ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ «ВОСХОД»

Перевод инфраструктуры открытых ключей Российской федерации на применение криптографических стандартов нового поколения

Докладчик: Иван Ярославович Перевалов

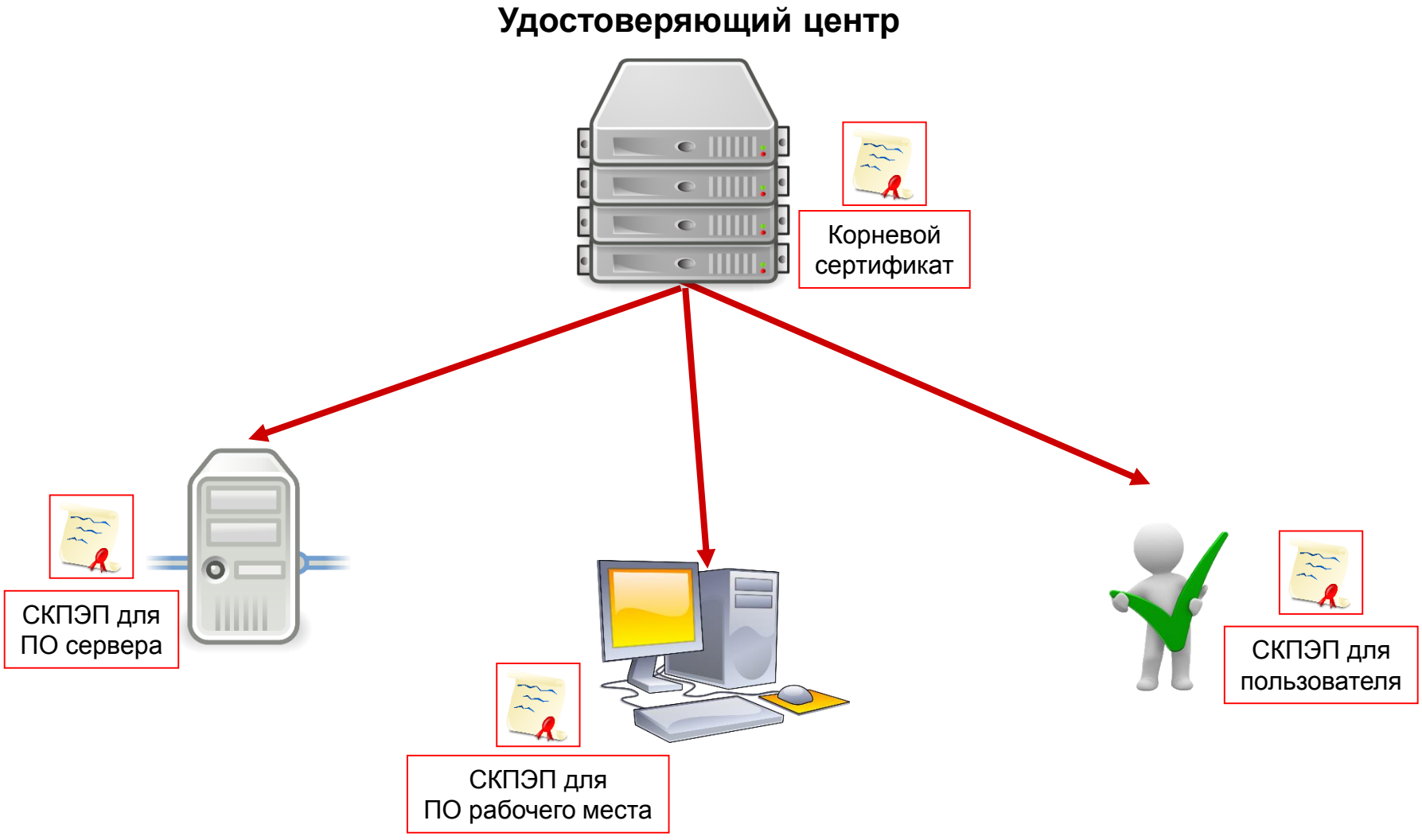
Дата: 22 марта 2017

Задача

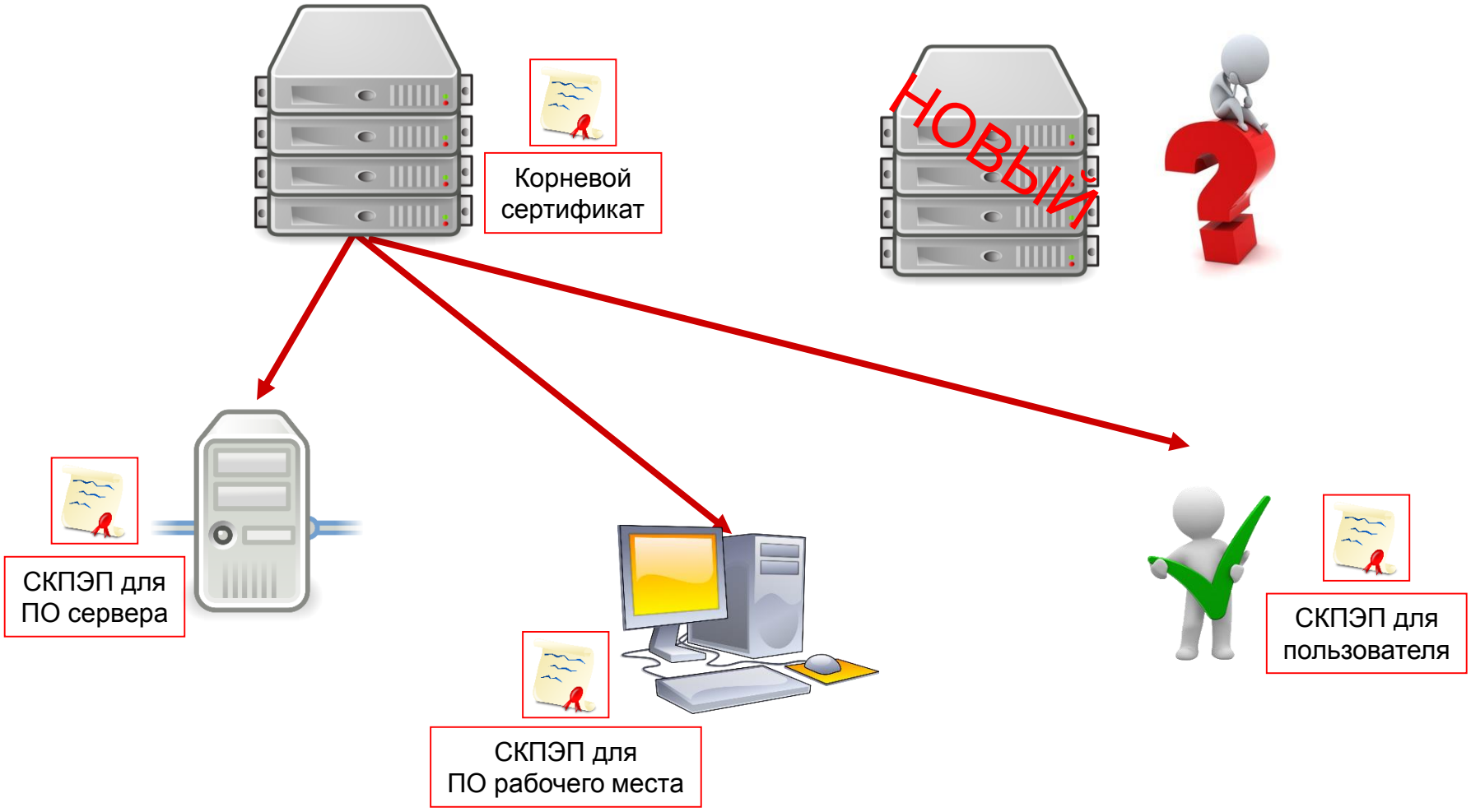
Согласно информационному письму ФСБ России № 149/7/1/3-58 от 31.01.2014 "О порядке перехода к использованию новых стандартов ЭЦП и функции хэширования":

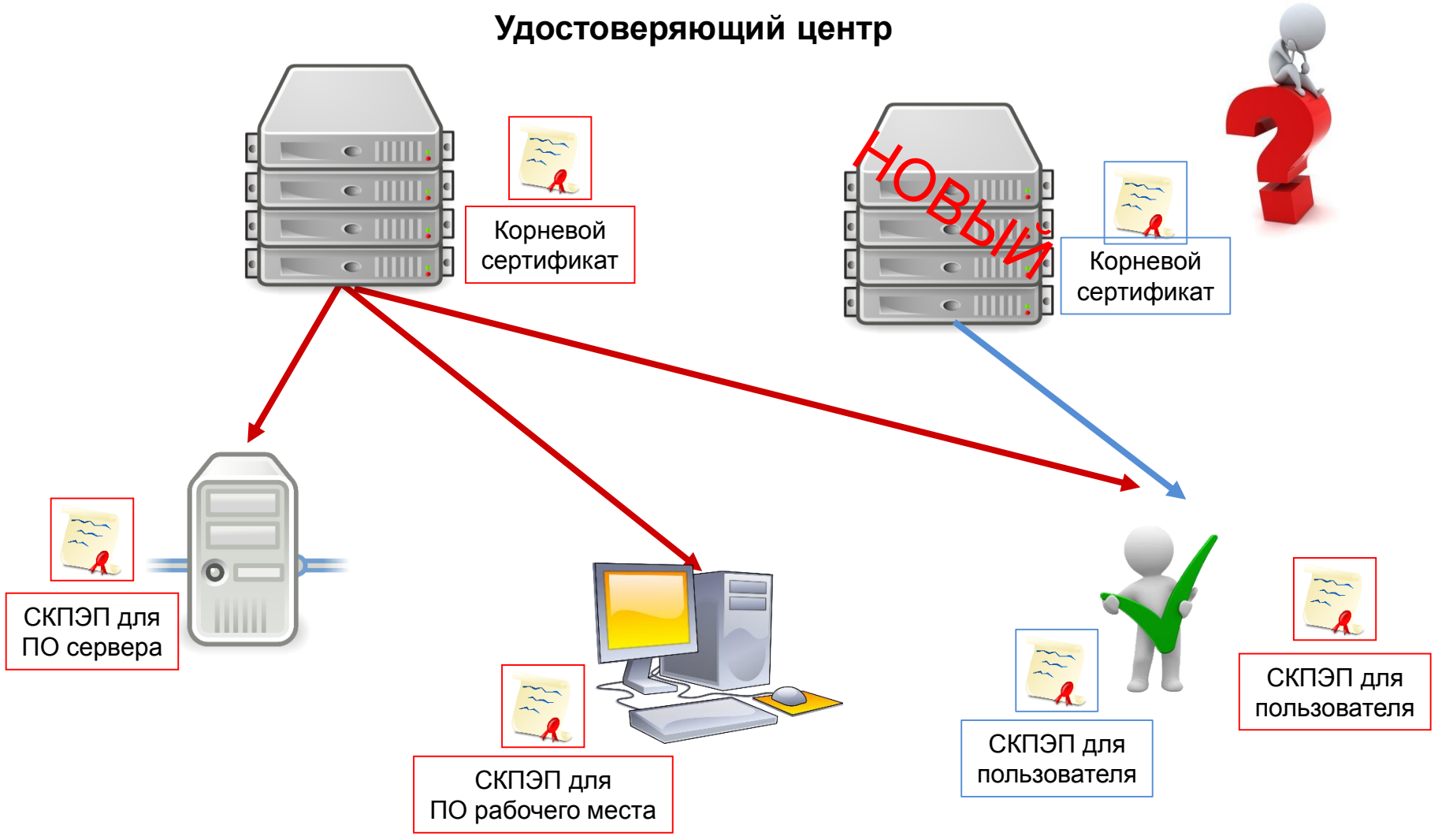
«Использование схемы подписи ГОСТ Р 34.10-2001 для формирования подписи после 31 декабря 2018 года не допускается».

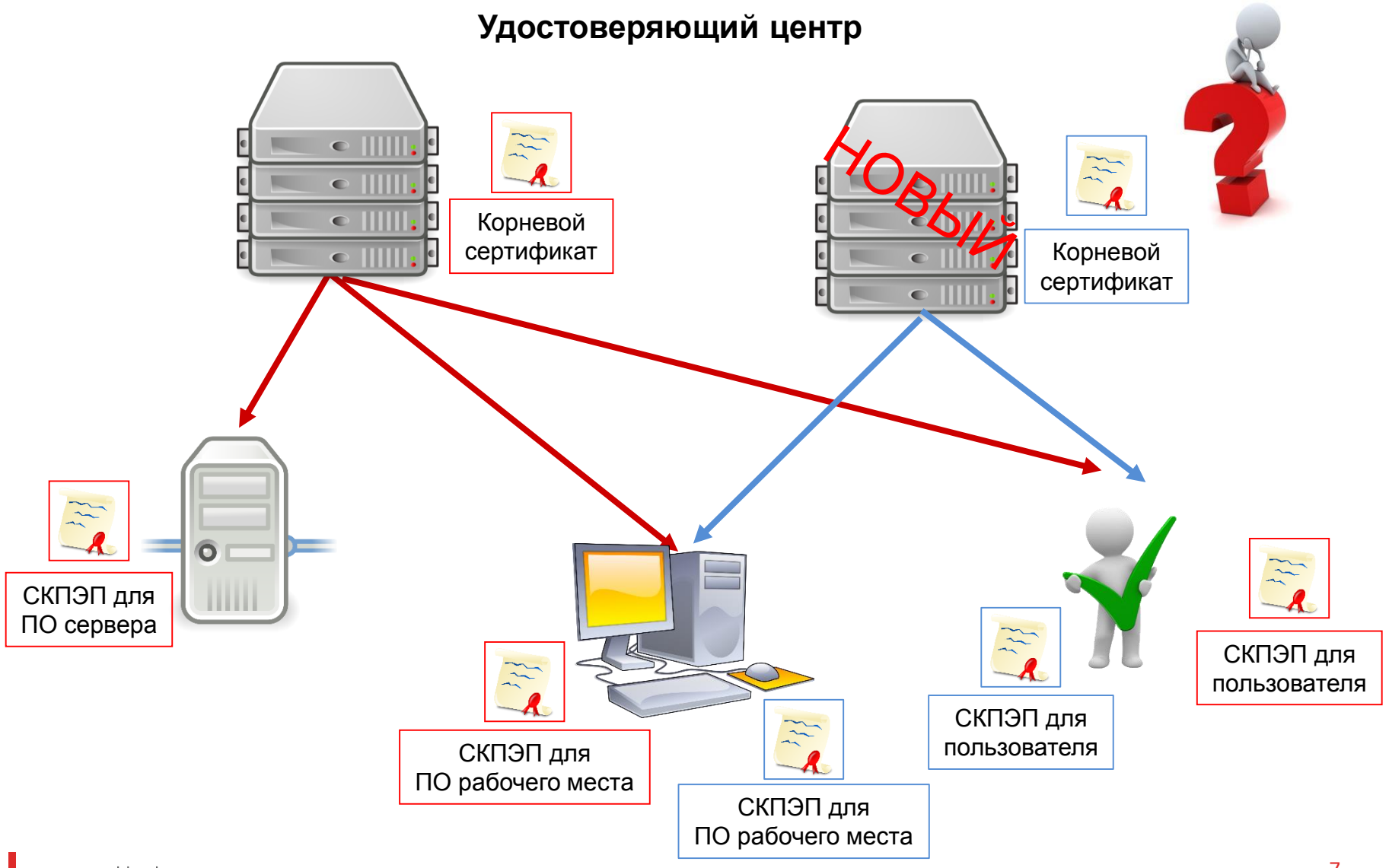
ИОК информационной системы


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

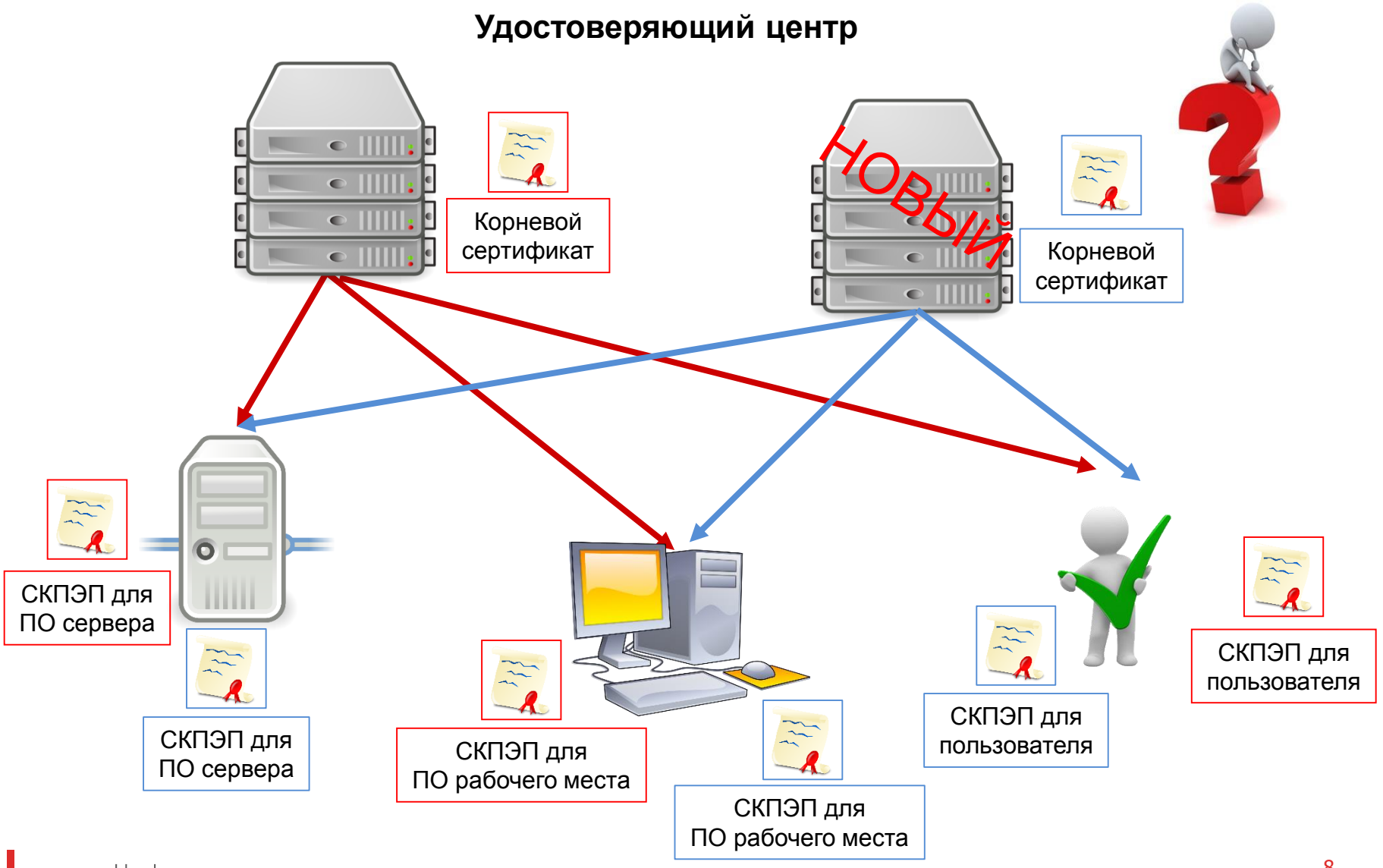
Удостоверяющий центр

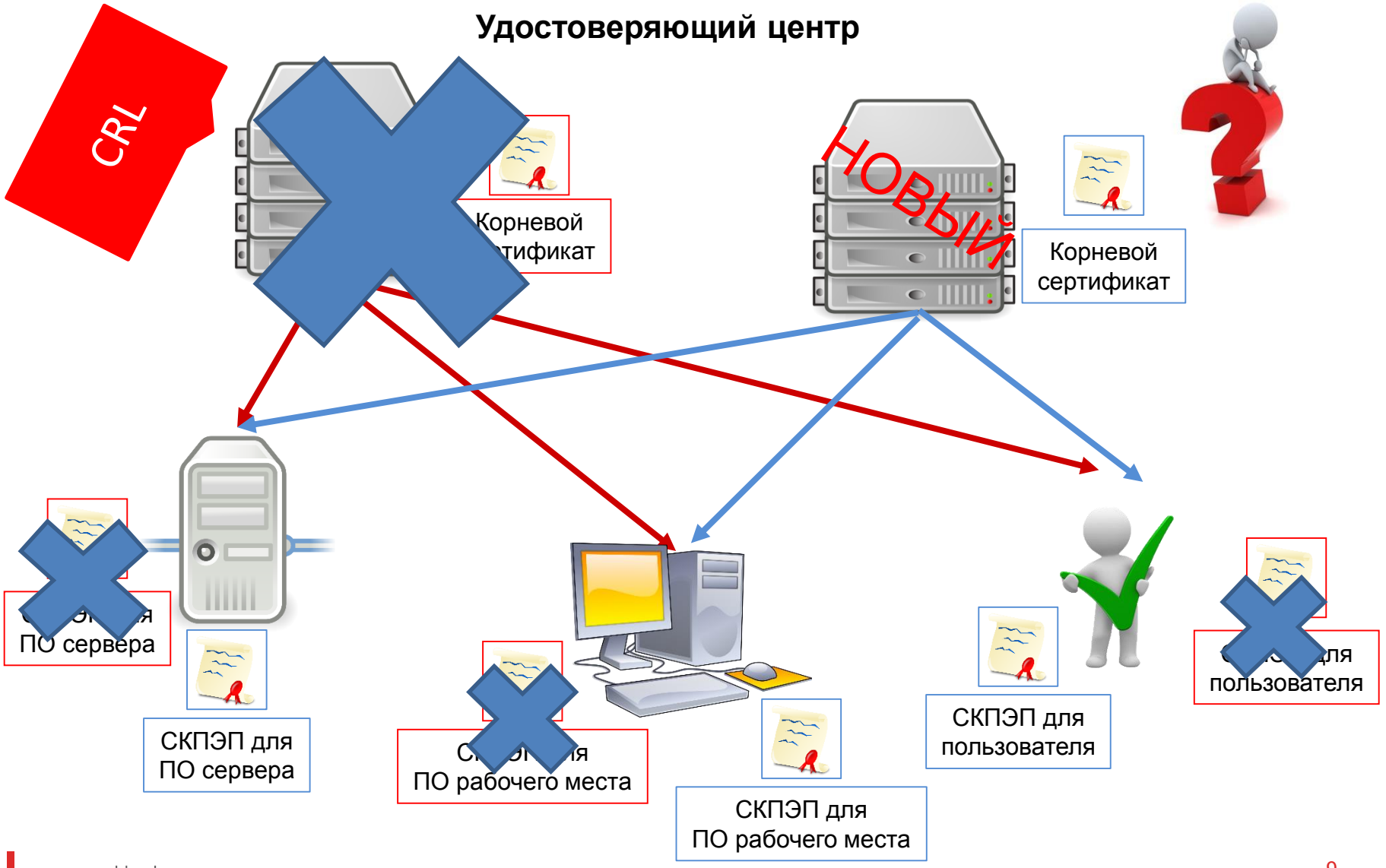


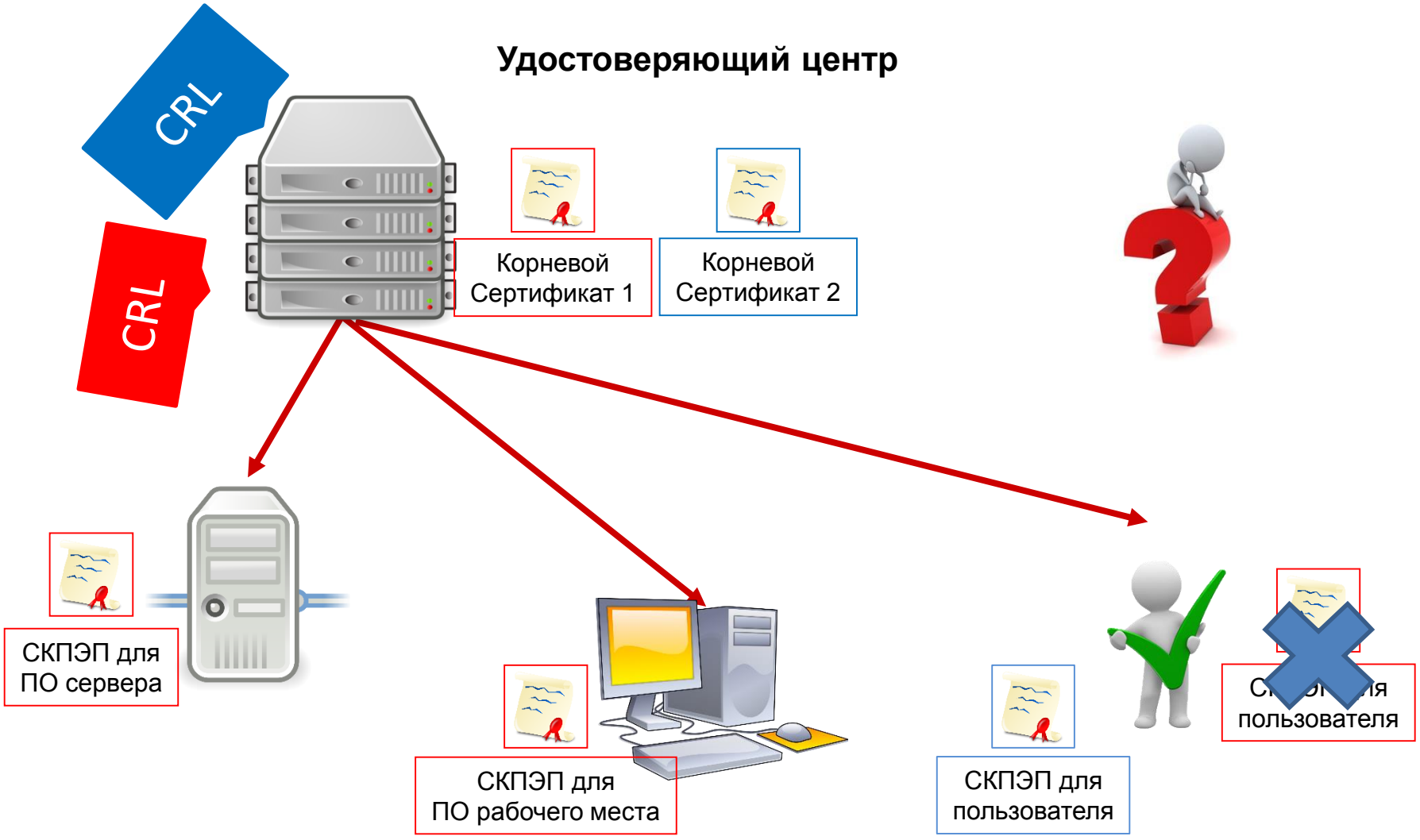

Удостоверяющий центр
НОВЫЙ
Корневой сертификат
Корневой сертификат
СКПЭП для ПО сервера
СКПЭП для ПО рабочего места
СКПЭП для пользователя
СКПЭП для пользователя

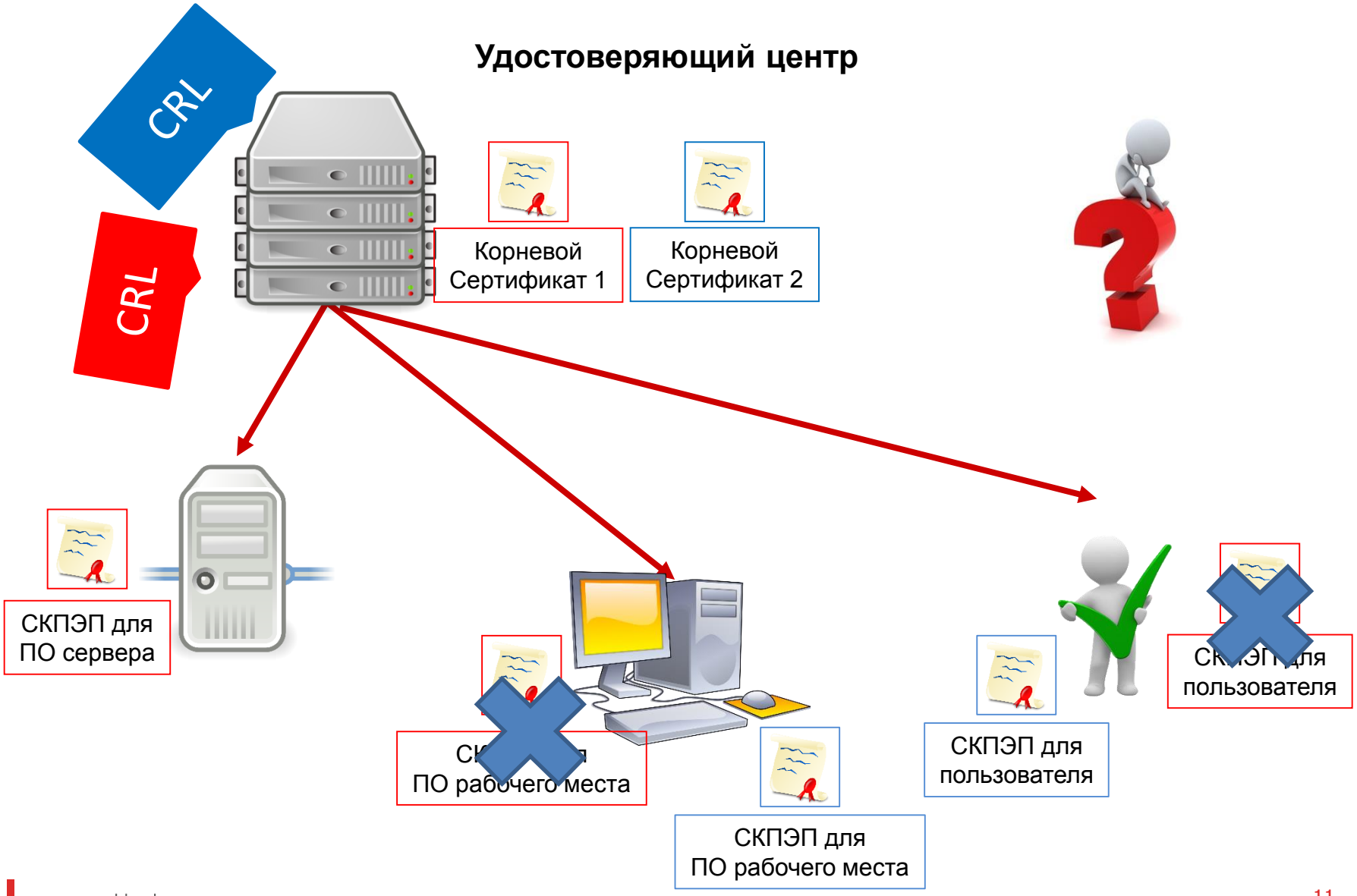

Удостоверяющий центр
НОВЫЙ
Корневой сертификат
Корневой сертификат
СКПЭП для ПО сервера
СКПЭП для ПО рабочего места
СКПЭП для ПО рабочего места
СКПЭП для пользователя
СКПЭП для пользователя

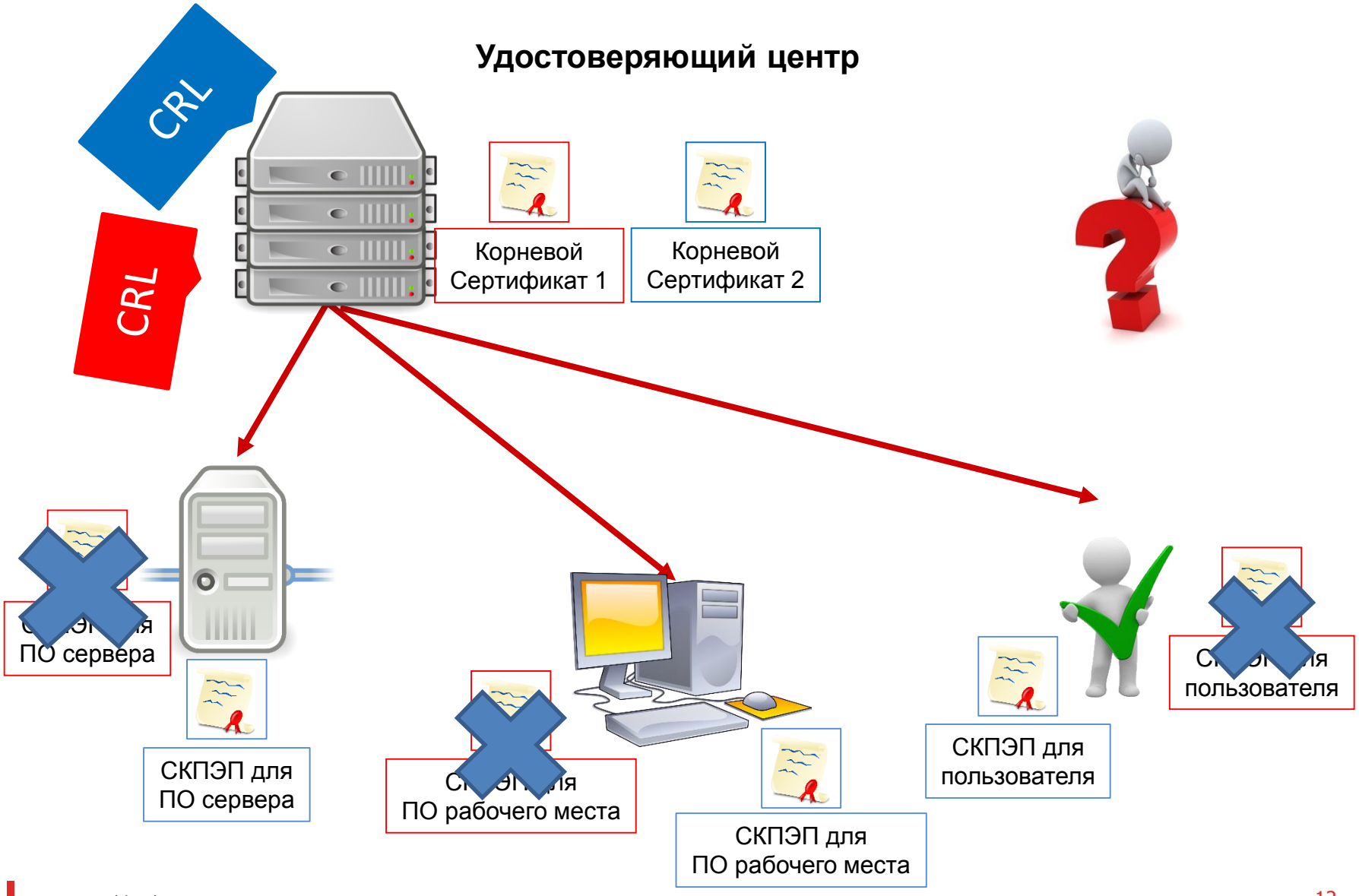
Удостоверяющий центр

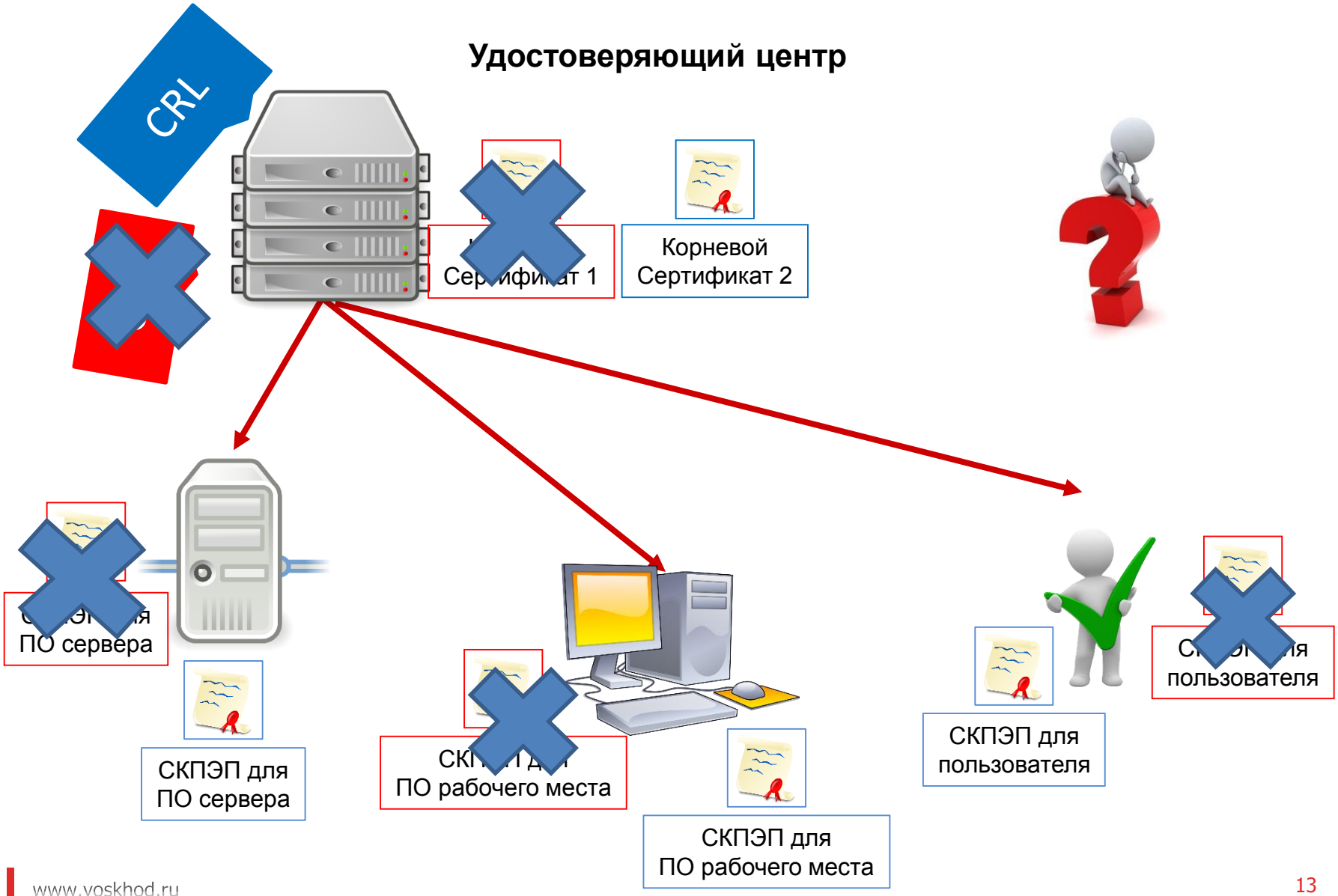


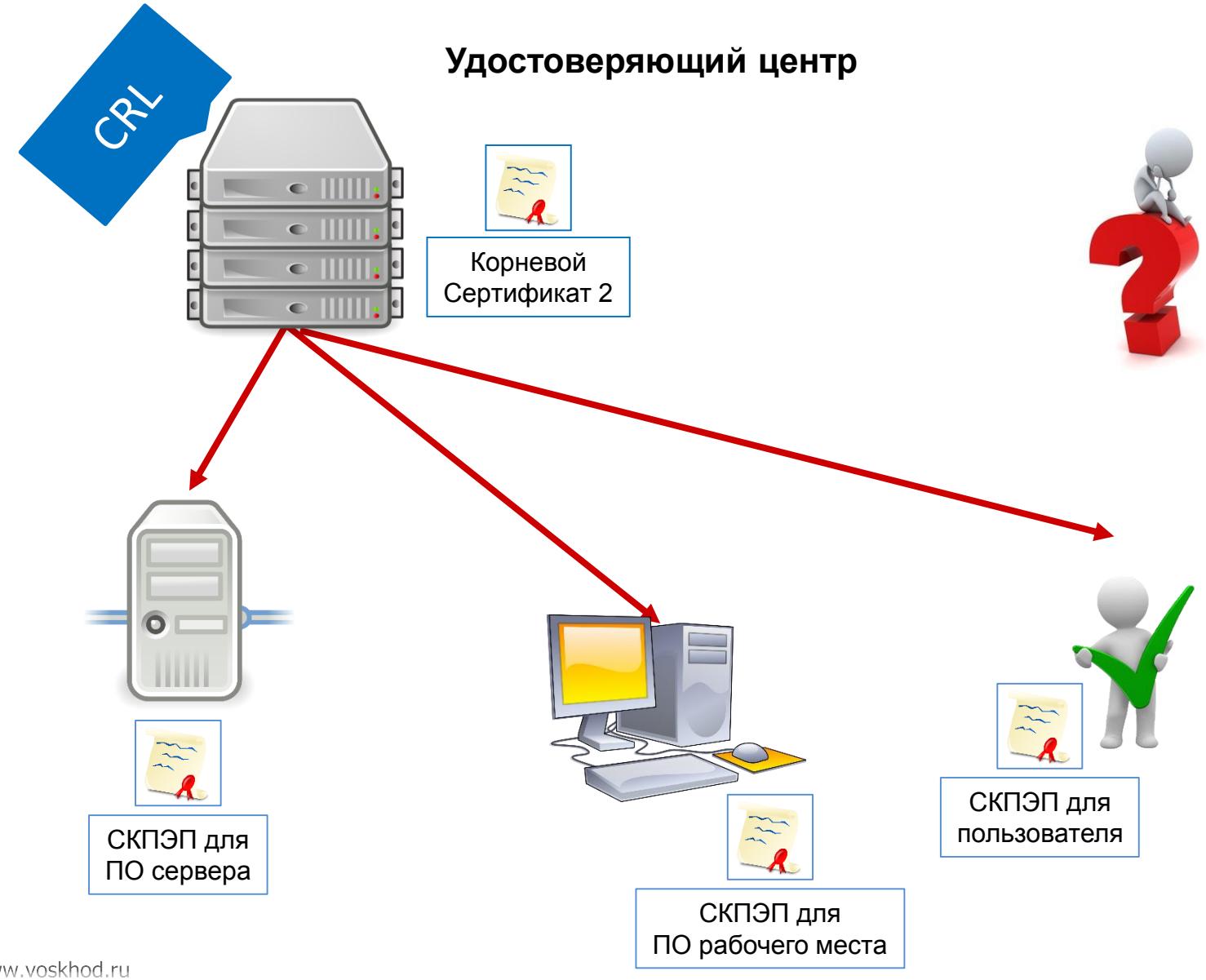

Удостоверяющий центр
CRL
Корневой
тификат
НОВЫЙ
Корневой
сертификат
ПО сервера
СКПЭП для
ПО сервера
ПО рабочего места
СКПЭП для
ПО рабочего места
СКПЭП для
пользователя
для
пользователя


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
пользователя
СКПЭП для пользователя

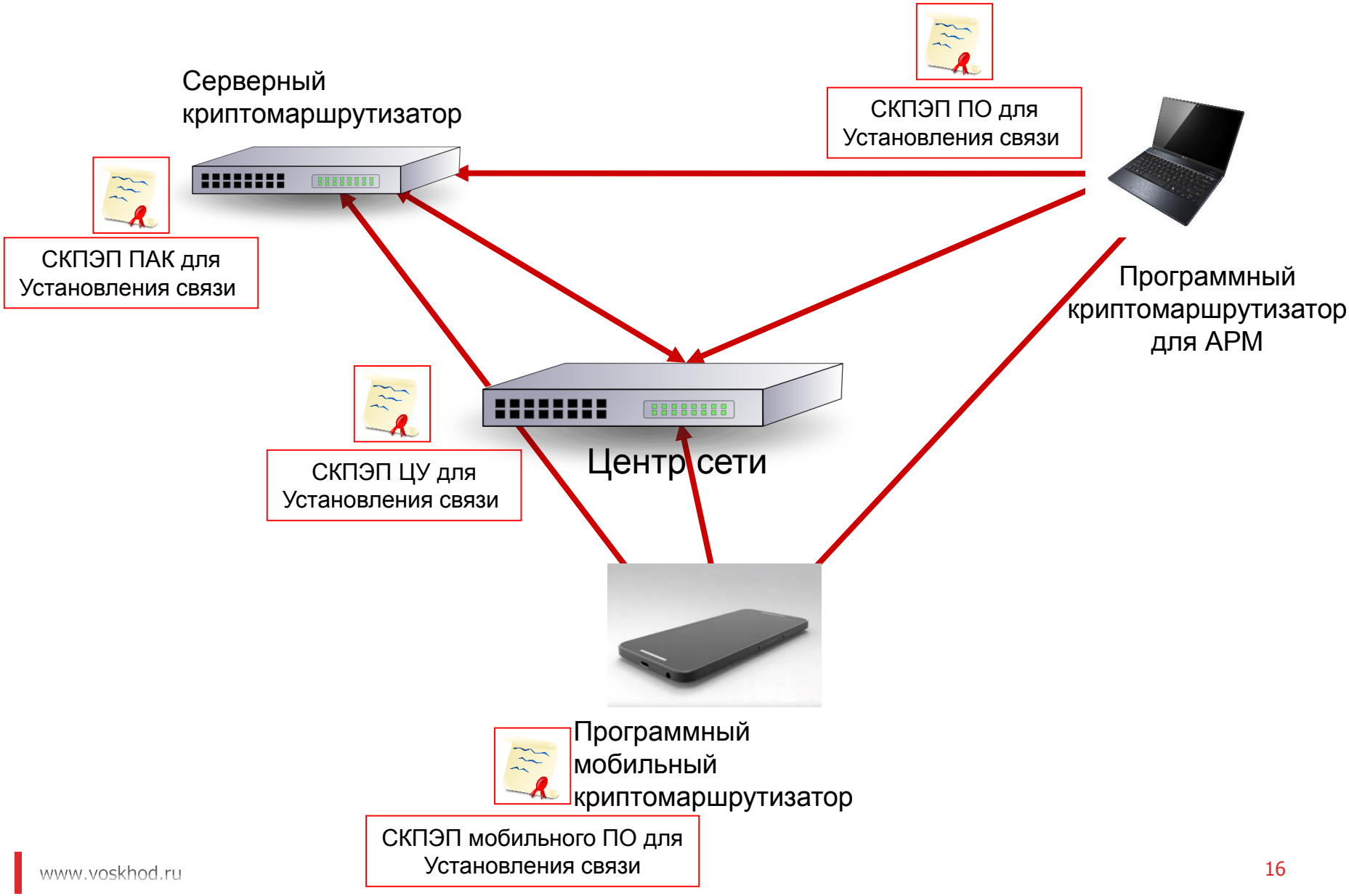

Удостоверяющий центр
CRL
Корневой
Сертификат 2
ПО сервера
СКПЭП для
ПО сервера
ПО рабочего места
СКПЭП для
ПО рабочего места
СКПЭП для
пользователя
пользователя


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

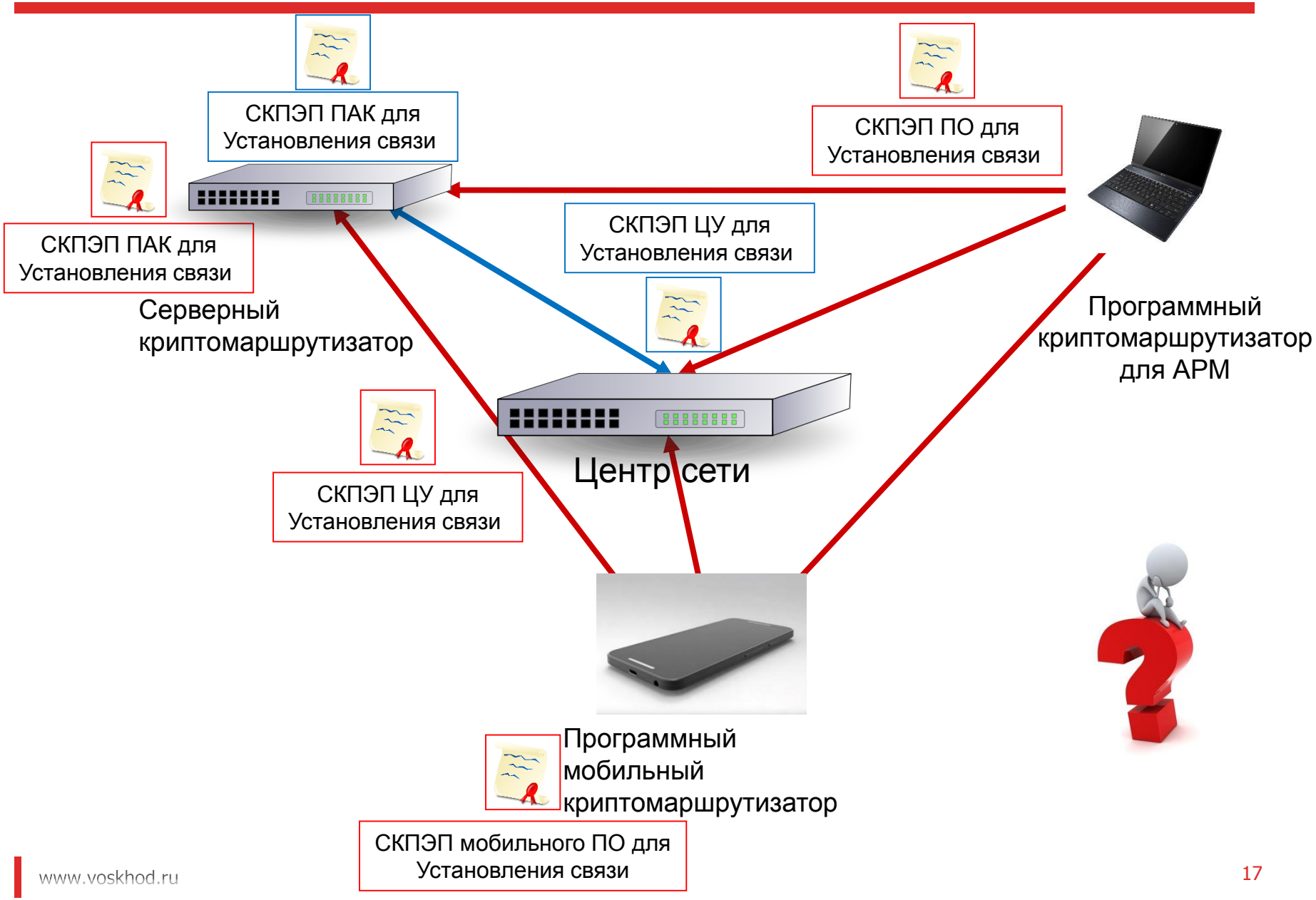
Удостоверяющий центр. Выводы

Новый УЦ	Обновленный УЦ
• Простота • Избыточность • Расходы на оборудование	• Сложность • Расходы на пересертификацию • Требования по поддержке режима перехода со стороны ПО

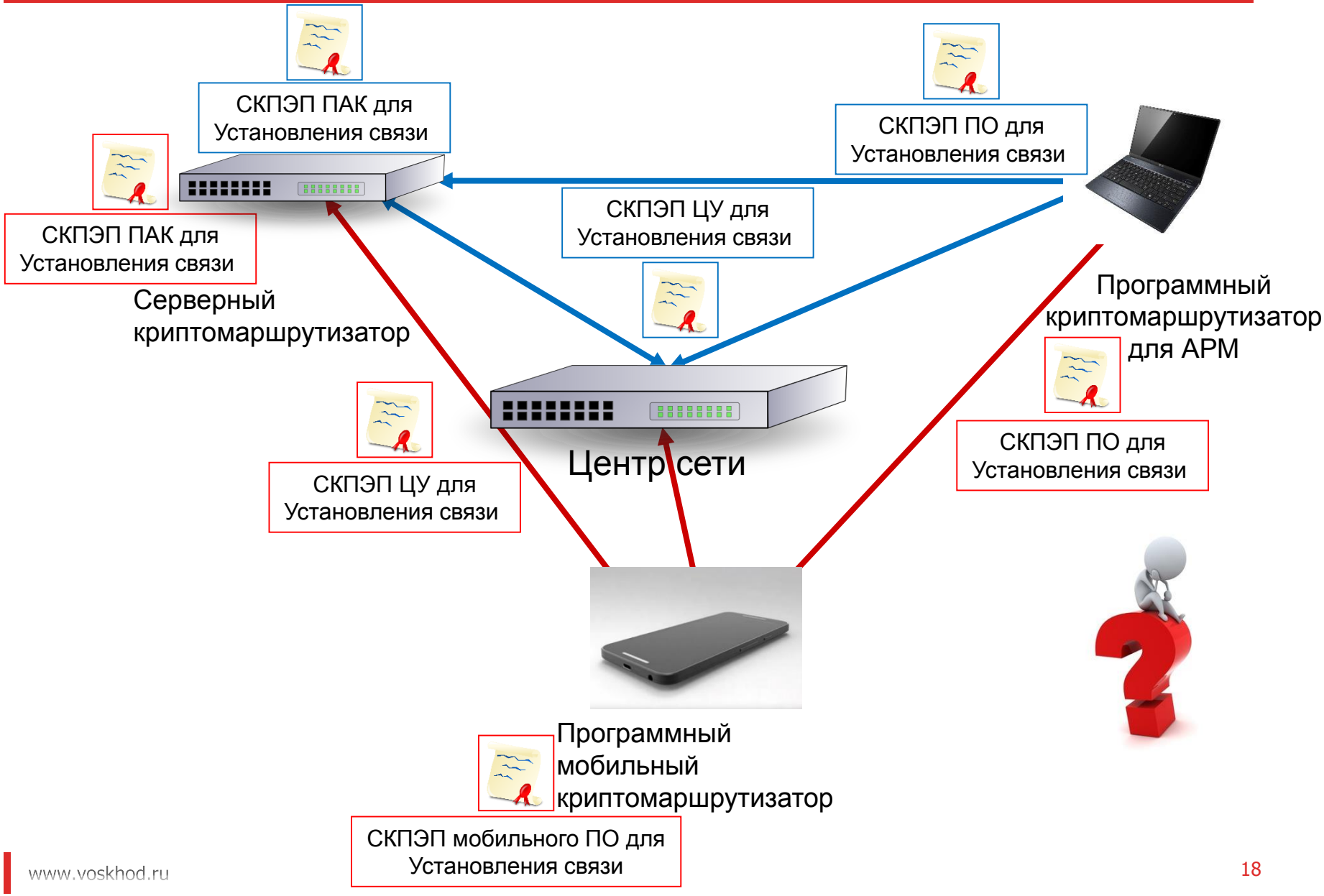
Защищенная сеть



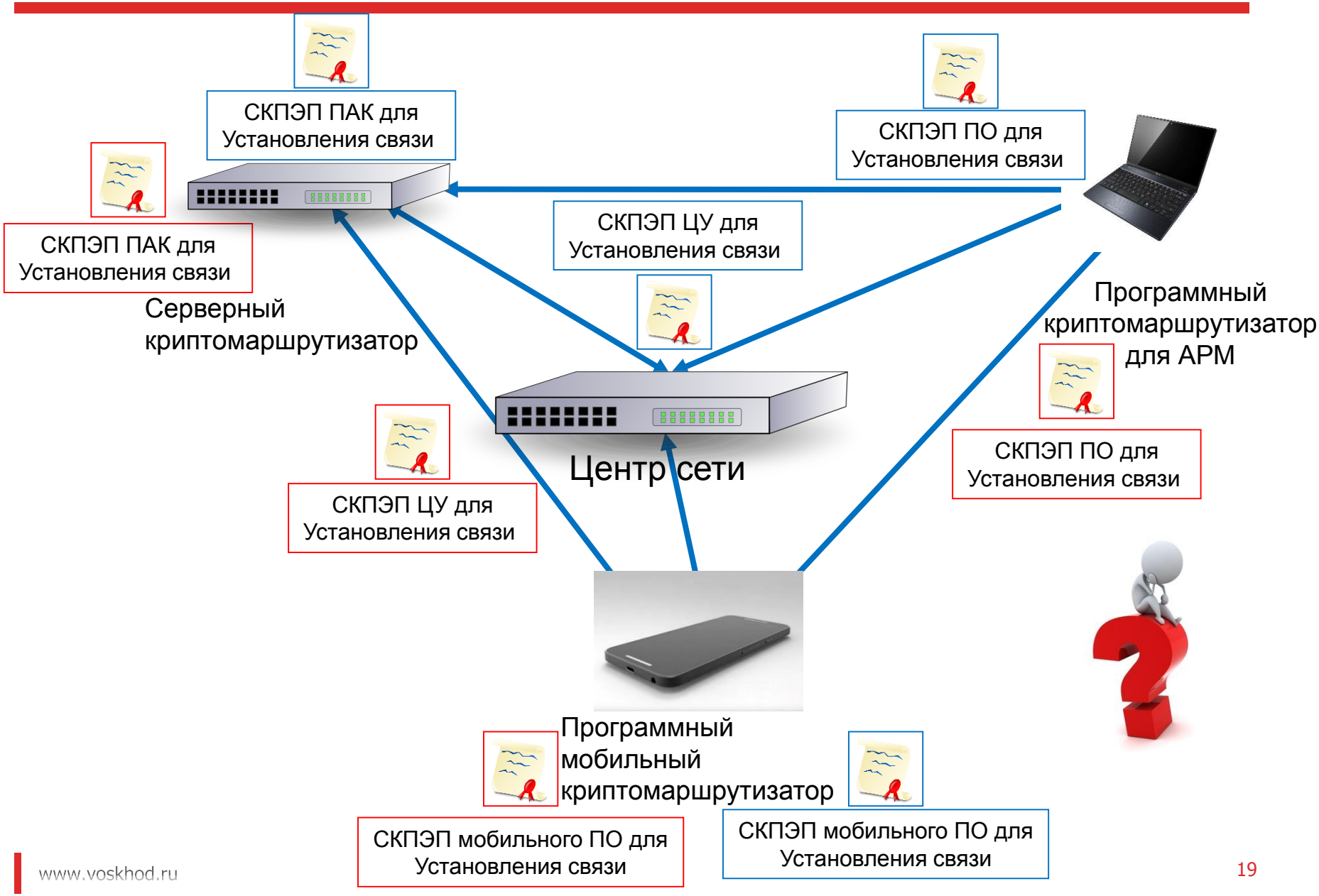
Защищенная сеть



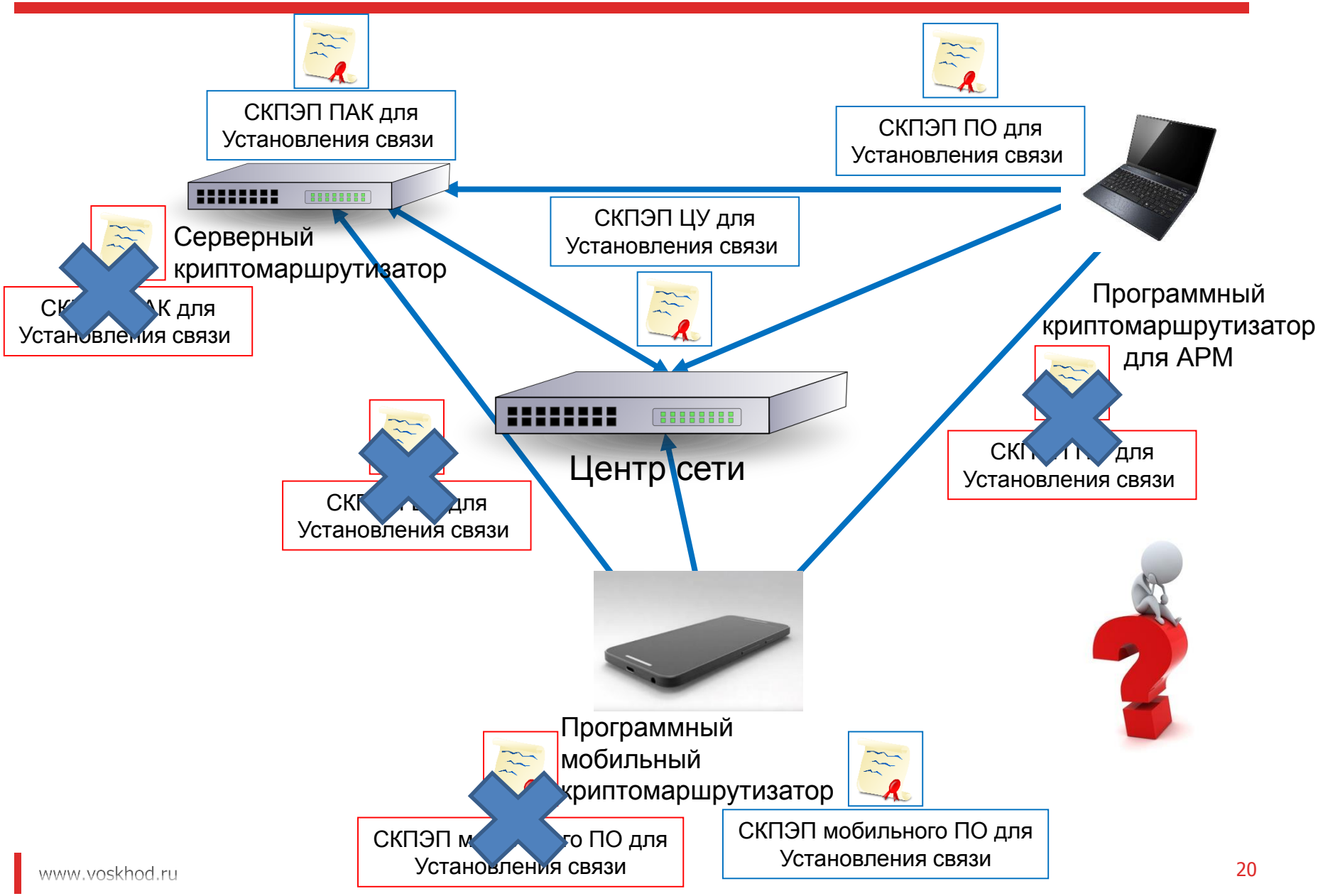
Защищенная сеть



Защищенная сеть



Защищенная сеть



Защищенная сеть

Серверный криптомаршрутизатор

Программный криптомаршрутизатор для АРМ

СКПЭП ПАК для Установления связи

СКПЭП ПО для Установления связи

Центр сети

СКПЭП ЦУ для Установления связи

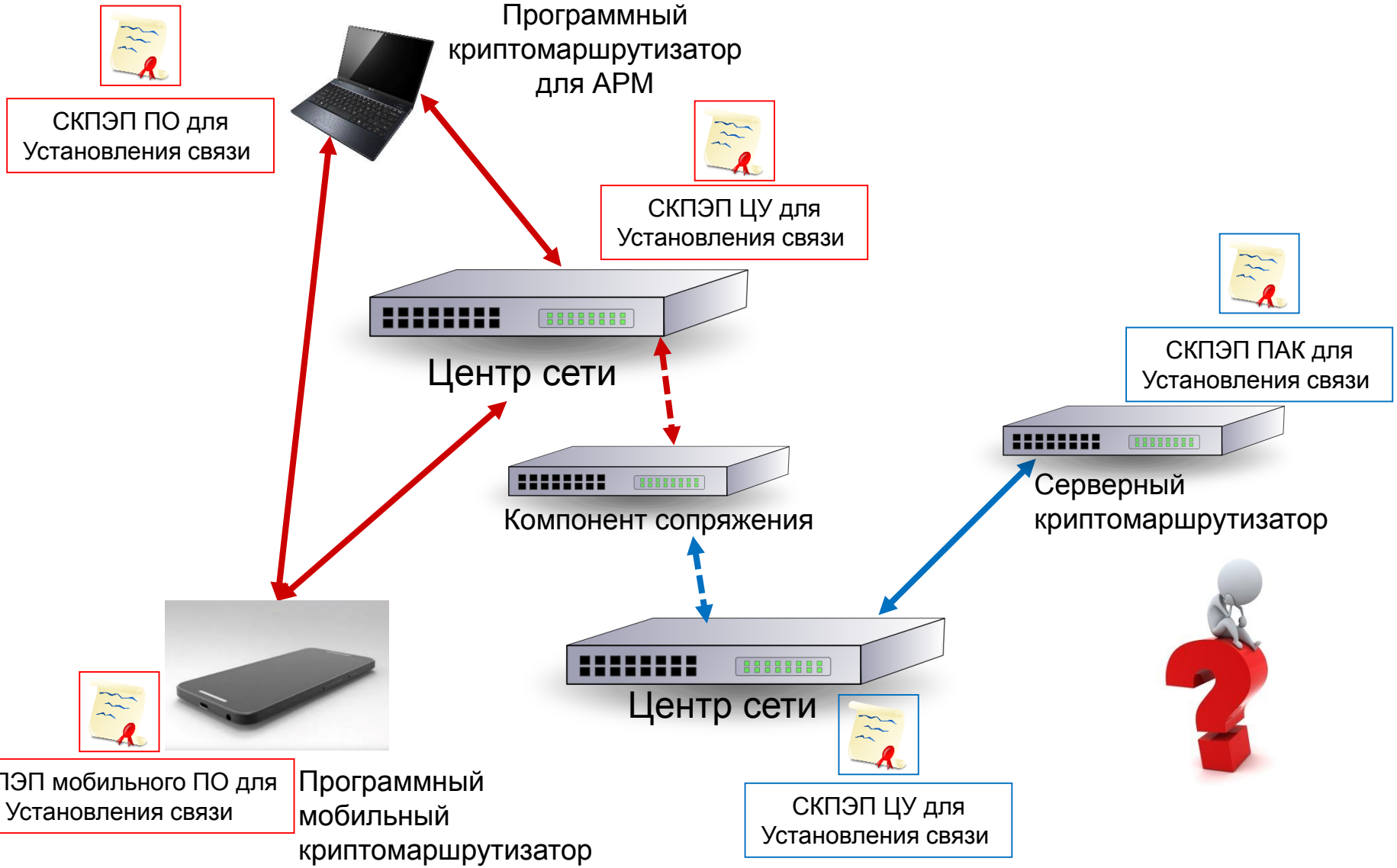
Центр сети

СКПЭП ЦУ для Установления связи

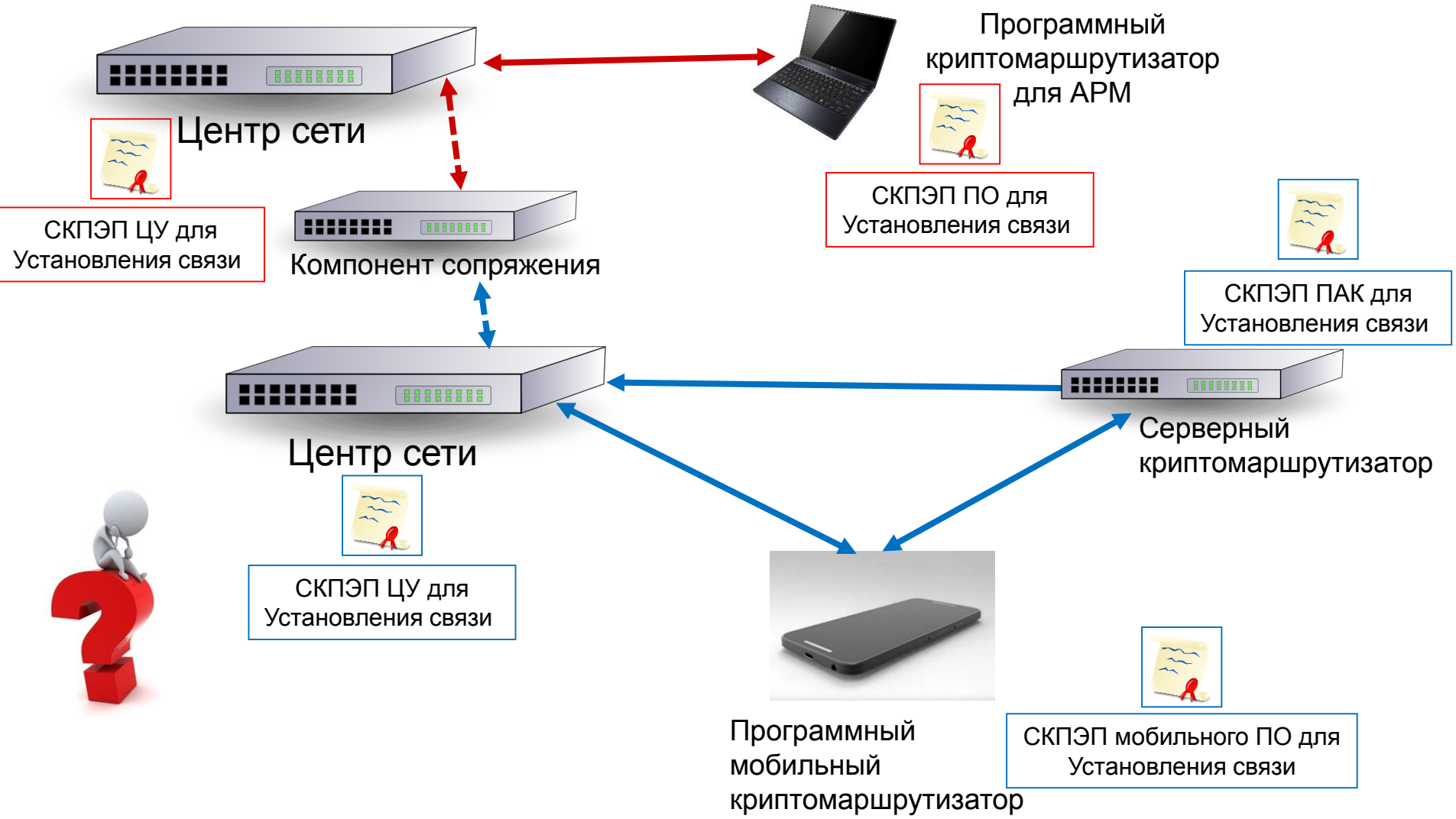
СКПЭП мобильного ПО для Установления связи

Программный мобильный криптомаршрутизатор

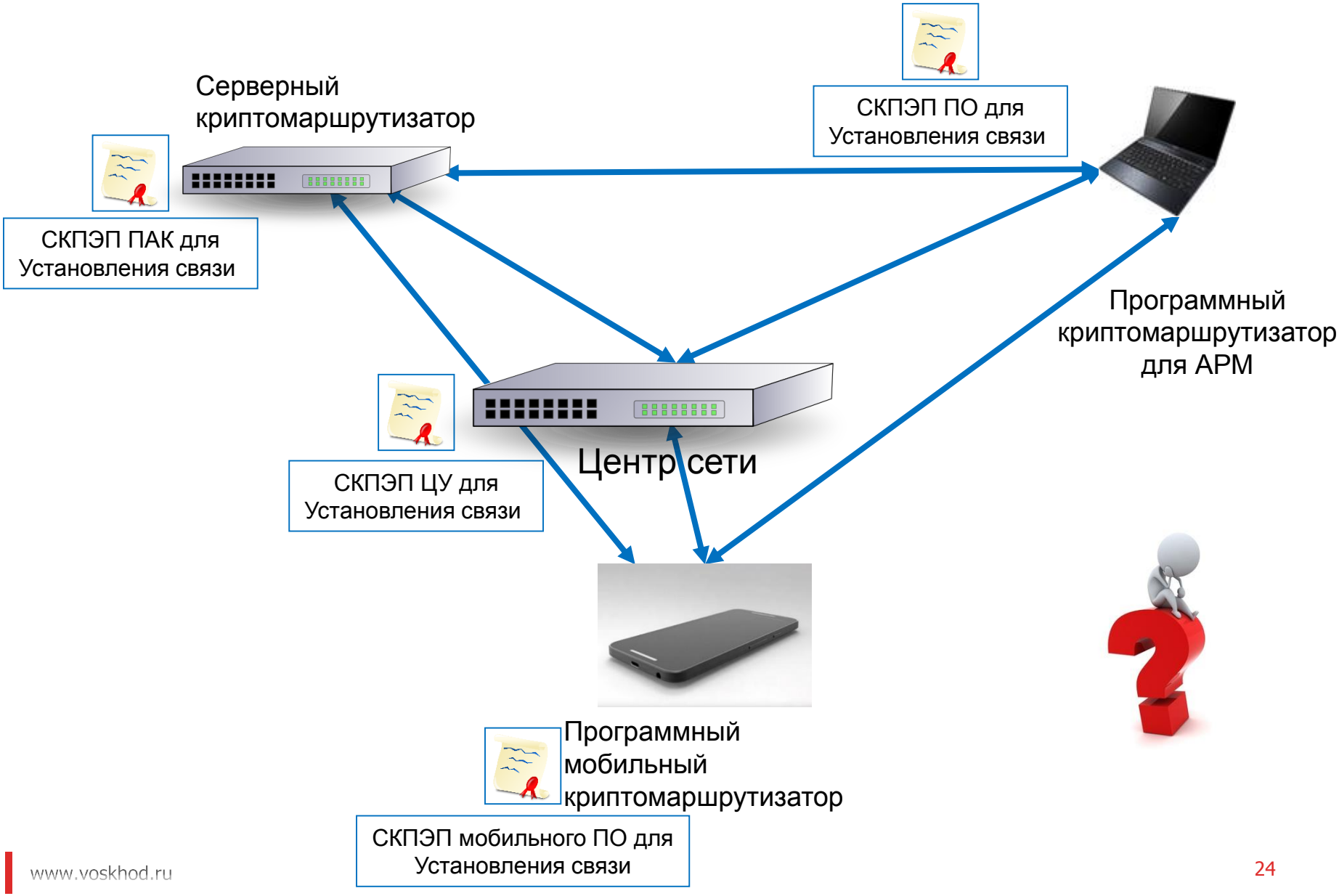
Защищенная сеть



Защищенная сеть



Защищенная сеть



Защищенная сеть. Выводы

Две сети	Смешанная сеть
• Простота • Избыточность • Дороговизна • Неэффективное сопряжение сетей	• Сложность • Оптимизация расходов • Нельзя реализовать своими силами

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

Ключевые носители

Интеллектуальные ключевые носители:

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

Неинтеллектуальные ключевые носители:

- Обновление документации

Работы НИИ «Восход» по переводу на ГОСТ 2012

- Проводятся работы по переводу ИС ГУЦ, ГУЦ УФО – на завершающей стадии
- Переведена ИС НР
- Запланирован переход в ГС «Мир»
- Все создаваемые системы

Итоги

- Каждая ИС требует свой порядок перехода
- Процессы перехода для всех подсистем взаимосвязаны
- Многое зависит от производителей СКЗИ
- Непреодолимые трудности, задачи по переходу нельзя решать без участия регуляторов