



**III ВСЕРОССИЙСКАЯ КОНФЕРЕНЦИЯ
ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:
«Открыто о будущем ЭЦП в России»**

Марий Эл, г. Йошкар-Ола, 15-17 сентября 2011г.

**Новеллы в законодательстве об электронной
подписи и как их применять.**

**Маслов Юрий
Коммерческий директор
ООО «КРИПТО-ПРО»
Эксперт НП «РОСЭУ»**

© 2000-2011 КРИПТО-ПРО

№63-ФЗ «Об Электронной подписи» Что нового?



Несколько видов электронной подписи – регулирование иных аналогов собственноручной подписи

Простая электронная подпись



Усиленная электронная подпись



Неквалифицированная электронная подпись

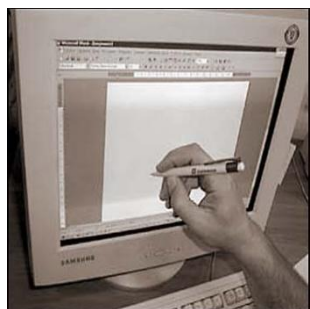
Квалифицированная электронная подпись



№63-ФЗ «Об Электронной подписи» Что нового?



Простая электронная подпись – самая неопределённая и туманная новелла



- ✓ Может реализовываться без использования криптографических средств (паролей, коды и т. д.).
- ✓ Находится внутри электронного документа;
- ✓ Формируется и проверяется с помощью ключа, который должен быть в тайне.
- ✓ Подтверждает факт формирования электронной подписи определенным лицом, но не позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания.
- ✓ Порядок применения должен определяться соглашением участников системы.

№63-ФЗ «Об Электронной подписи» Что нового?



Неквалифицированная электронная подпись – по факту, то привычная нам ЭЦП

PKI можно использовать, а можно и не использовать

- ✓ Реализуется с использованием криптографических средств.
- ✓ Позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания
- ✓ Создается с использованием средств электронной подписи.
- ✓ Могут использоваться сертификаты ключа проверки электронной подписи или не использоваться.
- ✓ Порядок применения должен определяться соглашением участников системы.



№63-ФЗ «Об Электронной подписи» Что нового?



Квалифицированная электронная подпись – подпись прямого действия



- ✓ Неквалифицированная электронная подпись
- +
- ✓ Ключ проверки электронной подписи указан в квалифицированном сертификате (сертификат издан аккредитованным удостоверяющим центром)
- ✓ Создается с использованием средств электронной подписи, получивших подтверждение соответствия требованиям ФЗ «Об ЭП»

PKI – основа построения информационной системы с квалифицированной электронной подписью

№63-ФЗ «Об Электронной подписи» Что нового?



Средства удостоверяющего центра и средства электронной подписи –
разные требования для разных видов подписи

При реализации неквалифицированной ЭП:

- 1. Средства ЭП – какие захотим (определяются оператором информационной системы, соглашением участников информационной системы)**
- 2. Средства Удостоверяющего центра – какие захотим (определяются оператором информационной системы, соглашением участников информационной системы)**

При реализации квалифицированной ЭП:

- 1. Средства ЭП – средства, получившие подтверждение соответствия требованиям, установленным ФЗ «Об ЭП»**
- 2. Средства Удостоверяющего центра – средства, получившие подтверждение соответствия требованиям, установленным ФЗ «Об ЭП»**

№63-ФЗ «Об Электронной подписи»

Что нового?



Квалифицированная электронная подпись – в первую очередь требуется наличие подзаконных актов

Правовые акты федеральных органов исполнительной власти согласно раздела «Разработка правовых актов федеральных органов исполнительной власти» Плана подготовки правовых актов в целях реализации федеральных законов «Об электронной подписи» и «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «Об электронной подписи», утвержденного распоряжением Правительства Российской Федерации от 12 июля 2011 г. № 1214-р.

№63-ФЗ «Об Электронной подписи» Что нового?



Квалифицированная электронная подпись – в первую очередь требуется наличие подзаконных актов

- | | | | | |
|-----|--|---------------------------------|------------------------|--|
| 7. | Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи (пункт 1 части 5 статьи 8 Федерального закона «Об электронной подписи») | приказ
ФСБ России | до 31 августа 2011 г. | ФСБ России,
Минкомсвязь России |
| 8. | Об утверждении требований к средствам электронной подписи (пункт 2 части 5 статьи 8 Федерального закона «Об электронной подписи») | приказ
ФСБ России | до 31 августа 2011 г. | ФСБ России,
Минкомсвязь России |
| 9. | Об утверждении требований к средствам удостоверяющего центра (пункт 2 части 5 статьи 8 Федерального закона «Об электронной подписи») | приказ
ФСБ России | до 31 августа 2011 г. | ФСБ России,
Минкомсвязь России |
| 10. | О порядке подтверждения соответствия средств электронной подписи, средств удостоверяющего центра и опубликования перечня таких средств (пункт 3 части 5 статьи 8 Федерального закона «Об электронной подписи») | приказ
ФСБ России | до 30 сентября 2011 г. | ФСБ России,
Минкомсвязь России,
Минэкономразвития России |
| 11. | О порядке аккредитации удостоверяющих центров, в том числе проверки соблюдения аккредитованными удостоверяющими центрами требований, которые установлены Федеральным законом «Об электронной подписи» и на соответствие которым эти удостоверяющие центры были аккредитованы (пункт 3 части 4 статьи 8 Федерального закона «Об электронной подписи») | приказ
Минкомсвязи
России | до 31 августа 2011 г. | Минкомсвязь России,
ФСБ России,
Минэкономразвития России |

№63-ФЗ «Об Электронной подписи» Что нового?



То, что раньше было разрешено как незапрещённое, стало явно разрешено!

- ✓ Иерархия УЦ - УЦ вправе наделить третьих лиц полномочиями по созданию и выдаче СКПЭП от УЦ, подписываемых электронной подписью, основанной на СКПЭП, выданном доверенному лицу этим УЦ.
- ✓ СКПЭП юридического лица - в случае выдачи СКПЭП юридическому лицу в качестве владельца СКПЭП наряду с указанием наименования юридического лица указывается физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности.
- ✓ Использование средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.
- ✓ Копия СКПЭП на бумажном носителе, в случае если СКПЭП создаётся в форме электронного документа.

№63-ФЗ «Об Электронной подписи»

Что нового?



То, что раньше было разрешено как незапрещённое, стало явно разрешено!

- ✓ **Одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов).**
- ✓ **Передавать ключи иным лицам (ст. 10 «обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия»)**

Реализация квалифицированной электронной подписи



Реализация квалифицированной ЭП



*После появления всех указанных подзаконных
нормативно-правовых актов можно ожидать
появление информационных систем,
использующих квалифицированную
электронную подпись.*

НЕ РАНЕЕ!!!!



Реализация электронной подписи А ещё чего надо дожидаться?

Реализация ЭП

Статья 3 ФЗ «Об ЭП», п.2
Виды электронных подписей, используемых органами исполнительной власти и органами местного самоуправления, порядок их использования, а также требования об обеспечении совместимости средств электронных подписей при организации электронного взаимодействия указанных органов между собой устанавливает Правительство Российской Федерации

Этого тоже надо будет дожидаться

Реализация квалифицированной электронной подписи

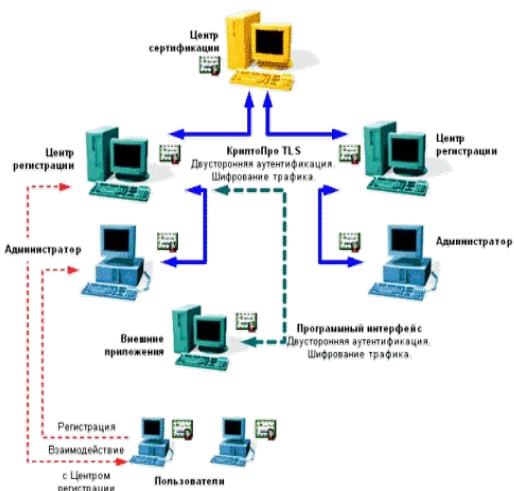
Чего ожидать и какие средства могут претендовать на гордое звание «Средство ЭП» и «Средство УЦ»?



Реализация квалифицированной ЭП

1. Вряд ли кардинально изменится взгляд на средства ЭП (средства ЭЦП) у федерального органа исполнительной власти в области обеспечения безопасности

2. Средство ЭП – СКЗИ «КриптоПро CSP» версии 3.6



3. Средство УЦ – ПАК «Удостоверяющий центр «КриптоПро УЦ» версии 1.5



PKI для Электронной подписи
ПАК «Удостоверяющий центр «КриптоПро УЦ» версии 1.5
ПАК «Службы УЦ» версии 1.5

ПАК «КриптоПро УЦ» 1.5 (исполнения 1 и 2) – есть сертификат ФСБ России.
В части требований к квалификационному сертификату позволяет заносить в сертификаты юридических лиц ОГРН (но: это не тривиальная операция для администратора УЦ, не поддерживаются сервисные функции по сортировке и фильтрации по этому полю)

ПАК «КриптоПро УЦ» 1.5 (исполнения 3 и 4) – добавлена штатная возможность заносить новые поля (в частности ОГРН) в Subject сертификата с поддержкой сервисных функций. Заключение ФСБ России – конец 2011 г. Сертификация - начало 2012 года.

ПАК «Службы УЦ» 1.5 – включает КриптоПро OCSP и КриптоПро TSP. Сертификация - начало 2012 года.



СПАСИБО ЗА ВНИМАНИЕ!

Вопросы?

КРИПТО-ПРО – ключевое слово в защите информации

<http://www.cryptopro.ru>
info@cryptopro.ru

Тел./факс:
+7 (495) 780-48-20
+7 (495) 660-23-30