暗号化 kryptographie किप्टोगाफी salauksen крыптаграфія การอ่านรหัส krip РусКрипто dulmál cripteagrafaíochta 密码 kriptografi cifrado קריפטוגרפיה mật mã họ grafia კრიპტოგრაფის криптография круптоуо́сфроп cryptography 暗号化 kriptografija رمز نویسی kriptografija و المحالية kriptografija رمز نویسی mật mã học криптографія criptografía ծածկագիտություն kryptografía კრიპტოგრაფიის криптография криπτογράφηση cryptography 暗号化 kryptographie किंप्टोगाफी salauksen крыптурарія การบนระหา ktyptografia (крурулі) круптурафия криптография крожтоура́фуют суртовуству 暗号化 kryptographie िह्योगाफी salauksen крыптаграфія การอ่านรหัส kriptografij сіфер kriptogrāfiju 암호화 crittografia dulmá criptografiju 암호화 kriptografiju 암호화 практика применения» крыптаграфія กาเอานรหัส kriptografija رمز نویسی kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado הריפטוגרפיה mật mã học криптографія criptografía ծածկագիտությո**ή** куртодгаба жей криптографія сгіртод стуртодгарну від куртодгарні курт и ктіртодгабі обладо тэ электронной подписи в современной эпохе crittografia dulmá cripteagrafaíochta 密码 kriptografi cifrado קריפטוגרפיה mật mã học криптографія criptografia ծածկագիտություն криптография крилтоура́фион cryptography 暗号化 kryptographie किप्टोगाफी salauksen крынтаграфія на НОДРИИ. διωδίμιαμη μπιτρημία kryptografía კრοპტოგრაფοου κριπτογράφηση κρυπτογράφηση cryptography 暗号化 cryptographie μανεμισμο salauks masilov cryptographie μανεμισμο salauks mât mã học криптографія criptografía δωδίμας hunıpınılı kryptografía збозტოვნაფიοს криптография крυπτογράφηση cryptography salauksen крыштаграфія การอ่านรหัส kriptografija من نويسي kript©ā2009章2014ra长尺川自丁rD+如果Ota 密 mật mã học криптографія criptografía дидицинипіріпій kryptografía збоздозбозоов

# Вынуждены:



Регламентировать использование квалифицированной ЭП

Ограничивать круг доверенных УЦ из числа аккредитованных



mật mã học криптографія criptografía δωδկագիտություն kryptografía კრიპტოგრაფიის криптография кρυπτογράφηση cryptography 暗号化

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



kriptogrāfīju 암호화 crittografīa dulmál cripteagrafaíochta 密码 kriptografī cifrado קריפטוגרפיה mật mã học криптографія criptografía ծածРегламент трименения квалифицированной Обакной Самкзен крыптаграфія מיל נעשט kriptogrāfiju 암호화 crittografía dulmál cripteagrafaíochta 密码 kriptografi cifrado קריפטוגרפיה

mật mã học криптографія criptografía δωδկագիտություն kryptografía კრიპტოგრაფიის криптография кρυπτογράφηση cryptography 暗号化

криптография κρυπτογράφηση cryptography 暗号化 kryptographie किप्टोगाफी salauksen крыптаграфія การอ่านรหัส kriptografija رمز نویسی

### 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)



криптография кролтоурафуноу стуртодгарну 暗号化 kryptographie किप्टोगाफी salauksen крыптаграфія מל יעניים ктіртодгабіји 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado קריפטוגרפיז mật mã học криптографія criptografía ошо אוייניטוגרפיז mât mã học криптографія стіртодгабіа ошо Регламент применения крвптаграфія по по криптографія ктіртодгабіји 암호화 crittografía dulmál cripteagrafaíochta 密码 kriptografí cifrado קריפטוגרפיז הווניסוגרפיז הווניסוגרפיז אוייניטוגרפיז אייניטוגרפיז אוייניטוגרפיז אוייניטוגרפיז אוייניטוגרפיז אייניטוגרפיז אוייניטוגרפיז אייניטוגרפיז אוייניטוגרפיז אייניטוגרפיז אייניטוגר

# 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).



# 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)





# 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



криптография крожтоура́фηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen крыптаграфія การอ่านรหัส kriptografija رمز نویسی kriptogrāfiju 암호화 crittografia dulmāl cripteagrafaíochta 密码 kriptografi cifrado קריפטוגרפיה mật mã học криптографія criptografia обосуждение крожтоура́фηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen крыптаграфія пазатизма kriptografija رمزنوسی kriptogrāfiju 암호화 crittografia dulmāl cripteagrafaíochta 密码 kriptografi cifrado קריפטוגרפיה mật mã học криптографія criptografia ბობსოգիտություն kryptografia გრიპტოგრაფიის криптография крожтоура́фηση cryptography 暗号化

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!



# Формально по 63-Ф3:

Порядок реализации функций УЦ определяется самим УЦ

Существенными условиями выдачи квалифицированного сертификата являются:

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

#### Ho...

Может ли эти условия выполнить нотариус или операционист банка?



## Формально по 63-Ф3:

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

#### Ho...

По житейской логике УЦ должен обеспечивать достоверность информации в сертификате



# 

#### 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 (<a href="http://www.fsb.ru/fsb/science.htm">http://www.fsb.ru/fsb/science.htm</a> <a href="http://www.fsb.ru/files/PDF/Izveshenie\_na\_sait\_po\_trebovaniyam.pdf">http://www.fsb.ru/files/PDF/Izveshenie\_na\_sait\_po\_trebovaniyam.pdf</a>)

#### Требования ФНС России

- Порядок применения квалифицированных сертификатов ключей проверки электронных подписей в информационных системах ФНС России (утверждён приказом ФНС России от 08.04.2013 MMB-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@)



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

