Архитектура программного модуля цифровой подписи файлов

Кирюхин А.С., *студент*
Херсонский государственный университет, г. Херсон

Целью настоящей работы являлась разработка архитектуры и написание программного модуля, который обеспечивал бы генерацию и проверку цифровой подписи для документов различных форматов. Архитектура подобного рода должна быть минималистской, но с возможностью расширения в будущем.

Существование алгоритмов асимметричного шифрования позволило создать средство проверки подлинности информации – электронную подпись, которая и является предметом работы. Электронная подпись - это набор символов, который прикрепляется к документу либо идёт отдельно от документа и позволяет получателю твёрдо удостовериться, что сообщение пришло от конкретного автора и не было изменено в ходе передачи.

Так как длина сообщения должна быть меньше длины закрытого ключа, подпись генерируется на основе хэша документа, который генерируется алгоритмом SHA1 либо любым другим, который удовлетворяет внешним требованиям: доступностью, надёжностью и скоростью хэширования.

Подпись хэша, а не самого документа, делает программный модуль универсальным по отношению к форматам файлов, а также позволяет подписывать файлы любого размера. Это выгодно отличается от варианта с ограниченным набором подписываемых форматов.

Программный модуль опирается на две базовые подпрограммы: генерацию подписи с помощью хэша подписываемого файла и закрытого ключа пользователя, а также проверку документа с помощью открытого ключа отправителя. Они могут быть написаны на любом языке программирования. Для упрощения внутренней архитектуры все криптографические операции выполняются с помощью фреймворка OpenSSL. На основе вышеописанных базовых функций систему можно расширять по необходимости.

В реальной работе пользование такой системой обеспечивает проверку подлинности электронных документов, что является обязательным условием при переходе на электронный документооборот на предприятиях.