ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Механизмы криптографической защиты информации и единое пространство доверия электронной подписи

Аристархов Иван Владимирович

Камышев Сергей Николаевич

Приказ ФСБ России от 27 декабря 2011 года № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»

Средства ЭП Средства УЦ

Классы средств:
КС1, КС2, КС3, КВ1, КВ2, КА1

Иерархия уровней криптографической защиты информации

Приказ ФСБ России от 27 декабря 2011 года № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»

Квалифицированный сертификат

Сведения о классе средств ЭП владельца квалифицированного сертификата

Цель

Автоматизация определения результирующего уровня криптографической защиты информационного взаимодействия

Механизм включения сведений

- Дополнение certificatePolicies
- Набор объектных идентификаторов (пункт 27 Требований)
- Правила заполнения дополнения (пункт 29 Требований)

Алгоритм обработки информации о классе средств ЭП

Обработка дополнения certificatePolicies по алгоритму, описанному в RFC 5280

Построение набора объектных идентификаторов, определяющих класс средств ЭП и входящих во все сертификаты цепочки

Результат работы

Набор объектных идентификаторов, определяющих уровень криптографической защиты взаимодействия

Минимально возможное значение - объектный идентификатор для класса КС1

Уровень криптографической защиты информационного взаимодействия при обмене электронными документами, подписанными КЭП, не может превысить класс средств ЭП и средств ГУЦ

Класс средств ЭП и средств ГУЦ, с использованием которых создаются квалифицированные сертификаты для аккредитованных УЦ, является максимальным среди всех классов средств ЭП и средств УЦ, применяемых в ЕПД КЭП

Уровень криптографической защиты взаимодействия пользователей определяется минимальным классом используемых средств ЭП

Несоответствие «политик безопасности»

Последствия

- создание «ложного» квалифицированного сертификата аккредитованного УЦ
- создание «ложных» квалифицированных сертификатов пользователей
- навязывание ложной информации от имени пользователя аккредитованного УЦ

Приказ ФСБ России № 796 от 27 декабря 2012 г.

Пункт 35 «Требований к средствам удостоверяющего центра»

«При подключении средств УЦ к информационно-телекоммуникационной сети, доступ к которой не ограничен определенным кругом лиц, указанные средства должны соответствовать требованиям к средствам УЦ класса КВ2 или КА1.»

Востребованность таких средств УЦ в системах предоставления государственных и муниципальных услуг в электронной форме.

Средства УЦ, входящие в состав подсистемы ГУЦ и используемых для создания и выдачи квалифицированных сертификатов аккредитованным УЦ

класс КВ2

ГУЦ

Уполномоченный федеральный орган осуществляет функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров

Выдает аккредитованному удостоверяющему центру квалифицированный сертификат, созданный с использованием средств головного удостоверяющего центра

Механизмы

1. установления доверия ключу проверки ЭП аккредитованного УЦ (путем верификации его квалифицированного сертификата, выданного ГУЦ)

2. автоматизированной проверки статуса аккредитации УЦ в электронном документе (путем обеспечения однозначного соответствия статуса аккредитации УЦ и статуса его сертификата, выданного ГУЦ).

Уполномоченный федеральный орган

Обеспечивает хранение и круглосуточный доступ к такой информации, как наименования и адреса аккредитованных УЦ, реестр выданных и аннулированных уполномоченным федеральным органом квалифицированных сертификатов, а также перечни УЦ, аккредитация которых аннулирована, приостановлена или деятельность которых прекращена

В процессе проверки КЭП в электронном документе возможна проверка действительности аккредитации УЦ согласно указанным реестру и перечням

Альтернативные организационно-технические процедуры проверки действительности аккредитации УЦ

Особенности реализации средств ЭП и средств УЦ

Использование самоподписанных сертификатов аккредитованных УЦ в процедурах проверки КЭП

Отсутствие однозначной (автоматизированно контролируемой) взаимосвязи статуса самоподписанного сертификата аккредитованного УЦ со статусом аккредитации этого УЦ

Отсутствие у пользователя механизма автоматизированного контроля статуса аккредитации УЦ

Предложения

Обсуждение целесообразности применения самоподписанных сертификатов аккредитованных УЦ в схемах проверки КЭП

Обсуждение целесообразности иерархической схемы с ГУЦ в качестве корневого

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

СПАСИБО ЗА ВНИМАНИЕ