конференция РусКрипто

КРИПТО ПРО

Конференция «РусКрипто’2014»

Секция «Электронная подпись, практика применения»

Применение квалифицированной электронной подписи в современной эпохе

Маслов Юрий,
ООО «КРИПТО-ПРО»
maslov@cryptopro.ru

В жизни, как и в грамматике, исключений больше, чем правил. (Реми де Гурмон)

Вынуждены:

Регламентировать использование квалифицированной ЭП

Ограничивать круг доверенных УЦ из числа аккредитованных

Регламент применения квалифицированной ЭП

Условия оформляются и утверждаются оператором информационной системы (ЭДО)

Условия размещаются на сайте оператора ЭДО или обеспечивается их доступность участникам системы ЭДО иным способом

Оформлять в простой письменной форме и заключать письменное соглашение с участниками системы ЭДО – не требуется

Регламент применения квалифицированной ЭП

Определение момента подписания

Зачем? Так как срок действия сертификата ключа проверки электронной подписи устанавливается равным сроку действия ключа электронной подписи

Как? Момент подписания определяется либо по штампу времени (электронный документ, подписанный квалифицированной электронной подписью и устанавливающий существование определенного электронного документа на момент времени, указанный в штампе) либо по моменту поступления на сервер системы электронного документооборота (запись в журнале/логе, устанавливающая момент времени, когда бы получен положительный результат проверки электронной подписи определённого электронного документа)

Регламент применения квалифицированной ЭП

Определение дополнительного содержания квалифицированного сертификата

Зачем? Для обеспечения возможности руководителю организации, являющейся участником системы ЭДЛ, определить правомочия владельца квалифицированного сертификата

Как? Определение объектных идентификаторов (OIDs) и соответствующим им правомочиям владельца сертификата.

Пример формы заявления на изготовление сертификата с указанием ограничений на использование квалифицированного сертификата и местом куда ограничения могут быть записаны (EKU или certificatePolicies).

Регламент применения квалифицированной ЭП

Определение формата электронной подписи

Зачем? Так как формат ЭП нормативно не определён

Как? Описать какие форматы используются в системе ЭДО (отделённая или нет, классическая или усовершенствованная или гибридная)

Сеть доверенных УЦ из числа аккредитованных

Основные причины:

Ответственность в 1.5 миллионов слишком мала

Не каждый УЦ из числа аккредитованных оказывает услуги неопределённому кругу лиц

Не каждый УЦ из числа аккредитованных согласен вносить ограничения на использование квалифицированного сертификата

Не с каждым УЦ из числа аккредитованных можно договорить об оплате третьим лицом услуг УЦ определённым лицам

Вопрос на обсуждение

Аккредитованный УЦ ООО «КРИПТО-ПРО» оказывает услуги только с личной явкой заявителя (только централизованная модель)

У других УЦ похожая ситуация.

А было бы здорово ввести распределённую модель!

Порядок оказания услуг аккредитованным УЦ

Формально по 63-ФЗ:

Порядок реализации функций УЦ определяется самим УЦ

Существенными условиями выдачи квалифицированного сертификата являются:

- установить личность заявителя;
- под расписку ознакомить заявителя с содержимым квалифицированного сертификата.

Но…

Может ли эти условия выполнить нотариус или операционист банка?

Порядок оказания услуг аккредитованным УЦ

Формально по 63-ФЗ:

Согласно ст. 13 63-ФЗ УЦ обязан обеспечивать возможность создания ключей ЭП заявителем

Согласно ст. 17 и п.20 Приказа № 795 квалифицированный сертификат должен содержать наименование и класс средства ЭП владельца

Но…

По житейской логике УЦ должен обеспечивать достоверность информации в сертификате

Из положительного: выдаются единые сертификаты для систем сдачи отчётности

Требования ФСБ России

- Требования к форме квалифицированного сертификата ключа проверки электронной подписи, утвержденные приказом ФСБ России от 27 декабря 2011 г. № 795
- Извещение об использовании стандартных атрибутов имени commonName (общее имя), surname (фамилия), givenName (приобретенное имя) и дополнительных атрибутов имени поля «subject» в структуре квалифицированного сертификата ключа проверки электронной подписи (http://www.fsb.ru/fsb/science.htm http://www.fsb.ru/files/PDF/Izveshenie_na_sait_po_trebovaniyam.pdf)

Требования ФНС России

- Порядок применения квалифицированных сертификатов ключей проверки электронных подписей в информационных системах ФНС России (утверждён приказом ФНС России от 08.04.2013 ММВ-7-4/142@
- Информационное сообщение о мероприятиях по обеспечению применения квалифицированных сертификатов ключей проверки электронных подписей в информационных системах ФНС России (дополнение к приказу ММВ-7-4/142@)

Вопросы?

Маслов Юрий,
ООО «КРИПТО-ПРО»
maslov@cryptopro.ru