УДК 004

ПРОВЕРКА ПОДЛИННОСТИ ЭЛЕКТРОННЫХ ПОДПИСЕЙ В PDF ФАЙЛАХ

Чан Тхюи Зунг
Научный руководитель: А.А. Вичугова, к.т.н., доцент каф. АиКС, ИК, ТПУ
Национальный исследовательский Томский политехнический университет
634050, Россия, г. Томск, пр. Ленина, 30

Аннотация. *A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.*

Key words: Electronic signatures, PDF, RSA, MD5, Certificate.
Ключевые слова: Электронная подпись, закрытый ключ, открытый ключ, сертификат, хэш код.

Постановка задачи

На сегодняшний день основная часть информации, которой обмениваются частные лица и организации, представлена в электронном виде. Поэтому важно обеспечить защиту электронных данных, включая проверку документа на корректность информации о авторе и на целостность. Это позволит гарантировать подлинность документа, то, что документ не был изменен другим лицом. Для решения этой задачи широко применяется электронная подпись. Данная работа посвящена анализу применения технологий электронной подписи для подписания и верификации *PDF*-документов.

Принцип работы

Для подписания и проверки электронной подписи выбраны следующие криптографические алгоритмы: с открытым ключом *RSA* и хеширования *MD5*. Алгоритм *MD5* позволяет получить сокращенную информацию о документе, на основе данной информации можно судить о целостности документа.

Для шифрования и дешифрования подписи применяется алгоритм *RSA*, который требует пары ключей – открытого и закрытого. Для шифрования подписи требуется закрытый ключ, которых представлен в виде *pfx*-файла. Подпись содержит информацию о авторе, времена, месте и рисунке подписи, также хеш-код документа, полученный с помощью алгоритма *MD5*. Этот закрытый ключ использует только автор документа и он не доступен другим лицам. Зашифрованная подпись прикрепится к PDF-документу, и этот документ направляется получателю. Открытый ключ, сохраняющий в файле с расширением *cer*, свободно распространяется и используется для дешифрования и верификации электронной подписи. Пользователь использует открытый ключ для чтения информации о авторе и хеш-коде документа. Документ прошел проверку если информация о авторе верна и документ не был изменен другим лицом (хеш-код полученного документа и хеш-код, полученный после дешифрования подписи, совпадают).

Результат работы

Вышеописанные теоретические положения были реализованы на практике в виде программного приложения «Электронно-цифровая подпись». Пользовательский интерфейс программы состоит из *2* закладок: «Цифровые подписи» и «Проверить подписи».

На закладке «Цифровые подписи» автору документа необходимо указать путь к оригинальному *pdf*-файлу, путь к файлу закрытого ключа с расширением pfx, и путь к файлу, который будет получен после подписания. После указания всех путей к файлам, нажав кнопку

«Подписать» появится окно «Подробности», где пользователь может заполнять информацию о подписи, в том числе подписчик, место, время и рисунок подписи, также положение электронной подписи на *pdf*-документе. Если закрытый ключ и информация подписи верны, нажав кнопку «Подписать», электронная подпись будет зашифрована и прикрепится к *pdf*-файлу. Пользователь теперь может отправить зашифрованный документ получателю.

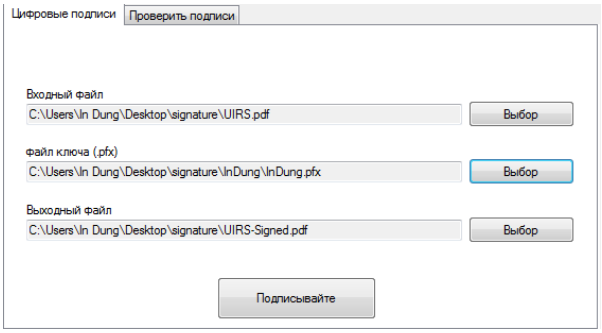

Рис. 1. Приложение «Электронно-цифровая подпись»

На закладке «Проверить подписи» получателю необходимо указать путь к полученным документу и файлу открытого ключа с расширением *cer*. Нажав кнопку «Проверить», начнется процесс верификации документа. Если открытый ключ соответствует закрытому ключу автора документа, вся информация подписи верна, имеется совпадение хеш-кода полученного документа и хеш-кода, полученный после дешифрования подписи, то выдается информация о корректности автора и целостности документа с подробной информацией о авторе. Результат получается на рис. 2.

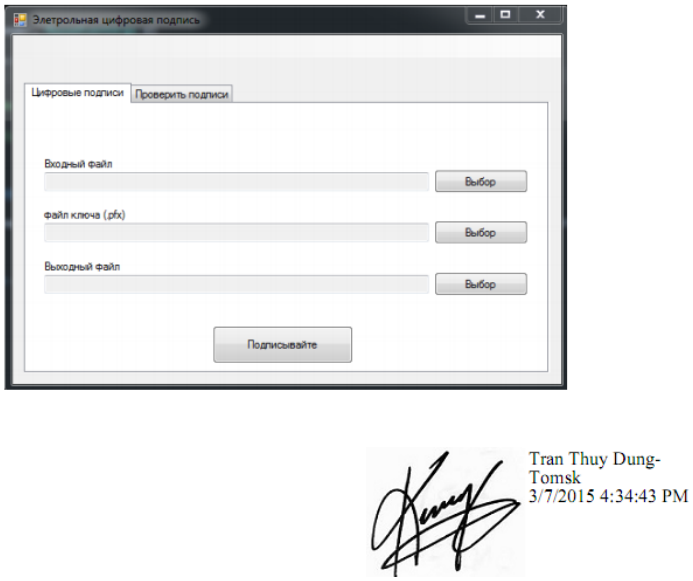

Рис. 2. Результат приложения

Разработанное программное обеспечение может быть использовано в качестве средства изучения и демонстрации возможностей криптографических технологий электронной подписи.

Список литературы

1. http://en.wikipedia.org/wiki/Digital_signature.
2. Digital Signatures for PDF documents.