Андрей ХВОСТОВЕЦ, АО «Термоком»

ЦИФРОВЫЕ СЕРТИФИКАТЫ И ЭЛЕКТРОННАЯ ТОРГОВЛЯ: ЭФФЕКТИВНАЯ ЗАЩИТА WEB-САЙТА

Abstract: *This article is about Digital IDs (also known as Digital Certificates) and the benefits they can bring to a business. The point is to get the reader to know some common things regarding Digital IDs.*

Предприниматели, которые практикуют электронные сделки посредством Web, могут в два счёта достигнуть высокого уровня конкурентоспособности, так как их потенциальные клиенты – весь мир. Однако существует несколько нюансов относительно безопасности в Web, которые следует принять во внимание во избежание риска. Клиент пошлёт информацию через Web лишь тогда, когда будет уверен, что его личная информация (номер кредитной карты, финансовые данные и т.п.) будет защищена.

По своей сути цифровой сертификат – это небольшой файл, содержащий в себе следующую информацию:

- имя и идентификатор владельца сертификата;
- открытый ключ подписи (шифрования);
- имя, идентификатор и цифровую подпись удостоверяющей организации;
- серийный номер, версию и срок действия сертификата.

Цифровой сертификат выдается физическому лицу – владельцу закрытого ключа электронной цифровой подписи (шифрования), соответствующего открытому ключу. Владелец сертификата может быть уверен в том, что информация, передаваемая им электронным способом, не будет прочитана, искажена или подменена за время передачи через Интернет. Цифровой сертификат можно рассматривать как электронное удостоверение пользователя по аналогии с традиционным удостоверением (паспортом), которое позволяет удостовериться в том, что при обмене электронными документами Вы имеете дело с определённым лицом.

Защищённый Web-сайт даст нашему бизнесу такие неоспоримые преимущества, как безопасная торговля он-лайн и потоковая обработка процессов при страховании, использовании кредитных карт и т.д. Однако, чтобы преуспеть на этом рынке, нам необходимо знать обо всех угрозах нашей безопасности в Интернет, владеть технологиями, ликвидирующими их, чтобы, таким образом, завоевать доверие клиентов.

Обычные сделки основаны на физических аспектах. В супермаркетах клиенты охотнее используют свои кредитные карты, так как они сами могут рассмотреть и пощупать товар и, таким образом, судить о магазине. В связи с отсутствием этих аспектов в Интернете, в нём гораздо труднее обеспечить безопасность нашего предприятия. Зная о рисках, связанных с электронными сделками, предприятия могут приобрести решения, которые их исключают. Киаким рискам относятся:

- Spoofing (имитация) – «дешёвые» веб-сайты и лёгкость имитации уже существующих страниц предельно упрощают создание подделок. Мошенники часто перехватывают номера кредитных карт посредством искусно сделанных копий настоящих сайтов.
- Несанкционированное раскрытие (unauthorized disclosure) – когда информация о сделке предаётся «напрямую», хакеры могут свободно перехватить передачу и извлечь из неё конфиденциальные сведения о покупателе.
- Несанкционированные действия – конкуренты или неудовлетворённый покупатели могут взломать сайт, так, что это приведёт к неполадкам или невозможности дальнейшего оказания услуг.
- Подлог данных – содержимое сделки можно перехватить и изменить, пока оно находится в пути, как случайно, так и нарочно. Имена пользователей, номера кредитных карт и числовые значения посылаемых денежных сумм при этом обладают наибольшей уязвимостью.

Цифровой сертификат – не что иное, как электронный эквивалент лицензии на предпринимательскую деятельность. Цифровые сертификаты выдаются заслуживающей доверия третьей стороной, имеющей на это полномочия (Certificate Authority, CA). Уполномоченная сторона, выдающая сертификат, поручается за наше право использовать наше же название и URL. Однако, возможна выдача цифровых сертификатов и физическим лицам.

Перед выдачей сертификата CA изучает «рекомендации», а также выполняет тщательную проверку того, насколько компания соответствует тому, что она должна из себя представлять. Затем CA выдаёт компании цифровой сертификат, являющийся, в своём роде, электронной рекомендацией.

Цифровой сертификат VeriSign работает в совокупности с технологией SSL, являющейся стандартом для безопасных коммуникаций, основанных на Web. После установки цифрового сертификата сервер автоматически активирует SSL, устанавливая безопасный канал связи с браузером покупателя. Наш сайт теперь может безопасно взаимодействовать с любыми пользователями Mozilla Firefox, Microsoft Internet Explorer, a

также некоторыми популярными почтовыми программами. Будучи однажды активированной цифровым сертификатом, технология SSL сразу же обеспечивает следующие необходимые для безопасных электронных транзакций компоненты:

- Аутентификация – проверяя электронный сертификат, покупатели могут убедиться, что веб-сайт действительно принадлежит компании, а не злоумышленнику. Это придаёт им уверенности для посылки конфиденциальной информации.
- Конфиденциальность сообщений – SSL шифрует всю информацию, которой веб-сервер обменивается с клиентами, используя уникальный ключ сеанса. Для безопасной передачи сеансового ключа пользователю сервер зашифровывает её с помощью своего же открытого ключа. Каждый сеансовый ключ используется лишь однажды, во время одного-единственного сеанса с одним-единственным клиентом. Эти уровни защиты конфиденциальности обеспечивают невозможность прочтения информации в случае перехвата.
- Целостность сообщений – при посылке сообщения как отправляющий, так и получающий компьютеры генерируют особый код, основанный на содержимом сообщения. Если хотя бы один из символов сообщения по пути будет изменён, получающий компьютер сгенерирует другой код, а затем сообщит отправляющему, что сообщение недействительно. Таким образом, обе задействованные стороны могут быть уверены, что они видят в точности то, что послала им другая сторона.

В целом, повсеместное внедрение цифровых сертификатов является необходимым шагом на пути к развитому информационному обществу, так как это будет способствовать росту электронного документооборота, а также его безопасности. Основной проблемой будет относительно высокая стоимость предоставляемых услуг, однако, со временем, с появлением большего числа пользователей, стоимость будет постепенно снижаться.