

 **ABLOY®**

 **CLIQ™**



**ABLOY® PROTEC<sup>2</sup>**

Техническая брошюра

## Система PROTEC<sup>2</sup> CLIQ™

PROTEC<sup>2</sup> CLIQ™ - это легкая в использовании система контроля доступа, основанная на механических дисковых цилиндрах и электронной идентификации. ABLOY PROTEC<sup>2</sup>, основанный на запатентованном механизме цилиндра с вращающимися дисками, обеспечивает механическую безопасность вашего объекта, в то время как технология CLIQ™ предлагает гибкий контроль ключей, прав доступа и создание журналов событий. Система PROTEC<sup>2</sup> CLIQ™ соединяет обе технологии в одно эффективное решение.

Ключи PROTEC<sup>2</sup> CLIQ™ могут быть обновлены через настенный или мобильный программатор. А ключи PROTEC<sup>2</sup> CLIQ™ с функцией Connect позволяют пользователям обновлять ключи через мобильное приложение CLIQ™ Connect на своем смартфоне в любом месте без необходимости посещать объект запирания.

### ▶ ИНТЕЛЛЕКТУАЛЬНАЯ КОМБИНАЦИЯ ЭЛЕКТРОНИКИ, МЕХАНИКИ И ОТКРЫВАНИЯ В РЕАЛЬНОМ ВРЕМЕНИ ЧЕРЕЗ МОБИЛЬНОЕ ПРИЛОЖЕНИЕ

#### Электронная технология CLIQ™

- Технология CLIQ™, специально разработанная для индустрии запирания, имеет уникальную идентификацию для каждого открывания, которое обеспечивается зашифрованным взаимодействием ключей и цилиндров
- Батарейка внутри ключа обеспечивает беспроводное функционирование временного графика доступа и календаря записей журнала событий
- Права доступа, ограниченные по дате и времени, легко могут быть изменены удаленно.
- Технология CLIQ™ легко и без лишних затрат дополняет и расширяет возможности механической системы



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

- Долговечная конструкция без пружин и штифтов
- Система блокировки дисков в цилиндре – запатентованная технология, которая предотвращает попытки взлома отмычками
- Надежная защита от бампинга и “подбора” ключа
- Патент на ключи и устройство цилиндра действует до 2031
- 1,97 миллиардов различных комбинаций ключа
- Симметричный ключ, который можно вставить в замок любой стороной
- Одному пользователю нужен всего один ключ для всех дверей
- Надежная работа в суровых условиях



#### Технология CLIQ™ Connect

- Ключи CLIQ™ Connect могут быть обновлены через приложение для смартфона
- Дистанционное обновление ключа в режиме реального времени в любом месте
- Актуальные права доступа проверяются при вводе ключа в цилиндр
- Во время обновления прав доступа система считывает последние события ключа и отправляет их на сервер администратора.
- Проверка PIN-кода позволяет подтвердить подлинность ключа при отсутствии подключения к интернету.



## Веб-интерфейс CLIQ™ Web Manager для легкого управления системой

Веб-менеджер CLIQ™ позволяет изменять права доступа в любое время и в любом месте, где Вам это необходимо



## Области применения

PROTEC<sup>2</sup> CLIQ™ используется Профессиональными Пользователями в различных сферах, таких как коммунальное хозяйство, телекоммуникационный сектор, нефтегазовый сектор, перевозки и транспорт, больницы, государственные учреждения, банки, музеи, железная дорога.

## ▶ КЛЮЧИ

Ключи PROTEC<sup>2</sup> CLIQ™ имеют металлический стержень и пластиковую головку, в которой размещены электроника и батарейка. Все ключи PROTEC<sup>2</sup> CLIQ™ снабжены часами, работающими в режиме реального времени, и памятью, для того чтобы обеспечить работу функций, основанных на времени, и для создания и записи журнала событий.

Ключи PROTEC<sup>2</sup> CLIQ™ доступны с функцией CLIQ™ Connect. CLIQ™ Connect ключ позволяет сотрудникам обновлять изменения доступа в ключах, сделанные администратором, из любого места, используя приложение CLIQ™ Connect на своем смартфоне.

### Спецификация ключей PROTEC<sup>2</sup> CLIQ™

- Срок службы батарейки в ключе до 10 лет, её легко заменить, открыв пластиковую крышку головки ключа.
- Срок службы батарейки в ключе CLIQ™ Connect со встроенным модулем Bluetooth 4.0 до 1 года.
- Батарея CR2450
- Ключи сопровождают свою работу звуковым сигналом и светодиодной индикацией, расположенной с обеих сторон ключа
- Все ключи PROTEC<sup>2</sup> CLIQ™ имеют возможность размещения чипа RFID с дополнительной RFID головкой. Также доступны отдельные пластиковые головки для смарт-карты MIFARE 1K. Это позволяет использовать тот же самый ключ в системе контроля доступом.
- Дополнительные цветные пластиковые головки для ключей обеспечивают легкое ориентирование между ключами различных пользовательских групп.
- Все ключи имеют класс защиты IP57
- Рабочая температура ключей от -20°C до +50°C



## Обычный пользовательский ключ

Обычный пользовательский ключ способен открывать все цилиндры PROTEC<sup>2</sup> CLIQ™, если этот ключ или группа ключей запрограммированы в цилиндре. Права доступа управляются занесением одного или нескольких ключей в память цилиндра. Права доступа изначально задаются на заводе в соответствии с планом запираения. В дальнейшем эту информацию можно изменить с помощью программного ключа. Предназначен для ситуаций, когда права доступа стабильны и изменения происходят редко.



## Динамический ключ

В отличие от обычного пользовательского ключа, динамический ключ предназначен для ситуаций, когда права доступа меняются часто. Динамический ключ имеет список цилиндров или групп цилиндров, которые занесены в память ключа с помощью CLIQ™ Web Manager. Это делает управление правами доступа гибким, так как ключ может быть удаленно запрограммирован на открывание определенного замка, необходимого в данное время.



## Программный ключ

Программный ключ используется для доступа в программном обеспечении веб-менеджера CLIQ™ Web Manager. Администратор может создавать задачи в CLIQ™ Web Manager и переносить их в цилиндр с помощью программного ключа. Журналы событий цилиндра могут быть считаны с помощью данного ключа.



## CLIQ™ Connect ключ

CLIQ™ Connect ключ также доступен с технологий Bluetooth, что обеспечивает надежный способ обновления прав доступа.



# ПРОДУКЦИЯ PROTEC<sup>2</sup> CLIQ™

## CLIQ™ КЛЮЧИ



СРОК СЛУЖБЫ БАТАРЕИ

СРОК ДЕЙСТВИЯ ЗАДАН АДМИНИСТРАТОРОМ

ЖУРНАЛ СОБЫТИЙ

ЖУРНАЛ ВНЕШНИХ СОБЫТИЙ

СПИСОК ЗАМКОВ И ГРУПП ЗАМКОВ, К КОТОРЫМ ЕСТЬ ДОСТУП

ЕЖЕНЕДЕЛЬНОЕ РАСПИСАНИЕ

СОВМЕСТИМОСТЬ С МОБИЛЬНЫМ ПРИЛОЖЕНИЕМ

ОТКРЫВАНИЕ В РЕАЛЬНОМ ВРЕМЕНИ ЧЕРЕЗ МОБИЛЬНОЕ ПРИЛОЖЕНИЕ

ЖУРНАЛ СОБЫТИЙ В РЕАЛЬНОМ ВРЕМЕНИ

ПРОВЕРКА PIN-КОДА

### PROTEC<sup>2</sup> CLIQ™

Пользовательский ключ	TQ406/TQG406	до 10 лет	х	2000	20		50				
Динамический ключ	TQ406/TQG407	до 10 лет	х	2000	20	3500	50				
Программный ключ	TQ403/TQG403	Up to 10y	х	8000							



### CLIQ™ Connect ключи

Пользовательский ключ	TQB406/QGB406	1 год	х	2000	20		50	х			х
Динамический ключ	TQB407/QGB407	1 год	х	2000	20	800	50	х			х
Программный ключ	TQB403/QGB403	1 год	х	8000				х			х
Ключ с функцией онлайн открывания	TQC407/QGC407	1 год	х	2000	20	800	50	х	х	х	х

Все новые ключи PROTEC<sup>2</sup> CLIQ™ Remote и CLIQ™ Connect ключи совместимы с устройствами удаленного программирования.

## ИНСТРУКЦИИ ПО ЭКСПЛУАТАЦИИ

После того, как ключ вставлен в цилиндр, дождитесь звукового сигнала перед тем, как поворачивать ключ. Сигналы могут быть такими:

<p>1 короткий сигнал и зеленый светодиод</p> <p><b>OK</b></p> <p>Ключ распознан и принят, замок может быть открыт после сигнала</p>	<p>3 коротких сигнала и красный светодиод</p> <p><b>STOP</b> / </p> <p>Ключ отклонен, неверный код или диапазон времени</p>	<p>3 длинных сигнала и зеленый светодиод</p> <p> =  / </p> <p>Заряд батарейки низкий или ключ замерз (попробуйте согреть ключ в своей руке)</p>	<p>Нет сигнала</p> <p> = </p> <p>В этом случае замок не может быть открыт. Замените батарейку или обратитесь к системному администратору</p>
---	---	---	--

Для нормальной работы вашего ключа PROTEC<sup>2</sup> CLIQ™, пожалуйста, обратите внимание на следующие меры предосторожности:



Не бросайте ключ



Берегите ключ от попадания грязи и влаги



Не пытайтесь открыть дверь, потянув за ключ, зафиксированный в замке. Используйте ручку.



Не подвергайте ключ действию экстремальных температур  
MAX +50°C  
MAX -20°C



Для замены батарейки в ключе снимите крышку и вставьте новую батарейку в ключ



Неправильные смазочные материалы могут быть опасны для электроники цилиндра. Используйте только масло ABLOY.

## УСТРОЙСТВА ПРОГРАММИРОВАНИЯ

Права доступа в ключах PROTEC<sup>2</sup> CLIQ™ могут быть обновлены с помощью локального программатора, а также с помощью удаленного программатора. Способность работать удаленно позволяет собирать журналы событий, обновлять права доступа, задавать временные рамки и возвращать права доступа ключам (функция ревалидации).

### Настенный программатор PDA100

Настенный программатор PDA100 – это устройство для программирования ключей, которое устанавливается внутри помещений. Связь между CLIQ™ Web Manager, настенным программатором и ключами PROTEC<sup>2</sup> CLIQ™ зашифровано для большей безопасности.

- Настенный блок удаленного программирования
- Надежная система запираения блока
- Нет хранилища данных
- Класс защиты IP42
- Подключение по локальной сети
- Питание от адаптера 12-24 В или через сеть Ethernet (PoE)
- Поддержка прокси-сервера
- Технология Plug and Play\*
- Возможность обновление оффлайн



### Мобильный программатор PDA200

Мобильный программатор – индивидуальное переносное устройство для программирования, позволяющее получать обновления прав доступа ключа PROTEC<sup>2</sup> CLIQ™ в любой точке мира. Мобильный программатор работает так же, как настенный программатор, но получает питание от батареек типа AAA и подключается к интернету через мобильный телефон (Bluetooth) или ноутбук (USB).

- Работает от 4 стандартных батареек серии AAA
- PDA200 Bluetooth и USB (для мобильных телефонов и компьютеров)
- Поддержка прокси-сервера
- Технология Plug and Play\*
- Обновление оффлайн



\*Установка Plug and Play для программаторов доступна в системе программного обеспечения CLIQ™ Web Manager (CWM) версии 6 и более поздних версиях.

Другие требования:

- CLIQ™ Web Manager с интеграцией DCS
- Версии 6.0 или выше
- Использование DHCP
- Отсутствие прокси настроек для удаленного программатора

## Внешний настенный программатор PDA120

Внешний настенный программатор – это устройство удаленного программирования, которое может быть установлено снаружи зданий или в агрессивной среде. Так же как и настенный программатор для внутренних помещений, внешний настенный программатор соединяется с удаленным сервером через Ethernet и поддерживает PoE.

- Класс защиты от воды и пыли IP57
- Уровень защиты от взлома IK9



## Считыватель CLIQ™ TQ124

Считыватель CLIQ™ – это контроллер, управляемый реле, который передает сигнал другим устройствам или системам, таким как электрические замки или системы тревожной сигнализации. Считыватель CLIQ™ может быть установлен снаружи здания и имеет класс защиты IP53. Внутри считывателя установлен цилиндр PROTEC<sup>2</sup> CLIQ™, который управляется только ключами, имеющими право доступа.

Корпус считывателя CLIQ™ устанавливается снаружи здания рядом со входом. Он соединен проводом с реле, которое может быть установлено с внутренней стороны двери.

Реле срабатывает только когда у ключа есть соответствующее право доступа. Считыватель может быть запрограммирован с помощью программного ключа.

- Питание 12-24 постоянного тока -10/+15%
- Потребляемая мощность 60 мА
- Реле – максимальная мощность 0,8А 30V AC/DC, сопротивление 20W
- Максимальная длина шнура между корпусом и электроникой 1 метр
- Провод необходимо обрезать на нужную длину, наращивать провод нельзя



## Настенный программатор со считывателем PDA110

Программатор PDA110 состоит из двух частей. Настенный программатор и присоединенный к нему считыватель. Программатор устанавливается внутри помещения, в то время как считыватель, имеющий класс защиты от влияния внешней среды IP53, устанавливается снаружи рядом с входной дверью. Считыватель соединен с настенным программатором кабелем длиной 2 метра.

- Максимальная длина кабеля 2 метра
- Остальные характеристики такие же как у PDA100
- Ключи могут быть обновлены в обеих частях
- Не содержит реле





## Программатор PDA500

Программатор PDA500 – это программирующее устройство PROTEC<sup>2</sup> CLIQ™ ключей, которое соединено с персональным компьютером. Программатор используется для авторизации администратора в системе CLIQ™ Web Manager с помощью программного ключа и для программирования PROTEC<sup>2</sup> CLIQ™ ключей.

- Подключение к компьютеру через USB (в комплекте)
- Plug and Play установка
- Питание от USB



## CLIQ™ Connect

Пользовательские ключи PROTEC<sup>2</sup> CLIQ™ и программные ключи также доступны в версии CLIQ™ Connect ключей, которые могут быть запрограммированы через мобильное приложение CLIQ™ Connect. Обновить право доступа возможно в любое время и в любом месте. Выгрузка информации в журнал событий CLIQ™ Web Manager происходит в режиме реального времени при обновлении ключа.

Ключ для открывания в реальном времени через мобильное приложение

Ключи с функцией открытия через Интернет используют приложение CLIQ™ Connect для проверки прав доступа в реальном времени в момент ввода ключа в цилиндр. Это позволяет контролировать доступ в реальном времени в местах, где отсутствует стационарный интернет.

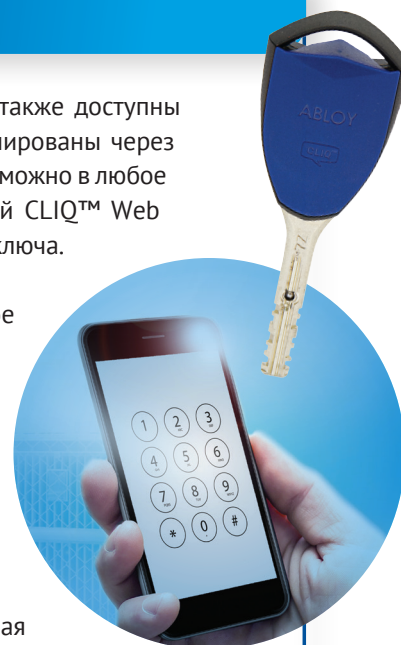
Для пользовательских ключей CLIQ™ Connect доступна лицензируемая функция проверки PIN-кода. Это позволяет подтверждать подлинность ключа при отсутствии подключения к интернету. Проверка PIN-кода выполняется в мобильном приложении CLIQ™ Connect, что повышает безопасность во многих аспектах.

CLIQ™ Connect ключи используют технологию Bluetooth Low Energy для связи с приложением для смартфонов. Приложение CLIQ™ Connect на мобильном устройстве подключается к удаленному серверу CLIQ™ через интернет, что позволяет обновить права доступа.

Мобильное приложение CLIQ™ Connect совместимо с iOS 8.0 или более поздней версией. Для платформы Android рекомендована версия 5.0 и более поздние. Мобильное приложение доступно в App Store и Google Play.

Можно привязать до трех ключей к одному мобильному телефону на базе iOS при использовании приложения CLIQ™ Connect. При использовании мобильных телефонов на базе Android можно привязать только один ключ.

Для корректной работы мобильного приложения CLIQ™ Connect используйте программное обеспечение с Web-доступом (CWM) 6 и более поздней версии.



## CLIQ™ устройства

	УДАЛЕННОЕ ОБНОВЛЕНИЕ КЛЮЧЕЙ	ОБНОВЛЕНИЕ ОФФЛАЙН	РЕЛЕ	ТИП СОЕДИНЕНИЯ	ПИТАНИЕ	ПРОВЕРКА PIN-КОДА	
Настенный программатор	✓	✓		LAN	12/24 В или POE		
Мобильный программатор USB/Bluetooth	✓	✓		Bluetooth к смартфону	4 x AAA батарейки / USB		
Программатор PDA500	(✓) 1			USB к ПК	USB		
Настенный программатор со считывателем	✓	✓		LAN	12/24 В или POE		
Внешний настенный программатор	✓	✓		LAN	12/24 В или POE		
Мобильное приложение	✓			Bluetooth к CLIQ™ Connect ключу	Смартфон, IOS/Android	✓	
Считыватель CLIQ™ TQ124			✓		12/24 В		

1) Требуется CLIQ™ Web Manager (CWM) версии 6 (и более поздняя) и приложение CLIQ™ Connect для ПК

## ФУНКЦИИ ЦИЛИНДРА

Цилиндр PROTEC<sup>2</sup> CLIQ™ содержит уникальный механический цилиндр PROTEC<sup>2</sup> с девятью вращающимися дисками. Также Цилиндр PROTEC<sup>2</sup> CLIQ™ содержит электронную часть, которая контролирует электронную блокировочную систему. Электронный контроль блокировки цилиндра осуществляется с помощью использования маленького электрического двигателя, управляющего поворотом вращающегося диска. В цилиндре нет встроенного источника питания. Это означает, что нет необходимости в проводах или замене батареек в цилиндре.

Конструкция ключа PROTEC<sup>2</sup> CLIQ™ позволяет ему работать не только с электронными цилиндрами PROTEC<sup>2</sup> CLIQ™, но и с механическими цилиндрами PROTEC<sup>2</sup> с одиннадцатью дисками. Головка ключа PROTEC<sup>2</sup> CLIQ™ содержит электронику ключа и батарейку для питания электроники цилиндра и самого ключа. Электронная связь между ключом и цилиндром осуществляется через биполярный гальванический контакт. Стержень ключа выступает в роли одного полюса, другим полюсом является полоска изолированного металла на головке ключа. Напряжение, необходимое для функционирования цилиндра, передается через эти контакты.

Когда ключ вставлен в цилиндр, активируется электронное общение между ключом и цилиндром. Если ключ авторизован для открытия цилиндра, батарейка внутри ключа активирует функции открывания и закрывания электронной блокировки цилиндра. Журнал событий цилиндра и ключа сохраняются одновременно.

## ПАМЯТЬ ЦИЛИНДРА

- 1800 авторизованных групп ключей и программируемых ключей вместе, теоретически возможно максимум 65535 ключей в каждой группе
- Список из 3000 ключей с отказанным доступом
- Журнал событий на последние 2000 событий
- Журнал событий последних 20 событий от ключей из других систем

## РАСШИРЕННАЯ ФУНКЦИОНАЛЬНОСТЬ ЦИЛИНДРА

### Последовательная синхронизация

CLIQ™ цилиндры также доступны с функцией «последовательной синхронизации», которая программируется в памяти цилиндра на заводе.

Для данного типа блокировки необходимо два ключа. Когда в цилиндр вставлен первый ключ, замок никак не реагирует и не открывается. В течение одной минуты вставьте второй ключ в цилиндр, и замок будет открыт. Синхронизация возможна в течение одной минуты.

## АССОРТИМЕНТ ПРОДУКЦИИ

### Широкий ассортимент продукции – один ключ



Надежные, имеющие класс защиты IP68, навесные замки с технологией CLIQ™ для самых суровых условий эксплуатации.



Цилиндры, подходящие к любым видам дверей. Также доступны с защитой от пыли.



Замки для мебели и оборудования с технологией CLIQ™ и без нее.



Депозиты для безопасного хранения ключей.

## CLIQ™ Web Manager

CLIQ™ Web Manager (CWM) – это система программного обеспечения с Web-доступом, которая управляет и контролирует электромеханическую систему запираения CLIQ™, а также позволяет полностью контролировать авторизации доступа и действия владельцев ключей. Система CLIQ™ предлагает решение, которое обеспечивает надежность механических ключей и цилиндров, а также безопасность и гибкость, присущие электронным замкам. Интерфейс программного обеспечения CLIQ™ Web Manager доступен на 22 языках. Информация данной брошюры соответствует 6 и более поздним версиям CLIQ™ Web Manager.

### ▶ ОСНОВНЫЕ СВОЙСТВА

#### 1. Безопасный вход в программное обеспечение

- a. Для входа в программное обеспечение необходима тройная аутентификация: локальное устройство программирования для доступа к приложению, программный ключ с PIN-кодом и уникальный сертификат программного ключа.

#### 2. Пользователи и продукты

- a. Создание, импорт и редактирование информации о пользователях ключами
- b. Выдача и возврат ключей
- c. Управление потерянными ключами
- d. Управление сломанными ключами и цилиндрами, а также замена продуктов
- e. Изменение статуса цилиндра и информации о местоположении
- f. Работа с цилиндрами в различных часовых поясах
- g. Управление устройствами удаленного программирования
- h. Поиск, просмотр и экспорт информации о пользователях

#### 3. Права доступа

- a. Определение, ограничение и изменение прав доступа
- b. Права доступа с временным интервалом доступны для всех пользовательских ключей. Возможна установка периода действия ключа (неактивен, активен в промежуток времени или постоянно активен), а также создание расписания на неделю и дополнительной ревалидации для всех пользовательских ключей.

#### 4. Журналы событий

- a. Просмотр и экспорт данных из журнала событий для ключей и цилиндров. Журнал событий автоматически считывает информацию с пользовательских ключей во время их удаленного программирования.

#### 5. Отчеты

- a. Распечатка отчетов о выдаче и возврате ключей
- b. Просмотр, экспорт и распечатка отчетов по ключам, цилиндрам, пользователям и журналам событий

### ▶ РАСШИРЕННЫЕ ВОЗМОЖНОСТИ

#### 1. Полномочия администратора

- a. Используются для определения функций, которые может выполнять администратор системы запираения. Функции, видимые в программном обеспечении, зависят от роли, назначенной программным ключом, используемым администратором, вошедшим в систему. Администраторы имеют доступ только к тем функциям, которые необходимы им в работе. Например, администратор может иметь доступ только к функциям выдача/возврат ключей и управлению потерянными или сломанными ключами.

## 2. Домены

а. Позволяют контролировать определенные части системы запираания. Домен состоит из набора цилиндров или групп цилиндров, обычно сгруппированных по географическому или административному признаку. Программные ключи, связанные с таким доменом, обладают правами администрирования только в отношении включенных в эту группу цилиндров.

## 3. Удаленное программирование

а. Позволяет записывать и считывать информацию на пользовательские и программные ключи, когда ключ вставлен в удаленное программирующее устройство. Когда ключ вставлен в удаленное программирующее устройство, выполняются задания на удаленное программирование; обновляется время в ключе; считывается журнал событий с ключа.

С помощью программного ключа возможно программирование заданий для цилиндров.

б. Система CLIQ™ также может включать в себя ключи CLIQ™ Connect, которые программируются через мобильное приложение для смартфонов CLIQ™ Connect.

## 4. Открывание в реальном времени через мобильное приложение

а. Данная функция может быть установлена на ключах CLIQ™ Connect. Когда ключ вставлен в цилиндр, он запрашивает доступ у программного обеспечения CLIQ™ Web Manager через приложение для смартфонов. Если такие права доступа одобрены в программе, то ключ может открыть замок. Ключ запрашивает подтверждение для каждого цилиндра, к которому он может получить доступ.

## 5. Ревалидация ключа

а. Данная функция гарантирует обновление ключей через определенный временные интервалы. Ключ должен быть вставлен в удаленный программатор (ревалидирован) в определенный промежуток времени, чтобы оставаться активными. Получив подтверждение ключ остается активным в течение количества дней, часов и минут, определенного в качестве интервала ревалидации, начиная с момента подтверждения. Если ревалидация ключа не выполняется в пределах предусмотренного интервала, ключ становится неактивным до тех пор, пока опять не будет выполнена ревалидация.

## 6. Группы цилиндров

а. Это набор цилиндров, которые используются для упрощения администрирования системы запираания с множеством цилиндров. Доступ может предоставляться к группе цилиндров точно также, как и одиночному цилиндру. Для повышения гибкости можно использовать комбинации групп цилиндров и одиночных цилиндров. Группы цилиндров предварительно определяются на заводе, но впоследствии цилиндры можно перемещать между группами. Рекомендуется тщательно планировать группы заранее.

б. Примечание! Механические цилиндры не могут принадлежать к группе цилиндров.

## 7. Профили доступа

а. Используются для предоставления людям, имеющим определенные роли, требуемых прав доступа без необходимости конфигурировать каждый ключ индивидуально. Ключи могут быть связаны с профилем доступа. Сотрудники, имеющую определенную роль, такую как уборка офиса, связываются с соответствующим профилем доступа.

Профили доступа являются динамическими (изменение профиля доступа автоматически изменяет состояние авторизаций ключей, заданное в CWM). Изменение профиля доступа порождает задание на удаленное обновление для связанных с профилем ключей.

## 8. Гибкая ревалидация

а. Это дополнительная расширенная функция, которая делает возможной установку интервала ревалидации ключа отдельно для каждого профиля доступа и каждой группы цилиндров. Гибкая ревалидация полезна, когда система запираания требует разный уровень конфиденциальности цилиндров. Например, доступ в серверное помещение может регулироваться строже, чем доступ в переговорную. Или для субподрядчиков можно установить более короткий интервал ревалидации, чем для сотрудников.

## 9. Временные группы доступа

а. Используются для временного расширения прав доступа ключей путем связывания их с некоторым набором профилей доступа. Права доступа временной группы доступа представляют собой объединение прав доступа включенных в нее профилей доступа и действуют в течение периода времени, ограниченного начальной и конечной датами.

Настоятельно рекомендуется применять временные группы доступа в сочетании с ревалидацией

ключей. В качестве примера можно представить ситуацию, когда одному или нескольким прибывшим по вызову техникам-ремонтникам необходимо обеспечить доступ к нескольким профилям доступа на время ремонтных работ. На практике в такой ситуации ключ добавляют во временную группу доступа и программируют в местном или удаленном ПУ. Когда временная группа доступа перестает быть действительной для некоторого ключа, автоматически создается задание дистанционного обновления, предназначенное для удаления этой временной группы доступа из ключа.

## 10. Обновление оффлайн

а. Это функция, которая позволяет выполнять ревалидацию ключей на удаленном программаторе даже в том случае, когда временно потеряно сетевое соединение. Это полезно в ситуациях, когда важно, чтобы срок действия ключа можно было продлить даже при неустойчивом сетевом соединении. Обновления прав доступа в режиме оффлайн невозможны. Оффлайновое обновление конфигурируется независимо для каждого удаленного программатора.

## 11. Интеграция

а. Делает возможной связь с другими системами, например, системами управления кадрами через интерфейс сервиса SOAP

## ▶ ДОПОЛНИТЕЛЬНЫЕ УСЛУГИ ОТ ASSA ABLOY

ASSA ABLOY предоставляет дополнительные услуги для установки CLIQ™ Web Manager. Ниже приведен список услуг, которые могут быть интегрированы с такими установками. Все сервисы размещены на серверах ASSA ABLOY.

### Цифровой контент -сервер

Цифровой контент-сервер (DCS) управляет и безопасным образом доставляет такой контент как сертификаты, данные блокировки, прошивки и программные лицензии на устройства CLIQ™ Web Manager. DCS автоматически интегрируется в любую среду CLIQ™ Web Manager размещенную на серверах Abloy. DCS может интегрироваться также и с собственными локальными серверами клиентов. Если установка не интегрирована с DCS, то цифровой контент, может быть загружен из DCS с использованием внешних учетных записей администратора. Abloy создает такие внешние учетные записи администратора DCS для всех клиентов с собственными локальными серверами.

### Служба каталогов

Служба каталогов является дополнением к DCS. Она предоставляет правильные URL-адреса удаленного сервера CLIQ™ в качестве службы удаленного доступа устройств программирования и приложений CLIQ™ Connect. Эта услуга позволяет использовать функции самонастройки для удаленных устройств программирования. Программа CLIQ™ Connect для ПК является альтернативой Java для работы CLIQ™ Web Manager.

### Обновление CLIQ™ Connect

Служба обновления CLIQ™ Connect предоставляет обеспечение программе CLIQ™ Connect для клиентских ПК с установленном CLIQ™ Web Manager.

## ВАРИАНТЫ УСТАНОВКИ

Существует два варианта установки. Клиент может выбрать программное обеспечение как услугу (SaaS), или же самостоятельно установить систему на собственный сервер.

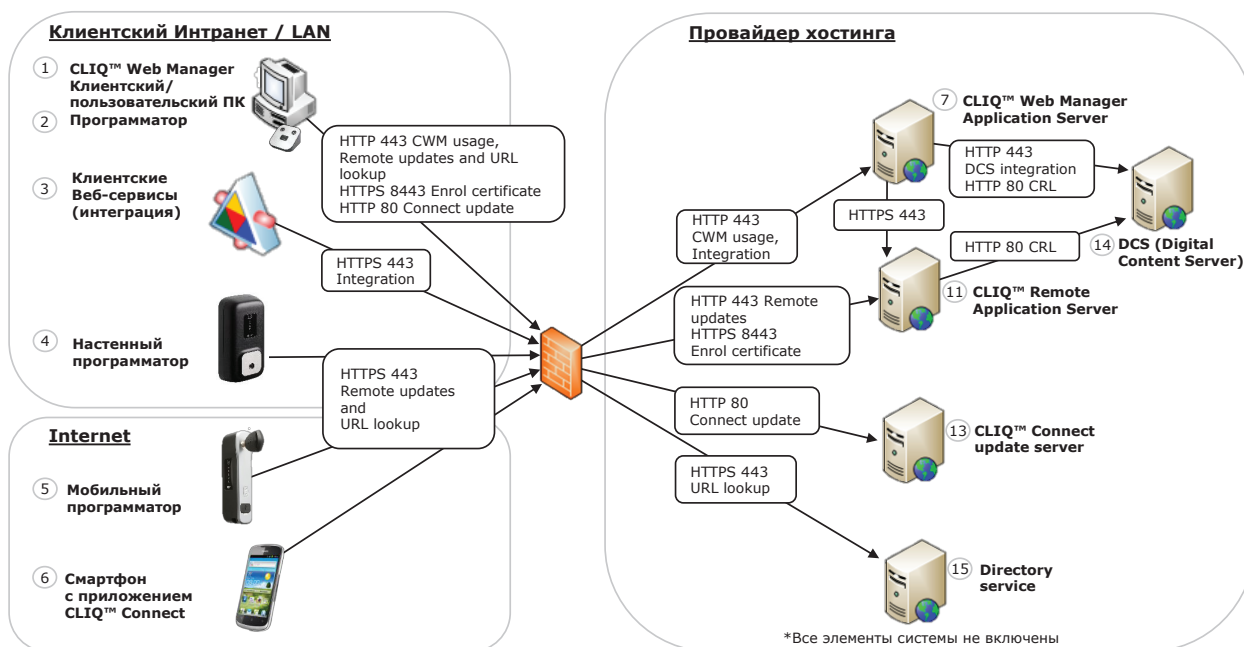
### Программное обеспечение как услуга (SaaS)

Программное обеспечение как услуга означает, что установка и обслуживание CLIQ™ Web Manager предоставляется компанией Abloy Oy. Обновление программного обеспечения, резервное копирование баз данных и импорт расширений в систему записывания выполняются автоматически. Заказчику необходимо лишь настроить сетевые подключения для CLIQ™ Web Manager и удаленного сервера CLIQ™, а также разместить на компьютерах пользователей ПО CLIQ™ Web Manager.

В Abloy размещены следующие среды CLIQ™ Web Manager:

- Доступность услуг: круглосуточно 7 дней в неделю (24/7). Соглашение об уровне предоставления услуг (SLA) - 99,9%, за исключением планового обслуживания;
- Все сервисы CLIQ™ контролируются 24/7;
- Профессиональная поддержка доступна 24/7.

Ниже на рисунке представлен обзор программного обеспечения в качестве сервиса. Сети и устройства клиента отображены с левой стороны картинки, а хостинг-провайдера изображен в правой части. Обратите внимание на требуемые сетевые соединения и направления стрелок, указывающих, где инициируются соединения на рисунке.



Сервис	Пример URL	Аббревиатура	Расшифровка
CLIQ™ Web Manager	https://cwm02.abloy.com:443/CLIQWebManager	HTTP	протокол передачи гипертекстовых документов
CLIQ™ Remote	https://remote02.abloy.com:443/CLIQRemote	HTTPS	расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
Enrolment	https://remote02.abloy.com:8443/CLIQWebManagerEnrolment	CRL	список аннулированных сертификатов
Сервер CLIQ™ Connect Update	http://cliqconnect.assaabloy.com	URL	единообразный определитель местонахождения ресурса

Примечание. Можно настроить прокси-сервер между удаленными устройствами программирования и удаленным сервером CLIQ™. Настройки прокси настраиваются в сети пользовательского интерфейса CLIQ™ Manager и конфигурируются во время фазы развертывания на удаленные устройства программирования.

## Самостоятельная установка клиентом

Система CLIQ™ Web Manager может быть установлена на собственный сервер клиента. В таком случае клиент отвечает за установку системы, обновление программного обеспечения, поддержку сервера, резервное копирование баз данных и другие задачи, такие как обновление версии программного обеспечения и установки расширений. Abloy предоставит клиентам пакеты для установки ПО, включая сертификаты CLIQ™. Эти сертификаты включают специальные сертификаты MKS для каждого удаленного устройства и ключа программирования, а также сертификаты для его инсталляции. Файл сертификата для установки называется «serverbundle.ccb». Имя хоста удаленного сервера CLIQ™ (например, CLIQ™ remote.mycompany.com) встроено в файл serverbundle для того, чтобы сделать установку CLIQ™ более безопасной и использовать стандартные методы безопасности. Поэтому клиент должен сообщить компании Abloy название хоста удаленного сервера CLIQ™ до того момента, как файл «serverbundle» будет создан и доставлен клиенту.

## TLS сертификат для CLIQ™ Web Manager

Клиенту необходимо приобрести или создать TLS сертификат для сервера CLIQ™ Web Manager. Доступ к приложению осуществляется с помощью веб-браузеров с клиентских ПК. TLS сертификаты должны выдаваться центром сертификации (CA в английском сокращении), который является доверенным клиентом веб-браузеров; в противном случае браузеры не смогут аутентифицировать сервер. Пользователи будут проинформированы предупреждением безопасности о том, что данному серверу нельзя доверять.

Настоятельно рекомендуется получать сертификаты, выданные ЦС, которым по умолчанию доверяют поддерживаемые веб-браузеры. Примерами таких центров сертификации являются VeriSign, Comodo и RapidSSL. Обратитесь в ваш центр сертификации за помощью в приобретении продукта. Назовите им названия - «сертификат TLS» или «сертификат SSL».

Поскольку сертификат должен быть выдан на надлежащее название хоста сервера (Полностью определённое имя домена, т.е. FQDN) - например, «CLIQ™ webmanager.mycompany.com», то можно заказывать сертификаты только от ЦС, если вы являетесь законным владельцем используемого домена. К примеру «mycompany.com». Обратитесь в ЦС по вашему выбору за инструкциями о том, как приобрести сертификаты сервера TLS. Сертификаты сервера TLS требуются при установке и настройке приложения CLIQ™ на серверах. На этапе заказа необходимо указать FQDN для обоих серверов (например, CLIQ™ webmanager.mycompany.com и CLIQ™ remote.mycompany.com).

Ниже приведен список требований к сертификатам

- Максимальная длина полного доменного имени - 81 символ
- Минимальная длина ключа RSA составляет 2048 бит
- Минимальный алгоритм хеширования подписи - SHA-2 / SHA256
- Поддерживаемые форматы: PKCS # 1, Base64 и PEM (в открытом виде, без шифрования).
- Для каждого сервера необходимы два файла: файл сертификата сервера TLS и файл закрытого ключа TLS

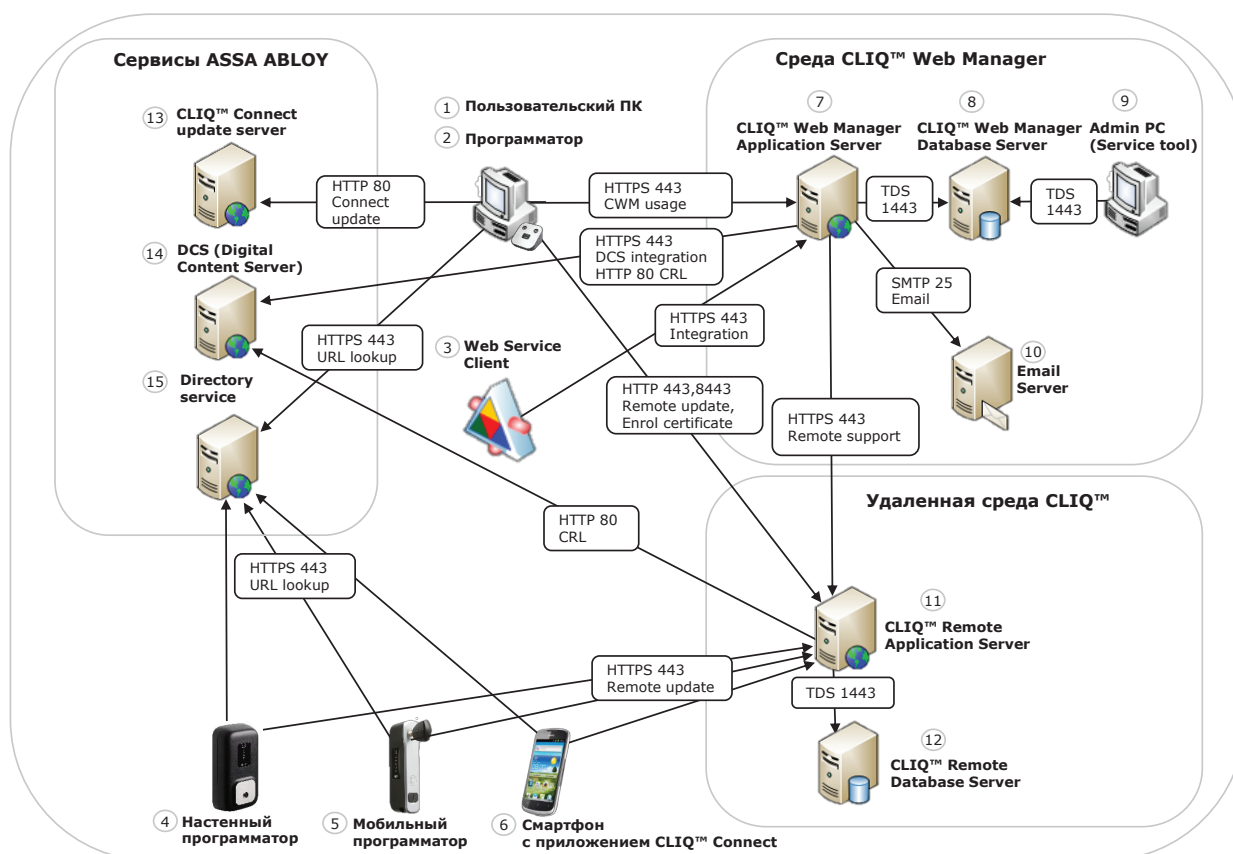
## Настройка системы

Рекомендуемая настройка содержит четыре выделенных сервера: сервер приложений CLIQ™ Web Manager, CLIQ™ Web (сервер базы данных менеджера), сервер удаленного администрирования CLIQ™ и сервер удаленной базы данных CLIQ™. Серверы могут быть как физическими, так и виртуальными. Основными причинами наличия четырех выделенных серверов являются безопасность, производительность и надежность.



## Внимание!

- Не поддерживается установка баз данных на тот же сервер, что и CLIQ™ Web Manager или удаленного приложения CLIQ™.
- CLIQ™ Web Manager и удаленные приложения CLIQ™ не могут быть установлены на одном и том же сервере.
- Минимальная настройка - это три выделенных сервера, на которых обе базы данных установлены на одном и том же сервере базы данных. Для больших систем (> 1000 системных элементов) могут возникнуть проблемы с производительностью, поэтому эта настройка не рекомендуется.
- Обе эти базы данных могут быть расположены в существующем решении кластера SQL (если они доступны).
- Важным моментом является синхронизация времени серверов. Все серверы должны использовать одно и то же системное время, и поэтому они должны быть синхронизированы с сервером NTP (протокол системного времени). По соображениям безопасности рекомендуется использовать серверы, физически разделенные брандмауэрами для минимизации воздействия каждого узла на несанкционированный сетевой трафик. Обзор системы изображен на рисунке ниже. Обратите внимание на то, что направление стрелок показывает, где начаты подключения и что брандмауэры удалены из изображения.



Сервис	Пример 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
СерверCLIQ™ Connect Update	http://cliqconnect.assaabloy.com

Аббревиатура	Расшифровка
HTTP	протокол передачи гипертекстовых документов
HTTPS	расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
CRL	список аннулированных сертификатов
URL	единообразный определитель местонахождения ресурса
TDS	поток табличных данных
SMTP	простой протокол передачи почты

# Программное обеспечение

Ниже приведен список элементов системы с пояснениями:

1. Клиентский ПК используется администраторами системы запирающего для доступа к CLIQ™ Web Manager. Доступ к программному обеспечению CLIQ™ Web Manager осуществляется с помощью веб-браузера и приложения Java или приложения CLIQ™ Connect для ПК.
2. Локальное устройство программирования (localPD) подключается к клиентским ПК, что обеспечивает доступ к программному обеспечению CLIQ™ Web Manager. Левый порт программатора предназначен для программных ключей, а правый порт - для пользовательских ключей.
3. Программное обеспечение CLIQ™ Web Manager может быть интегрировано с собственными ИТ-системами клиентов через сетевой интерфейс сервисов SOAP.
4. Настенное программирующее устройство предназначено для программирования пользовательских и программных ключей. Эти устройства подключены к удаленному серверу CLIQ™.
5. Мобильный программатор работает также как настенный, но подключается к интернету через мобильный телефон с использованием технологии Bluetooth.
6. Смартфон с приложением CLIQ™ Connect используется для программирования доступа ключей CLIQ™ Connect.
7. Сервер приложений CLIQ™ Web Manager является ключевой частью системы, в которой работает программа CLIQ™ Web Manager. На этот сервер установлены два сервиса: служба CLIQ™ Web Manager tomcat и Apache.
8. Сервер базы данных CLIQ™ Web Manager содержит в себе базу данных для приложений CLIQ™ Web Manager.
9. ПК администратора предназначен для создания и обновления событий в программе CLIQ™ Web Manager и в CLIQ™ Remote. База данных CLIQ™ Web Manager управляется программным обеспечением Service Tool.
10. Почтовый сервер необходим для рассылки электронной почты держателям ключей. Например, для ожидающих обновления ключа.
11. Если интеграция с DCS активирована, сертификаты удаленных ПУ генерируются с помощью CWM, в то время как сертификаты программных ключей генерируются посредством приложения для записи сертификата. Приложение для записи сертификата (Enrolment Application) - это веб-приложение, которое устанавливается во время установки системы.
12. Мобильное приложение CLIQ™ Connect позволяет владельцам ключей выполнять обновление, ревалидацию и проверку PIN-кода для своих ключей CLIQ™ Connect с мобильного устройства.
13. Ключи CLIQ™ Connect имеют две прошивки - прошивку ключа CLIQ™ и прошивку Bluetooth. Из мобильного приложения можно обновить только прошивку Bluetooth; обновление прошивки ключа CLIQ™ выполняется в ПУ.
14. Цифровой контент-сервер управляет и доставляет цифровой контент, необходимый для установки CLIQ™ Web Manager.
15. Служба каталогов - это вспомогательный сервис для поиска правильного URL CLIQ™ Remote. Программаторы и CLIQ™ Connect автоматически будут использовать эту службу каталогов.

В CLIQ™ Web Manager можно настроить прокси-серверы между следующими элементами системы:

- Между сервером CLIQ™ Web Manager и сервером цифрового контента. Этот прокси-сервер настраивается во время установки CLIQ™ веб-менеджера на сервере через инсталлятор. После этого параметры установки могут быть изменены.
- Между удаленными серверами CLIQ™ и удаленными устройствами программирования. Настройки прокси-сервера назначены в пользовательском интерфейсе CLIQ™ Web Manager и настраиваются на удаленные программные устройства.

Ниже приведено краткое описание всех сетевых подключений, необходимых для системы CLIQ™ Web Manager. Обратите внимание на то, что все соединения иницируются конечной точкой 1. SSL / TLS и требуют взаимной аутентификации с использованием клиентских сертификатов. При этом все подключения должны быть сквозными соединениями, которые не могут быть прекращены.

## СЕТЕВЫЕ СОЕДИНЕНИЯ

Точка 1	Протокол/ порт TCP	Точка 2	Назначение
Пользовательский/клиентский ПК	HTTPS / 443	Сервер CLIQ™ Web Manager	Пользовательский интерфейс CLIQ™ Web Manager user interface
Клиент веб-сервиса (интеграция)	HTTPS / 443	Сервер CLIQ™ Web Manager	Вызов веб-сервиса
Пользовательский/клиентский ПК	HTTPS / 8443	Удаленный сервер CLIQ™	Задействование сертификатов ключей программирования
Удаленные устройства программирования (настенные / мобильные)	HTTPS / 443	Удаленный сервер CLIQ™	Задачи программирования
Смартфон с приложением CLIQ™ Connect	HTTPS / 443	Удаленный сервер CLIQ™	Задачи программирования
Сервер CLIQ™ Web Manager	TDS/1443	Сервер базы данных CLIQ™ Web Manager server	Соединение с базой данных
Сервер CLIQ™ Web Manager	HTTPS / 443	Удаленный сервер CLIQ™	Установление дистанционных функций
Сервер CLIQ™ Web Manager	SMTP/25	Сервер электронной почты	Функции электронной почты
Сервер CLIQ™ Web Manager	HTTPS / 443	Цифровой контент-сервер (DCS)	Доставка на инсталляцию цифрового контента
CLIQ™ Web Manager server	HTTP/80	Цифровой контент-сервер (DCS)	Загрузка списка аннулированных сертификатов
Удаленный сервер CLIQ™	TDS/1443	Удаленный сервер баз данных CLIQ™	Соединение с базой данных
Удаленный сервер CLIQ™	HTTP/80	Цифровой контент-сервер (DCS)	Загрузка списка аннулированных сертификатов
ПК администратора	TDS/1433	Серверы баз данных	Управление базами данных CLIQ™
Удаленные устройства программирования, смартфон CLIQ™ и приложения ПК	HTTPS / 443	Сервис директорий	Поиск корректного URL для удаленного сервиса CLIQ™
Пользовательский/клиентский ПК	HTTP/80	Сервер обновлений CLIQ™	Загрузка последнего приложения CLIQ™

## Мониторинг

CLIQ™ Web Manager и удаленные сервисы CLIQ™ могут отслеживаться из приложений файлов журнала, которые могут быть найдены с серверов.

- Сервер CLIQ™ Web Manager:
  - CLIQ WebManager.log из [установочной папки] \ tomcat \ logs
- Удаленный сервер CLIQ™:
  - CLIQ Remote.log из [установочной папки] \ tomcat \ logs

Следующие приложения должны отслеживаться со стороны сервера:

- Сервер CLIQ™ Web Manager:
  - Apache и CLIQ WebManager
- Удаленный сервер CLIQ™:
  - Apache и CLIQ Remote

## Настройка, обеспечивающая бесперебойную работу

Для обеспечения максимально возможной доступности сервисов можно настроить среду высокой доступности (HA) для CLIQ™ Web Manager. Среда HA содержит в себе следующие компоненты:

- Две пары серверов приложений, где одновременно один из них активен, а другой - пассивен;
  - Одна такая пара состоит из CLIQ™ Web Manager и удаленного сервера CLIQ™.
- Серверы баз данных для CLIQ™ Web Manager и CLIQ™ Remote. Базы данных можно установить на кластер aSQL.

Важно, чтобы приложения на обеих парах серверов не работали одновременно, поскольку приложения в разных парах серверов настроены на использование одних и тех же баз данных (например, CLIQ™ Web Manager в паре серверов №1 использует ту же базу данных, что и CLIQ™ Web Manager в паре серверов № 2.) Рекомендуется, чтобы эти пары серверов были бы расположены в разных центрах обработки данных. По крайней мере, до такого уровня, что если один центр обработки данных выйдет из строя, то другая пара в другом центре обработки данных продолжит функционировать.

И CLIQ™ Web Manager, и удаленные сервисы CLIQ™ требуют внешних IP-адресов и FQDN (полное имя домена) для того, чтобы клиенты могли пользоваться их услугами. Необходимо настроить политику маршрутизации таким образом, чтобы сетевой трафик всегда маршрутизировался применительно к активной паре серверов. На активном сервере имеются запущенные сервисы Apache и CLIQ™ Web Manager (или CLIQ™ Remote), тогда как на пассивном сервере эти сервисы остановлены.

Переключение сервисов между активной и пассивной парой серверов необходимо выполнить вручную, программное обеспечение CLIQ™ Web Manager не будет делать это автоматически. Сначала отключите сервисы с активной пары серверов, а затем запустите сервисы с пассивной пары. Это важно для того, чтобы избежать конфликтов с базами данных.

Пожалуйста, свяжитесь с дилерами Abloy, если вам нужна какая-либо дополнительная информация о настройке среды с высокой доступностью.

## Техническое обслуживание

Abloy выпускает в год примерно две основные версии CLIQ™ Web Manager. По мере необходимости публикуются небольшие выпуски исправлений (патчи). Abloy будет поддерживать текущую и две более ранние версии. Настоятельно рекомендуется регулярно обновлять программными вставками свои операционные системы, предлагаемые Microsoft.

## Безопасность

Безопасность PROTEC<sup>2</sup> CLIQ™ основана на объединении системы механического ключа с электронным правом доступа. Сверх того, для установления подлинности элементов системы используются TLS сертификаты. Все данные, передаваемые между ключами, цилиндрами, удаленными программаторами и CLIQ™ Web Manager зашифрованы. Все элементы CLIQ™ произведены и запрограммированы на заводе. Безопасность системы CLIQ™ Web Manager (далее CWM) основана на инфраструктуре открытого ключа (PKI - набор средств технических, материальных, людских и других средств, распределённых служб и компонентов, в совокупности используемых для поддержки криптозадач на основе закрытого и открытого ключа).

Она используется по следующим критериям.

1. Конфиденциальность: шифрование данных в пути и в состоянии покоя.
  - a. CWM призвана помешать злоумышленникам считывать данные, отправленные по любой используемой сети, включая Интернет - для того, чтобы злоумышленник, например, не смог бы предоставлять себе или кому-то еще доступ к цилиндрам, которые он не уполномочен использовать.
  - b. CWM призвана помешать злоумышленнику считывать сохраненные данные, используемые CWM - для того, чтобы злоумышленник, например, не мог бы позволить себе или кому-либо еще получать доступ к цилиндрам, которые он не вправе использовать. Для этого CWM использует различные методы шифрования и шифры.
2. Конфиденциальность: шифрование личной информации.
  - a. CWM должна запрещать злоумышленнику считывать конфиденциальные данные, такие, как информацию по сотрудникам, отправляемую через любую используемую сеть, включая Интернет - для того, чтобы злоумышленник, например, не мог бы сопоставлять сотрудников с конкретными ключами и рабочими позициями; таким образом, неприкосновенность личности сотрудников не страдает.
3. Целостность: защита от несанкционированного доступа и коррупции.
  - a. CWM должна иметь возможность проверять целостность данных, отправляемых по любой используемой сети, включая Интернет - для того, чтобы CWM могла бы быть уверена, что такие данные аутентичны и не редактируются злоумышленником, или же они не повреждены во время передачи. Это необходимо даже тогда, когда данные зашифрованы, так как злоумышленник все еще может редактировать зашифрованные данные, а данные могут быть повреждены во время их передачи.
4. Авторизация: кто может получить доступ.
  - a. CWM должна контролировать, кто может получить доступ к данным, к чему можно получить доступ и в какое время.
5. Подлинность: идентификация отправителя.
  - a. CWM должна знать идентификатор всех своих клиентов, с которыми она общается - для того, чтобы CWM могла использовать эти данные для проверки того, что клиент авторизован.

CLIQ™ Web Manager использует для шифрования сетевого трафика протоколы HTTPS/SSL/TLS.

Данные между замком CLIQ™, клиентом CLIQ™ Web Manager и ключом CLIQ™ зашифрованы на основе алгоритма 3DES 128 бит.

## Классификация и стандарты

<b>IP классификация</b> обозначение IP68	<b>EN60079-0 и EN 60079-11</b> одобрено ATEX	<b>EN1303:2005 и EN 15684:2012</b> Класс 6	<b>SFS 5970/7020</b> класс 1 и класс 3
<p>Код IP обозначает насколько хорошо продукт защищен от проникновения пыли и воды.</p> <p>Код IP68 – самая высокая степень защиты – означает полную герметичность</p> 	<p>Одобрено ATEX – это означает, что продукт может быть использован в агрессивной среде в присутствии любых типов газов, паров и воспламеняющихся частиц*</p>  <p>*температура воспламенения опасных веществ должна быть не ниже 135 °C</p>	<p>Ресурс прочности (число циклов 100000) и степень защиты ключей (100000 комбинаций)</p> 	<p>Подбор ключа и физическое воздействие.</p>



# ДВОЙНАЯ ЗАЩИТА



МЕХАНИЧЕСКОЕ  
ЗАПИРАНИЕ



ЭЛЕКТРОННЫЙ КОНТРОЛЬ  
ДОСТУПА



# Награды, полученные технологией двойной проверкой безопасности контроля доступа.

## ABLOY® PROTEC<sup>2</sup>



Подробнее  
на сайте  
[abloy.com](http://abloy.com)