Проблемы стандартизации некоторых доверенных сервисов на базе PKI

Сабанов Алексей Геннадьевич,
к.т.н., доцент МГТУ им. Баумана,
Эксперт ISO/C1/SC27/WG5,
Член ТК362, РГ ТК 26, ТК122
Зам. ген. директора ЗАО "Аладдин Р.Д."."

О каких проблемах будет идти речь

- Целенаправленного планирования и создания системы стандартов, покрывающих потребности развития цифровизации страны, к сожалению, пока нет
- Планирование разработки стандартов идет снизу вверх от РГ внутри ТК, не каждая инициатива приветствуется
- Каждый ТК действует внутри своих полномочий («поляны» разделены)
- В итоге в системе национальных стандартов до сих пор нет аутентичного (официального перевода) или модернизированного варианта основного PKI-стандарта X.509 и многих других, в том числе переработанных под нормативно-правовую базу РФ
- Сегодня будем обсуждать проблемы стандартов, регулирующих доверенные сервисы, обеспечивающих юридическую силу электронным документам (ЮС ЭД)

Аладдин

Что такое доверенный сервис

Доверенный сервис - сервис безопасности, квалифицированный по определенному уровню доверия.

уровень доверия (assurance level): степень доверия, соответствующая специальной шкале, применяемой в методе обеспечения доверия. *Степень доверия обычно определяется усилиями, затраченными на выполнение определенных действий.*

метод обеспечения доверия: общепризнанная спецификация получения воспроизводимых результатов обеспечения доверия.

доверие (assurance): выполнение соответствующих действий или процедур для обеспечения **уверенности** в том, что оцениваемый объект соответствует своим целям безопасности.

уверенность (confidence): убежденность в том, что оцениваемый объект будет функционировать в соответствии с заданным или установленным порядком (то есть корректно, надежно, эффективно, в соответствии с политикой безопасности) ГОСТ Р 54581-2011/ISO/IEC/TR 15443-1:2005, пункты 2.4,10,11,18).

Аладдин

Какие доверенные сервисы на базе PKI нужны для ЮС ЭД?

1. Аутентификация (ГОСТ Р 58833-2020; ISO 29115: 2013, ISO/IEC 10181-2:1996, 9798-3:1998);
2. Электронная подпись (ГОСТ Р 34.10-2012; ISO 7498-2, ISO/IEC 13888-1);
3. Метка доверенного времени (RFC 3161 «Time-Stamp Protocol (TSP)», ставится TSA (Time-Stamp-Authority);
4. Валидация сертификата ключа проверки подписи (RFC 2459);
5. Проверка полномочий подписанта (ITU-T X.509, v.7);
6. Доверенная гарантированная доставка документов и сообщений.

Аладдин

Роль аутентификации в PKI

- Идентификация и аутентификация – сервисы безопасности на базе PKI, обеспечивающие совместно с другими сервисами (штампы времени, проверка валидности цифровых сертификатов, электронная подпись, проверка полномочий, доверенная гарантированная доставка сообщений и документов) достижение определенного уровня доверия к электронным транзакциям, сообщениям и документам;

- Идентификация и аутентификация должны обеспечивать достижение определенного уровня доверия к определению лица, подписавшего документ. Для этого требуется корректное решение задачи доступа субъекта прикладному ПО, из которого поступает вызов СКЗИ для подписи документа;

- Аутентификация совместно с волеизъявлением при подписании документа, наличия штампа времени и проверки полномочий позволяет решить задачу неотказуемости от совершения подписи.

Аладдин

Аутентификация

1. Решение Коллеги Евразийской Комиссии от 9 июля 2018 г. N 110 «Об УЦ ЕАК»
2. Решение Коллеги Евразийской Комиссии от 25 сентября 2018 г. N 154 «Об УЦ службы ДТС интегрированной ИС ЕАС»
3. Решение Коллегии ЕАС Рекомендация от 12 марта 2019 г. N 9 «О перечне стандартов и рекомендаций в области ИБ, применяемых в рамках реализации цифровой повестки Евразийского экономического союза»
4. Федеральный закон 476-ФЗ, ст.8, ч.4, п.4.1; ст.15,ч.1,п.1; ст.16,ч.3.1 (остальные 12 раз упоминается ЕСИА).

Аладдин

Метка доверенного времени

1. Решение Коллеги Евразийской Комиссии от 9 июля 2018 г. N 110 «Об УЦ ЕАК» (структура штампа времени)

2. Решение Коллеги Евразийской Комиссии от 25 сентября 2018 г. N 154 «Об УЦ службы ДТС интегрированной ИС ЕАС» (упоминание RFC 3161)

3. Решение Коллегии ЕАС Рекомендация от 12 марта 2019 г. N 9 «О перечне стандартов и рекомендаций в области ИБ, применяемых в рамках реализации цифровой повестки Евразийского экономического союза» (перечень стандартов)

4. Постановление Правительства от 29 декабря 2008 г. N 1057 «Об утверждении Положения о межведомственной интегрированной автоматизированной системе федеральных органов исполнительной власти, осуществляющих контроль в пунктах пропуска через государственную границу Российской Федерации» (…нужен штамп времени)

Аладдин

Метка доверенного времени – детализация 1

Решение Коллеги Евразийской Комиссии от 9 июля 2018 г. N 110 «Об УЦ ЕАК»

7.4. Структура штампа времени

Все ответы TSP-службы (штампы времени) содержат следующие поля:

Policy ID - идентификатор политики, в соответствии с которой выпущен штамп времени;

Serial Number - серийный номер (идентификатор) штампа времени;

Accuracy (microseconds) - точность часов TSP-службы, мкс;

Ordering: 0; HasNonce: 1; TSA - идентификационные данные TSP-службы;

Stamp time - дата и время подписания штампа времени TSP-службой;

Hash algorithm - идентификатор алгоритма хеширования;

Hash size - размер хеша, байт; Hash - значение хеша;

Certificate of signer of time-stamp: идентификационные данные Владельца сертификата TSP-службы (Уполномоченного лица УЦ Комиссии);

Verification of time-stamp: результат проверки штампа времени.

Verification of certificate of signer of time-stamp: результат проверки сертификата оператора TSP-службы. Certificates from time-stamp (1):

Common Name = TSP-служба УЦ Комиссии, OU = УЦ Евразийской экономической комиссии, O = Евразийская экономическая комиссия, C = RU, E = info@eecommission.org

Метка доверенного времени – детализация 2

Решение Коллеги Евразийской Комиссии от 25 сентября 2018 г. N 154 «Об УЦ службы ДТС интегрированной ИС ЕАС»

1.2.2.2. Сервис штампов времени

В инфраструктуре открытых ключей интегрированной системы реализованы сервисы штампов времени. Сервисы штампов времени генерируют штампы времени в соответствии с рекомендациями RFC 3161 (Time-Stamp Protocol) - протоколом штампов времени. Каждый штамп времени удостоверяется исключительно при помощи ключей ЭЦП, созданных специально для сервисов штампов времени.

Решение Коллегии ЕАС Рек. от 12 марта 2019 г. N 9 перечень стандартов

99. СТБ 34.101.78-2018 "Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей".

101. СТБ 34.101.80-2018 "Информационные технологии и безопасность. Расширенные электронные цифровые подписи".

102. СТБ 34.101.81-2018 "Информационные технологии и безопасность. Протоколы службы заверения данных".

103. СТБ 34.101.82-2018 "Информационные технологии и безопасность. Протокол простановки штампа времени".

Сервисы безопасности в федеральных законах

№ ФЗ	Аутентификация	ЭП	Штамп времени	Валидация	Полномочия	ДТС
476	Да	Да	-	Да	Да	Да
149	-	Да	-	-	-	-
63	-	Да	-	Да	Да	Да

Доверенная третья сторона по 63-ФЗ

Статья 18.1. Доверенная третья сторона (с 1 января 2021г.)

Доверенная третья сторона оказывает услуги:

1) по подтверждению **действительности электронных подписей**, используемых при подписании электронного документа, в том числе установлению фактов того, что соответствующие сертификаты действительны на определенный момент времени, созданы и выданы аккредитованными удостоверяющими центрами, аккредитация которых действительна на день выдачи этих сертификатов;

2) по проверке **соответствия всех квалифицированных сертификатов**, используемых при подписании электронного документа, требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами;

3) по проверке **полномочий** участников электронного взаимодействия;

4) по **созданию и подписанию** квалифицированной электронной подписью доверенной третьей стороны квитанции с результатом проверки квалифицированной электронной подписи в электронном документе с достоверной информацией о моменте ее подписания;

5) по хранению данных, в том числе документированию выполняемых доверенной третьей стороной операций.

Аладдин

Стандарты ГОСТ Р

Аутентичный	Национальный стандарт аутентичен исходному, если он аутентичен по техническому содержанию и структуре и изложению или аутентичен по техническому содержанию и структуре, но может включать незначительные редакционные изменения
Модифицированный	Национальный стандарт модифицирован по отношению к исходному, если технические отклонения, которые допустимы, четко идентифицированы и их причины обоснованы. Национальный стандарт воспроизводит структуру исходного стандарта, однако изменения в структуре допускаются при условии, что измененная структура обеспечивает легкое сравнение содержания двух стандартов. Модификация стандарта может также включать в себя изменения, допускаемые при аутентичном соответствии
Неэквивалентный (переработанный)	Национальный стандарт является неэквивалентным исходному стандарту по техническому содержанию и структуре, а любые изменения не были четко идентифицированы. Очевидно отсутствие четкого соответствия между исходным стандартом и национальным

Подведем итоги

Название сервиса безопасности	Аутентификация	ЭП	Штамп времени	Валидация	Полномочия
Упоминание о сервисе в федеральных законах	Да	Да	-	Да	Да
Технические требования в ФЗ и подзаконных актах	-	Да	-	-	-
Упоминание о сервисе в офиц. документах ЕАЭС	Да	Да	Да	Да	Да
Требования к технической реализации в офиц. документах ЕАЭС	-	Да	Да	Да	-
Требования к сервису в документах по стандартизации (ГОСТ)	Да	Да	-	-	-
Технические требования в международных стандартах	Да	Да	Да	Да	Да

Аладдин

Спасибо!

Будь собой в электронном мире! ®

Контакты:

Алексей Сабанов
asabanov@mail.ru
+7-985-924-52-09

Будь собой
в электронном мире! ®

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.17
Лицензии ФСБ России № 12632 Н от 20.12.12, № 30419 от 16.08.17
Лицензия Министерства обороны РФ № 1823 от 26.08.19
Система менеджмента качества компании соответствует требованиям стандарта ГОСТ Р ИСО 9001-2015 (ISO 9001:2015)
Сертификат соответствия - № РОСС RU.ФК14.К00011 от 20.07.18
Система менеджмента качества компании сертифицирована в системе добровольной сертификации "Военный Регистр" (РОСС RU.И1975.04ГШ02) и соответствует требованиям стандарта ГОСТ РВ 0015-002-2012
Сертификат соответствия - № ВР 21.1.13537-2019 от 25.04.19

Тел.: +7 (495) 223-00-01 E-mail: aladdin@aladdin-rd.ru Web: www.aladdin-rd.ru

Приведённая информация актуальна по состоянию на ***Сентябрь 2020 г.***