FAQ COMBIVIS connect

COMBIVIS connect server structure FAQ No.0005

Part	Version	Revision	Date	Status
en	7.0.023	002	2019-01-01	Released

Content

KEB Automation KG
Südstraße 38
32683 Barntrup, Germany
E-mail: info@keb.de
Tel. +49 5263 401-0
Fax +49 5263 401-116
www.keb.de

District Court Lemgo HRA 5649
DUNS-No. 314108728
VAT-No. DE309087075
Bank Details: Sparkasse Paderborn-Detmold
IBAN DE 19 4765 0130 0000 0060 07
BIC WELADE3L

General Partner:
Vittorio Tavella
KEB Verwaltungs-GmbH, Barntrup
District Court: Lemgo HRB 8965
Directors: Curt Bauer CMO,
Ralf Lutter COO, Vittorio Tavella CFO,
Wolfgang Wiele CTO

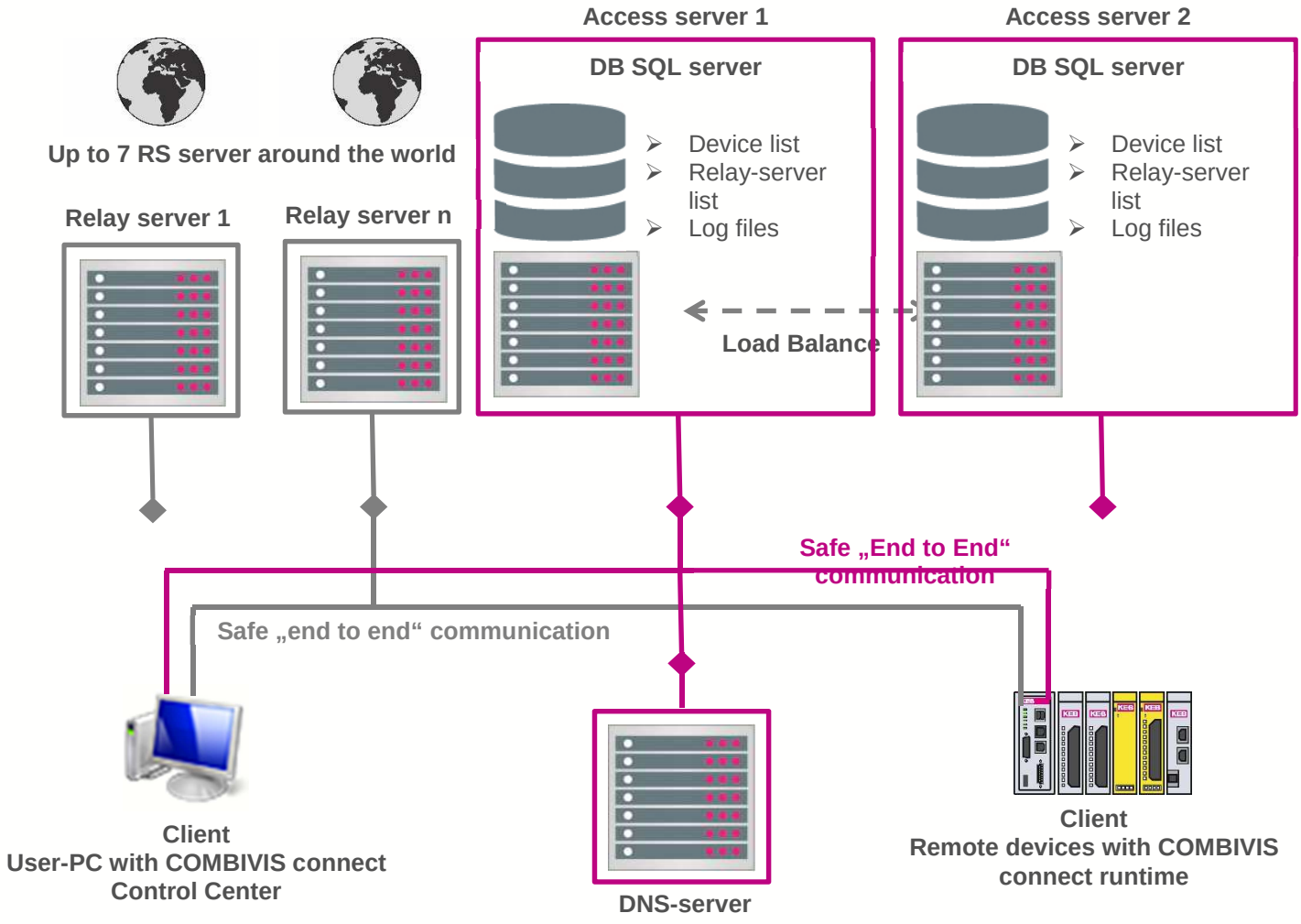
Introduction

This document describes the structure of the COMBIVIS connect server and the ports which are mandatory for build up a communication to these servers.

Server structure

The structure of COMBIVIS connect is consisting of access-, relay-, DNS-server and clients. The clients are the user PC, with COMBIVIS connect Control Center, and the remote device with the COMBIVIS connect runtime.

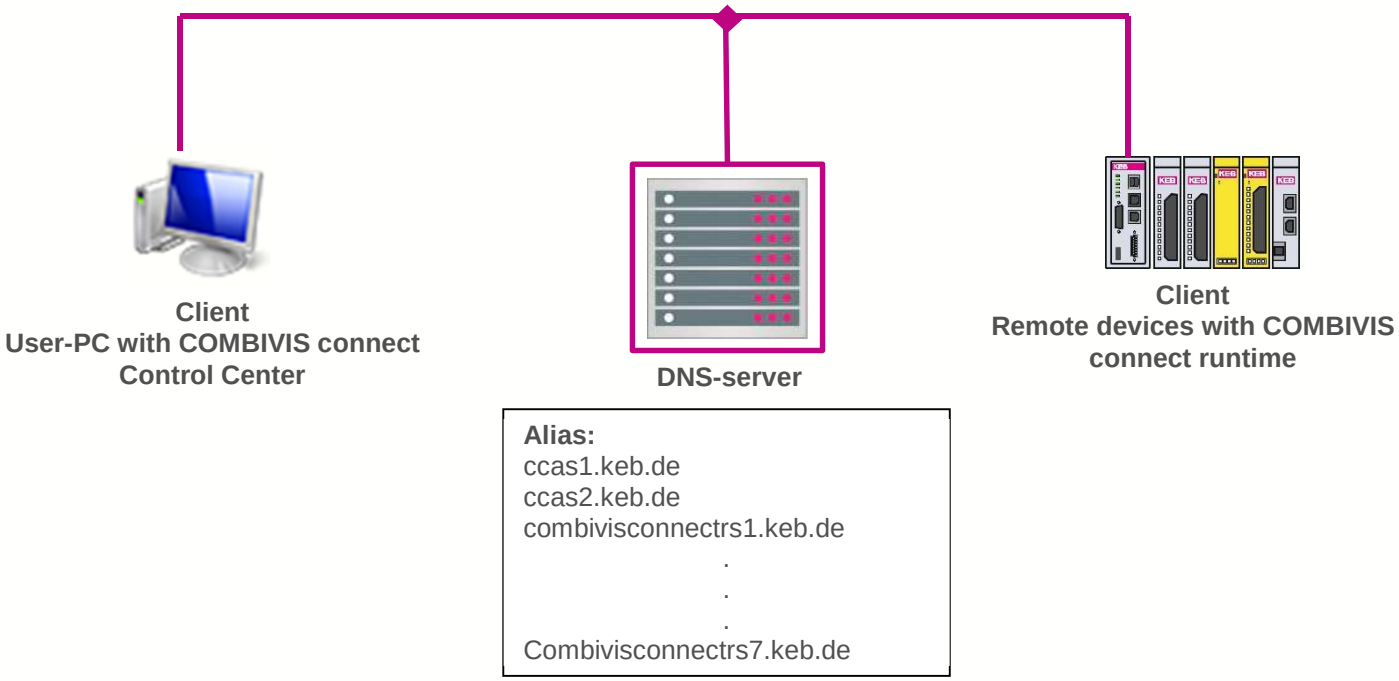
The server structure security is certificated by the german security organization ProtectEM. It´s based on the BSI (German federal office for information security) ISA 99 and IEC 62443.



Clients: COMBIVIS connect Control Center and Runtime

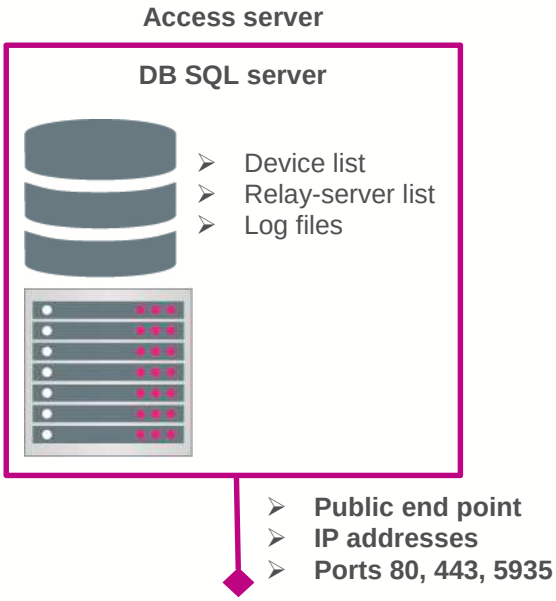
The software interface COMBIVIS Connect Control Center is running on the user-PCs and the COMBIVIS connect runtime on the remote device. From version 7 both programs choose the access server by themselves.

The clients interview the DNS server of the providing alias of the server names at the boot-up procedure of COMBIVIS connect Control Center and runtime. The DNS will provide the corresponding IP-addresses. This technique makes the solution more flexible in the direction of client and server because of updating or adding IP-addresses.



Access server

The access server is used to manage the user access and device access. These information will be stored in device-, relay server- and log-file- lists. After the devices were verified, a relay server will be assigned to build up the final end-to end communication. The relay server with the best performance (lowest latency) will be analysed be a “Load Balance” algorithm. Each server can use the ports 80 (HTTP), 443 (HTTPS) and 5935 (Custom). The access server uses a dynamic name, which are connected to a static IP-address.



Server names and ports

For a successful communication with the server it´s mandatory to use one of the following ports: 80 (HTTP), 443 (HTTPS), 5935 (Custom)

Also following server names have to be unblocked in the firewall settings:

Access-server:

- ccas1.keb.de
- ccas2.keb.de

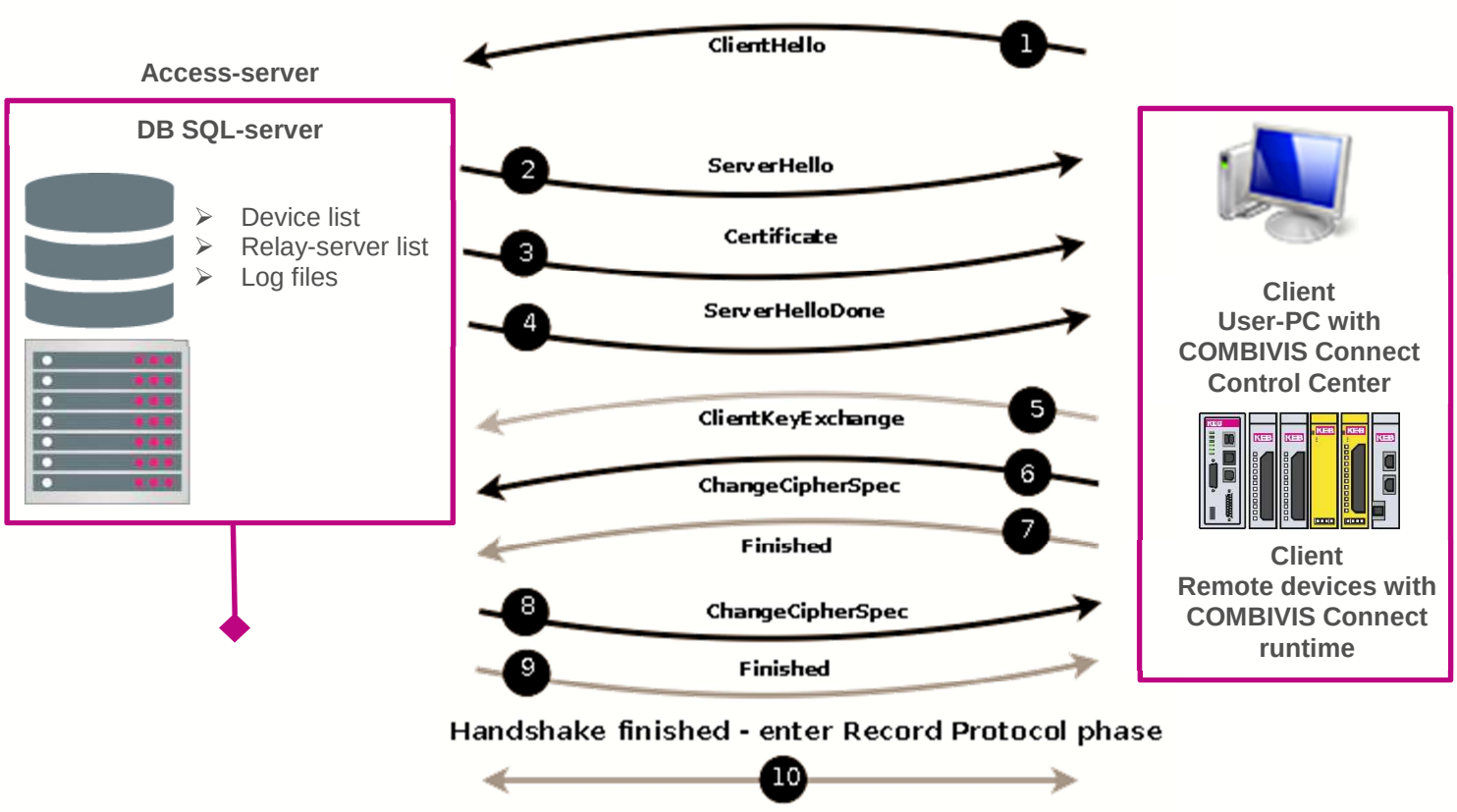
Relay-server:

- combivisconnectrs1.keb.de
- combivisconnectrs2.keb.de
- combivisconnectrs3.keb.de
- combivisconnectrs4.keb.de
- combivisconnectrs5.keb.de
- combivisconnectrs6.keb.de
- combivisconnectrs7.keb.de

The firewall should be able to handle dynamic server names. This gives the opportunity to select the rules independent from the IP-addresses of the server, which could be changed in the future.

TLS/SSL protocol sequence (handshake)

Before the exchange of data between the both clients starts, the TLS(SSL) protocol initialize a handshake sequence between access server and clients (see handshake diagram below). The access server will verify the certificate, cipher specifications and keys.



Action after TLS (SSL) handshake

1. The access server verify the authentication:
   - COMBIVIS connect Control Center (domain name, user password)
   - COMBIVIS connect Runtime (certificate)
2. The access server verifies the device list which can be reached by the client.
3. Once refresh the device list, the access server appoints the relay server to be use.
4. Through access server both clients decide the best routing on the direction of relay server; the best in performance (latency) is going to be selected on both sides
   - Session key exchange between both clients (every session a new key is going to be generated). Perfect forward secret (PFS)
5. Once the rules are fixed, both are going to be connected to the relay server and route the traffic.
   - Remote Desktop
   - VPN tunnel

Disclaimer

KEB Automation KG reserves the right to change/adapt specifications and technical data without prior notification. The safety and warning reference specified in this manual is not exhaustive. Although the manual and the information contained in it is made with care, KEB does not accept responsibility for misprint or other errors or resulting damages. The marks and product names are trademarks or registered trademarks of the respective title owners.

The information contained in the technical documentation, as well as any user-specific advice in verbal or in written form are made to the best of our knowledge and information about the application. However, they are considered for information only without responsibility. This also applies to any violation of industrial property rights of a third-party.

Inspection of our units in view of their suitability for the intended use must be done generally by the user. Inspections are particular necessary, if changes are executed, which serve for the further development or adaption of our products to the applications (hardware, software or download lists). Inspections must be repeated completely, even if only parts of hardware, software or download lists are modified.

Application and use of our units in the target products is outside of our control and therefore lies exclusively in the area of responsibility of the user.

KEB Automation KG
Südstraße 38 • D-32683 Barntrup
fon: +49 5263 401-0 • fax: +49 5263 401-116
net: www.keb.de • mail: info@keb.de