ProxerSafe and KeySafe systems

System Design

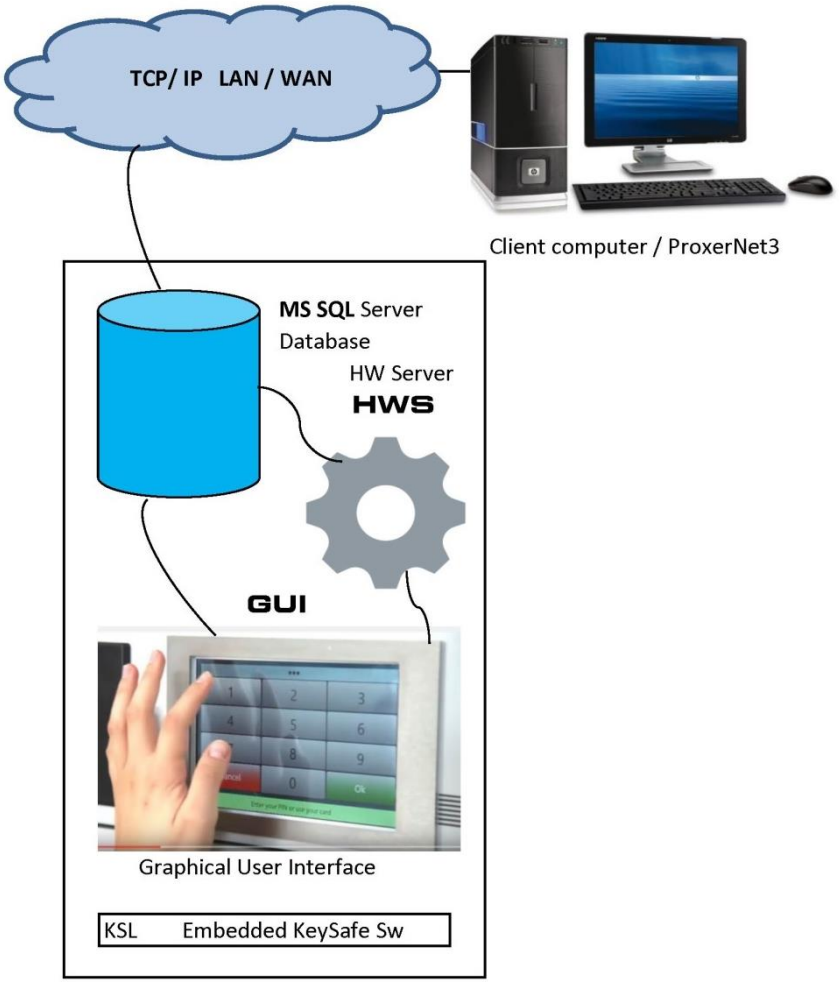
Technical and IT details of the operation of KeySafe/ProxerSafe intelligent key and value storage cabinets

- Hardware:
  - in each cabinet there is a separate, 8" touchscreen operated computer with Windows 10 OS and Ethernet TCP/IP RJ45 network interface
  - the units of the cabinet (RFID card reader, cabinet lock, Rack-compatible key modules with 8 (or 16) key positions) are connected to this built-in computer over serial RS485 communication bus.
  - in the cabinet there are built-in uninterruptible power supply and power distributor system

- Software
  - The module named KeysafeGUI runs on the touchscreen of the cabinet, and keeps contact with the user. It displays the status of the cabinet, the name of the keys, searching for a key is possible, etc. It is connected to the HWServer and the database.
    - Administrators can modify the user rights, display events too, but due to the physical barriers (small screen, lack of keyboard) it is recommended only at small-scale systems.
  - The KeySafe HWServer module runs as a Windows background service and controls the hardware units of the cabinet (door lock, key modules, RFID reader) according to the database; logs the events into the database and keeps contact with the KeysafeGUI interface. It has no own interface.
  - The system stores the master data and transaction data in Microsoft SQL database management system. 2017 or newer version is highly recommended. At "stand-alone operation with local and central synchronized databases" operation mode Microsoft SQL Server Standard or Enterprise must run on the server, Express or WebEdition is not sufficient.
  - Client: The ProxerNet software (a multiuser Windows client program) KeySafe module ensures the comfortable management of the system. In ProxerNet KeySafe module the master data (users, keys, rights) can be reviewed, edited, key events followed-up and printed. This program is suggested to be installed on the administrator's PC. The software connects to the MS SQL database. This program cannot be used on the built-in touchscreen of the cabinet.

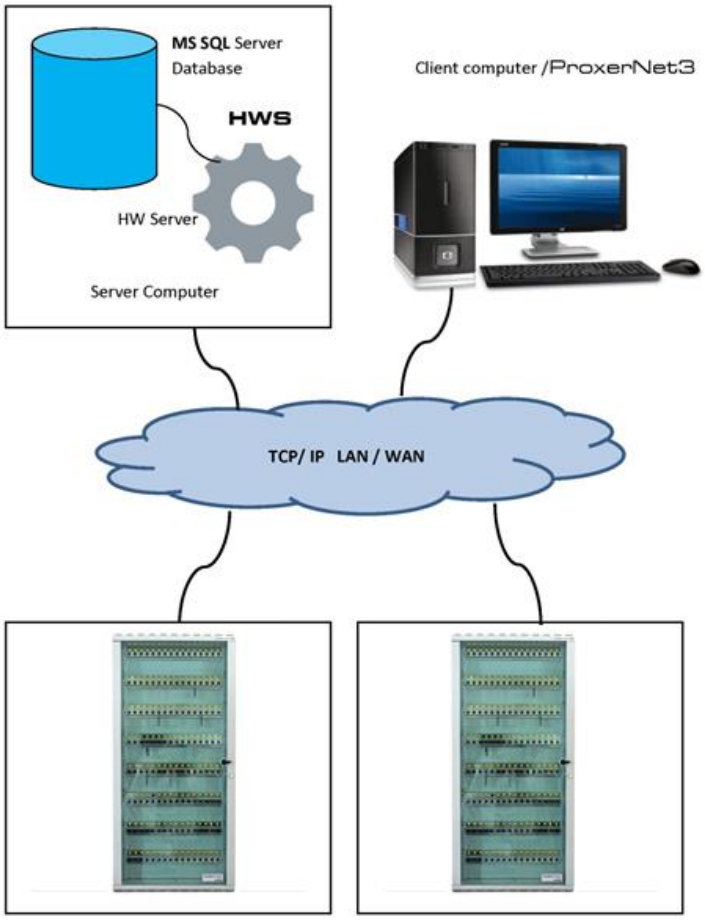
Possible operation mode of the cabinets:

1. **Stand-alone (offline) operation (not recommended at systems with multiple cabinets)**
   - all three software components run independently on the built-in computer of the cabinet (KeysafeGUI, HWServer, database server)
   - cabinets can be connected, master data can be queried and maintained one by one from the client programs
   - this version is able to operate in offline mode, meaning that the cabinet keeps on operating even if it loses all connections.



2. **Operation controlled and managed from a central server**
   - (only the interface (KeysafeGUI) runs on the cabinet in case it has a built-in touchscreen)
   - HWServer service and the MS SQL database are on an external (remote) computer or on two separate computers. This server can be even a virtual machine.
   - common database: all cabinets use common (shared) master data and event logs

- this operation mode requires continuous TCP/IP network connection between the cabinets and the server
- if the connection breaks with one of the cabinets, the cabinet cannot access the common database and HWServer service, thus it fails to operate.



3. Stand-alone operation with local and central synchronized databases

- the cabinets work independently, but do database synchronization (data exchange) with the central database
- in case the connection gets lost with one of the cabinets, the cabinet doesn't access the central database, but it keeps on operating according to the last status of its own database
- when the network connection is restored, the databases get in synchrony automatically

The conditions of the "Stand-alone operation with local and central synchronized databases" operation mode are:

- a Windows server computer (can be virtual and/ or shared) with TCP/IP and host (DNS) connection to the cabinets
- Microsoft SQL Server 2017 (or newer) software Standard (or broader e.g. Enterprise) version (the Express or Web Edition are not sufficient); and the central KeySafe database copy is on it as well
- ensuring access to the MS SQL database manager:

- remote access via Internet; username, password
- full access rights for reading and writing, saving and restoring database and managing the replication
- R/W rights to the local disk folder for saving and restoring database