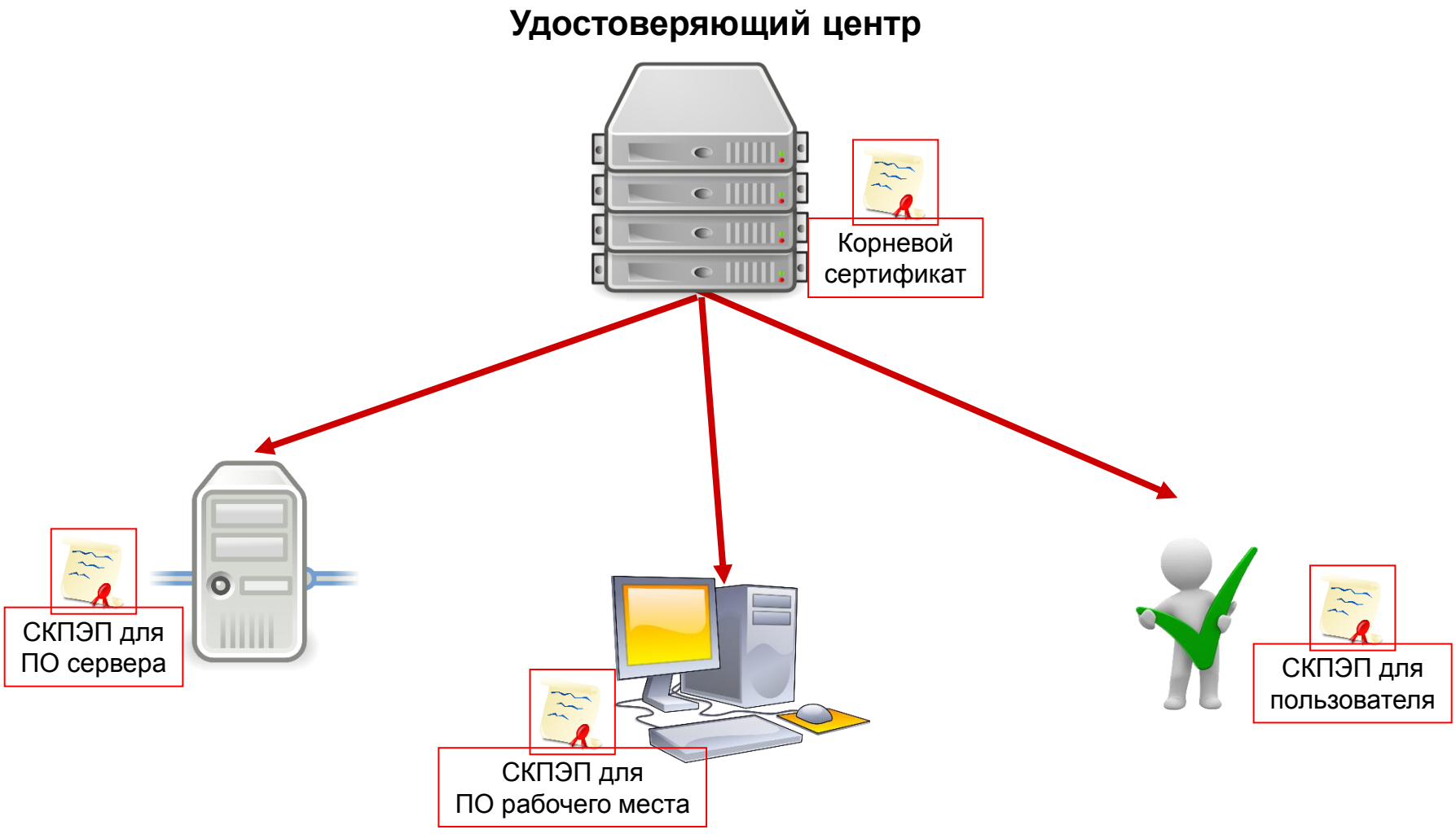
Организационные аспекты перевода крупных информационных систем на использование криптографических алгоритмов ГОСТ 2012 года на примере ГС ПВДНП

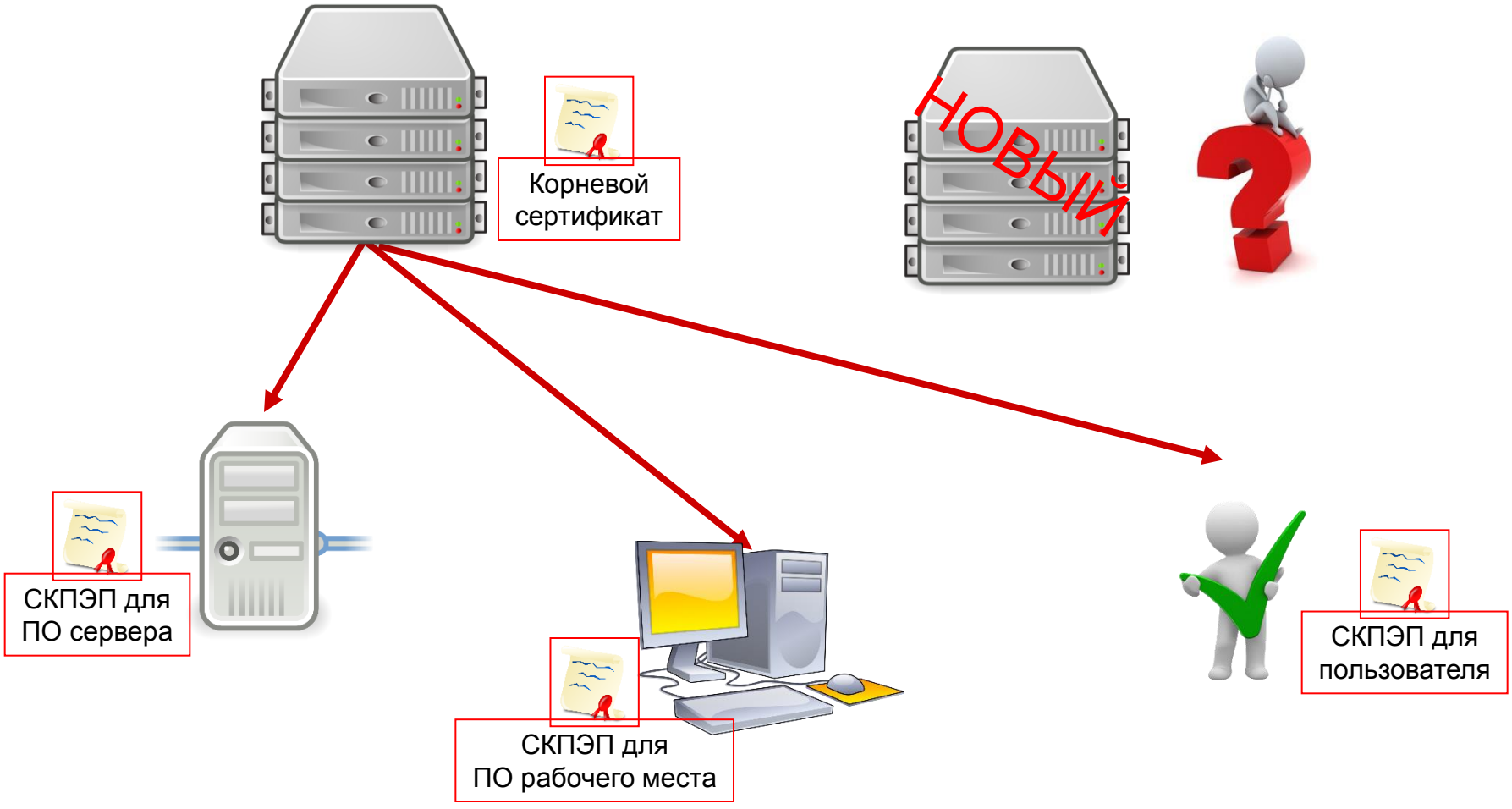
Докладчик: Вылегжанин Никита Александрович

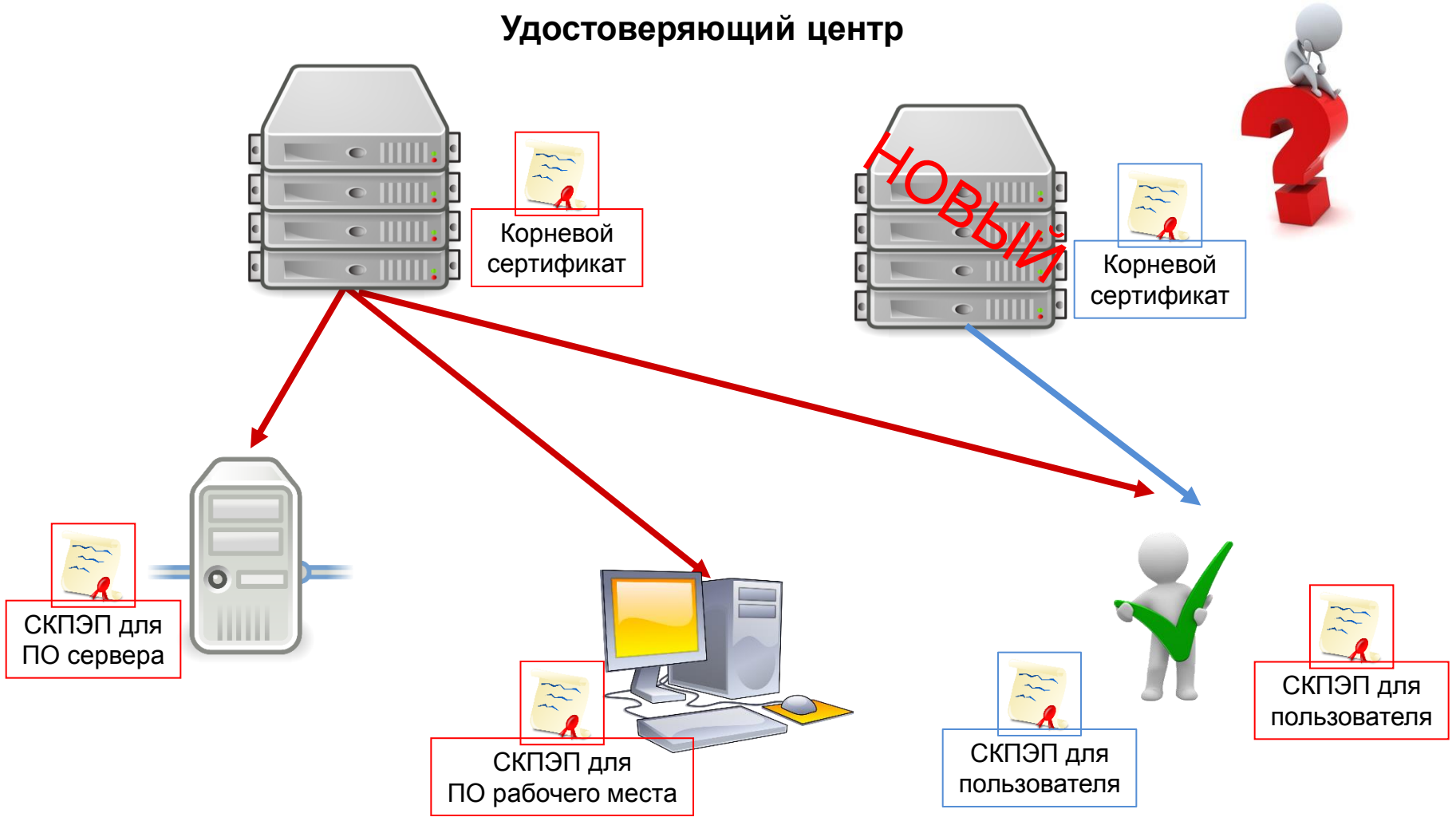
Дата: 14-16 сентября 2016 года

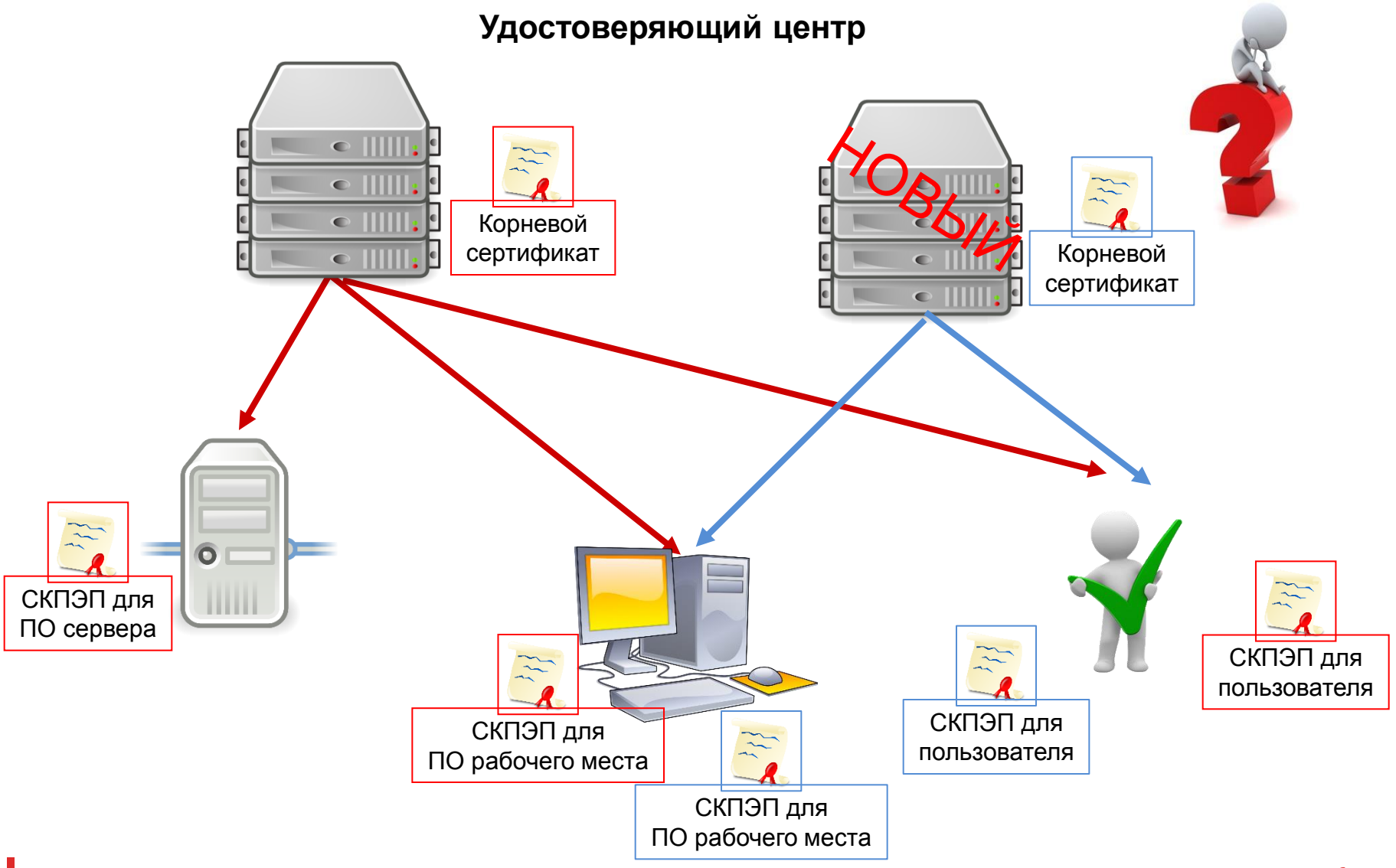
PKI Информационной системы.

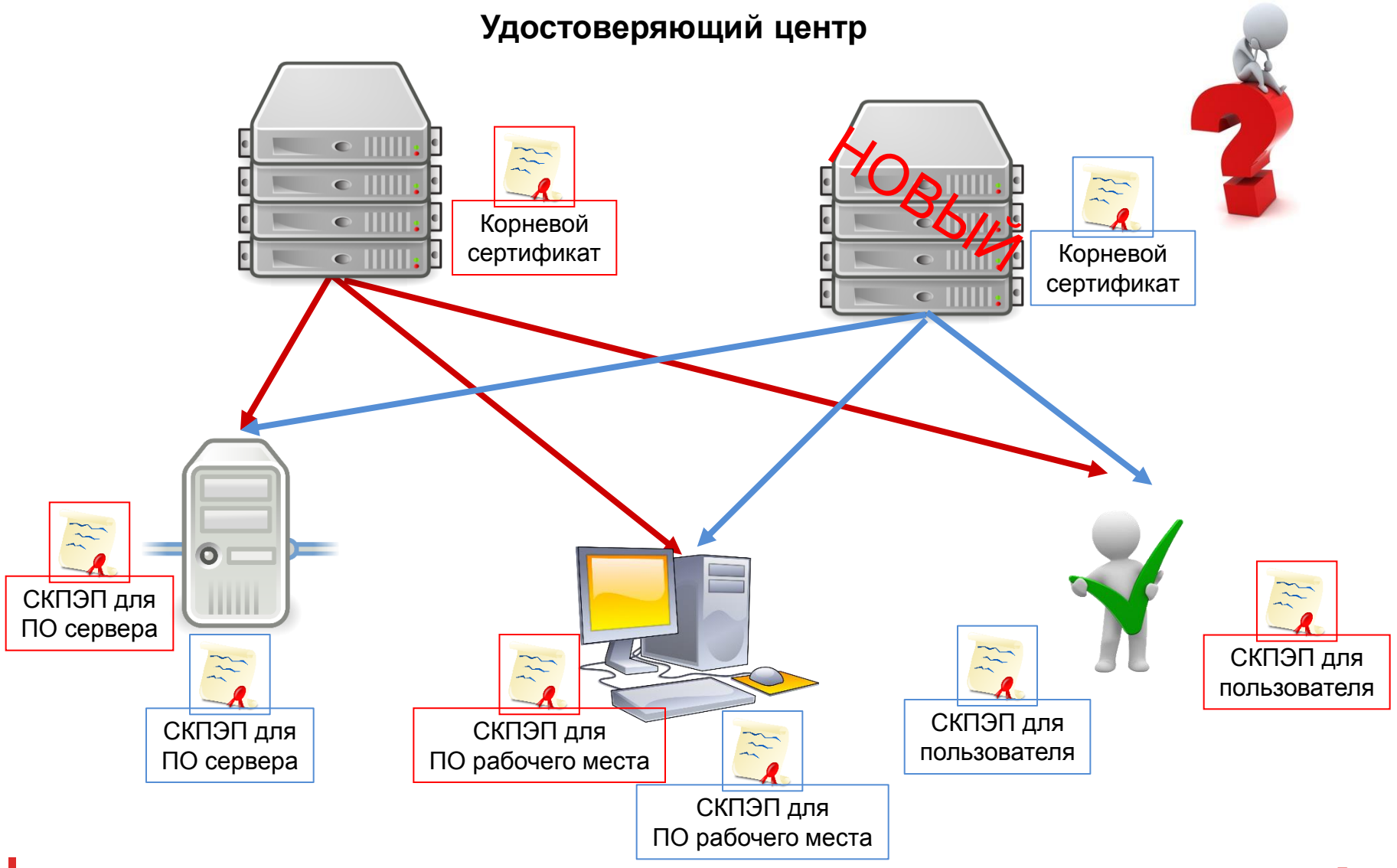

Удостоверяющий центр
Корневой сертификат
СКПЭП для ПО сервера
СКПЭП для ПО рабочего места
СКПЭП для пользователя

Удостоверяющий центр

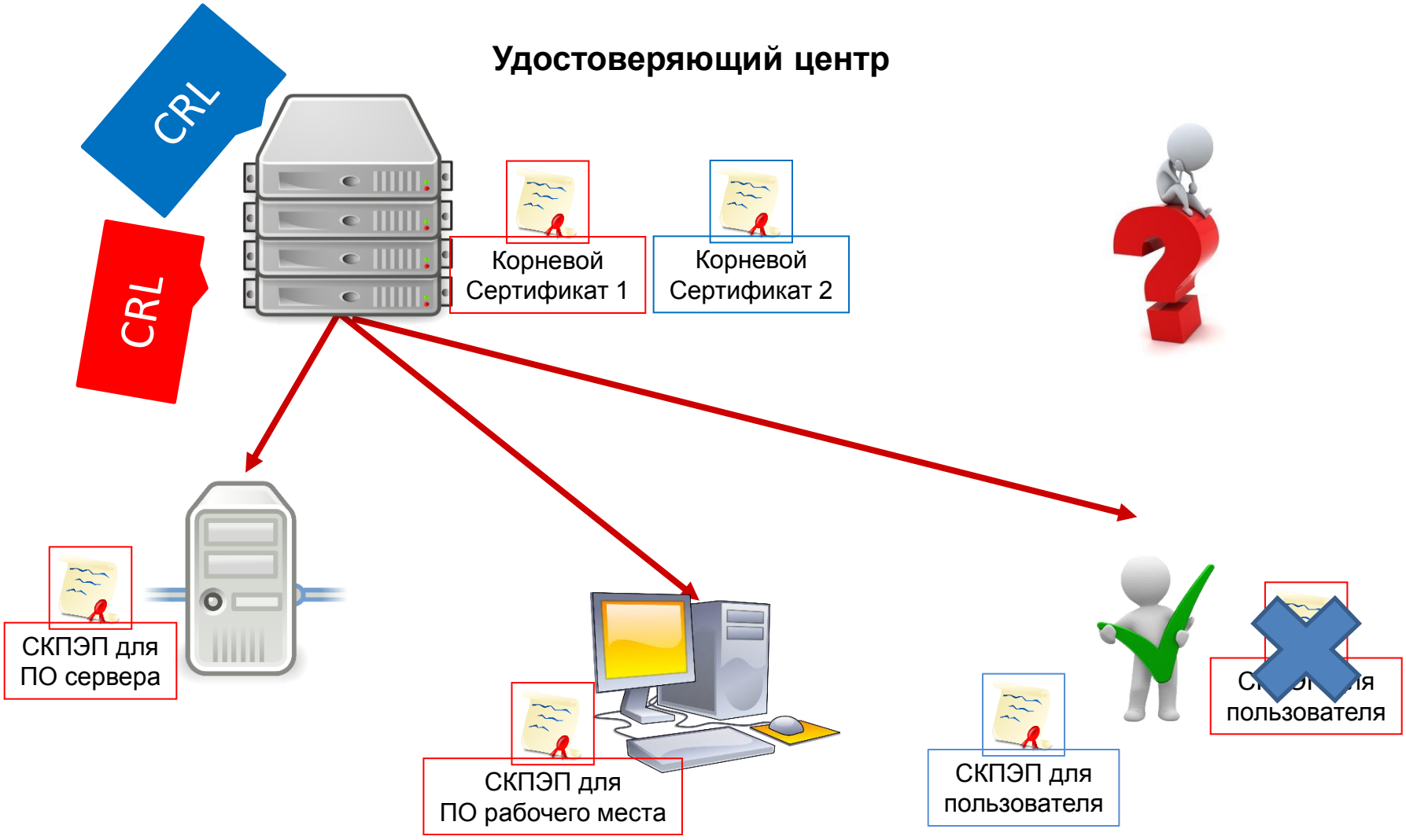


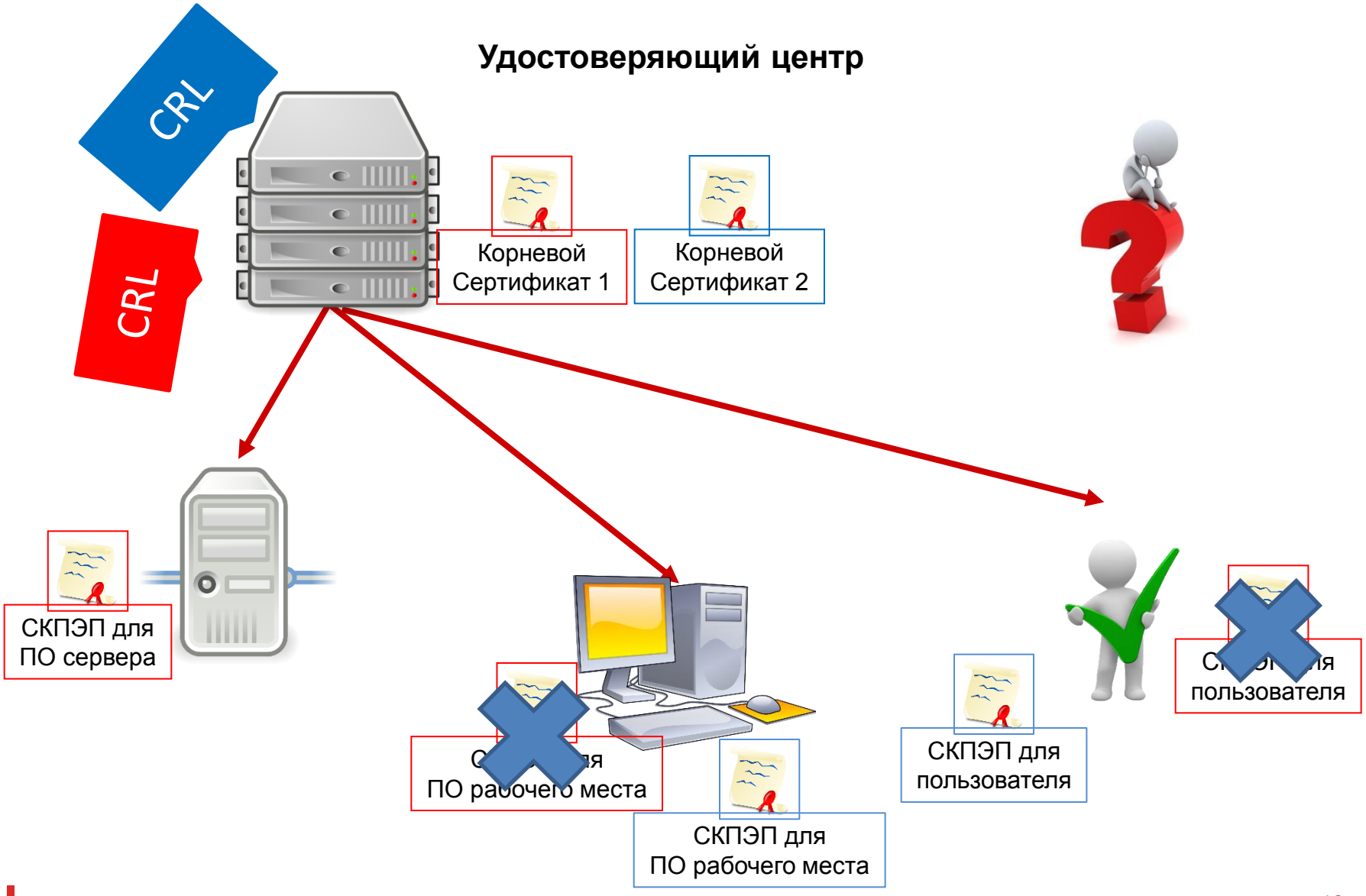

Удостоверяющий центр
НОВЫЙ
Корневой сертификат
Корневой сертификат
СКПЭП для ПО сервера
СКПЭП для ПО рабочего места
СКПЭП для пользователя
СКПЭП для пользователя

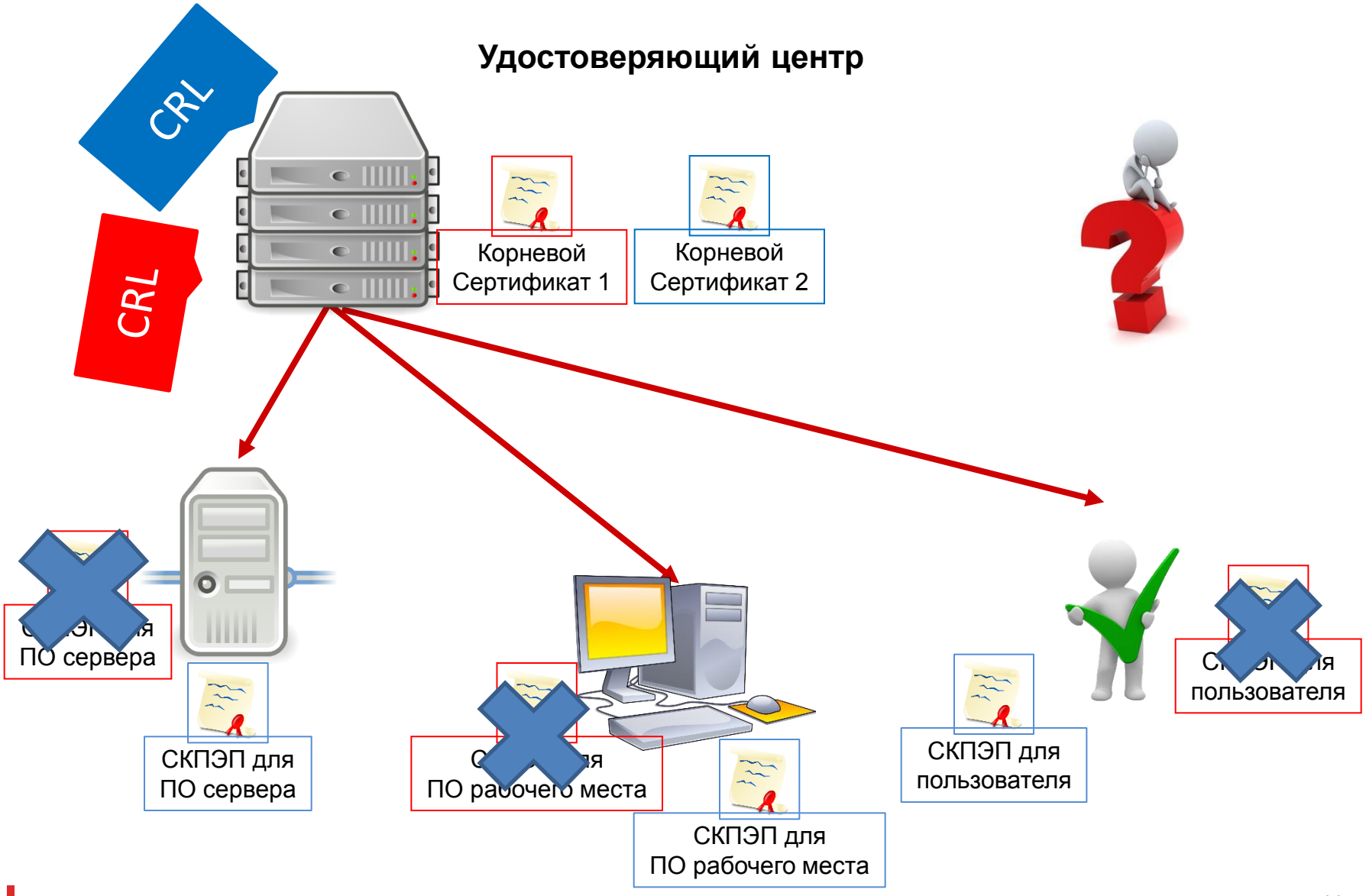

Удостоверяющий центр
НОВЫЙ
Корневой сертификат
Корневой сертификат
СКПЭП для ПО сервера
СКПЭП для ПО рабочего места
СКПЭП для ПО рабочего места
СКПЭП для пользователя
СКПЭП для пользователя

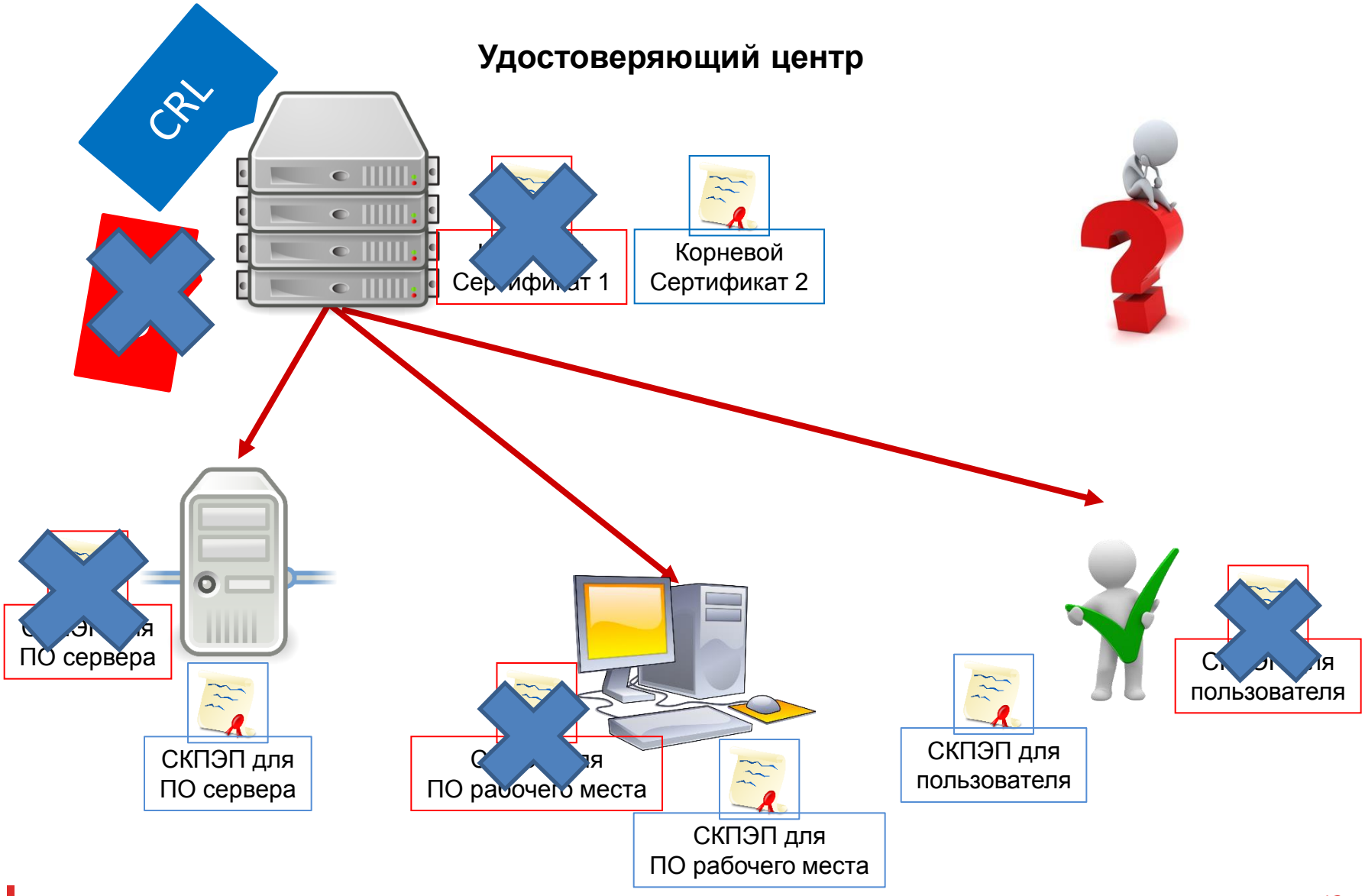

Удостоверяющий центр
НОВЫЙ
Корневой сертификат
Корневой сертификат
СКПЭП для ПО сервера
СКПЭП для ПО сервера
СКПЭП для ПО рабочего места
СКПЭП для ПО рабочего места
СКПЭП для пользователя
СКПЭП для пользователя

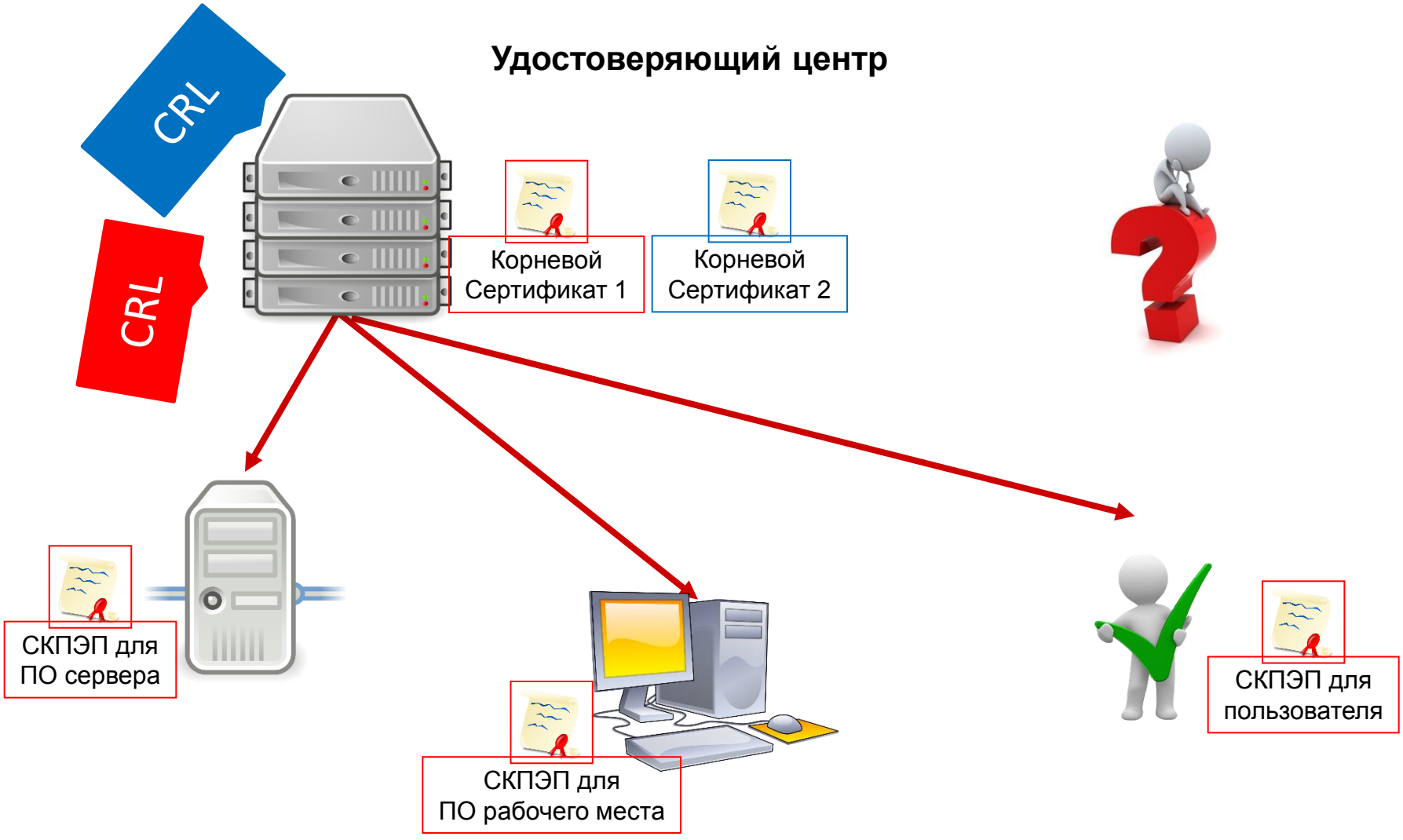

Удостоверяющий центр
CRL
Корневой
тификат
НОВЫЙ
Корневой
сертификат
ПО сервера
СКПЭП для
ПО сервера
ПО рабочего места
СКПЭП для
ПО рабочего места
СКПЭП для
пользователя
пользователя


Удостоверяющий центр
CRL
CRL
Корневой Сертификат 1
Корневой Сертификат 2
СКПЭП для ПО сервера
СКПЭП для ПО рабочего места
СКПЭП для пользователя
пользователя


Удостоверяющий центр
CRL
CRL
Корневой Сертификат 1
Корневой Сертификат 2
СКПЭП для ПО сервера
ПО рабочего места
СКПЭП для ПО рабочего места
СКПЭП для пользователя
пользователя


Удостоверяющий центр
CRL
CRL
Корневой Сертификат 1
Корневой Сертификат 2
ПО сервера
СКПЭП для ПО сервера
ПО рабочего места
СКПЭП для ПО рабочего места
СКПЭП для пользователя
пользователя

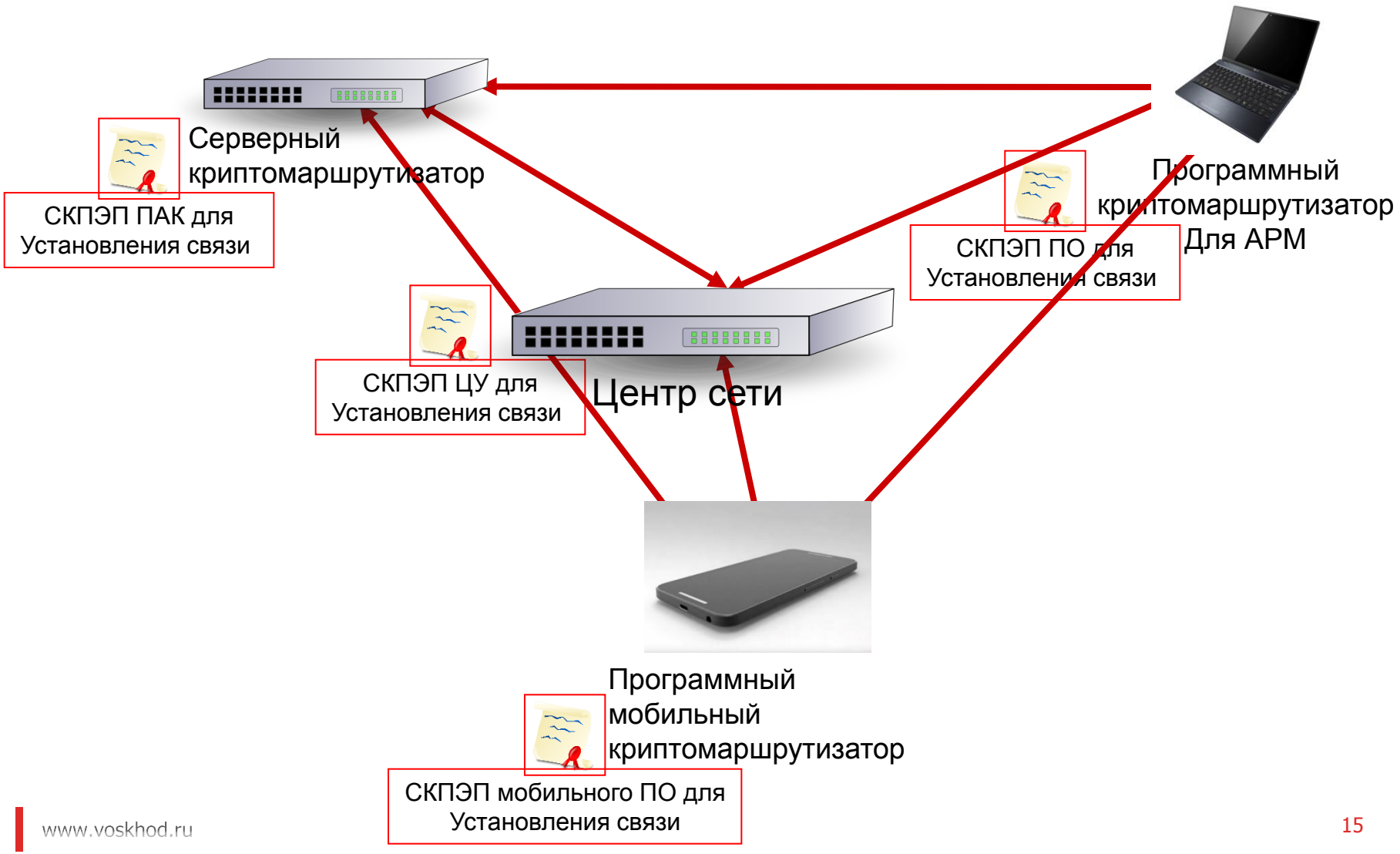

Удостоверяющий центр
CRL
Корневой
Сертификат 2
ПО сервера
СКПЭП для
ПО сервера
ПО рабочего места
СКПЭП для
ПО рабочего места
СКПЭП для
пользователя
пользователя


Удостоверяющий центр
CRL
CRL
Корневой Сертификат 1
Корневой Сертификат 2
СКПЭП для ПО сервера
СКПЭП для ПО рабочего места
СКПЭП для пользователя

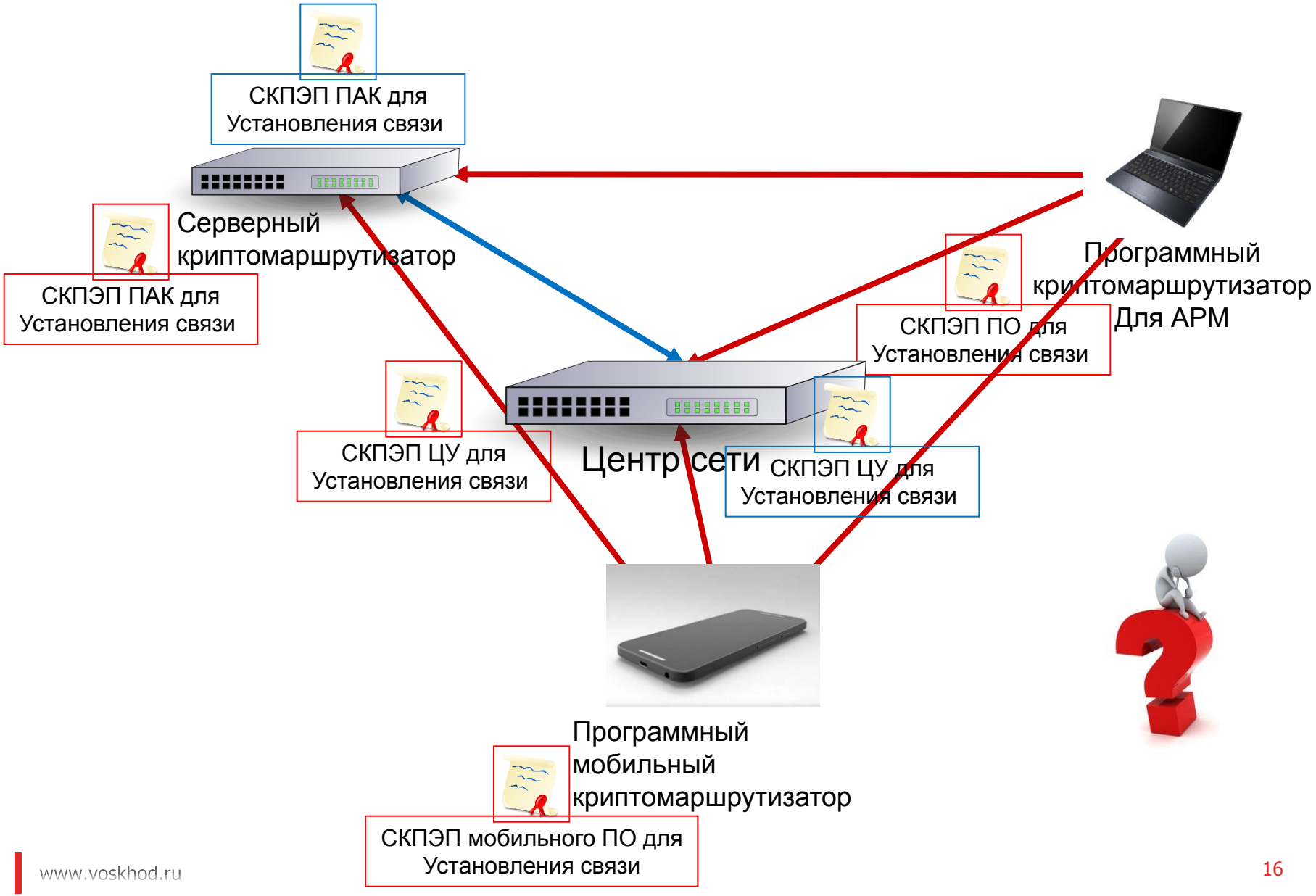
Удостоверяющий центр. Выводы.

Новый УЦ	Обновленный УЦ
• Простота • Избыточность • Дороговизна	• Сложность • Оптимизация расходов • Требования по поддержке режима перехода со стороны ПО

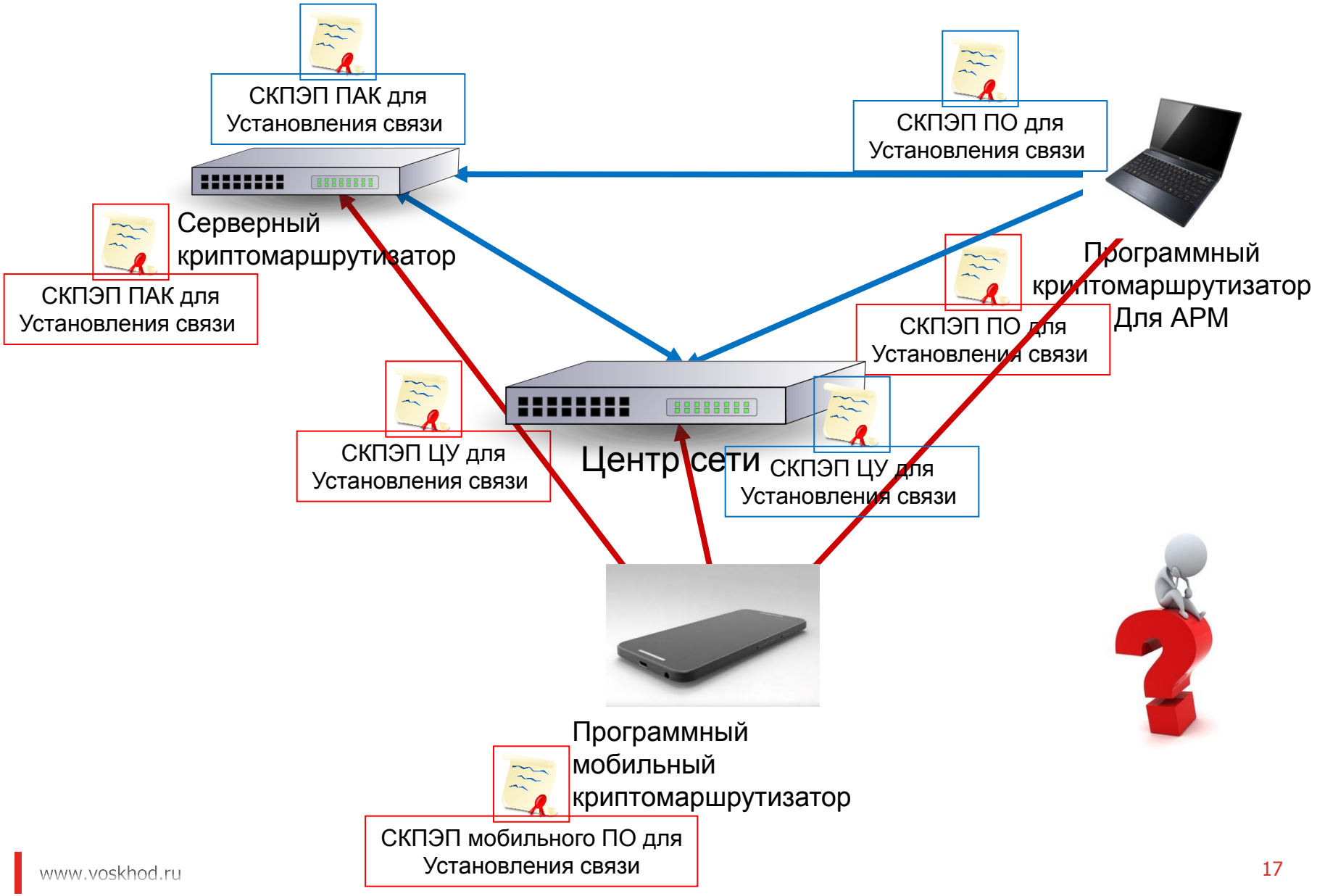
Защищенная сеть



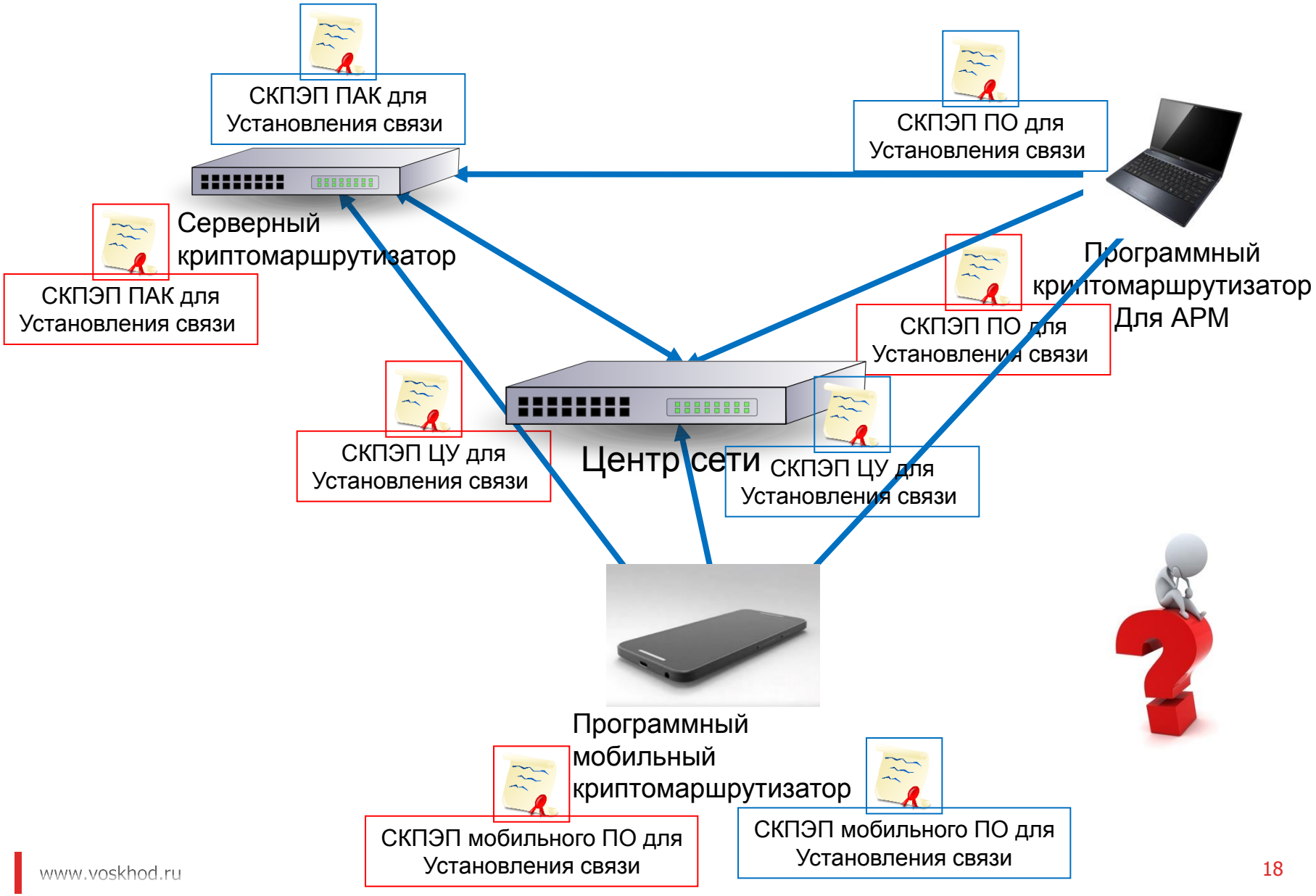
Защищенная сеть



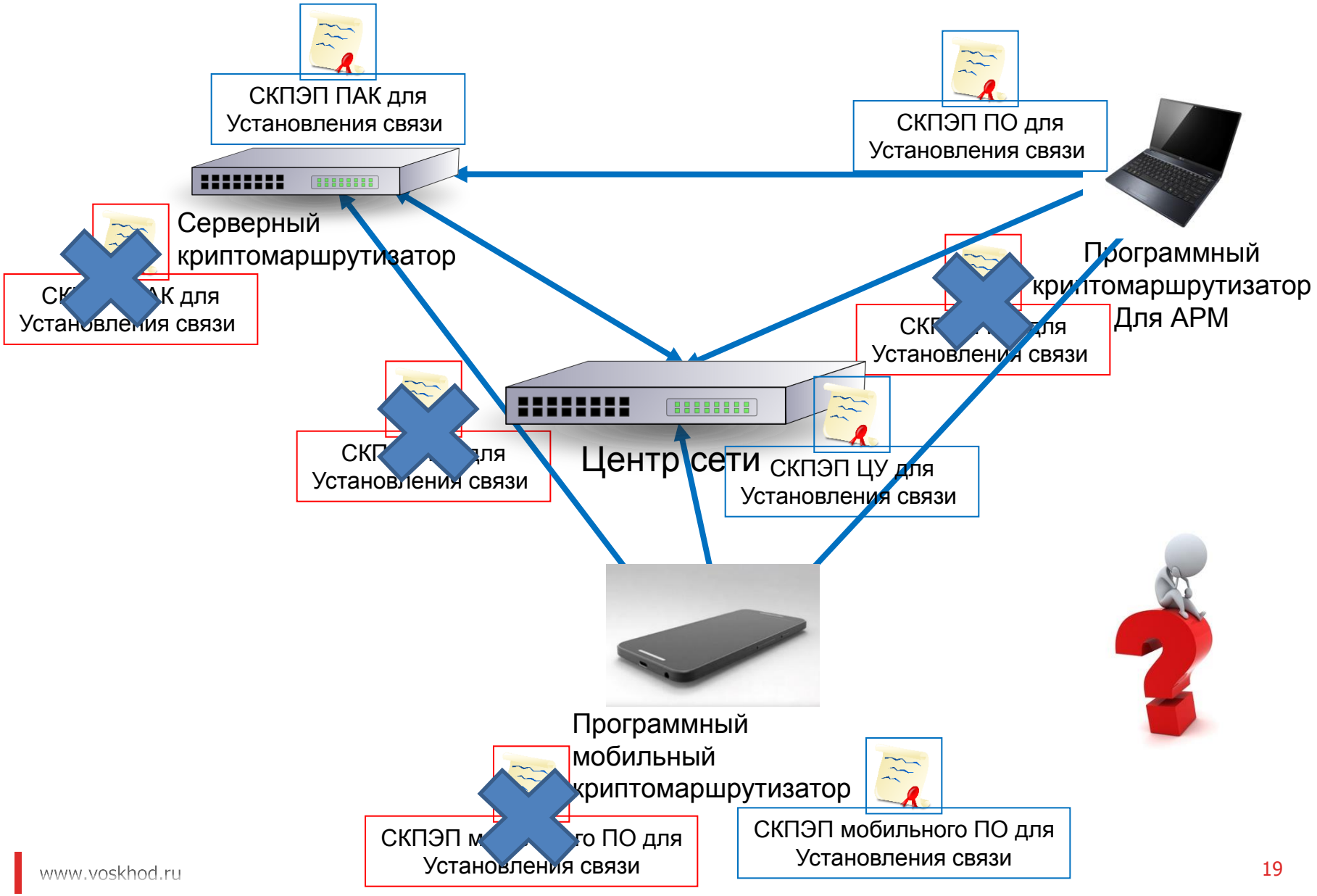
Защищенная сеть



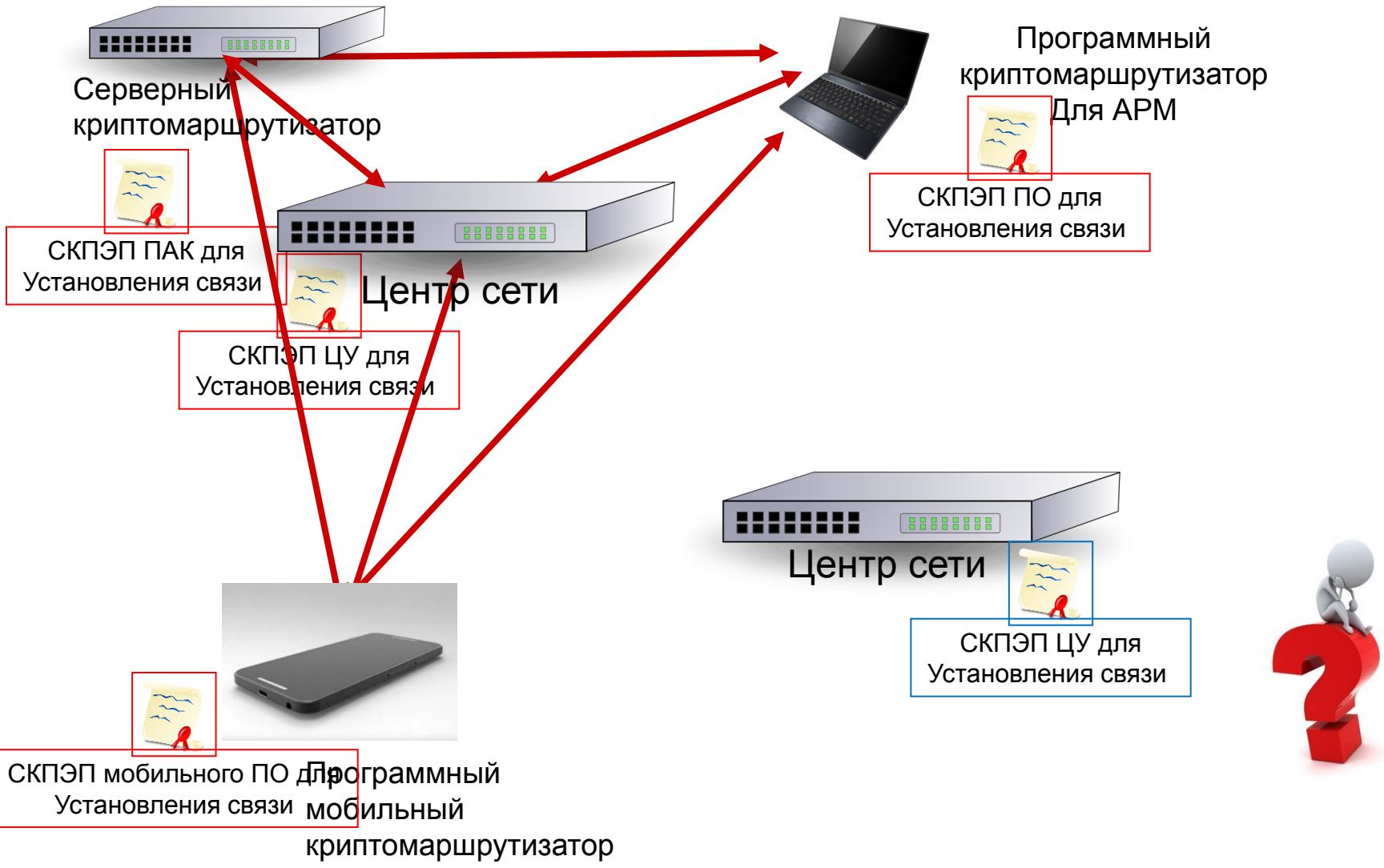
Защищенная сеть



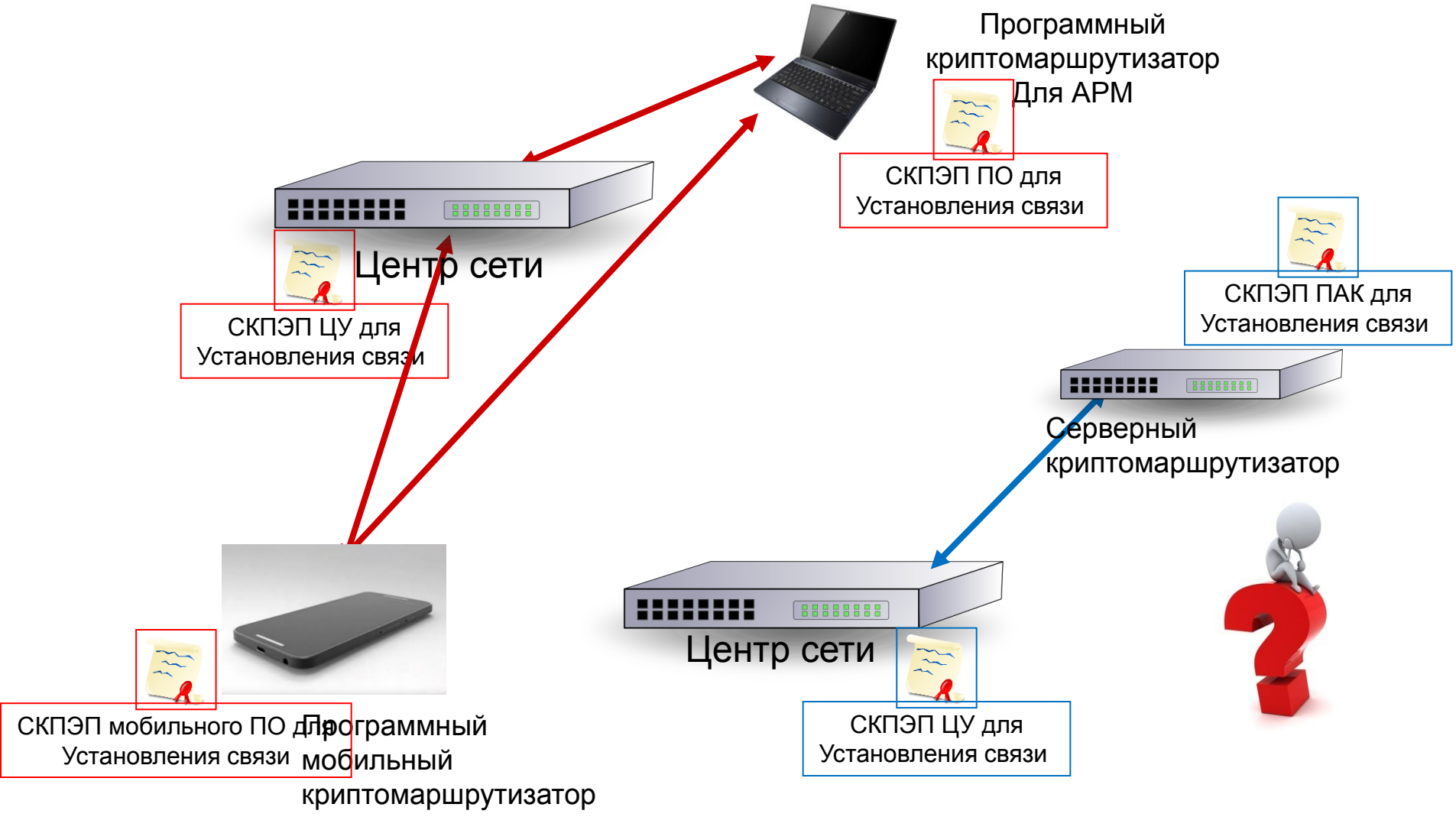
Защищенная сеть



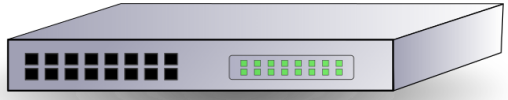
Защищенная сеть



Защищенная сеть



Защищенная сеть



Центр сети

СКПЭП ЦУ для Установления связи

Программный криптомаршрутизатор Для АРМ

СКПЭП ПО для Установления связи

СКПЭП ПАК для Установления связи

Центр сети

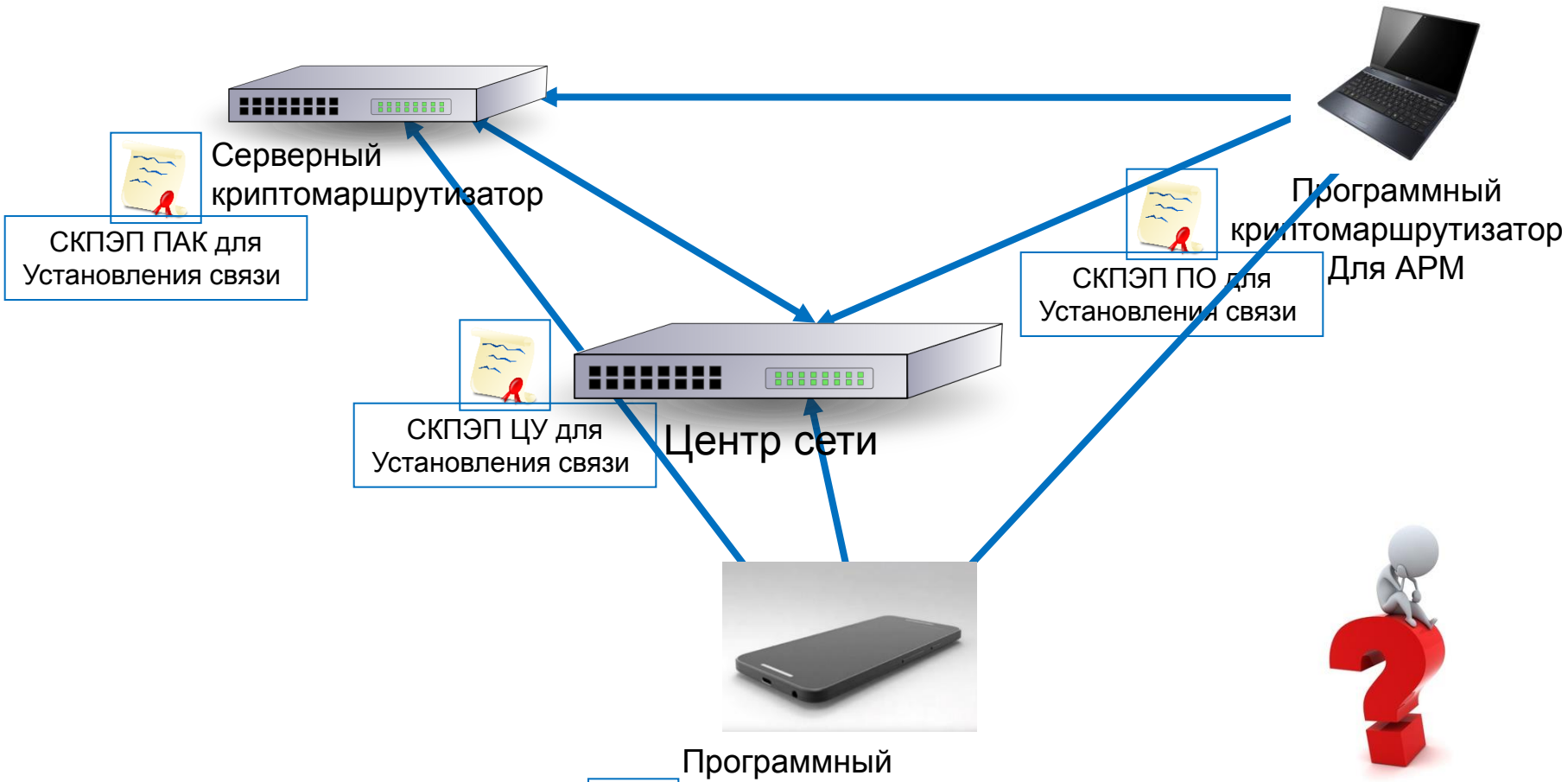
Серверный криптомаршрутизатор

СКПЭП ЦУ для Установления связи

Программный мобильный криптомаршрутизатор

СКПЭП мобильного ПО для Установления связи

Защищенная сеть



Защищенная сеть. Выводы.

Две сети	Смешанная сеть
• Простота • Избыточность • Дороговизна • Неэффективное сопряжение сетей	• Сложность • Оптимизация расходов • Требования по поддержке режима перехода со стороны ПО

Средства ЭП.

- Замена или обновление ПТК?
- Доработка прикладного ПО
- Привязанность к обновлению УЦ
- Поддержка старых алгоритмов пока они есть в системе

Ключевые носители.

- Повсеместная замена ключевых носителей
- Привязанность к обновлению УЦ и средств ЭП
- Распространение вместе со средствами ЭП
- Касается ключевых носителей с криптографией

Итоги.

- Каждая крупная ИС требует свой порядок перехода
- Необходимо гармонизировать процессы перехода для всех подсистем
- Большое значение имеют производители средств
- Большое значение имеет мнение регуляторов в части допустимости совмещения стандартов в рамках переходного периода
- Упрощение организации влечет усложнение программных и аппаратных комплексов
- Успешный переход отечественных IT-компаний на новые ГОСТы возможен только при их совместной работе с производителями СКЗИ и регуляторами в области ИБ

Спасибо за внимание