



# **ABLOY**<sup>®</sup> **PROTEC<sup>2</sup>**

Technical brochure

## PROTEC<sup>2</sup> CLIQ™ SYSTEM

PROTEC<sup>2</sup> CLIQ™ is an easy to use access control system based on detainer disc cylinders and electronic identification. Thanks to our double technology, the access is double secured. ABLOY PROTEC<sup>2</sup> which is based on the patented rotating disc cylinder mechanism, takes care of the mechanical security at your site, while electronic CLIQ™ technology allows flexible control of keys, access rights and audit trails. PROTEC<sup>2</sup> CLIQ™ combines both technologies into one effective solution.

PROTEC<sup>2</sup> CLIQ™ keys are also available as Connect keys that can be wirelessly programmed using CLIQ™ Connect smartphone application in addition to Remote PDs and local PD. This enables the users to update their keys while in the field.

### ▶ AN INTELLIGENT COMBINATION OF ELECTRONICS AND MECHANICS AND ONLINE OPENING WITH SMARTPHONE APPLICATION

#### Electronic CLIQ™ technology

- CLIQ™ technology which is especially designed for locking industry provides unique identification for every opening through encrypted communication
- Battery inside the key provides wireless function of time and calendar with complete audit trail
- Calendar and time-based access rights are easy to change remotely
- Mechanical system is easily and cost-efficiently expandable with CLIQ™ properties



#### Mechanical ABLOY PROTEC<sup>2</sup>

- Durable design without springs and pins
- Disc Blocking System – patented feature that stops attempts to manipulate the discs
- Bump proof and virtually pick proof
- The key and cylinder features are patented until 2031
- 1,97 billion different key combinations
- The symmetrical key can be inserted both ways
- Only one key needed for each user
- Reliable function in severe environments



#### CLIQ™ Connect technology

- CLIQ™ Connect keys can be updated with a smartphone application
- Enables keys to be updated by the keyholders while working in the field
- For keys with the Online opening feature the key's access rights are checked in real time when the key is entered to a cylinder
- Key audit trail is transferred to CLIQ™ Web Manager when the key is updated in the smartphone application



# Overview

## CLIQ™ Web Manager for easy management

Browser-based CLIQ™ Web Manager allows to change access rights whenever and wherever required.



## Applications

PROTEC<sup>2</sup> CLIQ™ is used among Professional End Users such as utilities, telecom, petroleum, transportation, hospitals, governmental institutions, banks and museums and railways.

## ▶ KEYS

The PROTEC<sup>2</sup> CLIQ™ key has a metal shaft and a watertight plastic bow which holds the electronics and battery. All PROTEC<sup>2</sup> CLIQ™ keys are equipped with a realtime clock and a memory to allow time-based functions and collection of audit trails.

The PROTEC<sup>2</sup> CLIQ™ keys are also available as CLIQ™ Connect keys. CLIQ™ Connect keys can be updated via bluetooth using CLIQ™ Connect smartphone application.

### PROTEC<sup>2</sup> CLIQ™ user key specifications:

- Battery lifetime up to 10 years of operation and battery easy to change by opening a plastic cover.
- For bluetooth operated CLIQ™ Connect keys, battery lifetime is 1 year.
- Battery type is CR2450
- Buzzer indication and bicolor LED on both sides of the key
- Additional RFID cover available for use with access control readers
- Additional color covers available
- IP57 certified
- Operating temperature is -20 -+70
- Time functionalities available in all user keys (Validity settings, schedules, time stamps in audit trails)



## Normal user key

Normal user key is intended for cases where access rights are stable (e.g. grand master key) or changes are very rare. Changing the access rights for normal user key is done by changing electronic openings inside CLIQ™ locks via C-key, since there is no list of authorised locks on the key. Electronic openings in locks are defined in the locking planning software when the system is ordered and preprogrammed to the locks at the factory.



## Dynamic key

Dynamic key is intended for cases when access rights often change as it is easy to program changed access rights directly to user keys. Authorised cylinder needs to be programmed to dynamic keys via customer software (locally or remotely).



## C-key

C-key is used as a credential to access the CLIQ™ Web Manager software. Administrator can create programming tasks in CLIQ™ Web Manager and the tasks are distributed to C-key with local PD or Remote programming devices (eg. Wall PD or CLIQ™ Connect app) in the field. Also cylinders' audit trails can be retrieved with a C-key.




## CLIQ™ Connect key

All keys are also available as bluetooth versions which enables them to be updated wirelessly.



# PROTEC<sup>2</sup> CLIQ™ products

## CLIQ™ keys





		BATTERY LIFE	CUSTOMER DEFINED VALIDITY	AUDIT TRAIL	FOREIGN AUDIT TRAIL	LIST OF LOCKS	WEEKLY SCHEDULES	COMPATIBLE WITH CONNECT APP	ONLINE OPENING	REALTIME AUDIT TRAIL
<b>PROTEC<sup>2</sup> CLIQ™</b>										
Normal user key	TQ406	Up to 10y	x	2000	20		50			
Dynamic key	TQ407	Up to 10y	x	2000	20	3500	50			
C-key	TQ403	Up to 10y	x	8000						
<b>CLIQ™ Connect keys</b>										
Normal user key	TQB406	1 y	x	2000	20		50	x		
Dynamic key	TQB407	1 y	x	2000	20	800	50	x		
C-key	TQB403	1 y	x	8000				x		
Online opening key	TQC407	1 y	x	2000	20	800	50	x	x	x

All new PROTEC<sup>2</sup> CLIQ™ Remote and CLIQ™ Connect keys are compatible with Remote programming devices.

## OPERATION INSTRUCTIONS

Use the cylinders with the key in a normal way, like using mechanical cylinders.

After inserting the key into the cylinder's keyway wait for the sound signal before starting to turn the key. Signals are:

1 beep and green LED	3 beeps and red LED	3 long beep and green LED	No beep
			
OK	STOP / Clock	Battery icon / Thermometer icon	Battery icon
Key accepted, the lock can be opened after the beep	The key is denied, it is unauthorized by either code or time	The battery maybe weak or cold (try warming the key in your hand).	If there is no beep, try again. The battery can also be dead and needs replacing. In that case the lock can not be opened. Please contact the system administrator.

To ensure proper function of your PROTEC<sup>2</sup> CLIQ™ key, please note following precautions:



Avoid exposing the key to excessive heat or coldness.

Remove the battery cover and then insert a new battery to the key.

Incorrect lubrication is harmful for cylinder electronics. Use only ABLOY oil.

## PROGRAMMING DEVICES

PROTEC<sup>2</sup> CLIQ™ keys can be updated locally via the local programming device or remotely with the remote programming devices. Remote features allow collection of audit trails, updating key's access rights, schedules and enables the use of key revalidation.

### Wall PD PDA100

Wall PD is an indoor remote programming device which is used for updating keys. The communication between CLIQ™ Remote server, Wall PD and the PROTEC<sup>2</sup> CLIQ™ key is encrypted for maximum security.

- Wall mounted remote programming unit
- Locking system specific
- No data storage
- IP42 rated
- LAN connection
- Power through 12-24 voltage adapter or PoE (Power over Ethernet)
- Support for proxy server
- Plug&play capability\*



### Mobile PD PDA200 & PDA210

Mobile PD is a portable and personal programming device which is an optimal choice for a keyholder when PROTEC<sup>2</sup> CLIQ™ key needs to be updated in various locations. Mobile PD acts the same way as the Wall PD regarding key update, but gets power from AAA-batteries and connection to Internet via a mobile phone (Bluetooth) or laptop (USB).

- Powered by standard 4x AAA batteries
- PDA 200 Bluetooth & USB (for mobile phone and PC)
- Support for proxy server
- Plug&play capability\*



\*Plug&play installation for Remote PDs is available in CWM version 6.x and later

Other requirements:

- CLIQ™ Web Manager with DCS integration
- Firmware 6.0 or higher
- DHCP in use
- No proxies set up for Remote PD

## Outdoor Wall PD PDA120

Outdoor Wall PD is a remote programming device which can be installed outdoors and in hostile locations. Like the Wall PD, outdoor Wall PD connects to remote server via Ethernet and supports PoE.

- IP57 Water & dust protection
- IK9 Attack resistance



## CLIQ™ reader TQ124

The CLIQ™ reader is a relay-controlled device which sends a signal to other devices or systems such as electric locks or alarm systems. CLIQ™ reader can be installed outdoors as it fulfills IP53 rating. It has an PROTEC<sup>2</sup> CLIQ™ cylinder inside thus it accepts only a key with correct access rights.

The housing of the CLIQ™ reader is installed outdoors next to the entrance. It is wired with the relay box which can be installed indoors. Relay operation is performed only when a key has correct access. Also the reader can be programmed with a C-key as any other CLIQ™ lock.

- Power input 12-24 VDC -10 / +15%
- Power consumption 60mA
- Relay load max. 0,8A 30V AC/DC resist 20W
- Max. 1 meter length of the wire between escutcheon and electronics.
- Note to cut the cable to proper length, do not extend the cable.



## Wall PD with reader PDA110

The Wall PD with reader consists of 2 parts. It is a Wall PD with a reader attached. The Wall PD is installed indoors while the reader, which has IP53 rating, is installed outdoors next to the entrance door. The reader is attached to the Wall PD with a 2 meter cable.

- Maximum wire length 2 meters
- Inside unit specs same as PDA100
- Keys can be updated in both devices
- Does not contain a relay box





## Local programming device PDA500

Local PD is a PROTEC<sup>2</sup> CLIQ™ key programming device which is connected to a PC. Local PD is used to authenticate administrators to CLIQ™ Web Manager system with the C-key and to program PROTEC<sup>2</sup> CLIQ™ keys locally.

- USB connection to PC
- Requires drivers (plug-and-play installation)
- USB powered



## CLIQ™ Connect

PROTEC<sup>2</sup> CLIQ™ user keys and C-keys are also available as CLIQ™ Connect keys that can be programmed using the CLIQ™ Connect smartphone application in addition to the Remote PDs and the Local PD. This enables the keyholders and administrators to update their keys while in the field. Also the audit trail is transferred to CLIQ™ Web Manager when the key is updated.

Keys with Online opening feature use the CLIQ™ Connect application to check access rights in real time when the key is inserted in a cylinder. This enables real time access control for locations without landline internet connection.

CLIQ™ Connect keys use Bluetooth Low Energy technology to communicate with the application. The CLIQ™ Connect application then uses the smartphone's internet connection to connect to the CLIQ™ Remote application server in order to update the key's access rights and validity.




CLIQ™ Connect smartphone application is compatible with iOS version 8.0 or later and Android version 4.4 or later. For faster communication on Android platform version 5.0 is recommended. The application is available at Apple App Store and Google Play.

To use the CLIQ™ Connect smartphone application CLIQ™ Web Manager version 5.2.1 or later is required. For the Online opening keys CLIQ™ Web Manager version 6.0 or later is required.

End-to-end HTTPS connections (TCP port 443) must be allowed to CLIQ™ Remote server and directory services.

# PROTEC<sup>2</sup> CLIQ™ products

## CLIQ™ Devices

	REMOTE UPDATE OF CLIQ KEYS	OFFLINE UPDATE	OPERATES RELAY	CONNECTION TYPE	POWER	
Wall PD	✓	✓		LAN	12/24VDC or POE 3W	
Mobile PD USB/ Bluetooth	✓	✓		Bluetooth to smartphone, USB to PC	4 x AAA battery / USB	
Local PD	✓ 1)			USB to PC	USB	
Wall PD with reader	✓	✓		LAN	12/24VDC or POE 3W	
Outdoor Wall PD	✓	✓		LAN	12/24VDC or POE 3W	
Connect APP	✓			Bluetooth to CLIQ™ Connect Key	Smartphone, IOS/Android	
CLIQ™ reader TQ124			✓		12/24VDC 1,5W	

1) requires CWM ver. 6 and CLIQ™ Connect PC APP

## ▶ CYLINDER FUNCTION

PROTEC<sup>2</sup> CLIQ™ cylinder contains mechanical cylinder structure of unique PROTEC<sup>2</sup> structure with nine discs. In addition the cylinder contains PROTEC<sup>2</sup> CLIQ™ cylinder electronics which controls the electronic blocking system. This electronically controlled cylinder blocking is realized by using a small electric motor to guide the turning of one detainer disc. The cylinder itself has no electric power source. This means no need for wiring or battery changing in the cylinders.

PROTEC<sup>2</sup> CLIQ™ key structure allows it to operate not only the PROTEC<sup>2</sup> CLIQ™ electronic cylinders but also mechanical PROTEC<sup>2</sup> cylinders with eleven discs. PROTEC<sup>2</sup> CLIQ™ key bow contains key electronics and battery to power the functions of the cylinder and the key itself in a watertight package. Electronic communication between the key and the cylinder happens via bipolar galvanic contacts. The key shaft itself functions as one pole the other one being an insulated metal strip on the side of the key shaft. Also the power to carry out the cylinder's functions, is supplied via these contacts.

When a key is inserted into a cylinder, the electronic communication is activated between the key and the cylinder. If the key is authorised to open the cylinder, the battery in the key powers the opening and closing function of the electronic blocking of the cylinder. Both cylinder audit trail and key audit trail are stored simultaneously.

## CYLINDER MEMORY

- 1,800 authorized key groups, theoretical maximum 65,535 keys in each group
- A list of 3,000 denied keys
- Audit trail of last 2,000 events
- Audit trail of last 20 events from keys in other systems

## ADVANCED CYLINDER FEATURES

### Sequence lock

CLIQ™ cylinders are also available with the Sequence lock feature that can be programmed to the cylinder memory in the factory.

This lock type will require two valid keys to be entered to the cylinder before the lock can be opened. When the first valid key is inserted, the lock does not indicate or open. If a second valid key is entered within 1 minute, the lock will open.

## PRODUCT RANGE

### Wide product range - one key fits all



Robust and IP68 classified padlocks with CLIQ™ functionality for the harshest conditions.



Suitable lock cylinders for every door. Also available in dust protected versions.



Cabinet locks and cam locks with or without CLIQ™.



Key deposits for storing route keys securely.

## CLIQ™ Web Manager

CLIQ™ Web Manager (CWM) is a Web-based software that enables the management and control of PROTEC<sup>2</sup> CLIQ™, an electromechanical locking system enabling full control over access authorizations and key holder activities. The CLIQ™ system presents a solution that ensures the reliability of mechanical keys and cylinders as well as the security and flexibility inherent in electronic locks. The CLIQ™ Web Manager user interface is currently available in 22 different languages. The information in this brochure is valid for CLIQ™ Web Manager version 7 and later.

### BASIC FEATURES

#### 1. Secure login to management software

- a. Triple authentication login requires local programming device, C-key with PIN code and a valid C-key certificate for the web browser.

#### 2. Users and products

- a. Creating, importing and editing user information
- b. Handing out and handing in keys to users
- c. Managing lost keys
- d. Managing broken keys and cylinders and also product replacements
- e. Changing cylinder status and location information
- f. Handling cylinders in different time zones
- g. Managing remote programming devices
- h. Searching, viewing and exporting information on users and products

#### 3. Access rights

- a. Defining, restricting and changing access rights
- b. Time based access rights are available for all user keys. It is possible to set validity settings (inactive, active between a time period or always active), weekly schedules and an additional revalidation for all user keys.

#### 4. Audit trails

- a. Collecting, viewing and exporting key and cylinder audit trails. Audit trail events can be automatically collected from user keys during remote programming.

#### 5. Receipts and reports

- a. Printing key hand out and hand in receipts
- b. Viewing, exporting and printing reports of system like keys, cylinders, persons and audit trails.

### ADVANCED FEATURES

#### 1. Administration roles

- a. are used for defining the functions a locking system administrator is allowed to perform. The functions visible in software depend on the role assigned to the C-key used by the administrator who is logged in. Administrators only have access to functions they need in their work. For example, an administrator responsible for key management may only have access to the hand out/hand in and the key lost/broken procedures.

## 2. Domains

- a. are an administrative grouping feature which allows control over the specific parts of a locking system where administrators have access to. A domain consists of a set of cylinders/cylinders groups, user keys and persons typically associated with a geographic or administrative region. C-keys associated with a domain are only given administration rights for the included cylinders.

## 3. Remote programming

- a. is a feature for writing information to user keys and C-keys via remote programming devices. For user keys it is possible to change cylinder authorizations (only for dynamic keys), validity settings and weekly schedules via remote updates. The latest audit trails can also be downloaded automatically from the key to the software during remote update. For C-keys it is possible to assign cylinder programming tasks via remote updates.
- b. CLIQ™ system can also include CLIQ™ Connect keys which support remote programming via CLIQ™ Connect smartphone application.

## 4. Online opening

- a. is a feature that can be set on CLIQ™ Connect keys. Once a key is entered to a cylinder, it will request access rights from the CLIQ™ Web Manager software via smartphone app. If access rights are approved in the software the key can open the lock. Key will always request online opening for every cylinder it can access.

## 5. Key revalidation

- a. is a feature ensuring that keys are updated at certain time intervals. With key revalidation, keys must be inserted in a Remote PD ("revalidated") at specified time intervals to stay active. Once revalidated, the key stays active for the number of days, hours, and minutes specified as the revalidation interval, counting from the time it was revalidated. If a key is not revalidated within the specified interval, it becomes inactive until it is revalidated again.

## 6. Access profiles

- a. are used to give people who have specific roles the required accesses without having to configure each key individually. Keys and users can be associated to access profiles. The access profile then determines where the associated users and keys have access to. Access profiles can be freely defined in the software for example per user group office workers, cleaners, maintenance, etc. Access profiles work dynamically. If changes are made on access profile, system will generate remote programming tasks for each associated key automatically.

## 7. Flexible revalidation

- a. is a feature that makes it possible to set the key revalidation interval per access profile. This feature is useful when the security level of cylinders or access profiles in the system varies. For example access to server room is considered to be more sensitive than access to a meeting room or more frequent revalidation might be required for subcontractors as compared to company's own employees.

## 8. Temporary access groups

- a. are used to temporarily expand the access of keys by associating them with a selection of access profiles. The access of a temporary access group is the combined access of the included access profiles during a time period that is defined with a start date and an end date. Start date defines the time when temporary access rights are available from remote programming devices and end date defines the time when access right removal tasks are downloadable. This feature should be used together with key revalidation to ensure keys are frequently updated. This feature is useful for example in a case where one or more maintenance technicians are on call and need temporary access for multiple sites during their shift.

## 9. Offline update

- a. is a function that enables keys to be revalidated through a Remote PD even if the device has temporarily lost its network connection. This is useful in situations when it is critical that a key can get its validity extended even if the network connection is unstable. Updates of accesses cannot be made in offline mode. Offline Update is configurable per Remote PD.

## 10. Integrations

- a. with a third party systems (like HR system, or an access control software) are possible through SOAP Web Services interface.

## 11. PIN validation

- a. PIN validation is a new feature in CLIQ Web Manager 7 and is available for CLIQ Connect keys. With PIN validation it is possible to activate a CLIQ Connect key via the CLIQ Connect app without the need for network coverage. A PIN code will be needed instead. This will provide an additional layer of security. The CLIQ administrator in CLIQ Web Manager can still require the key holder to update the key via the CLIQ Connect app "in connected mode" (when the mobile phone has network coverage) on a regular basis as specified by the administrator. A "connected" update will send the audit trail data back to the software while a PIN update won't do that.

## ▶ ADDITIONAL SERVICES PROVIDED BY ASSA ABLOY

ASSA ABLOY provides additional services to CLIQ™ Web Manager Installations. Below is the list of services that can be integrated with installations. All services are hosted by ASSA ABLOY.

### Digital Content server

Digital Content Server (DCS) manages and delivers digital content, such as certificates, locking data, firmwares and software licenses to the CLIQ™ Web Manager installations in a secure manner. DCS is integrated automatically in all Abloy hosted CLIQ™ Web Manager environments. DCS can be integrated with customers own in-house installations as well. If an installation is not integrated with DCS, the digital content like certificates, locking data and software licenses can be downloaded from DCS using external admin accounts. Abloy will create DCS external admin accounts for all customers with their own in-house installations.

### Directory service

Directory service is an addition to DCS. It provides the correct CLIQ™ Remote server URLs as a service for remote programming devices and CLIQ™ Connect applications. This service enables plug and play functionality for remote programming devices, use of CLIQ™ Connect smartphone application to program CLIQ™ Connect keys and as well as use of CLIQ™ Connect PC application to program remote programming tasks for CLIQ™ keys. CLIQ™ Connect PC application is an alternative option for Java in CLIQ™ Web Manager Client PC.

### CLIQ™ Connect update service

CLIQ™ Connect update service provides CLIQ™ Connect PC application software to CLIQ™ Web Manager client PCs.

## INSTALLATION OPTIONS

Customer has two options when ordering CLIQ™ Web Manager software. Customer can either choose software as a services (SaaS) or an in-house installation option.

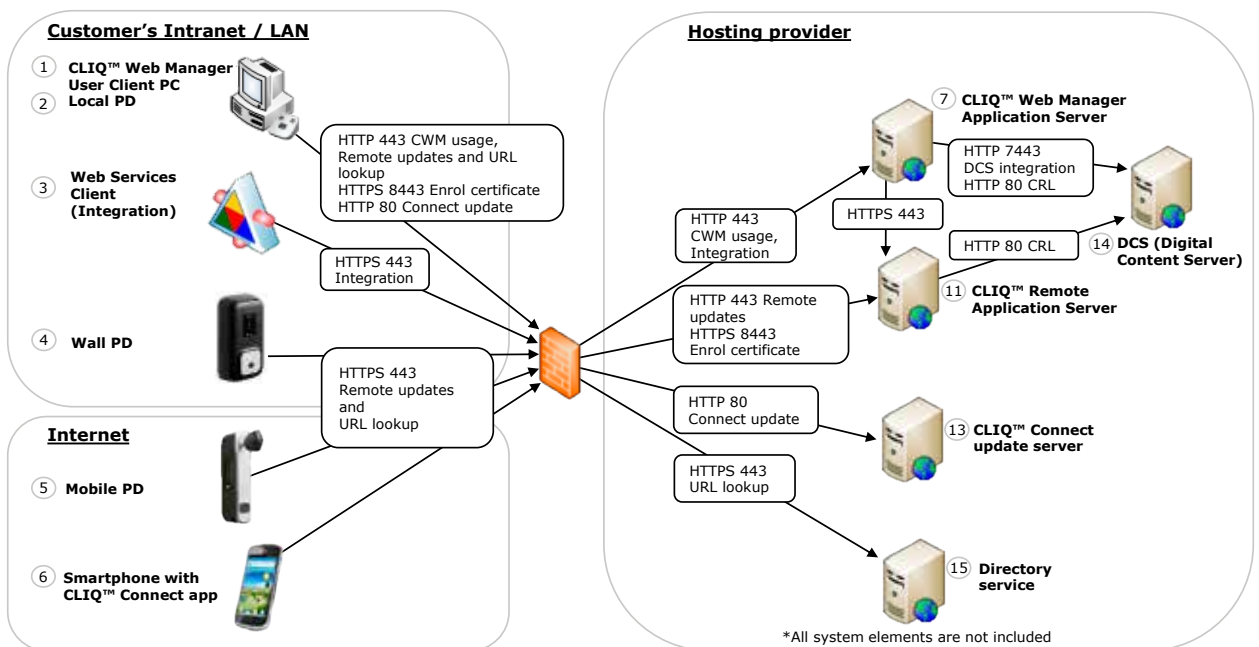
### Software as a Service (SaaS)

Software as a Service means that installation and maintenance of CLIQ™ Web Manager environment is provided as a service by Abloy Oy. Software upgrades, backups of databases and importing extensions to locking system are done automatically. Customer only needs to setup network connections to CLIQ™ Web Manager and CLIQ™ Remote services and deploy client PC(s) for CLIQ™ Web Manager software usage.

Abloy hosted CLIQ™ Web Manager Environments:

- Service availability: 24/7, High-availability environment (SLA 99.9%, excluding planned maintenance)
- All CLIQ™ services are monitored 24/7
- Professional support available 24/7

Below picture presents the overview of software as a service setup. Customer's network and devices are found on the left side of the picture and hosting provider's environment is depicted on the right side. Please notice the required network connections and the direction in which the arrows are pointing. The arrows are pointing outwards from where connections are initiated.



Service	Example URL
CLIQ™ Web Manager	https://cwm02.abloy.com:443/CLIQWebManager
CLIQ™ Remote	https://remote02.abloy.com:443/CLIQRemote
Enrolment	https://remote02.abloy.com:8443/CLIQWebManagerEnrolment
CLIQ™ Connect Update server	http://cliqconnect.assaabloy.com

Abbreviation	Explanation
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
CRL	Certificate Revocation List
URL	Uniform Resource Locator

Note: It is possible to setup a proxy server between remote programming devices and CLIQ™ Remote server. Proxy settings are set up in CLIQ™ Web Manager user interface and configured to remote programming devices during deployment phase.

## Customer's own in-house installation

CLIQ™ Web Manager system can be installed in customer's own environment. Customer is then responsible of setting up, installing and maintaining the environment for CLIQ™ system, installing the software, taking regular backups of databases and other maintenance tasks such as software version updates and installing extensions.

Abloy will provide software installation packages including CLIQ™ certificates to customers. Certificates includes MKS specific certificates for each remote programming device and C-key and also certificates for installation. The certificate file for installation is called serverbundle.ccb. CLIQ™ Remote server's hostname (e.g. CLIQ™ remote.mycompany.com) is embedded in the serverbundle file to make CLIQ™ installation more secure and use standard security methods. The customer must therefore let ABLOY know the CLIQ™ Remote server's hostname before the serverbundle file can be created and delivered.

## TLS certificates for CLIQ™ Web Manager

Customer needs to purchase or create TLS certificates for CLIQ™ Web Manager application and CLIQ™ Web Manager Enrolment application. Both applications are accessed using web browsers from client PCs. TLS certificates needs to be issued by a certificate authority (CA) that is trusted by these web browsers; otherwise web browsers cannot authenticate the server. The users will be presented with a security warning if the server cannot be trusted. Enrolment application is used for fetching new certificates for C-keys and CLIQ™ Web Manager application is the management software. Enrolment application is installed if DCS integration is in use and is deployed on the CLIQ™ Remote server. It is highly recommended to get certificates issued by a CA that is trusted by default by the supported web browsers to avoid configuration at each client. Examples of such CAs are VeriSign, Comodo and RapidSSL and the product name for this type of certificate is usually "TLS certificate" or "SSL certificate".

As the certificate must be issued to the correct server host name (Fully Qualified Domain Name, FQDN), e.g. "CLIQwebmanager.mycompany.com", it is only possible to order certificates from a CA if you are the legitimate owner of the domain used, in this example "mycompany.com".

Contact the CA of your choice for instructions on how to purchase TLS server certificates. TLS server certificates are required when installing and configuring CLIQ™ Web Manager. Customer will need one certificate for CLIQ™ Web Manager application and one for enrolment application. In the ordering phase, it is required to mention FQDNs for both servers (e.g. CLIQ™webmanager.mycompany.com and CLIQ™ remote.mycompany.com). Alternatively a wildcard / multidomain certificate can be used (e.g. \*.mycompany.com) on both servers.

Below is the list of requirements for certificates

- Maximum length of FQDN is 81 characters
- Minimum RSA key length is 2048 bits
- Minimum signature hash algorithm is SHA-2/SHA256
- Supported formats are PKCS#1, Base64 and PEM (in cleartext, no encryption).
- Two files needed per server: TLS server certificate file and TLS private key file

## System setup

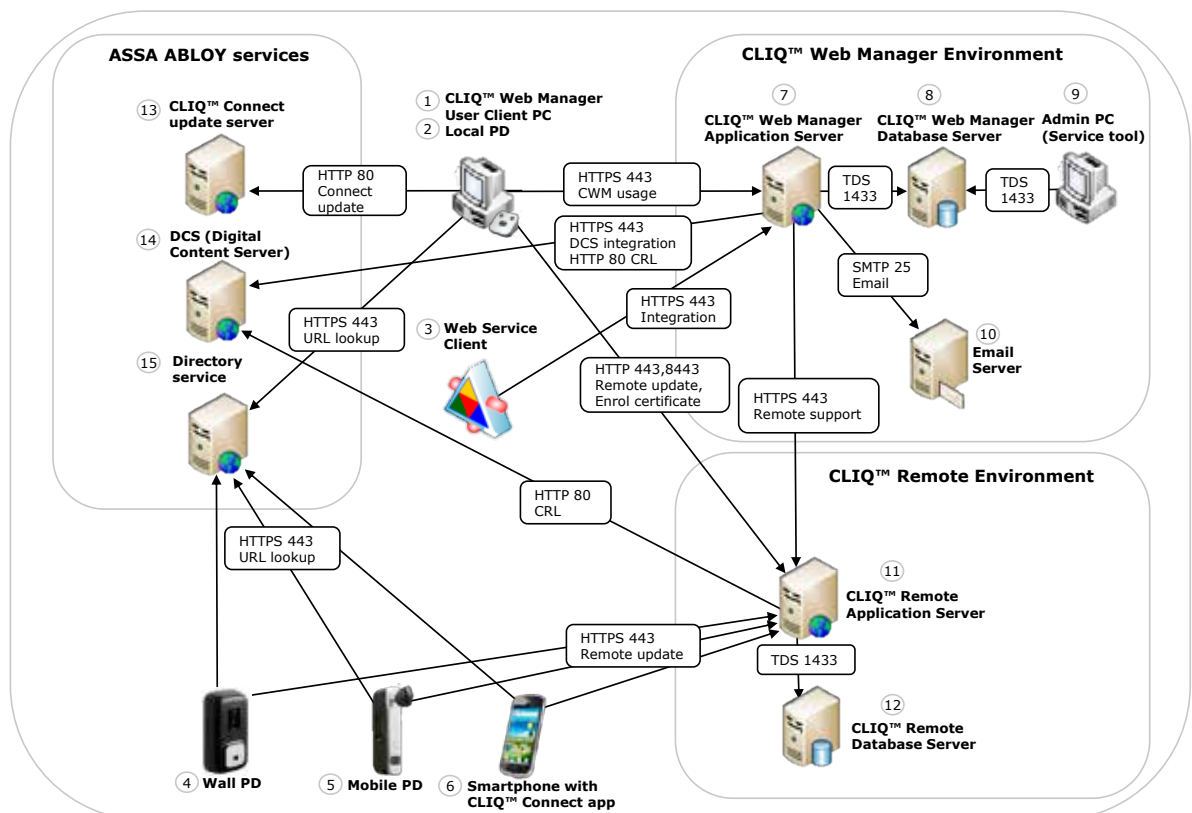
The recommended setup contains four dedicated servers: CLIQ™ Web Manager application server, CLIQ™ Web Manager database server, CLIQ™ Remote application server and CLIQ™ Remote database server. Servers can be either physical or virtual servers. The main reasons for having four dedicated servers are security, performance and reliability. Mobile PDs and CLIQ™ Connect Phone applications will connect to CLIQ™ Remote service via Internet. The Remote service must therefore be accessible from Internet. The suggested setup is to place CLIQ™ Remote environment (application + database) in DMZ while locating the CLIQ™ Web Manager server on the Intranet (LAN). No CLIQ™ sensitive information is stored on the CLIQ™ Remote side.



## Note!

- It is not supported to install databases on the same server as the CLIQ™ Web Manager or CLIQ™ Remote application.
- CLIQ™ Web Manager and CLIQ™ Remote applications cannot be installed in the same server.
- Minimum setup is three dedicated servers, where both databases are installed in one database server. For large systems (>1000 system elements) this setup can cause performance issues and is therefore not recommended
- Both databases can be located in an existing SQL cluster solution if available.
- Time synchronization of servers is important. All servers need to use the same system time and therefore shall be synchronized to a NTP (Network Time Protocol) server.

For security reasons it is recommended to use servers physically separated by firewalls to minimize the exposure of each node to unauthorized network traffic. An overview of the system is depicted in below picture. Please notice that direction of arrows shows where connections are initiated and that firewalls are discarded from picture.



Service	Example URL
CLIQ™ Web Manager	https://cwm.customer.domain.com:443/CLIQWebManager
CLIQ™ Remote	https://remote.customer.domain.com:443/CLIQRemote
Enrolment	https://remote.customer.domain.com:8443/CLIQWebManagerEnrolment
CLIQ™ Connect Update server	http://cliqconnect.assaabloy.com

Abbreviation	Explanation
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
CRL	Certificate Revocation List
URL	Uniform Resource Locator
TDS	Tabular Data Stream
SMTP	Simple Mail Transfer Protocol

# Standards and approvals

Below is the list of system elements with explanations

1. CLIQ™ Web Manager User Client PC is used by administrators of CLIQ™ locking systems to access the CLIQ™ Web Manager software. CLIQ™ Web Manager software is accessed by using a web browser and a Java applet or CLIQ™ Connect PC application.
2. Local programming device (Local PD) is connected to client PCs enabling access to CLIQ™ Web Manager software. The left key port of Local PD is intended for C-keys and right port is for user keys.
3. CLIQ™ Web Manager software can be integrated with customers' own IT systems through SOAP Web Services interface.
4. Wall mounted programming device is used for programming user keys and C-keys. These devices are connected to CLIQ™ Remote server.
5. Mobile programming device is similar to wall mounted programming device, except it is a handheld device and utilizes the data connection of the mobile phone by using Bluetooth technology.
6. Smart phone with CLIQ™ Connect application is used to program access right for CLIQ™ Connect keys.
7. CLIQ™ Web Manager application server is the key part of the system, where CLIQ™ Web Manager application is running. Two services are installed to this server: CLIQ™ Web Manager tomcat service and apache service.
8. CLIQ™ Web Manager database server contains the database for CLIQ™ Web Manager application.
9. Admin PC is intended for creating and updating CLIQ™ Web Manager and CLIQ™ Remote databases. CLIQ™ Web Manager database is managed by a software called Service Tool.
10. Email server is needed to be able to send emails to key holders, informing them about pending key updates etc.
11. CLIQ™ Remote server application server handles key update jobs. Update jobs are created in CLIQ™ Web Manager and sent to the CLIQ™ Remote server. Two services are installed on this server: CLIQ™ Remote tomcat service and apache service. CLIQ™ Remote web application and CLIQ™ Web Manager Enrolment application are deployed on this server by default. The Enrolment applications is only installed if CLIQ™ Web Manager is integrated with DCS server. The Enrolment application is used for fetching new certificates for C-keys.
12. CLIQ™ Remote database server contains the database for CLIQ™ Remote application.
13. CLIQ™ Connect update server is used for downloading the latest CLIQ™ Connect PC application to CLIQ™ Web Manager Client PCs.
14. Digital Content Server is managing and delivering digital content to CLIQ™ Web Manager installations.
15. Directory service is a background service for searching the correct service URL for CLIQ™ Remote server. Remote PDs and CLIQ™ Connect applications will use directory service automatically.

In the CLIQ™ Web Manager it is possible to setup proxy servers between the following system elements.

- Between CLIQ™ Web Manager server and Digital Content Server. This proxy is set up during the installation of CLIQ™ Web Manager. Installation parameters can be changed afterwards.
- Between CLIQ™ Remote server and remote programming devices. Proxy settings are assigned in CLIQ™ Web Manager user interface and configured to remote programming devices during Remote PD deployment phase.

Below is the summary of all network connections. Note that all connections are initiated by end point 1. SSL/TLS requires mutual authentication using client certificates. All connections must be end-to-end connections which cannot be terminated between.

# Standards and approvals

## NETWORK CONNECTIONS

END POINT 1	PROTOCOL / TCP PORT	END POINT 2	PURPOSE
User client PC	HTTPS / 443	CLIQ™ Web Manager server	CLIQ™ Web Manager user interface
Web Service client (Integration sw)	HTTPS / 443	CLIQ™ Web Manager server	Web Service calls
User client PC	HTTPS / 8443	CLIQ™ Remote server	Enrol C-key certificate
Remote programming device (Wall PD or Mobile PD)	HTTPS / 443	CLIQ™ Remote server	Programming tasks
Smartphone with CLIQ™ Connect application	HTTPS / 443	CLIQ™ Remote server	Programming tasks
CLIQ™ Web Manager server	TDS / 1433	CLIQ™ Web Manager database server	Database connection
CLIQ™ Web Manager server	HTTPS / 443	CLIQ™ Remote server	Establish remote functionalities
CLIQ™ Web Manager server	SMTP / 25	Email server	Email functionalities
CLIQ™ Web Manager server	HTTPS / 7443	Digital Content Server (DCS)	Deliver digital content to installation
CLIQ™ Web Manager server	HTTP / 80	Digital Content Server (DCS)	Download certificate revocation list
CLIQ™ Remote server	TDS / 1433	CLIQ™ Remote database server	Database connection
CLIQ™ Remote server	HTTP / 80	Digital Content Server (DCS)	Download certificate revocation list
Admin PC	TDS / 1433	Database servers	Manage CLIQ™ databases
Remote programming devices, CLIQ™ Connect smartphone and PC applications	HTTPS / 443	Directory service	Searching correct URL for CLIQ™ Remote service
User client PC	HTTP / 80	CLIQ™ Connect update server	Downloading latest CLIQ™ Connect PC application

# Standards and approvals

## Monitoring

CLIQ™ Web Manager and CLIQ™ Remote services can be monitored from the applications log files, which can be found on the servers.

- CLIQ™ Web Manager server
  - CLIQ WebManager.log from [installation folder]\tomcat\logs
- CLIQ™ Remote server
  - CLIQ Remote.log from [installation folder]\tomcat\logs

The following applications need to be monitored from server side:

- CLIQ™ Web Manager server
  - Apache and CLIQ WebManager
- CLIQ™ Remote server
  - Apache and CLIQ Remote

## High-Availability setup

To achieve highest possible service availability, it is possible to setup a high-availability (HA) environment for CLIQ™ Web Manager. HA environment consists of the following.

- Two pairs of application servers, where one is active and another is passive at a time.
  - One pair consists of CLIQ™ Web Manager and CLIQ™ Remote servers.
- Database servers for both CLIQ™ Web Manager and CLIQ™ Remote. Databases can be installed to a SQL cluster.

It is important that the applications on the server pairs are not running at the same time since the applications are configured to use same databases.

It is recommended that these server pairs are located in different datacenters. At least to the level that if one datacenter goes down the other pair in the second datacenter will continue to function.

Both CLIQ™ Web Manager and CLIQ™ Remote services require external IPs and FQDNs (fully qualified domain names) for customers to reach the services. It is needed to setup a routing policy that will route the network traffic to the server pair that is active. Apache and CLIQ™ Web Manager (or CLIQ™ Remote) services are running on the active server pair while they are stopped on the passive pair. Service failover between an active and passive server pair needs to be done manually, CLIQ™ Web Manager software will not do this automatically. First, shutdown the services from the active server pair and then start the services from the passive pair. This is important in order to avoid database conflicts.

## Maintenance

Normally there are two major versions of CLIQ™ Web Manager per year. Minor patch releases might also be released if needed. Abloy will support the current and two earlier major versions. It is highly recommended to update operating system patches offered by Microsoft regularly to the servers.

## Security

PROTEC<sup>2</sup> CLIQ™ security is based on mechanical key system combined with CLIQ™ electronic access rights. A CLIQ™ system can be mechanically keyed alike or masterkeyed, but all systems are still always mechanically different. On top of this, TLS certificates are used to authenticate elements of the system. All data between keys, cylinders, remote programming devices and CLIQ™ Web Manager is encrypted.

CLIQ™ elements are produced in high security factory premises. All sensitive CLIQ™ data exported by the factory is encrypted, imported and stored centralized in the CLIQ™ Web Manager database. All business logic for handling CLIQ™ security is kept centralized in CLIQ™ Web Manager server. No CLIQ™ sensitive data is stored on the CLIQ™ Remote application server and therefore CLIQ™ Remote server can be used in the demilitarized zone (DMZ).

The security of CLIQ™ Web Manager system is based on Public Key Infrastructure (PKI). It is used for the following reasons.

- 1. Confidentiality: Encryption of data in transit and in rest**
  - a. CWM needs to prevent an attacker from reading data sent over any network used including the Internet so that an attacker for example cannot give himself or someone else access to cylinders he should not be authorized to use.
  - b. CWM needs to prevent an attacker from reading stored data used by CWM so that an attacker for example cannot give himself or someone else access to cylinders he should not be authorized to use. To do this CWM uses various encryption techniques and ciphers.
- 2. Privacy: Encryption of private information**
  - a. CWM needs to prevent an attacker from reading sensitive data such as employee information sent over any network used including the Internet so that an attacker for example cannot map employees to specific keys and work positions and so that personal integrity of employees isn't compromised.
- 3. Integrity: Message tampering and corruption protection**
  - a. CWM needs to be able to verify the integrity of data sent over any network used including the Internet so that CWM can be certain the data is authentic and not edited by an attacker or corrupted during transfer. This is required even though the data is encrypted since an attacker can still edit encrypted data and data can still be corrupted during transit.
- 4. Authorization: Who can access**
  - a. CWM needs to be in control of who can access, what can be accessed and at what time.
- 5. Authenticity: Identification of sender**
  - a. CWM needs to know the identity for all clients it communicates with so that CWM can use that data to verify that the client is authorised and for traceability in logs.

CLIQ™ Web Manager is using HTTPS/SSL/TLS protocols for encrypting the network traffic. Please see the network connections and used protocols from the previous section. Data between the CLIQ™ key and CLIQ™ lock and between CLIQ™ key and CLIQ™ Web Manager client are encrypted using 128-bit AES.

# DOUBLE SECURED



MECHANICAL  
LOCKING



ELECTRONIC  
ACCESS CONTROL



Telemedia



Transportation/Logistics



Designed for you

# AWARD WINNING

Double secured access  
control technology

## ABLOY<sup>®</sup> PROTEC<sup>2</sup>



Read more  
and see  
the video at  
[abloy.com](http://abloy.com)