blueSmart App

Authentification procedure and system requirements

blueSmart App

Authentification procedure with blueSmart app

The blueSmart app offers the possibility of **unilateral** and **bilateral** TLS 1.2 authentification.

The **unilateral authentification** is standardly used for internet browsers, for instance. For this authentification procedure only a valid TLS certificate is required on the server. The mobile device verifies its trustworthiness.

For the **bilateral authentification** a valid TLS certificate is additionally needed on the mobile device, enabling mutual authentification of server and client. This means an increased handling effort for the user of the blueSmart app, as the certificate must be renewed on expiry or on new installation of the app.

It is possible to use either self-signed certificates or CA certificates. Using CA certificates reduces the effort of setting up the mobile device because these certificates are allowed to be automatically verified by the mobile device. On the other hand, self-signed certificates first need to be converted into the .cwh file format, even for unilateral authentification, and after that they need to be imported to the mobile device and the blueSmart app.

Winkhaus recommends unilateral authentification using a CA certificate.

System requirements and ways of communication between mobile device and administration software

Communication between the blueSmart app and the administration software takes place via the (mobile) data connection of the mobile device and the internet connection of the server. In order to allow the connection to be sufficiently secured, we are indicating several options in the figures on the next page.

Data connection via VPN tunnel

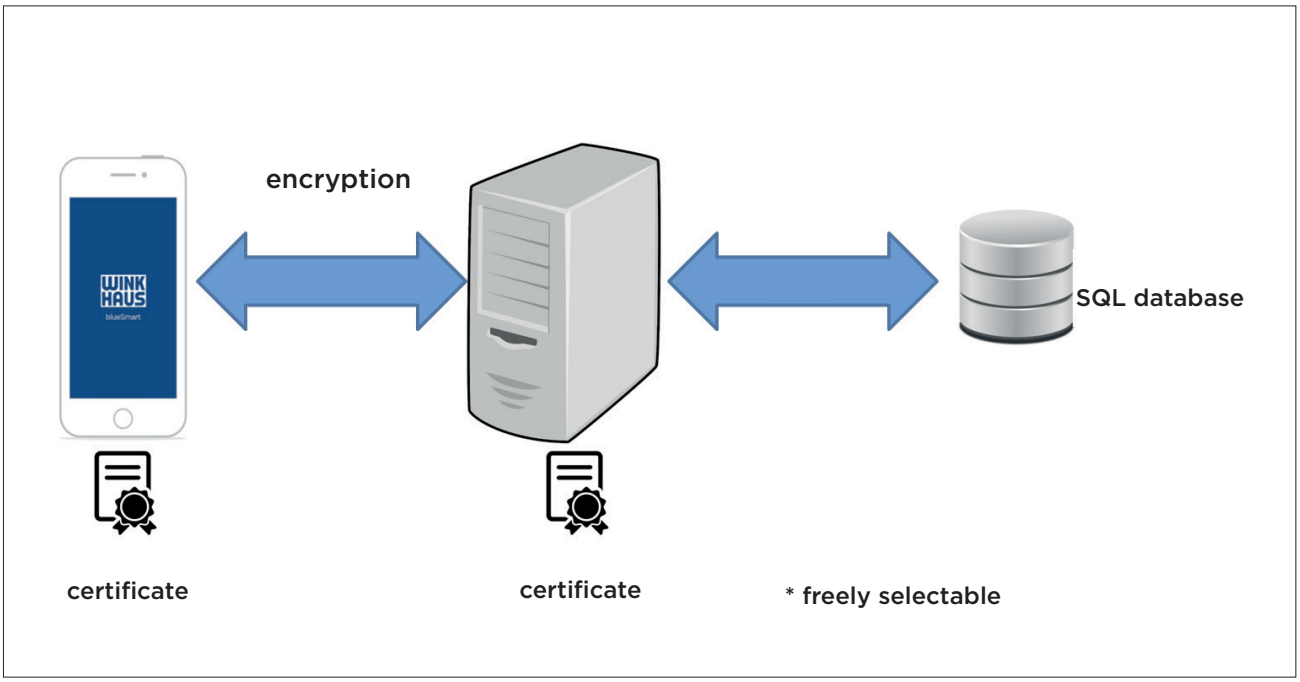

Figure 1: Data connection via VPN tunnel

In order to establish the data connection via a VPN tunnel, as shown in figure 1, it is necessary to store an internal URL on the Active Key on initialising the Active Key for remote authorisation and programming. The certificate needs to be issued on this URL. An internal DNS server within the company network is required for resolving the URL. The applied VPN tunnel must be provided by the system administrator and set up by the user (if necessary with an additional app on the mobile device). It is not possible to establish a VPN tunnel with the blueSmart app. In case of an existing VPN tunnel, it goes without saying that it can also be used by the blueSmart app. The central administration software and the SQL database can be run on one server.

Data connection via DMZ

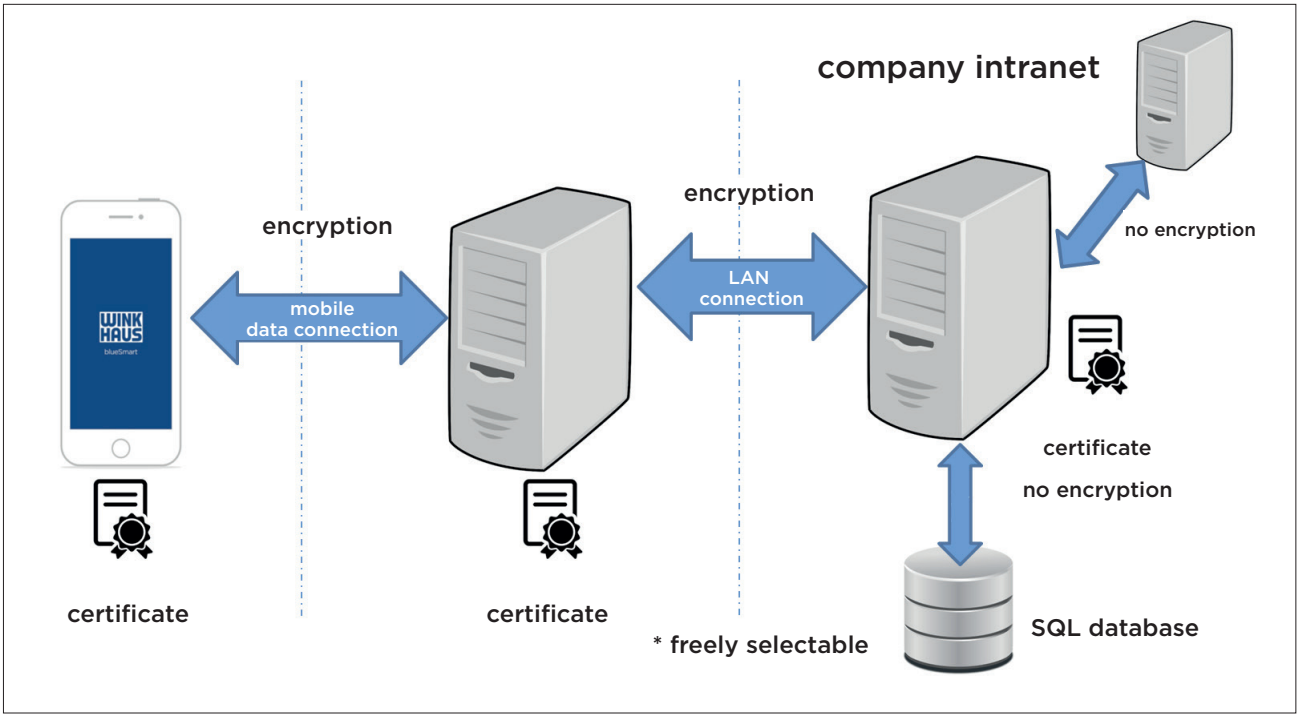

Figure 2: Data connection via DMZ

In order to set up the data connection shown in figure 2 using an additional server in a demilitarised zone (DMZ), an external URL is needed. The latter must be stored on the Active Key when the key is initialised. In this case the certificate must be issued on the external URL. As regards this kind of data connection, the connection between the mobile device and the DMZ server as well as the connection between the DMZ server and the internal server provide a TLS encryption. For the unilateral authentification this means that at least one valid certificate must exist on the DMZ server and the internal server.
The necessary certificate and communication settings are stored on the administration software and on the Active Key. Should these settings be changed, the Active Key must be made available to the system administrator.

General network and firewall settings, such as port releases, must be made by the system administrator. The ports for communication between the mobile device and the (DMZ) server can be adapted to the existing network structure. The central administration software and the SQL database can be run on one server. Also the internal server can be on the same server.

The following general requirements must be met in order to use the blueSmart app.

- Use of administration software blueControl Professional in version 4.5 or higher
- Use of software module Remote Authorisation and Programming (item no. 505 288 2)
- blueSmart Active Key (item no. 502 552 8)
- If more than 10 Active Keys are used as remote authorisation and programming keys, additional licences are necessary. Licence for 5 extra keys: item no. 505 288 3
- All components of the locking system to be administered must be equipped with the current firmware. Here is a list:
  - blueSmart cylinder ≥ 50
  - Intelligent blueSmart door handle (EZK) ≥ 32
  - blueSmart protective fitting (EZK-A) ≥ 34
  - blueSmart reader ≥ 22
  - blueSmart locker and cabinet lock (BS80) ≥ 11
  - blueSmart narrow frame reader (BSTI SR/BSTE SR): all FW versions
- The following mobile devices can be used: iPhone, iPod Touch and iPad with iOS version 10 or higher
- Synchronisation between the mobile device and the administration software requires an internet connection
- In case a VPN tunnel is used, it needs to be established by an external place (smartphone app)
- The functions of the blueSmart app cannot be used for cylinders type 6x
- The TLS certificate must be available as .CRT and .KEY files in the PEM format. This means the contents of these files must be enclosed with -----BEGIN xxx----- and -----END xxx-----.