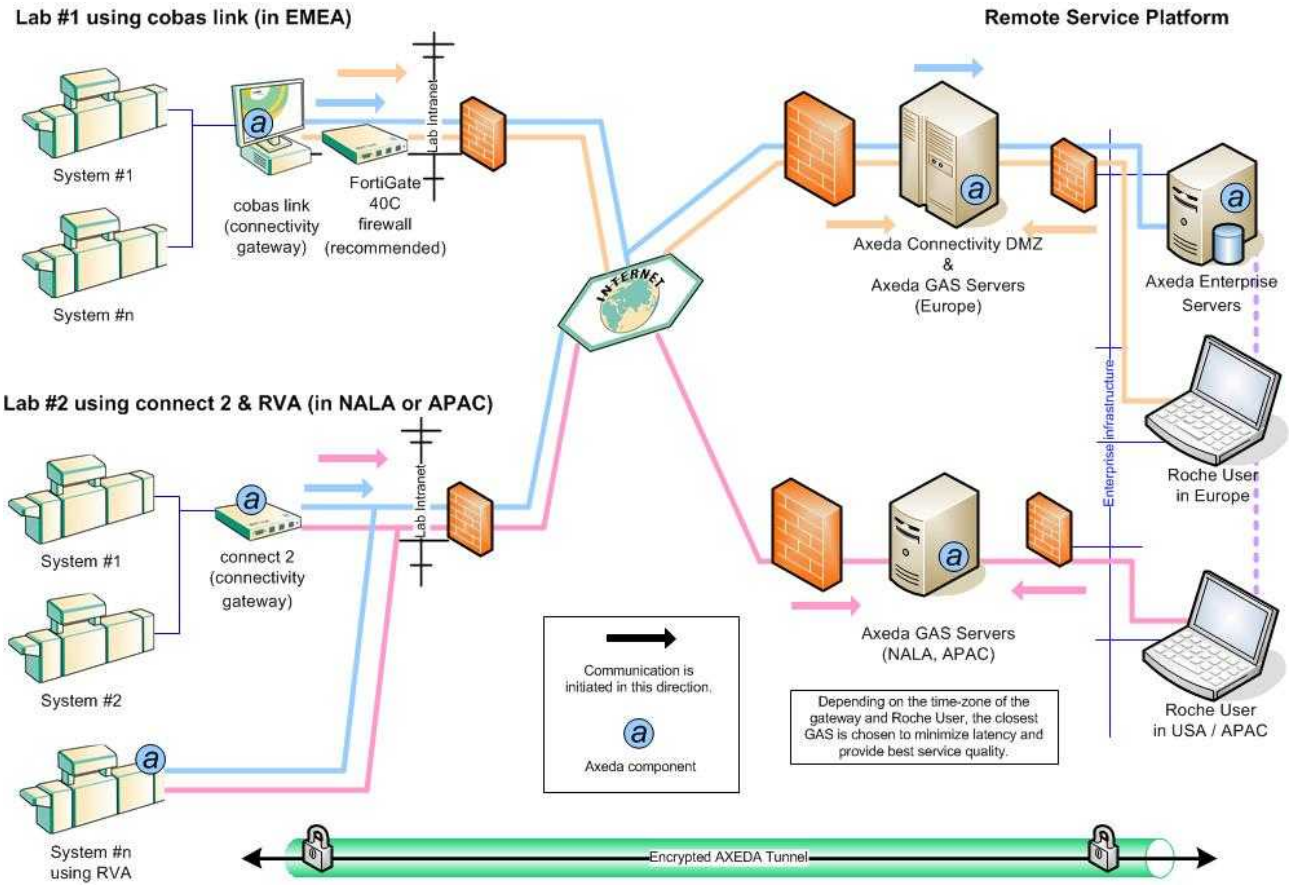
Please note:

In chapter 6.1, only the Axeda Agent communication is described in detail.

In chapter 6.2, only the RCL communication for the **cobas®** link is described in detail.

6.1 Axeda solution

The Axeda solution is available for the connect 2, Roche Vanilla Agent and the **cobas®** link.



The Axeda Tunnel ensures secure connectivity between the **gateway** in the laboratory and the **Axeda Enterprise** servers located in the Axeda On Demand Center (ODC). For transfer in both directions the data is encrypted between the tunnel services on the **gateway** in the Lab and the corresponding tunnel services.

The connection for all use-cases (bidirectional data transfer and screen sharing) is initiated by the **gateway**, i.e. from the laboratory point of view it is an outgoing connection only.

The **gateway** sends status information (blue line) on a regular base to the Axeda Enterprise Server. If a screen sharing session is initiated by an authorized **Roche** user, the request will be forwarded to the **gateway** and the Axeda GAS (Global Access Servers). For best performance, the request will be forwarded to a GAS near the **Roche** user. (purple and orange line)

For the connectivity between the Roche Corporate Network (RCN) and the ODC, a VPN is in place. For a schematic overview, see chapter 4.

6.1.1 Axeda Tunnel – HTTPS Tunnel

All Traffic between the components involved in the Axeda solution (**Gateway**, GAS, Enterprise and Roche User PC) is encrypted using the HTTPS protocol. The Axeda Gateway Agent initiates all communication between devices and the Enterprise Server. It sends XML-formatted data to the Enterprise Server through HTTP POSTs. After receiving a message, the Enterprise Server can reply to the agent with SOAP-formatted data. This response message can contain commands for the agent.

GAS servers are available in Europe, North America and Asia. Their only function is to minimize latency and maximize throughput by optimizing communication pathways for screen sharing.

Axeda Enterprise Servers provide management functionality for the Axeda infrastructure. Authentication is performed between the Axeda Enterprise Server and the Roche User. Only authorized **Roche** users can access the system.

6.1.2 Components description

Axeda (Gateway) Agent

The **Axeda (Gateway) Agent** is a communication package running standalone (RVA) or embedded on dedicated hardware (connect 2 or **cobas®** link). The gateway is located at customer site and functions primarily as a secure communication gateway between the system cluster and the Axeda On Demand Center for data transfer and screen sharing.

Axeda Global Access Server (GAS)

The primary use cases for GAS servers are:

- Perform handshake between incoming connections (from **gateway** and Roche user pc)
- Load balancing of Axeda screen sharing traffic.

The GAS servers are based on a standard internet server with installed 3rd party software. If one GAS server is not available, connection will automatically be established using another GAS server. Traffic is redirected to the GAS server closest to a **gateway** based on time zone settings.

Axeda Enterprise server

The primary use case of the Axeda Enterprise server is to manage devices (e.g. **gateways** and systems) and to initiate screen sharing sessions.

The functions / roles are:

- Provides a web user interface for verified users to establish screen sharing to Axeda Gateway Agents and its managed devices.
- Enables and manages secure communication to the Axeda Gateway Agent.

6.1.3 Connectivity requirements

In order the **Axeda Agent** is operating as expected, the following requirements must be met by the customer's infrastructure.

Basic connectivity requirements

To connect to the Enterprise and GAS Servers, the following IP addresses and ports need to be accessible from the system:

Description	IP	Hostname	Port	Protocol
Axeda On Demand Center (ODC) infrastructure				
Axeda Enterprise ODC	62.209.44.11	remoteservice.roche.com	443	TCP / SSL
Axeda DR Enterprise ODC	209.202.167.21	remoteservice-dr.roche.com	443	TCP / SSL
Axeda GAS1 ODC (EMEA)	62.209.44.21	remoteservice-gas1.roche.com	443	TCP / SSL
Axeda GAS2 ODC (EMEA)	62.209.44.22	remoteservice-gas2.roche.com	443	TCP / SSL
Axeda GAS3 ODC (NALA)	209.202.167.19	remoteservice-gas3.roche.com	443	TCP / SSL
Axeda GAS4 ODC (NALA)	209.202.167.20	remoteservice-gas4.roche.com	443	TCP / SSL
Axeda GAS5 ODC (APAC)	120.136.45.231	remoteservice-gas5.roche.com	443	TCP / SSL
Axeda GAS6 ODC (APAC)	120.136.45.230	remoteservice-gas6.roche.com	443	TCP / SSL
Roche Global Informatics (GI) infrastructure → reserved for later usage. Should be kept accessible if possible[1]				
Reserved	196.3.50.74		443	TCP / SSL
Reserved	206.53.227.31		443	TCP / SSL
Reserved	196.3.56.90		443	TCP / SSL
Reserved	196.3.47.149		443	TCP / SSL

DNS information is required in order the service is operational. If no DNS service is available, manual configuration via the systems' host file is required.

Description	IP	Hostname	Port	Protocol
Domain Name Service	customer specific	customer specific	53	TCP / DNS

The ODC Enterprise Servers are located at these places:

- Enterprise Germany, Frankfurt
- Disaster Enterprise Waltham, Massachusetts

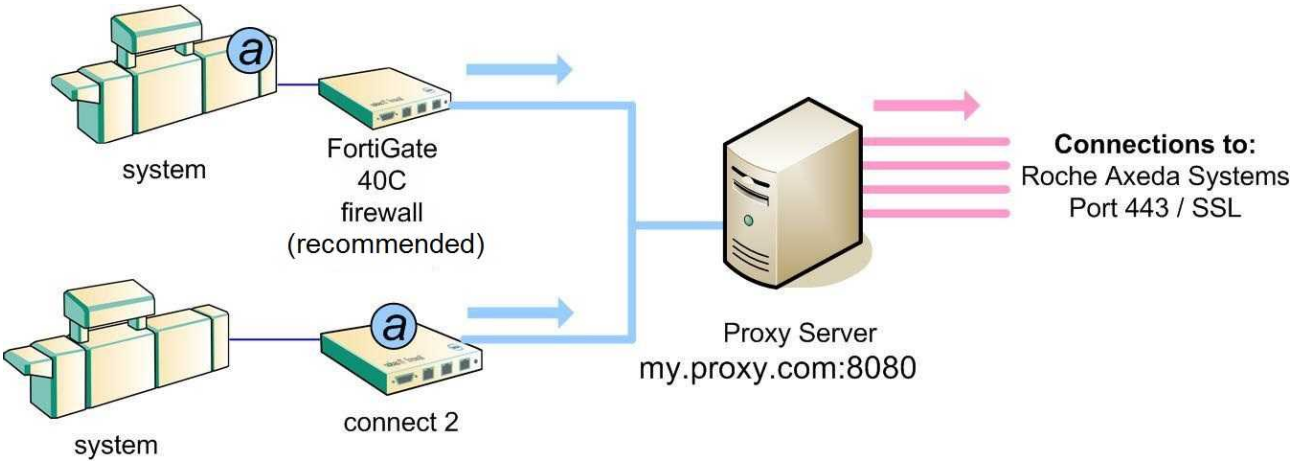
The ODC GAS Servers are located at these places:

- EMEA Germany, Frankfurt
- NALA Waltham, Massachusetts
- APAC China, Hong Kong

[1] These addresses were previously used for the Axeda sergate servers hosted by Roche IT, until 2012.

Advanced connectivity requirements

The Axeda Agent is proxy aware. **HTTP** and **SOCKS** proxy incl. authentication with username and password is supported. If there is a **Proxy Server** in place at the customer site, the Axeda solution needs **outgoing** connectivity to the proxy server **ONLY!** All traffic is directly redirected from the Roche Axeda Agent to the customer's proxy. While establishing the connection, the Roche Axeda agent informs the proxy about the final destination. This behavior is valid for any type of Axeda installation. The following picture shows a schematic example for a proxy installation:



SSL handshake requirements

During the establishment of the secured connection between the Roche Axeda agent and the Enterprise system, a so called SSL handshake is performed. During this handshake, the client and the server agree on an encryption standard and exchange certificates. Depending on the implementation, the client offers more or less encryption options. By default, the first option is chosen: "TLS_RSA_WITH_AES_128_CBC_SHA".
Intrusion Detection / Prevention systems or firewalls might not allow communication depending on how the SSL handshake looks like. For this reason, detailed specifications are listed below:

Client Hello packet for Roche Vanilla Agent 2.0

- Cipher Spec: TLS_RSA_WITH_AES_128_CBC_SHA
- Cipher Spec: TLS_RSA_WITH_RC4_128_SHA
- Cipher Spec: TLS_RSA_WITH_RC4_128_MD5
- Cipher Spec: SSL2_RC4_128_WITH_MD5

Client Hello packet for Roche Vanila Agent 2.1

- Cipher Spec: TLS_RSA_WITH_AES_128_CBC_SHA
- Cipher Spec: TLS_RSA_WITH_RC4_128_SHA
- Cipher Spec: TLS_RSA_WITH_RC4_128_MD5
- Cipher Spec: TLS_EMPTY_RENEGOTIATION_INFO_SCSV

The customer infrastructure must be configured to allow these types of packets including responses.

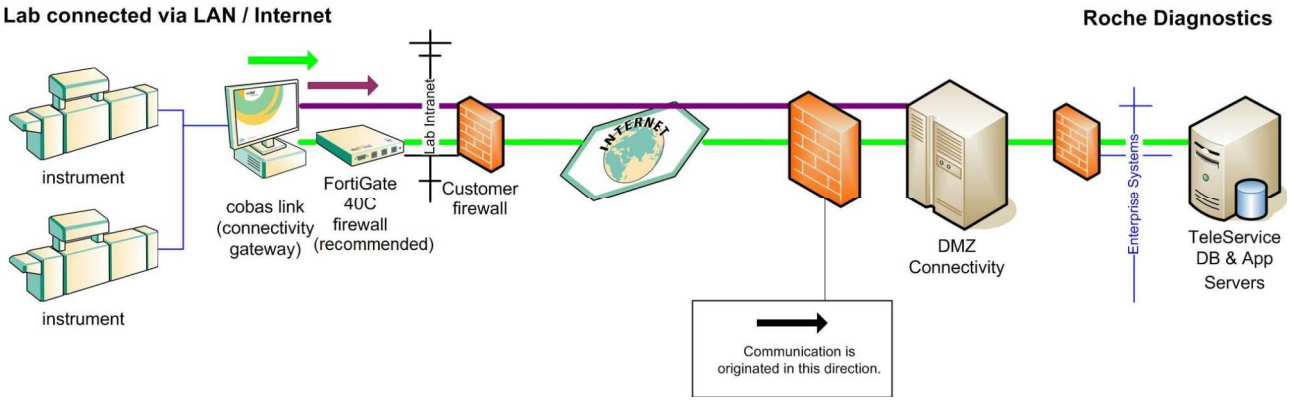
Certificates

Certificates are necessary for the SSL handshake. The Roche Axeda solution is based on Roche signed certificates. These certificates can be obtained from the Roche Certificate Authority by anyone from: http://certinfo.roche.com/

Intrusion Detection / Prevention systems or firewalls might not allow communication, until these certificates are manually loaded into the system.

6.2 Roche Connectivity Layer solution

The Roche Connectivity Layer solution is available for the **cobas®** link only.



1. (——— green, continuous line) The communication pathway assumes fix connection between the laboratory intranet and Internet. This communication pathway may be used for all use cases (bi-directional data transfer and remote screen sharing).
   The communication is originated from the **cobas®** link.

2. (——— purple, continuous line) The Symantec Antivirus LiveUpdate initiates a connection from the **cobas®** link to keep the virus definitions up to date. This is performed using the already existing LAN connection.

6.2.1 Roche Connectivity Layer Tunnel

Communication protocols

For the communication between **cobas®** link and Remote Service infrastructure (DMZ Connectivity Server) the following protocols are used.

- HTTP / **BITS** with encrypted payload (for download)
  If BITS is blocked fall back to pure HTTP is performed.
  This service is for e-Library and patches download.
- HTTP / **SOAP** with encrypted payload (for upload)
  This service is for monitoring data upload.
- HTTP with signed payload (for download)
  This service is for virus definition download..

* Screen sharing functionality has been decommissioned on the enterprise side.
The client side decommissioning is part of the Remote Service migration strategy.

HTTP Tunnel / Web Tunnel

Use Case: The “Web Tunnel” uses the HTTP protocol with *secure payload* for **data transfer** in both directions (Lab ⇔ Roche). It means the payload is encrypted, signed and compressed data. The data is in form of SOAP objects based on the XML definition proprietary for Roche / Hitachi content.

Symantec AntiVirus virus definitions are digitally signed by Symantec and transferred unencrypted via HTTP. AntiVirus Virus Definitions are tested by Remote Service and deployed afterwards to the **cobas®** links world-wide on a regular weekly to bi-weekly base. Immediate emergency deployment is possible.

6.2.2 Components description

cobas® link

The **cobas®** link is a communication package where communication software is running on a dedicated computer. The **cobas®** link is located at customer site and functions primarily as a secure communication gateway between the system cluster and the enterprise systems.

The primary use cases are bidirectional data transfer and screen sharing.

The roles of the **cobas®** link are:

- Gateway between connected systems in the lab and enterprise infrastructure.
- Increased protection of Lab intranet infrastructure against malicious code via Roche systems / Enterprise infrastructure
- Increased protection of Roche systems / instruments against malicious access

The interface to the instruments is specific for each instrument and is given by the proprietary instrument design (Roche and Hitachi). The data structures are defined in an XML schema and transferred as XML files, packets or SOAP objects.

Connectivity Server in the DMZ

The primary use cases are:

- Bidirectional data transfer via Internet

The functions / roles are:

- Connection point for all **cobas®** link systems via Internet.
- Protection of Roche intranet against external access

The Connectivity Server is based on a standard internet server with installed self developed application of the Message Broker and information forwarder (see below in the description of the web-tunnel). The application uses a simple database for managing the population of the connected **cobas®** link instances.

Remote Service DB & Application Servers

The instrument and user related information is stored and processed on the Remote Service DB & Application Servers. The technology is a standard relational database with a web user interface. Commercial tools are used for the DB, business processing and user interface. The data model, business logic and user interface correspond to the current business and organizational processes of Roche Diagnostics.

6.2.3 Connectivity requirements

In order the **Roche Connectivity Layer (RCL)** is operating as expected, the following requirements must be met by the customer's infrastructure.

Basic connectivity requirements

In order the RCL software can connect to the Remote Service infrastructure, the following IP addresses and ports need to be accessible from the system.

Description	IP	Hostname	Port	Protocol
TeleService DMZ	196.3.50.39	teleservice.roche.com	80	TCP / HTTP
TeleService DMZ	196.3.50.39	teleservice.roche.com	443	TCP / SSL

DNS information is required in order the service is operational.
If no DNS service is available, manual configuration via the systems' host file is required.

Description	IP	Hostname	Port	Protocol
Domain Name Service	customer specific	customer specific	53	TCP / DNS

Content Filter requirements

The RCL software is transporting encrypted data via port 80.
Content filter must not block this communication in order the system woks as expected.
For details, see section **"Advanced connectivity requirements"** below.

Advanced connectivity requirements

Proxies can be configured for Web-Tunnel (HTTP) connections.

The following is also required to ensure operation of the RCL:

- HTTP request / answer with binary payload
- HTTP/SOAP for data upload (ZIP / XML files)
- HTTP/BITS for data download (ZIP / EXE / TXT files)
- HTTP for virus definition download (m25 / ZIP files)

Certificate checks

As the cobas link has several Roche certificates installed, the operating system automatically connects to 196.3.50.147 / certinfo.roche.com on port 80 and 443 to verify revocation information. This service is not in use on the **cobas®** link and may be blocked by customer firewalls.

cobas® link specific requirements

- The cobas® link is supporting any type of IP-Address: DHCP or fixed.
- The cobas link is configured as a workgroup PC. (Domain membership is not supported.)
- The identifier for the computer name contains the serial number of the cobas® link, which is indispensable in support cases. This identifier cannot be changed.
- The **cobas®** link is designed to be turned on 24 hours / 7 days a week.

6.3 B2B VPN based on IPSec as carrier for Axeda and RCL connections

B2B (Business to Business) connections based on IPSec is an industry standard for inter-company collaboration over Internet. This chapter described the service offered by **Roche Mannheim** only.

Roche provides the **option** to establish a B2B VPN connection based on IPSec between Roche and customer to act as carrier. A dedicated VPN infrastructure for Remote Service is available at Roche Mannheim for this purpose only. B2B VPN connections enable connectivity between agreed IP-addresses and ports on both sides of the connection. Security controls to ensure this agreed connectivity are enforced by Roche but can also be enforced by the customer.

Please note: Traffic going through the VPN will exit the VPN depending on the use case:

- The Axeda Agent traffic will be forwarded from the RCN to the Axeda On Demand Center via a second B2B VPN.
- Screen sharing traffic will be forwarded from the RCN to the Axeda Global Access Servers via the internet.
- As the RCL enterprise systems are Roche internal only, no traffic forwarding is required and the traffic stays inside the RCN.

Roche accepts B2B connections to state of the art products of virtually all vendors like CISCO, Nokia, Checkpoint, etc. These connection parameters are supported by Roche:

Default IPSec VPN Configuration parameter

Phase 1 (Authentication)	**Setting**
Negotiation Mode	Preferred=Main; Optional=Aggressive
Encryption Algorithm	Preferred =AES-256; Optional =3DES-168
Hash Algorithm	Preferred =SHA-1/HMAC-168; Optional =MD5/HMAC-128
DH Key Group	Preferred =2; Optional =1/5/7
Lifetime	Preferred =28'000s; Optional=Other
Method	Mandatory=Pre-Shared Key
Phase 2 (SA / Key Exchange)	**Setting**
Protocol	ESP
Encryption Algorithm	Preferred =AES-256; Optional =3DES-168
Hash Algorithm	Preferred =SHA-1/HMAC-168; Optional =MD5/HMAC-128
PFS Key Group	Preferred =disabled/off; Optional =2 -1024bit
Lifetime	Preferred =28'000s; Optional=Other

Remark: as the Axeda solution is based on a globally distributed architecture, any B2BVPN implementation makes the advantage of the GAS Server with regard to performance useless. The B2BVPN is not required from a security perspective; all traffic is encrypted anyway.

Contact:
For B2B VPN requests, an HPSM ticket shall be raised to **EMEA-ITS-EMEA LAN WAN SERVICES** by those persons / affiliates who require a B2B VPN connection.

If a Roche B2B VPN is in place, the following addresses and ports need to be accessible.
These values might have to be configured manually in the systems' host file:

Description	NAT IP for B2BVPN	Hostname for VPN	Port	Protocol
Axeda On Demand Center (ODC) infrastructure				
Axeda Enterprise ODC	162.132.161.147	remoteservice.roche.com	443	TCP / SSL
Axeda DR Enterprise ODC	162.132.161.148	remoteservice-dr.roche.com	443	TCP / SSL
Axeda GAS1 ODC (EMEA)	162.132.161.149	remoteservice-gas1.roche.com	443	TCP / SSL
Axeda GAS2 ODC (EMEA)	162.132.161.150	remoteservice-gas2.roche.com	443	TCP / SSL
Axeda GAS3 ODC (NALA)	162.132.161.151	remoteservice-gas3.roche.com	443	TCP / SSL
Axeda GAS4 ODC (NALA)	162.132.161.152	remoteservice-gas4.roche.com	443	TCP / SSL
Axeda GAS5 ODC (APAC)	162.132.161.153	remoteservice-gas5.roche.com	443	TCP / SSL
Axeda GAS6 ODC (APAC)	162.132.161.154	remoteservice-gas6.roche.com	443	TCP / SSL
Roche Global Informatics (GI) infrastructure → will be migrated to the ODC infrastructure. [2]				
Reserved	162.132.161.141		443	TCP / SSL
Reserved	162.132.161.145		443	TCP / SSL
Reserved	162.132.161.144		443	TCP / SSL
Reserved	162.132.161.146		443	TCP / SSL

Description	NAT IP for B2BVPN	Hostname for VPN	Port	Protocol
TeleService DMZ	162.132.161.140	teleservicevpn.roche.com	80	TCP / HTTP
TeleService DMZ	162.132.161.140	teleservicevpn.roche.com	443	TCP / SSL

Note: For Windows system, the host file is located at: C:\"windir"\system32\drivers\etc\hosts.
Where "windir" is the Windows installation folder.

[2] These addresses were previously used for the Axeda sergate servers hosted by Roche IT, until 2012.

7 Connectivity Contact at Roche

Questions and comments can be addressed to the Roche connectivity contact for Remote Service:
Please forward inquires to “global.gcs_remote-service@roche.com “

Note: Roche Affiliates are encouraged to follow the established procedures for inquires.

8 Basic connectivity requirements for the Roche test environments

In case there is a requirement to have gateways or instruments connected to one of the test environments (VAL, VER, DEV), the following IP addresses and ports need to be accessible from the system:

Validation environment (environment 1)

Description	IP	Hostname	Port	Protocol
Axeda Enterprise ODC VAL	62.209.44.37	remoteservice-val.roche.com	443	TCP / SSL
Axeda GAS7 ODC (EMEA)	62.209.44.43	remoteservice-gas7.roche.com	443	TCP / SSL
Axeda GAS8 ODC (EMEA)	62.209.44.44	remoteservice-gas8.roche.com	443	TCP / SSL
TeleService DMZ	196.3.50.51	teleservice2.roche.com	80	TCP / HTTP
TeleService DMZ	196.3.50.51	teleservice2.roche.com	443	TCP / SSL
e-Content	N/A	econtent-val.emea.roche.com/	N/A	N/A
TSN	N/A	rkamv1208/RIG.PortalUI/	N/A	N/A

Verification environment (environment 2)

Description	IP	Hostname	Port	Protocol
Axeda Enterprise ODC VER	62.209.44.103	remoteservice-ver.roche.com	443	TCP / SSL
Axeda GAS10 ODC (EMEA)	62.209.44.75	remoteservice-gas10.roche.com	443	TCP / SSL
TeleService DMZ	198.21.20.150	teleservice4.roche.com	80	TCP / HTTP
TeleService DMZ	198.21.20.150	teleservice4.roche.com	443	TCP / SSL
e-Content	N/A	econtent-e2.emea.roche.com/	N/A	N/A
TSN	N/A	rkamv1200/RIG.PortalUI/	N/A	N/A

Development environment (environment 3)

Description	IP	Hostname	Port	Protocol
Axeda Enterprise ODC DEV	62.209.44.51	remoteservice-dev.roche.com	443	TCP / SSL
Axeda GAS9 ODC (EMEA)	62.209.44.55	remoteservice-gas9.roche.com	443	TCP / SSL
TeleService DMZ	198.21.20.144	teleservice3.roche.com	80	TCP / HTTP
TeleService DMZ	198.21.20.144	teleservice3.roche.com	443	TCP / SSL
e-Content	N/A	econtent-ver.emea.roche.com	N/A	N/A
TSN	N/A	rkamv1202/RIG.PortalUI/	N/A	N/A

9 Glossary

Axeda infrastructure / part of Remote Service Infrastructure

Software and Hardware required to provide the following services:

- Screen sharing incl. gateway monitoring
- e-library; e-PI and e-BC download to **cobas®** link and instruments (in development)
- Collecting monitoring data from **cobas®** link and instruments (in development)

Axeda ServiceLink / Axeda Enterprise Server

ServiceLink is the frontend web application of Axeda Enterprise Server. The user can manage and remote connect to the remote assets from ServiceLink. Axeda Enterprise is the backend of Axeda ServiceLink. This application server collects, stores, and serves data generated by Axeda Agents. It provides applications that are used to screen share, monitor and troubleshoot devices.

Axeda Global Access Servers (GAS)

GAS Servers are placed in in different world regions to establish the connection between the customer side and the DMZ (Axeda product). Multiple servers are used to improve connection performance.

Axeda (Gateway) Agent

An Axeda software component running on the client side - it is the counterpart of Axeda ServiceLink on the server side. Axeda Gateway Agent is the off-the-shelf version, whereas Roche Vanilla Agent is the tailored version for Roche.

Axeda Desktop Viewer

Axeda Desktop viewer is a 3rd party software for screen sharing, it is a special implementation of UltraVNC. It is the screen sharing client for Axeda Desktop Server.

Axeda Desktop Server

A software component by Axeda to establish screen sharing sessions, it is a custom implementation of UltraVNC. The component runs on the Axeda assets, e.g. Roche instruments.

cobas e-library

Date repository supplied e.g. on cobas link, containing assay, calibration and QC documents, customer letters, and instrument-readable data for the analyzers. It is either updated automatically using network connectivity or by installation of an e-library CD at regular intervals.

cobas® link

cobas link is a gateway system custom-made by Roche Diagnostics, providing a secure remote connection for data transfer between the customer network and the Roche Corporate Network.

It supports several use cases, such as screen sharing, download & display of cobas e-library data, upload of monitoring data, and serves as destination for the backup.

connect 2

connect 2 is a gateway system (hardware) custom-made by Roche Diagnostics, providing secure remote connection between Roche corporate Network and customer laboratories. Connect 2 interconnects Axeda Enterprise Server on one side with Roche Vanilla Agent / Axeda client software at the customer site.

FortiGate-40C firewall

Firewall selected by Roche for usage in customer laboratories. The **FortiGate-40C** firewall can be installed in combination with a **cobas**® link and is also verified for certain systems.

electronic Barcode (e-barcode / e-BC / Instrument readable data / IRD)

An electronic data item that is downloaded to the instrument, via Remote Service infrastructure. The e-barcode files contain the information necessary for the instruments to process assays. The e-BC transfers the same data to cobas® systems which is provided e.g. to Hitachi Modular systems via barcode transfer sheets and scanned with barcode scanner.

electronic package insert (e-PI / Human readable data / HRD)

A set of PDF files that replaces the paper-based reagent kit inserts, data types are method sheets, target value sheets, customer letters, important notes, etc. These files can be read on and printed from the cobas® e-library on cobas® link.

Hardware Gateway

See **cobas®** link or connect 2 for details

Personal Data

Personal data are e.g. sensitive customer data, patient medical data, data on suppliers and employees, other personal data. See the EU Data Protection Directive 95/46/EC for definition of personal data at: http://eur-lex.europa.eu/

pcAnywhere

3rd party software for screen sharing (used by the legacy Remote Service and Axeda Infrastructure).

RANGE (Basic)

RANGE is a remote IT access service. Through RANGE, users can access the Roche Network from almost any computer, including COE computers, those at Internet Cafes and personal computers by visiting https://range.roche.net. Usage of the service requires 2-factor authentication.

Roche Connectivity Layer (RCL)

Software installed on the **cobas®** link to enable communication to the legacy Remote Service infrastructure.

Roche IT infrastructure

The term ‘Roche IT infrastructure’ refers to the complete Roche IT infrastructure.
However, only the Remote Service and Axeda infrastructure is in scope of this documentation.

Roche Vanilla Agent (RVA)

Software installed on systems / instruments to enable communication to the Roche Axeda infrastructure. The Roche Vanilla Agent includes the Axeda Agent, Axeda Desktop Server and Deployment Utility (configuration utility). RVA is an extended version of the Axeda Agent, it provides "out-of-the-box" remote services, tailored for the needs of Roche Diagnostics.

Remote Service / Remote Service Infrastructure

Remote Service is a global platform for data exchange between diagnostic system solutions at customer sites and Roche Diagnostics.

Remote Service Data Warehouse (RSDW)

The Remote Service Data Warehouse is temporary data storage (XML) for uploaded instrument data (e.g. monitoring information). This data is then made available for other Roche business applications.

Software Gateway

See Roche Vanilla Agent for details.

TeleService-Net (TSN) / Legacy Remote Service infrastructure

Software and Hardware required providing the following services:

- cobas e-library (e-PI and e-BC download to **cobas®** link and instruments)
- Collecting monitoring data from **cobas®** link and instruments

UltraVNC Viewer

3rd party client software for screen sharing.

UltraVNC Server

3rd party server software for screen sharing.

WiFi

Capability of accessing a wireless network. WiFi stands for 'Wireless Fidelity'.

3G

Capability of connecting via the mobile network. 3G stands for 'third generation' of mobile telecommunications technology.