Remote Service

Security Information V05
10373981 GSS 000 04
Table of contents

1 Document History .................................................................................................................... 3
2 Purpose .................................................................................................................................... 4
3 Scope ....................................................................................................................................... 4
  3.1 In scope ............................................................................................................................. 4
  3.2 Out of scope ...................................................................................................................... 4
4 Introduction ............................................................................................................................. 5
5 Infrastructure characteristics ................................................................................................. 7
  5.1 Hosting / access details ................................................................................................. 7
6 Security information ................................................................................................................ 8
  6.1 General security requirements ........................................................................................... 8
    6.1.1 How should the Customer LAN be protected? ............................................................ 8
    6.1.2 How should the Customer WiFi network be protected? .............................................. 8
  6.2 Protection of connect 2 ...................................................................................................... 9
  6.3 Protection of Roche Vanilla Agent .................................................................................... 10
  6.4 Protection of cobas® link .................................................................................................. 12
  6.5 Protection of systems / instruments .................................................................................. 13
  6.6 Protection of the Roche / Axeda enterprise infrastructure ................................................ 14
7 Security Contact at Roche .................................................................................................... 15
8 Glossary ................................................................................................................................... 16
# Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Name</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>V00</td>
<td>11-JAN-2010</td>
<td>Thomas Maly</td>
<td>Creation of document.</td>
</tr>
<tr>
<td>V01</td>
<td>03-NOV-2010</td>
<td>Thomas Maly</td>
<td>Added information for Roche Vanilla Agent and connect 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Minor changes throughout the document.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Changed PAP to GSS document.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Digital Signature in DVS</td>
</tr>
<tr>
<td>V02</td>
<td>17-MAY-2011</td>
<td>Thomas Maly</td>
<td>Updated complete document to reflect new Axeda infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>hosted by Axeda in the On Demand Center.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Changed ‘cobas IT firewall’ to ‘FortiGate 40C’.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Added more details for the Virus Definition deployment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Glossary aligned with Remote Service Glossary 10013271 PJM 000 03.</td>
</tr>
<tr>
<td>V04</td>
<td>16-May-2014</td>
<td>R. Gwerder</td>
<td>Changed ‘Out of Scope’ as the UK is now on the global DMZ.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UltraVNC Viewer and UltraVNC Server added to the glossary</td>
</tr>
<tr>
<td>V05</td>
<td>16-Sep-2014</td>
<td>S. Rosu, R. Gwerder</td>
<td>Updated firewall recommendation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Updated connectivity diagrams</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Added mobile connectivity (3G) and Wifi for connect 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Updated glossary with ‘WiFi’ and ‘3G’</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Team email address updated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Added chapter with general security requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Changed title of the documentation set under chapter Scope</td>
</tr>
</tbody>
</table>

Disclaimer: Working copy if printed.
2 Purpose

The purpose of this document is to describe the security 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 Roche Remote Service Platform related to security.

Regulatory requirements of HIPAA as stated in DHHS 45 CFR Parts 160, 162, and 164 as well as EU Privacy Directive 95/46/EC focus on the legal and procedural aspects of Privacy and Security. 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 (DVS 10373982)
- Remote Service Security Information (DVS 10373981, this document)
- Remote Service Connectivity Information (DVS 10373979)

3.1 In scope

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

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

3.2 Out of scope

The Remote Service Data Warehouse (part of the Remote Service Platform) it is 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 are 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 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 Security information

The security aspects applicable to all products of Roche Diagnostics are defined in Divisional Quality Standards: DS15-01 “Product IT Security Principles” and DS16-01 “Product IT Security: Requirements and Implementation Rules”.

The aspects specific for Remote Service are described in the following chapters.

6.1 General security requirements

This section provides information regarding the general security requirements in the Customer Lab Network. These requirements must be observed for any of the following Ethernet or Wireless network configurations:

1. Roche system or Gateway is connected to Lab network for the purpose of communicating with local nodes (systems) on the same network
2. Roche system or Gateway is connected to Lab network for the purpose of connecting to the Internet through a customer network Gateway
3. Roche system or Gateway is connected to Internet over a dedicated network or line

6.1.1 How should the Customer LAN be protected?

It is the customer’s responsibility to ensure that the Customer LAN is secure and protected (e.g. Firewall, NAT Firewall). The following security requirements should be met:

1. Private IP Addresses are used for the network configuration and local nodes
2. Access to the Internet is through firewalled Gateway
3. Direct connections to Roche systems and Gateways are not allowed (i.e. inbound TCP/UDP connections are not allowed)
4. Outgoing connections from Roche systems and Gateways are allowed but limited to a list of Roche-requested IP addresses and from specific ports requested protocols (See latest version of “Remote Service Connectivity Information” in GRIPS)
5. Routing of NETBIOS over TCP is not allowed
6. Customer Network security best practices are observed:
   a. Use authorized Network equipment which includes, but is not limited to the following: access points, routers, switches, cables, computers, and various network components
   b. Only authorized personnel are allowed to administer and configure networking equipment
   c. Customer Network access is logged and monitored

In case any of the above requirements are not met, Roche systems and Gateways should not be connected to the customer LAN.

6.1.2 How should the Customer WiFi network be protected?

It is the customer’s responsibility to ensure that the Customer Wireless LAN is secure and protected (e.g. Firewall, NAT Firewall). The following security requirements should be met:

1. Follow the recommendations from 6.1.1 for basic LAN protection
2. Use firewalling router to route packet between wireless and wired LAN and WAN
3. It is strongly recommended to use WPA2 with a strong password as Wireless encryption
4. Use of any wireless node as wireless HOTSPOT is not recommended
5. Use best practices for wireless protected access
6. In case other devices are sharing the Customer WiFi they shall be properly protected as well

In case any of the above requirements are not met, Roche systems and Gateways should not be connected to the customer Wireless LAN.

6.2 Protection of connect 2

The following chapter provides a Q/A section in regards to the connect 2. Protection of Systems connected to the connect 2 is not part of this documentation and Remote Service is not responsible for their protection. Physical protection of the connect 2 must be ensured by the customer.

1) How is network access to the connect 2 protected?
   The connect 2 contains a tailored Linux and password protected BIOS (i.e. it has security relevant configuration of BIOS, system components & interfaces.)
   The connect 2 is protected against uncontrolled network access using Linux port filtering. On the network interface towards Roche, only IPs, ports & protocols required for the communication by the Remote Service applications are authorized.

2) How is user access to the connect 2 protected?
   connect 2 requires a valid Roche certificate to access its Web Interface.
   connect 2 does only allow to access the Web Interface via SSL (encrypted).
   Remote access is controlled via role based access privileges to the Axeda ServiceLink application.

3) Is the connect 2 protected against viruses and worms (malware in general)?
   Yes, connect 2 is protected against viruses and worms (malware in general) by highly secured interfaces. The risk of infection is mitigated on the connect 2 by a tailored Linux and a write protected system partition. connect 2 does not contain any CD / DVD or USB access.

4) Is (confidential) data protected in transit?
   All data transferred between connect 2 and Roche is encrypted.
   connect 2 uses a standard Axeda Agent for all communication.

5) Is the software on the connect 2 regularly updated?
   Roche will update the operating system and related software components with the current security patches published by the corresponding vendors if necessary.
   The regular process of distribution of the patches is automatic, however in certain cases it may be manually performed remotely or locally.
6) How are security patches being handled?
   Remote Service is regularly checking for applicable security updates. Updates are tested before deployment to ensure proper functionality. Back-end infrastructure patching is covered by Roche processes.

7) How is security of the connect 2 tested?
   The connect 2 has undergone a penetration test by an independent 3rd party company. The scope of the penetration test was related to the connect 2 device as such.

8) Are actions performed on the connect 2 logged?
   Access and changes are logged by the connect 2.

9) Is there a notification, when a Roche user accesses the connect 2?
   No. The connect 2 is not – and cannot be – equipped with any screen to display remote actions. The connect 2 does not have any video output connector.

10) Is there a notification, when a Roche user accesses a system / instrument?
    This is dependent on the system’s / instrument configuration and is not related to the connect 2. Remote access to the connect 2 does not require any end user confirmation.

11) What happens, when a new e-library is installed on the connect 2?
    e-library is not part of connect 2 and therefore not applicable.

12) How secure is the mobile connectivity (3G) for the connect 2?
    The mobile network may use additional encryption algorithms to protect the data traffic. For maximum security, both the operator and the mobile terminal (modem) should implement the latest standards.

13) How secure is the wireless connectivity (WiFi) for the connect 2?
    connect 2 implements WEP and WPA-PSK. It is recommended to use WPA-PSK.

6.3 Protection of Roche Vanilla Agent
The following chapter provides a Q/A section in regards to the Roche Vanilla Agent. Protection of Systems the Roche Vanilla Agent is installed on is not part of this documentation and Remote Service is not responsible for their protection.

1) How is network access to the Roche Vanilla Agent protected?
   Protection of systems hosting the Roche Vanilla Agent is not in scope of the RVA. Details can be obtained from the respective system / instrument documentation.

2) How is user access to the Roche Vanilla Agent protected?
   The RVA is a separate component designed to be installed on qualified Roche systems. User access is not in scope for the RVA. The user access to RVA is part of the system hosting
the RVA. E.g. access can be restricted by windows login. Remote access is controlled via role
based access privileges to the Axeda ServiceLink application.

3) **Is the Roche Vanilla Agent protected against viruses and worms (malware in general)?**
   The RVA is a separate component designed to be installed on qualified Roche systems.
   Antivirus protection is not in scope for the RVA. In case of security findings, the RVA can be
   updated remotely.

4) **Is (confidential) data protected in transit?**
   All data transferred between the Roche Vanilla Agent and Roche is encrypted.

5) **Is the Roche Vanilla Agent regularly updated?**
   Roche will update the Roche Vanilla Agent if necessary. The RVA is equipped with a self-
   updating mechanism.

6) **How are security patches being handled?**
   Remote Service is regularly checking for applicable security updates. Updates are tested
   before deployment to ensure proper functionality.
   Back-end infrastructure patching is covered by Roche processes.
   As the RVA is a separate component designed to be installed on qualified Roche systems,
   security patching of the underlying system is not in scope for the RVA. In case of security
   findings, the RVA can be updated remotely.

7) **How is security of the Roche Vanilla Agent tested?**
   Roche is using standard Axeda components for the Roche Vanilla Agent.
   Axeda is VeriSign security certified. Details can be obtained from the Axeda Homepage.

8) **Are actions performed with the Roche Vanilla Agent logged?**
   Screen sharing activities using an RVA is logged in ServiceLink.

9) **Is there a notification, when a Roche user accesses an RVA enabled system?**
   This depends on the system’s configuration. For most systems, a local confirmation is
   necessary to allow screen sharing sessions.

10) **Is there a notification, when a Roche user accesses a system / instrument?**
    This is dependent on the system’s / instrument configuration and is not directly related to the
    RVA itself.

11) **What happens, when a new e-library is installed on the RVA?**
    e-library is not part of RVA and therefore not applicable.
6.4 Protection of cobas® link

The following chapter provides a Q/A section in regards to the cobas® link. Protection of systems connected to the cobas® link is not part of this documentation and Remote Service is not responsible for their protection. Physical protection of the cobas® link must be ensured by the customer.

1) How is network access to the cobas® link protected?
   The cobas® link has basic hardening, i.e. it has security relevant configuration of BIOS, account groups / policies, system components & interfaces.

   The cobas® link is protected using security policies of the operating system. On the network interface towards Roche, only IPs, ports & protocols required for the communication by the Remote Service applications are authorized.

   It is recommended not to use the Wireless Interface on cobas® link because the security policies of the operating system are failing to provide the required security controls.

   Furthermore it is recommended to operate the cobas® link in a secure Customer Network environment only.

   An additional hardware FortiGate 40C firewall is mandatory if no customer firewall is in place. Additionally it is also recommended even if there is a customer firewall in between in order to enhance protection.

2) How is user access to the cobas® link protected?
   The cobas® link has defined special classes of users for specific use cases. The local administrator login password is distributed only to selected, specially authorized employees of Roche Diagnostics.

   Dedicated users for the customer are predefined. The password can be chosen by the customer and be changed at any time.

   Remote access is controlled via role based access privileges to the Axeda ServiceLink and the Remote Service Remote Help Desk application.

3) Is the cobas® link protected against viruses and worms (malware in general)?
   Every cobas® link is equipped with an anti-virus software and the automatic update of the virus signature files is performed regularly.

4) Is (confidential) data protected in transit?
   All data transferred between cobas® link and Roche is encrypted and digitally signed except Virus definitions. They are digitally signed only by Symantec. This prevents them from manipulation. Encryption is not required for Virus definition as the content is public.

5) Is the software on the cobas® link regularly updated?
   Roche will update the operating system and related software components with the current security patches published by the corresponding vendors if necessary.

   The regular process of distribution of the patches is automatic, however in certain cases it may be performed manually remotely or locally. Distribution of virus definitions is performed using the Symantec LiveUpdate functionality. Due to the additional testing performed, virus definition deployment is delayed up to two weeks – immediate emergency deployment is possible.
6) How are security patches being handled?
Remote Service is regularly checking for applicable security updates for the cobas link. Updates are tested before deployment to ensure proper functionality.

7) How is security of the cobas® link tested?
The cobas® link has undergone several penetration tests by independent 3rd party companies. The scope of some of these penetration tests is related to the complete Remote Service infrastructure, which includes the cobas® link.

8) Are actions performed on the cobas® link audited?
All access sessions to the cobas® link are logged (user id and time stamp for beginning and ending of the session).

9) Is there a notification, when a Roche user accesses the cobas® link?
The screen sharing application icon changes its color and logs are generated as mentioned above. Remote user’s best practice is to notify the local user (e.g. via chat function). In addition, the enterprise system generates an audit log for all remote access attempts.

10) Is there a notification, when a Roche user accesses a system / instrument?
This depends on the system’s configuration. For most systems, a local confirmation is necessary, to allow screen sharing sessions. This setting is gateway independent.
Remote access to the cobas® link does not require any end user confirmation.

11) What happens, when a new e-library is installed on the cobas® link?
New e-Libraries are automatically presented on the “New Entries” page. This is the default entry page for the local user.

6.5 Protection of systems / instruments
Protection of systems / instruments is not in scope of Remote Service. Details can be obtained from the respective system / instrument documentation.
6.6 Protection of the Roche / Axeda enterprise infrastructure

The following section provides a Q/A section in regards to the user access and audit trail of the Roche / Axeda enterprise infrastructure. General protection (e.g. network protection) of the infrastructure is not part of this documentation.

1) How is user access to the enterprise infrastructure protected?

Access control to the legacy Remote Service and Axeda infrastructure is controlled by the Roche active directory authentication and role based authorization at the Remote Service database.

The access to the Axeda and legacy Remote Service infrastructure is limited to Roche employees or designated 3rd parties contracted by Roche in certain countries.

Examples of roles at legacy Remote Service infrastructure:
- Remote Access User
- Country User
- Country Download Manager
- Country Registration Manager

Examples of roles at Axeda infrastructure:
- Remote Access User
- System Administrator

2) Are actions performed on the enterprise infrastructure audited?

An audit trail for capturing regulatory relevant operations / interactions is saved. Each local and remote access session is logged. For remote access the following information is stored in the database:
- Roche user ID
- name / ID of person at the laboratory, who authorized this session
- date / time of the session start and end
- remotely accessed system (cobas® link and system / instrument)
- type of the session
- session status, etc.

Regular reports of the audit trail of remote access sessions may be supplied to the healthcare organization on request.
The access rights of the authorized person can be traced historically. For remote access with Axeda the following information is stored in **Axeda ServiceLink**:

- Roche user id
- Date / time of the session start and end
- remotely accessed system (e.g. **cobas®** link and system / instrument),
- type of the session, pcAnywhere, Axeda Desktop Server
- session status, etc.

Operations on „sensitive“ data on the **Remote Service** infrastructure:
Release and transfer status of sensitive data and documents, which may influence the system / instrument processing, e.g., transfer from Roche to the lab/instrument of **e-BarCode** and **e-PackageInsert** (Test Applications, Lot data of Reagents, Calibrators, Controls, …) are audited.

**3) How is security of the Axeda On Demand Centers ensured?**

Axeda follows security best practices and complies to Roche guidelines and certifies their product by VeriSign. Details can be found on [http://www.axeda.com](http://www.axeda.com).

The current certification is available here (as of 07-APR-2011):

Processes between Axeda and Roche are defined to ensure security measures are in place. Roche performs security assessments (incl. vendor audit) of the hosting infrastructure.

**7 Security Contact at Roche**

Questions and comments can be addressed at the Roche security 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 Glossary

Axeda infrastructure / part of Remote Service Infrastructure
Software and Hardware required providing 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 to provide 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.