РУТОКЕН

XVII международная конференция по проблематике инфраструктуры открытых ключей и электронной подписи

Вырываясь из плена традиций

Владимир Иванов
Компания «Актив»
Директор по развитию

Форум
Россия 2019

Классификация ЭП

- Простая ЭП
- Усиленная ЭП
- Квалифицированная ЭП

Юридическая значимость документов

- Юридической значимостью может обладать документ, подписанный фактически любым видом ЭП
- Не зафиксированы виды документов, для обеспечения юридической значимости которых требуется тот или иной вид ЭП
- Не зафиксированы виды документов, которые не могут быть оформлены в электронном виде

Классификация СКЗИ

- Средства ЭП относятся к СКЗИ
- 6 типов нарушителей
- 6 классов СКЗИ
- Класс СКЗИ выбирается оператором системы в зависимости от типа нарушителя

Хранение ключей и создание подписи

- Файл, КЭП создается в оперативной памяти ПК
- Реестр, КЭП создается в оперативной памяти ПК
- Пассивный КН, КЭП создается в оперативной памяти ПК
- Активный КН, КЭП создается в оперативной памяти КН
- Интеллектуальный КН, КЭП создается в оперативной памяти КН
- DSS, КЭП создается в оперативной памяти DSS

РУТОКЕН

Связь класса СКЗИ с доверием к ЭП и юридической значимостью документов

Уровни доверия к аутентификации (Правительство Канады)

- **at Assurance Level 1:**
  - the minimum identity assurance requirements set out in the Guideline on Identity Assurance for Assurance Level 1 must be met
  - any of the token types identified in ITSP.030.31: User Authentication Guidance for Information Technology Systems for Assurance Level 1 or higher can be used for user authentication
- **at Assurance Level 2:**
  - the minimum identity assurance requirements set out in the Guideline on Identity Assurance for Assurance Level 2 must be met
  - any of the token types identified in ITSP.030.31 for Assurance Level 2 or higher can be used for authentication
- **at Assurance Level 3:**
  - the minimum identity assurance requirements set out in the Guideline on Identity Assurance for Assurance Level 3 must be met
  - two-factor authentication is required (refer to Appendix B for additional information)
- **at Assurance Level 4:**
  - the minimum identity assurance requirements set out in the Guideline on Identity Assurance for Assurance Level 4 must be met
  - a multi-factor cryptographic hardware device such as a smart card must be used

Government of Canada Guidance on Using Electronic Signatures
From Treasury Board of Canada Secretariat

Виды документов и соответствующие уровни доверия (Правительство Канады)

- Assurance Level 4
  - Онлайновые финансовые транзакции в случаях, когда требуется подпись
  - Заключение внешних контрактов на сумму, превышающую определенный предел
- Assurance Level 3
  - Утверждение заявления сотрудника на возмещение расходов
  - Заключение внешних контрактов на сумму, не превышающую установленного порога
- Assurance Level 2
  - Заявление на отпуск и его подтверждение
  - Заявка на поездку и ее подтверждение
  - Заявление сотрудника на возмещение расходов
- Assurance Level 1
  - Ежедневная переписка с низким уровнем важности

Виды документов, которые нельзя подписывать ЭП (Канада)

- Некоторые виды доверенностей
- Кодицилы и завещания
- Завещательные трасты
- Операции с недвижимостью
- Кредитные средства обращения и платежа (чеки, бонды и т.п.)
- Некоторые семейные документы, такие как бракоразводные и документы по усыновлению
- Некоторые требуемые по закону документы по раскрытию информации
- Различные официальные судебные документы

eIDAS: квалифицированная подпись

- advanced electronic signature
- that is created by a **qualified electronic signature creation device**,
- and which is based on a qualified certificate for electronic signatures

eIDAS: Qualified signature creation device

Используются технические и организационные меры которые гарантируют:

- Конфиденциальность ключей подписи
- Создание ключей подписи принятыми криптографическими способами
- Использование ключей подписи исключительно их владельцем
- Подтвержденное соответствие стандартам для квалифицированной подписи

Hardware Secure Module (HSM), USB token, Smart card

Защита ключей аутентификации и подписи

- Для хранения ключей и вычисления ЭП используется активный или интеллектуальный ключевой носитель — USB-токен или смарт-карта
- Извлечь и скопировать ключи невозможно
- Подпись создается в памяти ключевого носителя

Рутокен ЭЦП 2.0 + КриптоПро CSP 5.0

КРИПТОПРО + РУТОКЕН =

- Поддержка объектов PKCS#11
- Поддержка технологии ФКН-2
- Срок действия закрытого ключа – 3 года

Проекты, использующие активные и интеллектуальные ключевые носители

- ЕГАИС алкогольной розницы
- Защита транзакций в ДБО
- Защита КИМ ЕГЭ и ОГЭ
- Он-лайн кассы по 54-ФЗ

Какие выходы?

- Определить уровни доверия к подписи в зависимости от вида подписи и технологии
- Определить квалифицированную подпись аналогично европейскому законодательству и установить высший уровень доверия для нее
- Определить перечень видов документов, для обеспечения юридической значимости которых требуется тот или иной уровень доверия к подписи
- Определить список видов документов, которые нельзя оформлять в электронном виде

Контактная информация

Владимир Иванов

Электронная почта:

vov@rutoken.ru

Телефон:

+7 903 763-84-24
+7 495 925-77-90

Сайты:

www.rutoken.ru
www.aktiv-company.ru