ний яркости. Параметр ε используется для остановки алгоритма, когда изменения на каждой итерации становятся малы по сравнению с заданным параметром. Такие меры применяются, когда важным соображением является скорость вычислений.

Список литературы

1. http://en.wikipedia.org/wiki/Image_segmentation
2. Гонсалес Р., Вудс Р., Эддинс С. Цифровая обработка изображений в среде MATLAB, 2000.

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ ФАЙЛОВ PDF

Чан Тхюи Зунг
(г. Томск, Томский политехнический университет)
E-mail: bluesky25792@gmail.com

DIGITAL SIGNATURES FOR PDF DOCUMENT

Tran Thuy Dung
(s. Tomsk, Tomsk Polytechnik University)

Abstract. 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.

Keywords.: Electronic signatures, PDF, RSA, MD5, Certificate.

Постановка задачи. Информация является одним из ценнейших предметов современной жизни. Получение доступа к ней с появлением глобальных компьютерных сетей стало невероятно простым. 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».

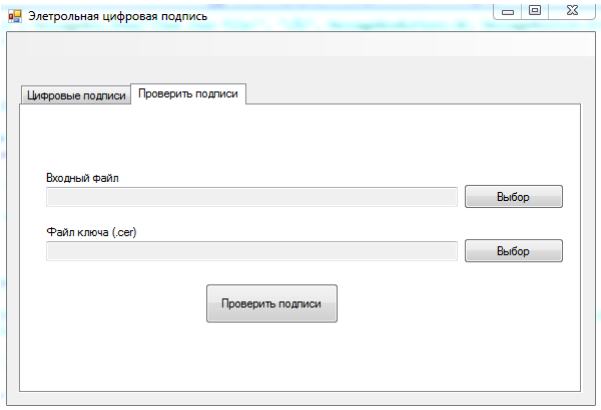

Рис. 1. Приложение «Электронно-цифровая подпись»

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.

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.

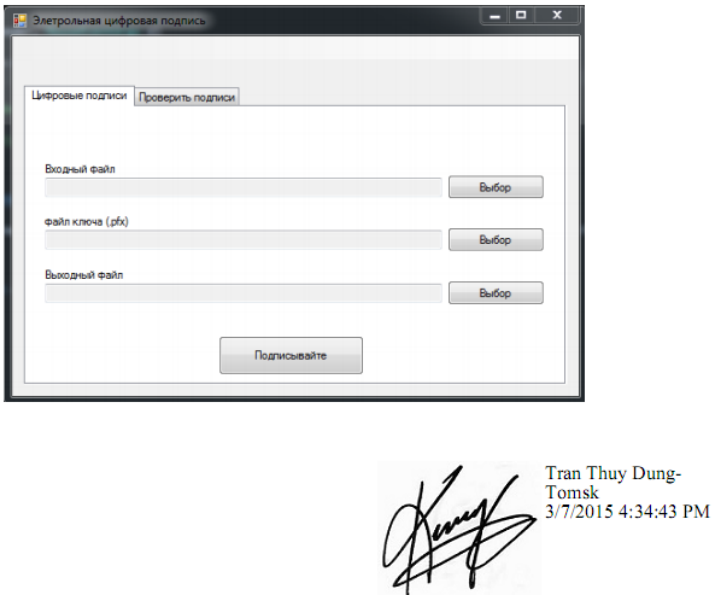

Рис. 2. Результат приложения

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.

АВТОМАТИЗИРОВАННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ ПРАВОВОЙ ИНФОРМАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Р.Р. Ягудина, Е.В. Чернова
(г. Магнитогорск, ФГБОУ ВПО «Магнитогорский государственный технический университет имени Г.И. Носова»)
E-mail: yagudina.regina02@mail.ru, HelenaVChernova@gmail.com

AUTOMATED REFERENCE OF LEGAL INFORMATION SYSTEMS FOR INFORMATION SECURITY

R.R. Yagudina, E.V. Chernova
(Magnitogorsk, Nosov Magnitogorsk State Technical University)

Abstract. This article discusses the automated answering systems that are used for access to legal information in the field of information security.

Keywords: automated referral system, legal information, information security, Consultant Plus, Garant, Codex.

Современное законодательство России находится в состоянии постоянного обновления и непосредственно Российская система права испытывает постоянное влияние процессов, которые происходят во всем целом мире. Правовая информация, передающаяся по свободным каналам Интернет, требует классификации и систематизации, т. к. в период перехода к информационному обществу происходит формирование новой культуры обращения с правовым знанием, новой культуры систематизации правовых предписаний. Основным признаком соответствия новой правовой культуре является готовность правовой систематизации к быстрым изменениям. Значит, чтобы успевать за этим процессом, необходимо непрерывное пополнение знаний, что невозможно без современных способов систематизации правовых актов, создания и функционирования справочных правовых систем. Их целью становится формирование современной и оптимальной инфраструктуры для научных исследований, законотворчества, применения права и правового образования.

На сегодняшний день, больше узнать о российском законодательстве помогают именно справочные правовые системы. Под справочной правовой системой будем понимать автоматизированную информационную систему, предназначенную для сбора, систематизации, хранения и поиска правовой информации по запросам пользователей. С ними работают бухгалтеры, юристы, финансовые специалисты, топ-менеджеры многих организаций, а также преподаватели, ученые-правоведы, студенты и даже школьники. На российском рынке сегодня присутствует три основных игрока – это компании «КонсультантПлюс», «Гарант» и консорциум «Кодекс» из Санкт-Петербурга [1].

Справочная правовая система Консультант Плюс – самая мощная (по контенту) из всех аналогичных систем. Она создана в конце XX в. «Консультант Плюс» – первая российская правовая система. Одной из причин, по которой системы «Консультант Плюс» используются как опытными, так и начинающими пользователями, является легкость и простота в работе. Система «Консультант Плюс» предоставляет широкие и удобные возможности для поиска,