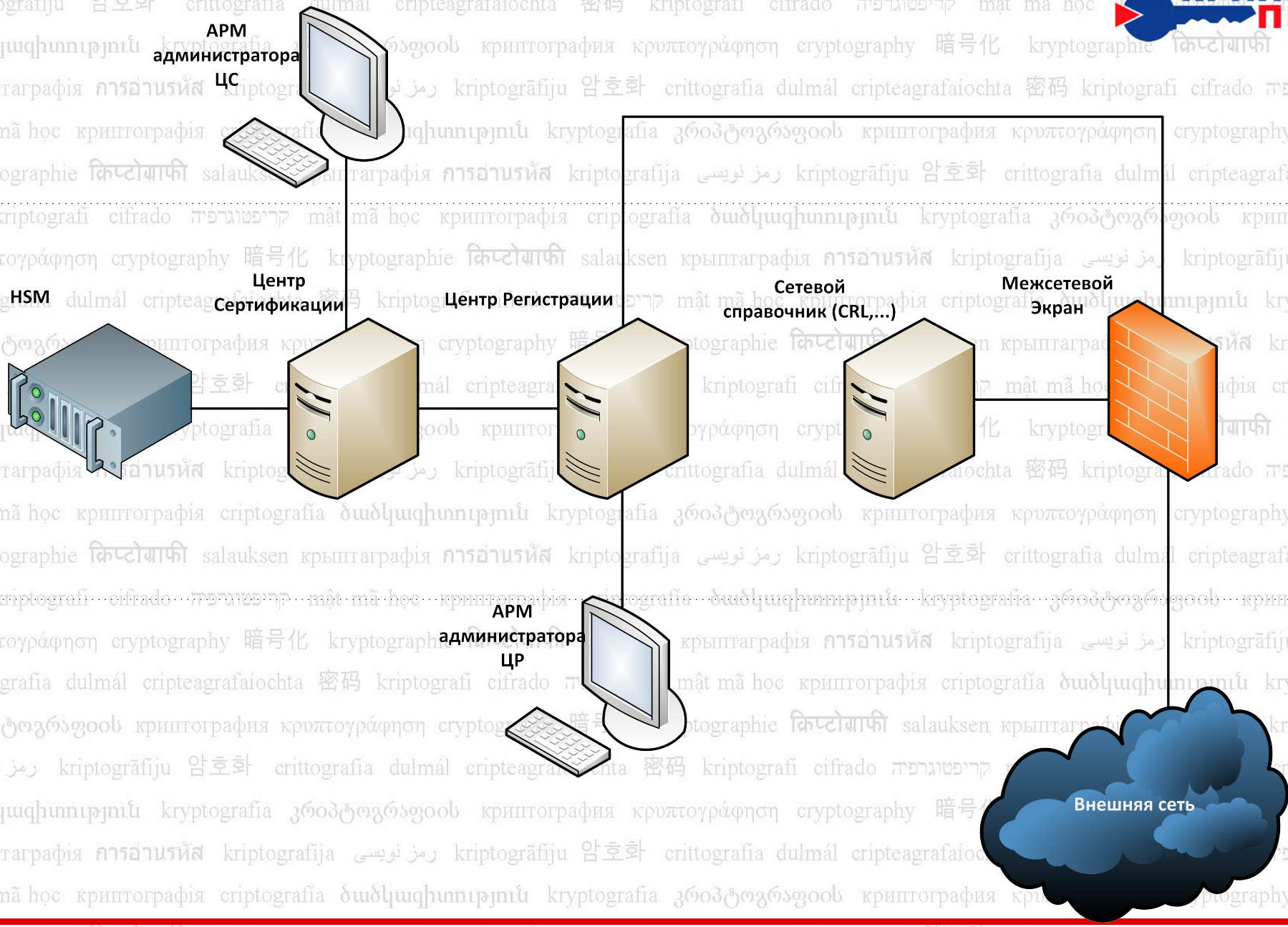
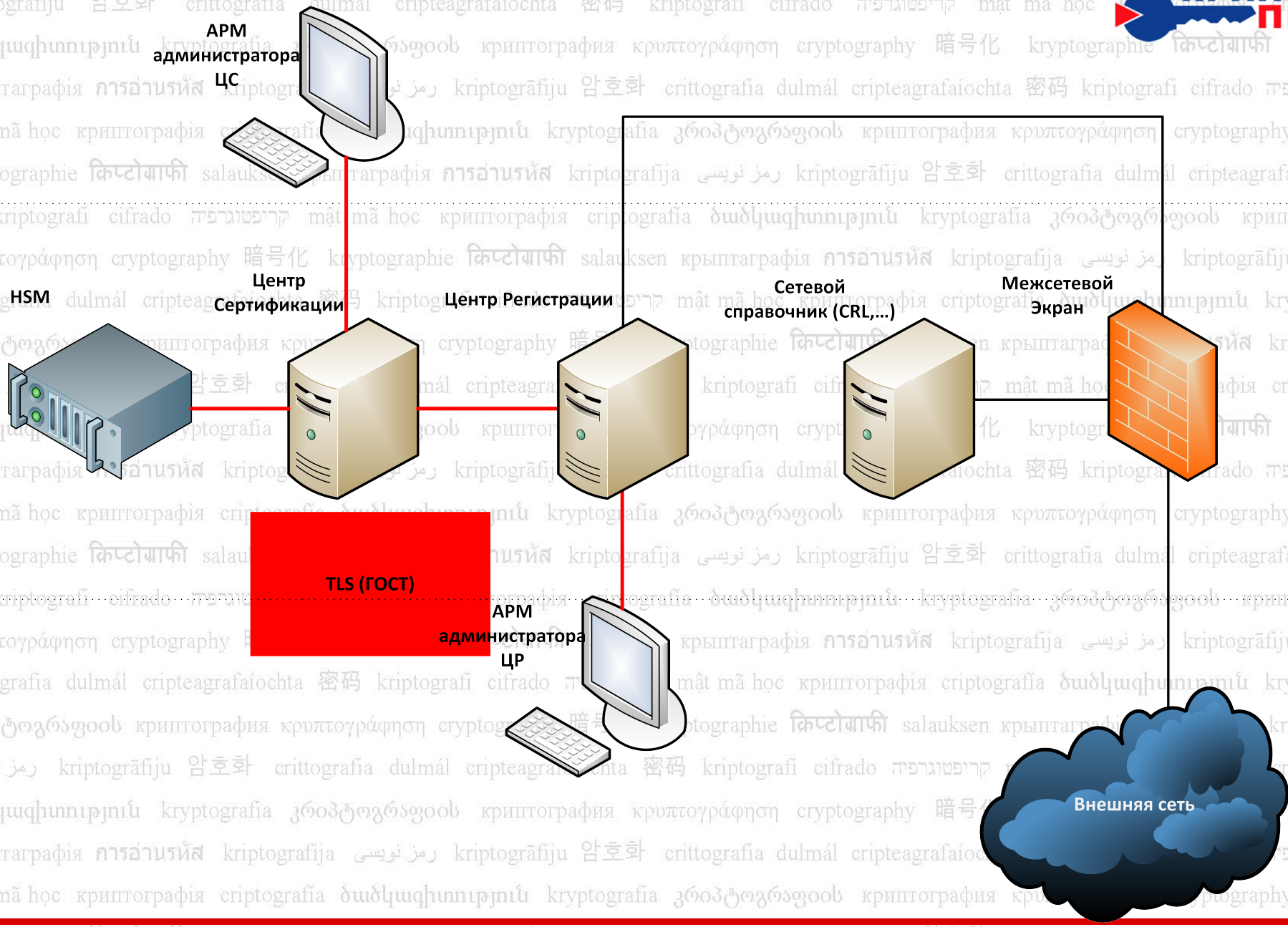
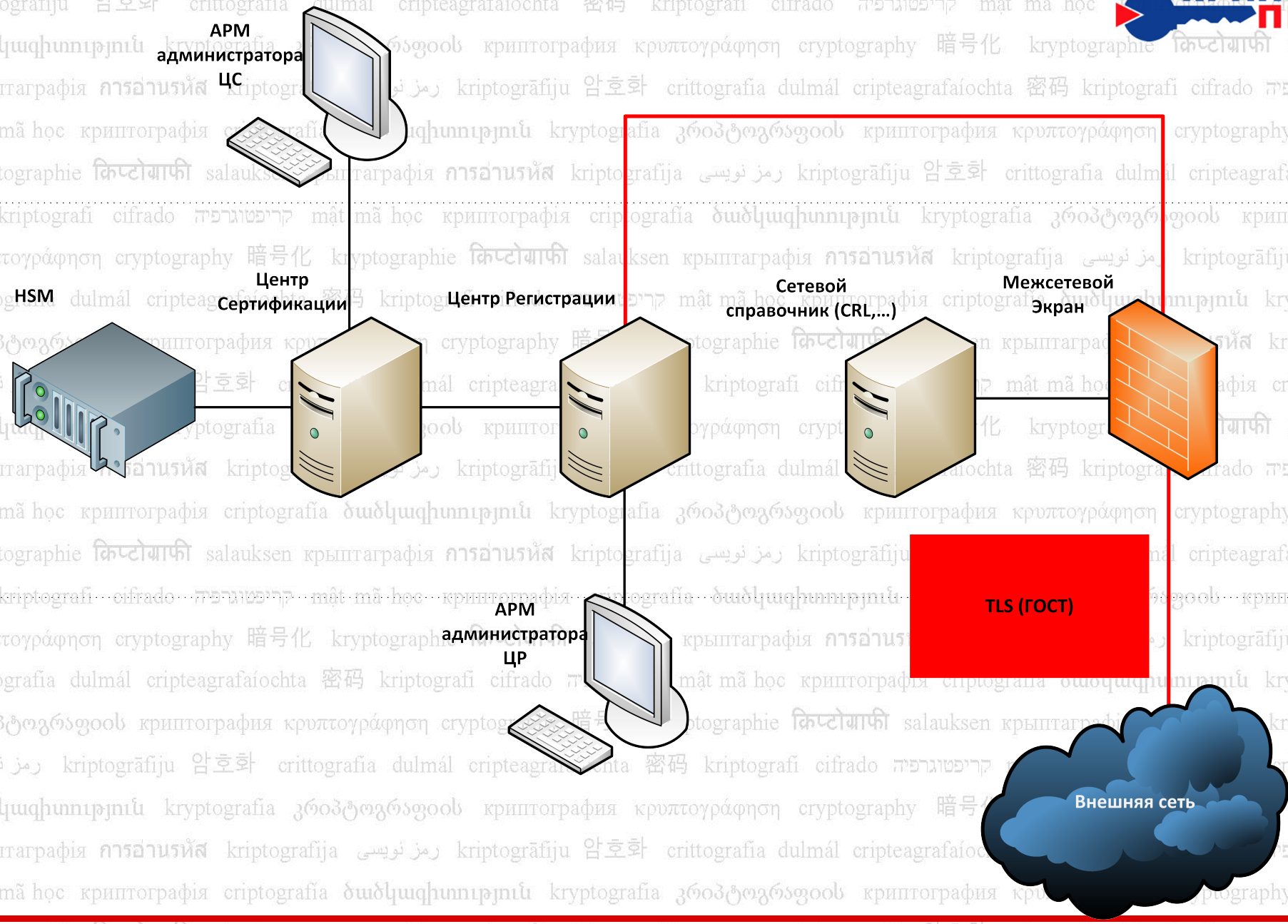
Актуальные вопросы перехода УЦ на новые криптографические ГОСТы в 2016 году

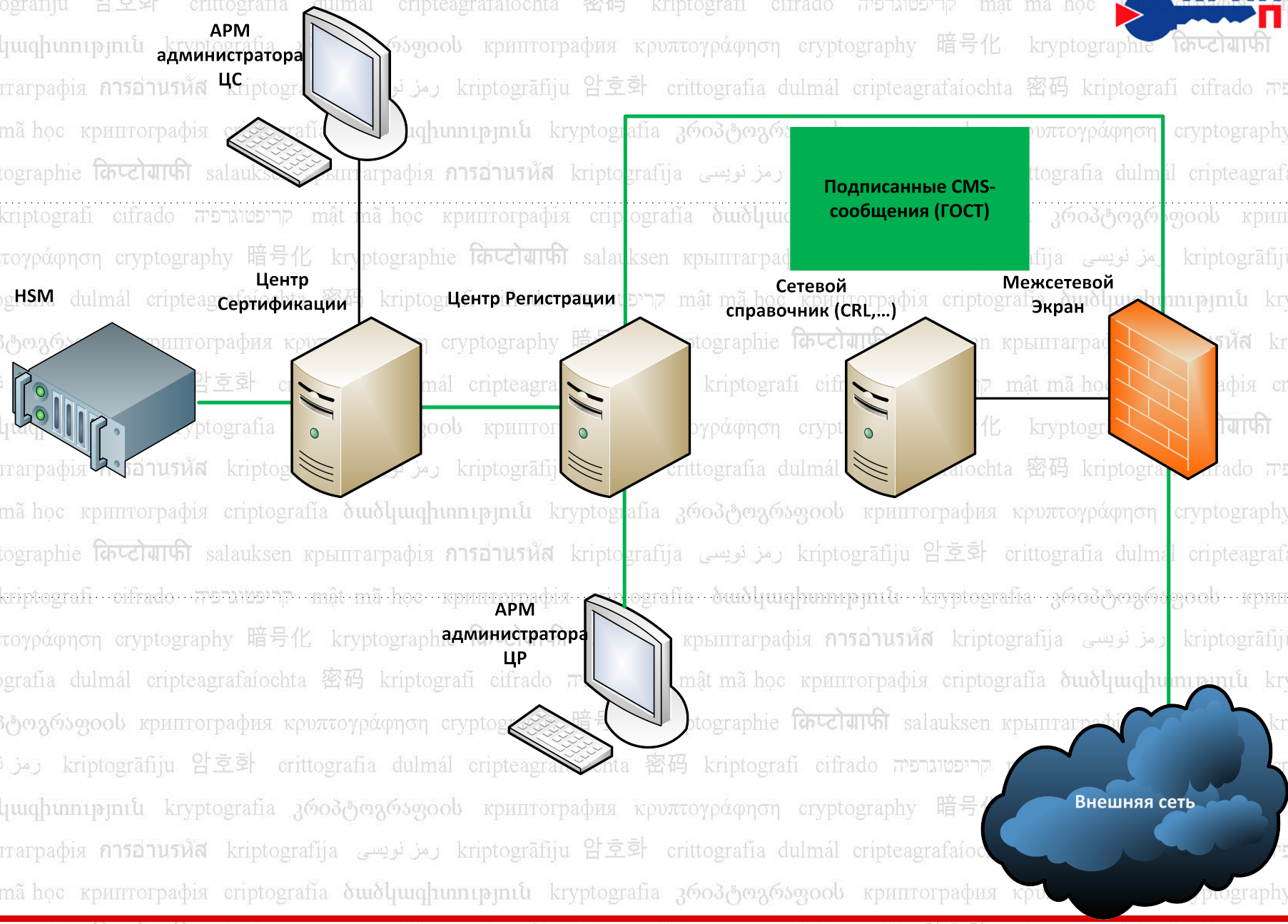
Смышляев Станислав Витальевич, к.ф.-м.н.,
начальник отдела защиты информации

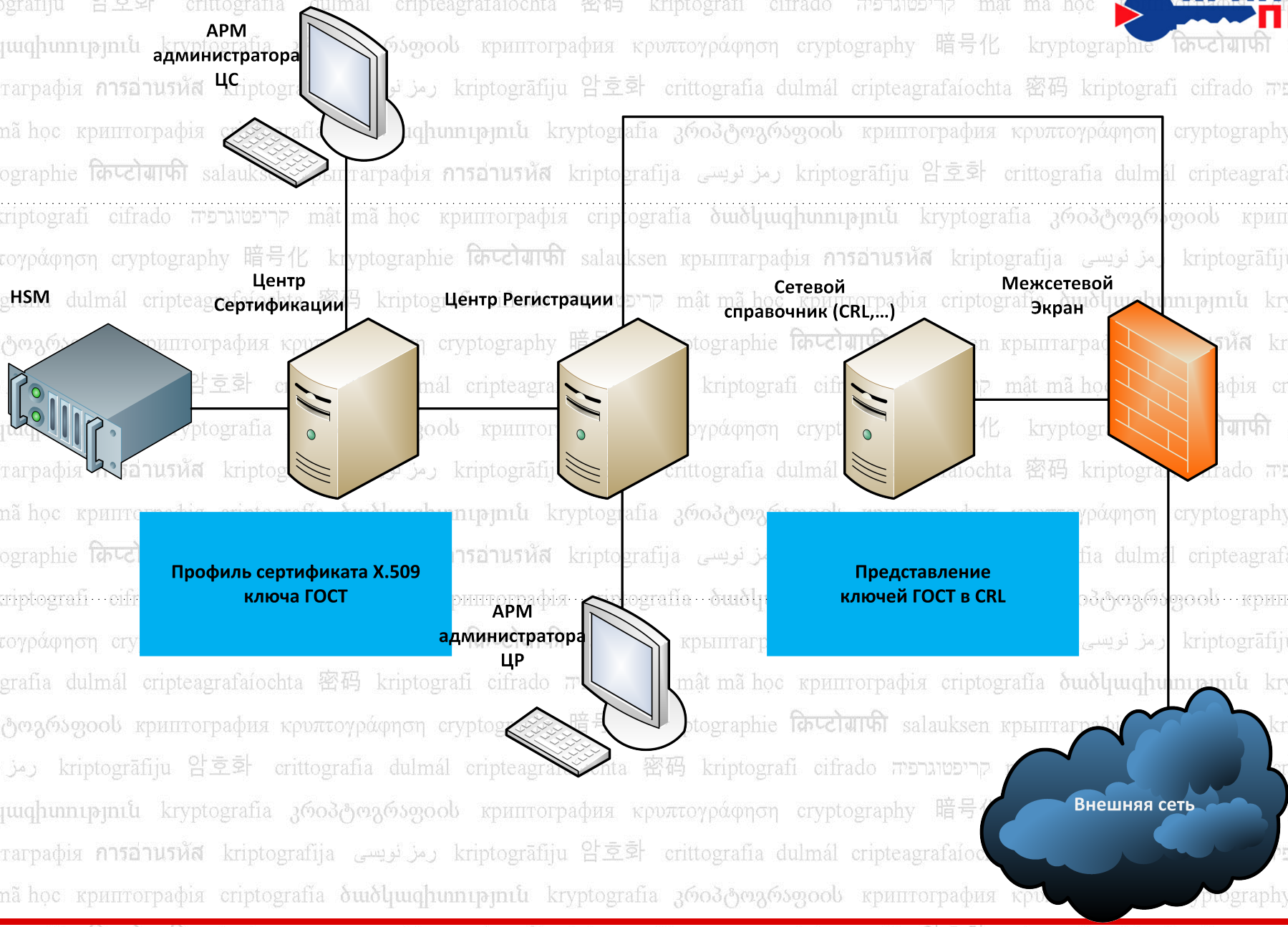
PKI-Форум Россия 2015









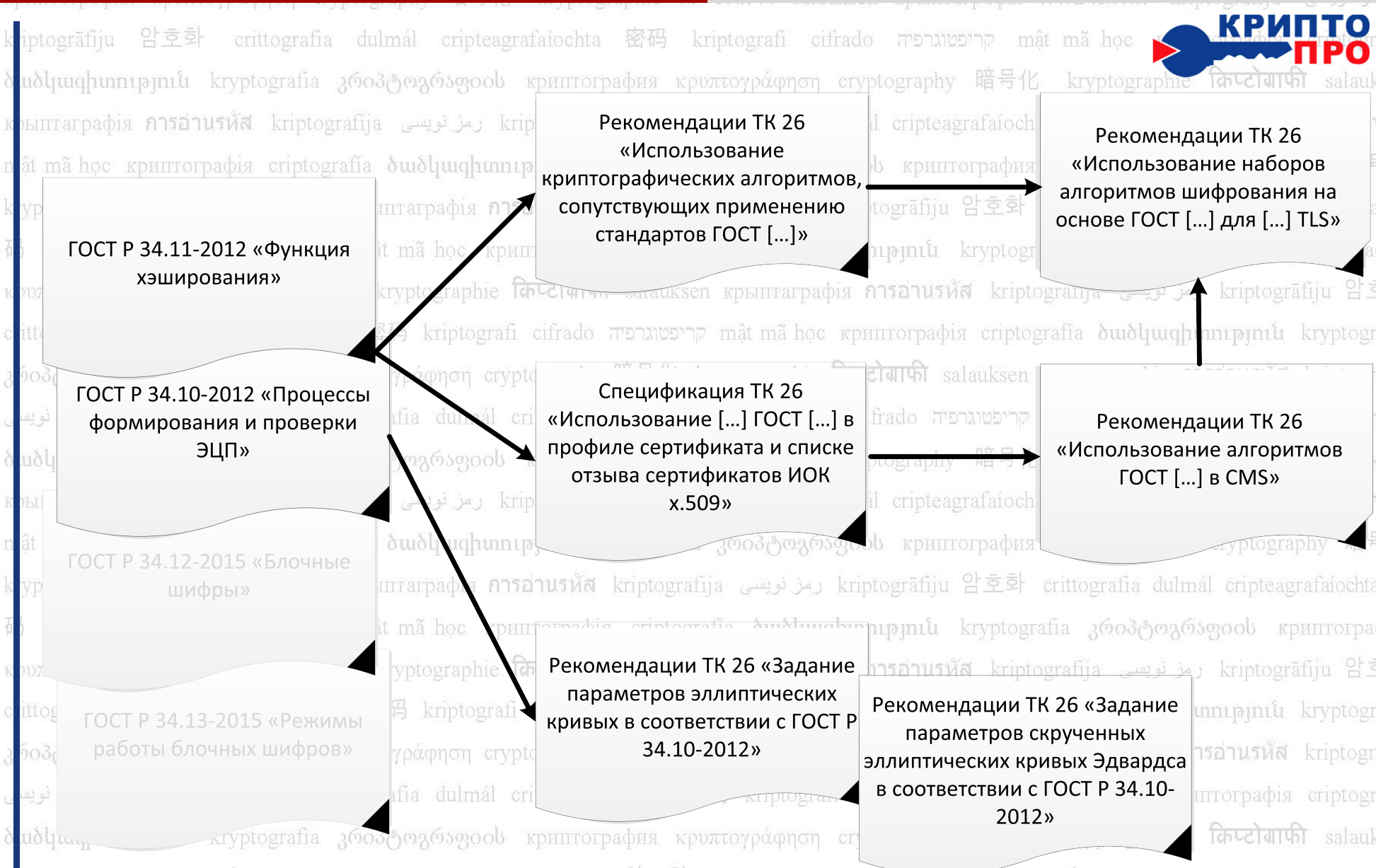


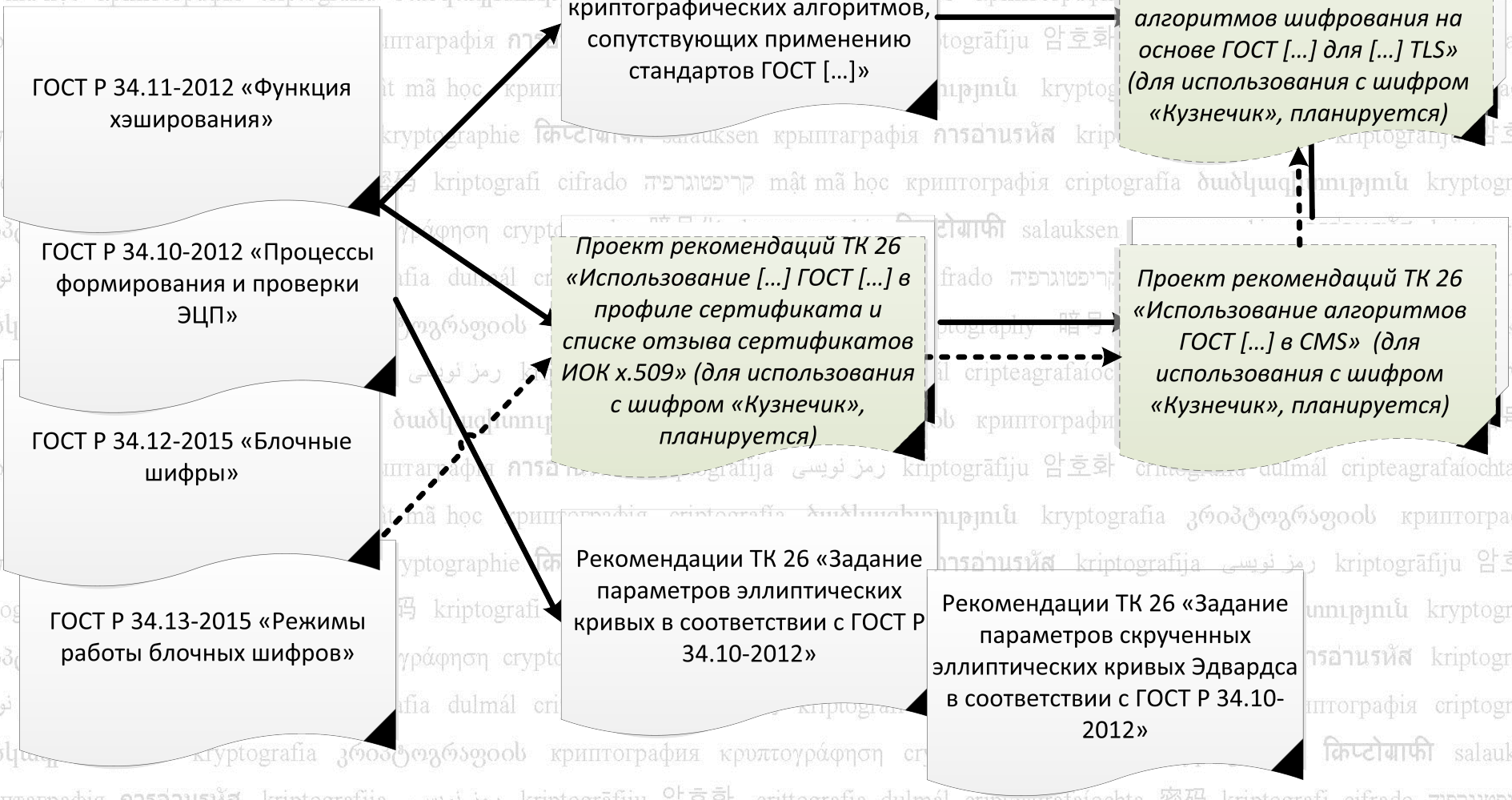
Технический комитет по стандартизации „Криптографическая защита информации“

- „Рекомендации по стандартизации. Использование криптографических алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012“.
- „Рекомендации по стандартизации. Задание параметров эллиптических кривых в соответствии с ГОСТ Р 34.10-2012“.
- „Рекомендации по стандартизации. Задание параметров скрученных эллиптических кривых Эдвардса в соответствии с ГОСТ Р 34.10-2012“.

Технический комитет по стандартизации „Криптографическая защита информации“

- „Техническая спецификация использования алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509“.
- „Рекомендации по стандартизации. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS“.
- „Рекомендации по стандартизации. Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)“.





„Техническая спецификация использования алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509“.

- Унификация формата ключей проверки ЭП ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.
- Полное методическое соответствие решениям RFC 4491.
- Минимизация проблем с расширением функционала ПО для поддержки ГОСТ Р 34.10-2012.

„Рекомендации по стандартизации. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS“.

- Решения основаны на сопутствующих алгоритмах из новых рекомендаций ТК 26.
- Унификация порядка работы с сообщениями, сформированными с помощью ключей ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.
- Полное методическое соответствие решениям RFC 4490 в части форматов.
- Минимизация проблем с расширением функционала ПО для поддержки ГОСТ Р 34.10-2012.

„Рекомендации по стандартизации. Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)“.

- Ввод новых наборов алгоритмов шифрования (cipher suite) TLS, опирающихся на сопутствующие алгоритмы из новых рекомендаций ТК 26.
- Совместимость ключей ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 при двусторонней аутентификации как в рамках новых наборов, так и в рамках старых.
- Возможность перехода на новые наборы (cipher suites) без немедленной смены ключа сервера на ключ ГОСТ Р 34.10-2012.

Важные даты при переводе УЦ на работу с ГОСТ Р 34.10-2012

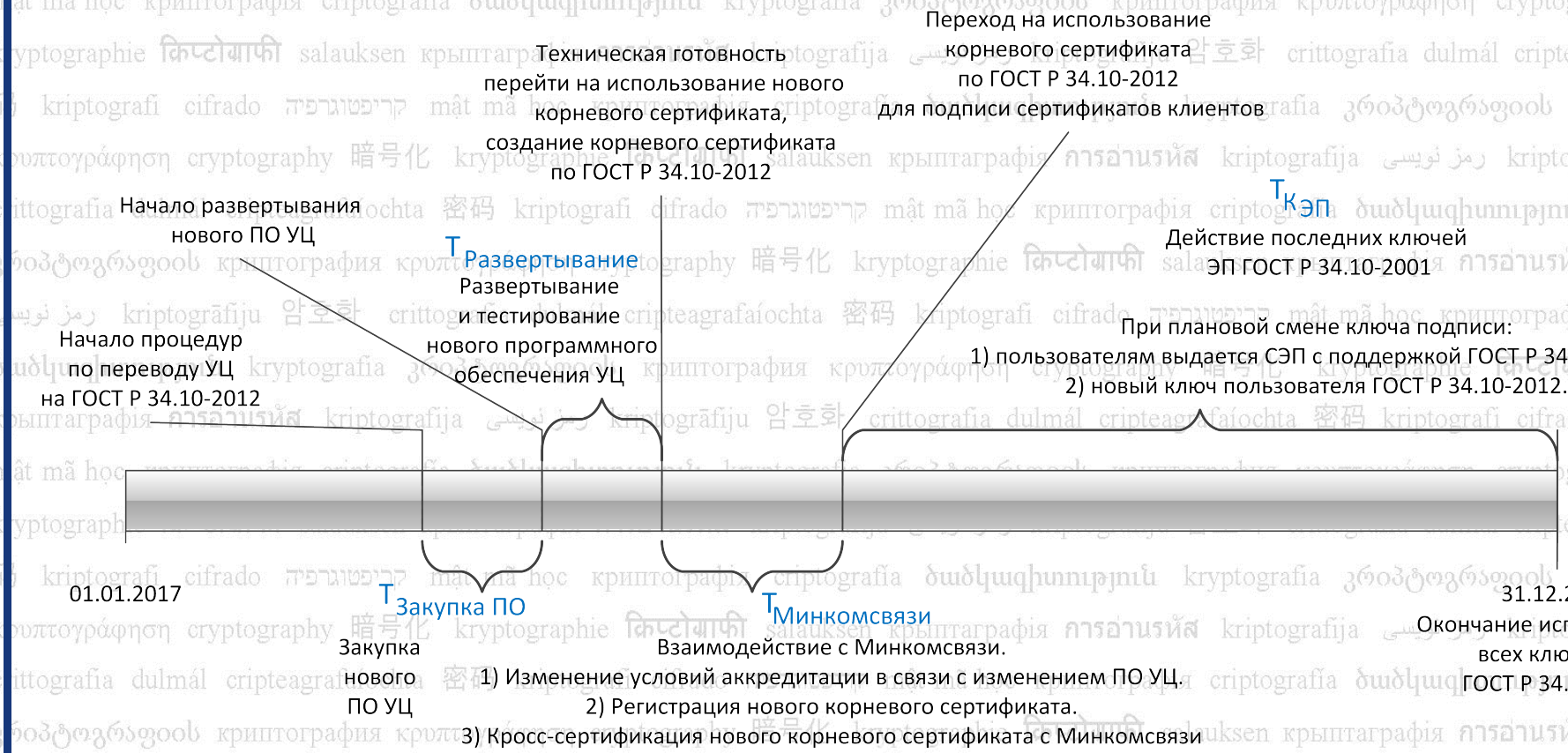
Окончание действия ключей ЭП ГОСТ Р 34.10-2001

После 31 декабря 2018 года не допускается формирование подписи в соответствии с ГОСТ Р 34.10-2001.

В соответствии с выпиской из документа ФСБ России №149/7/1/3-58 от 31.01.2014 „О порядке перехода к использованию новых стандартов ЭЦП и функции хэширования“:

Рассмотрим следующие временные промежутки:

- $T_{К_{ЭП}}$ — срок действия ключа ЭП, фиксируемый для клиентских сертификатов.
- $T_{Минкомсвязи}$ — время отправки и рассмотрения анкеты в Минкомсвязи: изменение ПО УЦ, изменение корневого сертификата, кросс-сертификация с Минкомсвязи.
- $T_{Развертывание\ ПО}$ — время развертывания и тестирования ПО УЦ с поддержкой ГОСТ Р 34.10-2012.
- $T_{Закупка\ ПО}$ — время закупки ПО УЦ с поддержкой ГОСТ Р 34.10-2012.



При следующих значениях длин временных интервалов:

- $T_{К_{ЭП}} = 1$ год — срок действия ключа ЭП, фиксируемый для клиентских сертификатов.
- $T_{Минкомсвязи} = 3$ месяца — время отправки и рассмотрения анкеты в Минкомсвязи: изменение ПО УЦ, изменение корневого сертификата, кросс-сертификация с Минкомсвязи.
- $T_{Развертывание\ ПО} = 2$ месяца — время развертывания и тестирования ПО УЦ с поддержкой ГОСТ Р 34.10-2012.
- $T_{Закупка\ ПО} = 2$ месяца — время закупки ПО УЦ с поддержкой ГОСТ Р 34.10-2012.

КРИПТО ПРО

Выводы

- В ТК 26 принят полный комплект документов, необходимых для разработки и экспертной оценки УЦ, СКЗИ и СЭП, обеспечивающих работу с PKI на основе ГОСТ Р 34.10-2012.
- На уровне форматов обеспечена унификация с ГОСТ Р 34.10-2001, сводящая к минимуму организационно-технические проблемы перехода на ГОСТ Р 34.10-2012.
- Разработка и обоснование сопутствующих алгоритмов для ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 проведены с нуля для обеспечения криптографической стойкости решений.
- Процедуры по переводу УЦ на ГОСТ Р 34.10-2012 необходимо начать не позднее 2 квартала 2017 года.

КРИПТО ПРО

Спасибо за внимание!

Вопросы?

- Материалы, вопросы, комментарии: svs@cryptopro.ru.