Доверенная цифровая подпись

Анилиз схем доверенной цифровой подписи и разработка модификации

Бугро Н.С.
ПОИТ, ФКСиС
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
e-mail: n.bugro@tut.by

***Аннотация* — В данном докладе анализируется развитие схем доверенной цифровой подписи, выявляются их недостатки. На основании анализа формируются требования к схеме доверенной цифровой подписи, и рассматривается схема, учитывающая описанные недостатки.**

Ключевые слова: криптография; алгоритм; протокол; электронная цифровая подпись; модификация

I. Введение

На сегодняшний день широко распространено использование электронных документов. Ввиду того, что обмен документами зачастую совершается по открытым каналам, возникают задачи сохранения секретности документа, проверки его целостности и аутентификации создателя документа. Наиболее эффективным решением данных задач является использование криптографических алгоритмов, в частности для аутентификации создателя документа наиболее подходящим методом является использование электронной цифровой подписи. Она позволяет контролировать целостность документа, аутентифицировать создателя документа, а также гарантирует то, что создатель документа не сможет отречься от авторства документа.

Тем не менее, традиционная цифровая подпись неудобна для некоторых практических задач. Например, в ситуации, когда лицу, ответственному за подпись документов, требуется отлучиться от своих обязанностей на некоторое время, традиционная цифровая подпись может предложить лишь передать секретный ключ доверенному лицу, что не является безопасным. В подобных нестандартных ситуациях приходится прибегать к модификациям цифровой подписи, таким как доверенная цифровая подпись (необходима в ситуации описанной выше), групповая цифровая подпись, слепая цифровая подпись и др.

II. Основные понятия

Доверенная цифровая подпись – это цифровая подпись, в которой изначальный подписчик передает свою возможность подписывать документы доверенному лицу, а доверенное лицо получает возможность подписывать документы от имени изначального подписчика [1].

III. Анализ существующих схем доверенной цифровой подписи

Первая схема была предложена в 1996 году [2,3]. Данная схема обладает такими недостатками, как неограниченная передача прав (доверенное лицо имеет возможность подписывать документы любого типа) и возможность доверенного лица передать право подписи от имени изначального подписчика третьему лицу. Данные недостатки приводят к тому, что доверенное лицо имеет возможность злоупотреблять доверенной подписью.

Позднее была предложена надежная схема пороговой доверенной цифровой подписи с ограничением типа подписываемых документов [2,4]. Однако на практике и у данной подписи были выявлены недостатки: данная подпись не поддерживает отзыва доверенности, хотя во многих ситуациях возникает необходимость в подобном механизме. Также позже было доказано, что пороговые схемы доверенной цифровой подписи не являются безопасными [2,5].

В 2006 была предложена схема доверенной цифровой подписи, использующей метки времени [2,6]. Использование меток времени позволило использовать механизм проверки срока истечения доверенности, а также позволяет отзывать доверенность до истечения срока по требованию изначального подписчика.

W.B.Lee и T.H.Chen предложили схему доверенной цифровой подписи, которая базируется на существующих криптографических алгоритмах хеширования, электронной цифровой подписи и использует службы меток времени [7]. Суть протокола заключается в том, что при инициализации схемы владелец подписи генерирует ключевую пару для доверенности, ставит метку времени и подписывает полученную доверенность. Далее сгенерированная доверенность передается доверенной стороне, которая, получив секретный ключ и подписанную доверенность, получает возможность подписывать документы. Для проверки подписи третья сторона использует вложенную доверенность. Положительной стороной данной схемы является то, что она использует проверенные временем математические алгоритмы, которые на данный момент имеют высокую криптостойкость. Также в случае, если некоторые алгоритмы будут взломаны, их можно заменить на другие и схема не потеряет актуальности. Одним из недостатков данной схемы является обязательное наличие защищенного канала для передачи доверенности и секретного ключа. Другим недостатком является то, что секретный доверенный ключ известен двум сторонам – владельцу подписи и доверенной стороне. Данный факт приводит к тому, что невозможно точно определить кем поставлена подпись.

IV. Разработанная модификация

На основе схемы доверенной цифровой подписи W.B.Lee и T.H.Chen разработана модифицированная схема, которая устраняет выявленные недостатки рассмотренной схемы.

Модификация схемы заключается в том, что ключевую пару для доверенной подписи генерирует не владелец подписи, а доверенная сторона. Далее доверенная сторона формирует запрос на получение доверенности, в который вкладывает открытый доверенной ключ. Получившийся запрос подписывается личным ключом доверенной стороны и передается владельцу подписи. После получения запроса на получение доверенности и его верификации владелец подписи генерирует доверенность и передает ее доверенной стороне. Т.к. секретная составляющая

доверенного ключа не передается по каналам связи, то необходимости в наличии секретного канала связи не возникает. Также доверенный секретный ключ остается известным только доверенной стороне, т.е. владелец подписи не имеет возможности подписывать документ от имени доверенной стороны.

V. Практические результаты

На основе разработанной модифицированной схемы разработана криптографическая библиотека и использующее е приложение. Реализованная схема использует алгоритм хеширования SHA1, алгоритмы электронной цифровой подписи RSA и DSA, а также центры сертификации и службы меток времени.

Использование центров сертификации позволило использовать механизмы отзыва доверенности, а использование служб меток времени делает возможным ограничение срока действия доверенности и контроль за его выполнением.

Анализ результатов работы программного средства показал практическую работоспособность разработанной схемы доверенной цифровой подписи, гибкость и удобство ее использования. Анализ времени выполнения операция показал высокую зависимость результатов от времени обращения к центрам сертификации и службам меток времени. Также значительное влияние на скорость выполнения операций оказывают используемые алгоритмы хеширования и электронной цифровой подписи. Сравнительный анализ времени выполнения генерации и верификации подписи для алгоритмов электронной цифровой подписи RSA, DSA и доверенной цифровой подписи с использованием RSA и DSA показан на (1).

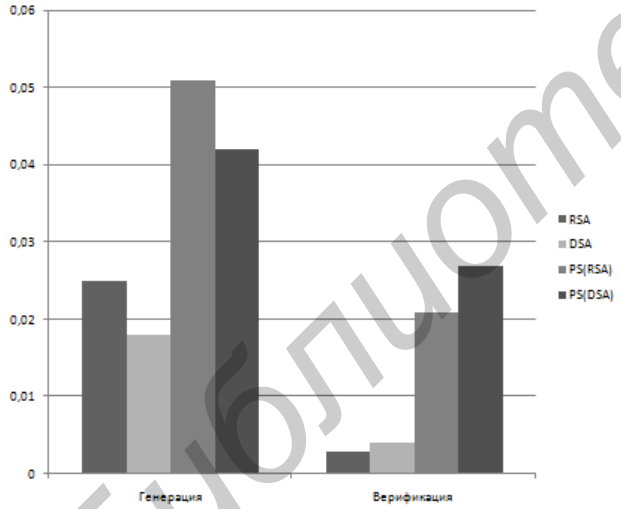

Рис. 1. Время выполнения операций

VI. Заключение

Схемы доверенной цифровой подписи появились не так давно, однако их уже описано достаточно большое их количество. Причиной этого может служить то, что определение всех требований к данному механизму невозможно, и первые схемы отвечали только некоторым базовым требованиям. Со временем в разработанных схемах находились уязвимости и требования ужесточались. На сегодняшний день большинство известных схем доверенной цифровой подписи считаются небезопасными. Исходя из данной тенденции, выглядит разумным использование протокольных схем, которые изолируют механизм доверенной цифровой подписи от математических алгоритмов цифровой подписи, и т.о. уменьшают вероятность выявления в математических алгоритмах уязвимостей. Предложенная модифицированная схема отвечает всем описанным требованиям, а реализация имеет модульную структуру и позволяет использовать любые алгоритмы хеширования, электронной цифровой подписи, центры сертификации и службы меток времени. Схема рекомендуется для использования в случае необходимости высокой гибкости, криптостойкости и низких требованиях к производительности и размеру генерируемой доверенной цифровой подписи.

[1] Б.Шнайер. “Прикладная криптография” - М.:Издательство ТРИУМФ, 2002 – 816с.

[2] M.Das, A.Saxena, D.Phatak. “Algorithms and approaches of proxy signature”, International Journal of Network Security, Nov 2009.

[3] M.Mambo, K.Usuda, E.Okamoto. “Proxy signatures: Delegation of the power to sign messages”, Transaction Fundamentals, 1996/9.

[4] S.Kim, S.Park, D.Won. “Proxy signatures revisited”, Proceedings of Information and Communications Security, 1997.

[5] H.Sun, N.Lee, H.Wang. “Threshold proxy signatures”, Proceedings of Computer & Digital Techniques, 1999/5.

[6] E.Lu, C.Huang. “A time-stamping service”, International Journal of Network Security, 2006/1.

[7] W.Lee, T.Chen. “Constructing a proxy signature scheme based on existing security mechanisms”, Information & Security, 2003/9.