Глоссарий доклада

1. ЭЛЕКТРОННЫЙ ДОКУМЕНТ.

- Документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационном сетям или обработки в информационных системах. *ФЗ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».*

- Документ, представленный в электронном виде в соответствии с требованиями формата для данного вида документа. *«Методические рекомендации по организации электронного документооборота при представлении налоговых деклараций (расчетов) в электронном виде по телекоммуникационным каналам связи», утв. Приказом ФНС от 02.11.2009 № ММ-7-6/534@.*

- Запись на машинном носителе информации, воспроизводимой на экране дисплея или бумажном носителе в порядке, установленном Национальным стандартом РФ ГОСТ Р 52292-2004 «Информационная технология. Электронный обмен информацией. Термины и определения». *Приказ Генпрокуратуры РФ от 31.05.2011 № 153.*

2. ЭЛЕКТРОННАЯ ПОДПИСЬ.

Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. *ФЗ от 06.04.2011 № 63-ФЗ «Об электронной подписи».*

Виды электронной подписи:

- простая электронная подпись;

- усиленная электронная подпись (усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись).

2.1. Простая электронная подпись.

Электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

2.2. Усиленная неквалифицированная электронная подпись.

Электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

- позволяет определить лицо, подписавшее электронный документ;

- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

- создается с использованием средств электронной подписи.

2.3. Усиленная квалифицированная электронная подпись.

Электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- ключ проверки электронной подписи указан в квалифицированном сертификате;

- для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

2.4. Ключ проверки электронной подписи.

Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи. *ФЗ от 06.04.2011 № 63-ФЗ «Об электронной подписи».*

2.5. Сертификат ключа проверки электронной подписи.

Электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и

подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи. *ФЗ от 06.04.2011 № 63-ФЗ «Об электронной подписи».*

2.6. Квалифицированный сертификат ключа проверки электронной подписи.

Сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи. *ФЗ от 06.04.2011 № 63-ФЗ «Об электронной подписи».*

2.7. Удостоверяющий центр.

Юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3. ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ. *НЕ ДЕЙСТВУЕТ*

Реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе». *ФЗ от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи», утратил силу с 01.07.2013.*

4. СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ.

Средства шифрования - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче.

- Аппаратные шифровальные (криптографические) средства - устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин.

- Программные шифровальные (криптографические) средства - программы для электронных вычислительных машин и их части, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных шифровальных (криптографических) средствах, информационных системах и телекоммуникационных системах, защищенных с использованием шифровальных (криптографических) средств.

- Программно-аппаратные шифровальные (криптографические) средства - устройства и их компоненты (за исключением информационных систем и телекоммуникационных систем), в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации с использованием программ для электронных вычислительных машин, предназначенных для осуществления этих преобразований информации или их части.

«Положение о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», утв. Постановлением Правительства РФ от 16.04.2012 № 313.

Средства криптографической защиты информации, или шифровальные (криптографические) средства (СКЗИ), предназначены для защиты информации при ее обработке, хранении и передаче по каналам связи. *Стандарт Банка России СТО БР ИББС – 1.0- 2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации». Принят распоряжением Банка России от 21.06.2010 № Р-705.*

5. 3D – SECURE.

Защищенный протокол авторизации пользователей для CNP-операций (без присутствия карты). Данная технология разработана для безопасности оплаты товаров и услуг в Интернете. Изначально протокол был предложен платежной системой VISA, но потом с некоторыми изменениями был принят и другими. У VISA протокол называется Verified by Visa (VbV), у MasterCard - MasterCard SecureCode (MCC), а у JCB International - J/Secure.

Данный протокол добавляет дополнительный шаг авторизации пользователя при оплате покупки в интернет-магазине. На первом шаге используется: номер карты, срок ее действия, имя держателя карты и код проверки ее подлинности (например, CVC2). На втором шаге, используя протокол 3D-Secure, сайт магазина показывает страницу банка - эмитента карты, на которой предлагается ввести дополнительный защитный код. Его клиент банка может получить: посредством СМС-сообщения на свой мобильный телефон, с помощью карточки разовых кодов или специального устройства, а также код может быть постоянным, заранее установленным самим клиентом.

Вся передаваемая информация от покупателя сохраняется на платежном сервере банка-эмитента, и интернет-магазин не имеет к ней никакого доступа. Это защищает данные от хищения.

При использовании протокола 3D-Secure ответственность за такие операции переносится с торговой точки на банк или клиента.

6. OID (OBJECT IDENTIFIER)

Объектные идентификаторы, определяющие отношения, при осуществлении которых электронный документ, подписанный электронной подписью, будет иметь юридическое значение.

OID, зарегистрированные в удостоверяющем центре, включаются в состав следующих расширений сертификата ключа подписи: Key Usage (использование ключа), Extended Key Usage (расширенное использование ключа), Application Policy (политики применения сертификата).

7. СЕРВИС «ДОВЕРЕННАЯ ТРЕТЬЯ СТОРОНА» (ДТС).

Организация, наделенная правом в соответствии с законодательством государства осуществлять деятельность по проверке электронной цифровой подписи в электронных документах в фиксированный момент времени в отношении составителя и (или) адресата электронного документа. *Соглашение между Правительством РФ, Правительством Республики Беларусь и Правительством Республики Казахстан от 21.09.2010 «О применении информационных технологий при обмене электронными документами во внешней и взаимной торговле на единой таможенной территории Таможенного союза».*

8. КОНТЕЙНЕР ЗАКРЫТОГО КЛЮЧА.

Набор файлов, в котором содержится сертификат открытого ключа и закрытый ключ пользователя.

9. КРИПТОПРОВАЙДЕР (CRYPTOGRAPHY SERVICE PROVIDER, CSP).

Независимый модуль, позволяющий осуществлять криптографические операции в операционных системах Microsoft, управление которым происходит с помощью функций CryptoAPI.

10. ПРОТОКОЛ SSL (SECURE SOCKET LAYER).

Протокол защищенных соединений - криптографический протокол, который обеспечивает установление безопасного соединения между клиентом и сервером. SSL изначально разработан компанией Netscape Communications. Впоследствии на

основании протокола SSL 3.0 был разработан и принят стандарт RFC, получивший имя TLS.

Протокол обеспечивает конфиденциальность обмена данными между клиентом и сервером, использующими TCP/IP, причём для шифрования используется асимметричный алгоритм с открытым ключом. При шифровании с открытым ключом используются два ключа, открытый и секретный, причем любой из них может использоваться для шифрования сообщения. Если для шифрования сообщения был использован открытый ключ, то для расшифровки должен использоваться секретный, и наоборот. В такой ситуации возможны два способа использования ключей. Во-первых, сторона, хранящая в тайне секретный ключ и опубликовавшая открытый, может принимать от противоположной стороны сообщения, зашифрованные открытым ключом, которые не может прочитать никто, кроме нее (ведь для расшифровки требуется секретный ключ, известный только ей). Во-вторых, с помощью закрытого ключа сторона-обладатель закрытого ключа может создавать зашифрованные сообщения, которые может прочесть кто угодно (ведь для расшифровки нужен открытый ключ, доступный всем), но при этом прочитавший может быть уверен, что это сообщение было создано стороной-обладателем секретного ключа.