Обзор платёжной системы WebMoney Transfer

Городов Павел
911 группа

МФТИ
г.Долгопрудный
2003г

Введение: Российские платёжные системы

В настоящее время на рынке работают три российские платежных системы: CyberPlat, PayCash и WebMoney.

Сравнивать, сопоставлять их между собой — дело неблагодарное, труднореализуемое, да и, в общем-то, неправильное.

CyberPlat – это по своей сути «банковская надстройка». Система, позволяющая в удобной форме, с хорошей скоростью и надежностью осуществлять банковские платежи. В исходном варианте системы и продавец, и покупатель должны были открыть действующий или транзитный счет в банке «Платина». Для клиента этот счет выглядел как учетная запись (account) в системе. Перевод денег на другую запись был фактически переводом денег со счета на счет. Поскольку деньги переводились «внутри» одного банка, то переводы осуществлялись мгновенно и независимо от времени суток и дня недели. Однако по ряду причин такая схема работы не подошла.

В настоящее время система сильно отличается от первоначального варианта и состоит из трех довольно независимых частей (которые, впрочем, используют общую технологию): CyberPos, CyberCheck, Internet Banking.

CyberPos ориентирован на сектор B2C и служит для проведения карточных платежей. Эта система позволяет российским юридическим лицам получить счет продавца (merchant account) и принимать платежи по пластиковым картам, как по международным, так и по российским STB и Union, а также по предоплаченным картам (с конца января). Сильной стороной системы является защищенность каналов передачи информации. Информация о кредитках хранится не у продавца, а в системе в защищенном виде. Кроме того, по словам представителя системы Владимира Спиридонова, система обладает интеллектуальной защитой от мошеннических (fraud) платежей и позволяет «на лету» отловить 80% из них.

CyberCheck ориентирован на сектор «бизнес-бизнес» и предназначен исключительно для работы с российскими юридическими лицами. Система предназначена для взаиморасчетов, секретного документооборота и позволяет совершить сделку, подписать документы и тут же произвести оплату. Система официально заявляет, что все документы, составленные и подписанные цифровым аналогом личной подписи в рамках CyberCheck, имеют юридическую силу и принимаются к рассмотрению арбитражными судами.

Internet Banking – позволяет полностью управлять своим банковским счетом в любое время, если ваш банк является участником системы. Счета в других банках могут поддерживаться через транзитный счет в «системном» банке.

Как оказалось, система ***CyberPlat*** является:

- Сильно замкнутой на Российском рынке
- Принфипиально банковской системой, поддерживающей взаимодействия физических лиц только через банковские счета.

PayCash – довольно давно известна на российском рынке. Однако в течение почти двух лет она пребывала в состоянии спячки, находясь в вялотекущем «тестовом» режиме. Буквально несколько месяцев назад «проснувшись», она сейчас резко наверстывает упущенное, отличаясь агрессивной маркетинговой политикой.

По своей сути PayCash – это рафинированные цифровые наличные. Денежная единица системы представляет собой частное платежное

обязательство (нечто вроде электронного чека с бланковым индоссаментом) в виде файла на диске, закрытое цифровой подписью эмитента. Утрата файла приводит к утрате денег. По заявлению руководителей PayCash, в будущем возможно появление механизма резервного копирования денег с синхронизацией денежного файла и его копии.

WebMoney (правильное название ***WebMoney Transfer***, но все говорят — WebMoney) — ветеран на рынке платежных систем. Она вовсю работает уже больше двух лет. Денежная единица — WM. Пожалуй, эта система первой вышла на промышленную эксплуатацию (хотя CyberPlat первым объявил о начале работы в марте 1998 года, полноценная эксплуатация системы началась позже). И это же единственная система из трех, которая уже реально работает на мировом рынке. В свое время она провела ряд очень удачных маркетинговых ходов, быстро выстроив в Интернете ряд сервисов с оплатой через WM и предоставив возможность пользователям начать зарабатывать реальные (хоть и небольшие) деньги. Это позволило быстро сформировать довольно большое ядро постоянных клиентов. Хотя система и обладает всеми потребительскими свойствами электронных наличных, специалисты системы не относят ее к этому типу, подчеркивая, что на диске компьютера пользователя хранятся не сами электронные деньги, а всего лишь закодированные записи о наличии денег у клиента. Деньги, в отличие от стопроцентных цифровых наличных, при потере файла-кошелька не пропадают. Собственно говоря, деньгам в системе WM может быть придан самый разнообразный статус, о чем будет сказано ниже.

Система обеспечивает высокую степень конфиденциальности и анонимности клиента (но только по его желанию), что обусловило появление в Сети большого количества отечественных и зарубежных финансовых пирамид, базирующихся на WM. Это нанесло некоторый вред репутации WebMoney среди пострадавших.

Специалисты считают, что WM-пирамиды свидетельствуют именно о «твердости» этой сетевой валюты — вряд ли создатели пирамид стали бы строить свои сооружения на зыбкой почве.

В WebMoney имеется внутренняя закрытая почта, сочетающая в себе, с моей точки зрения, черты электронной почты и ICQ, при помощи которой участники могут оперативно обмениваться письмами и документами. Сообщения пересылаются в цифровом конверте, позволяющем однозначно идентифицировать отправителя и не дающем прочесть ваше сообщение постороннему.

С точки зрения физического лица - конечного пользователя - единицы обращения WM и PayCash мало отличаются друг от друга. В любом случае, это просто сетевая валюта, которую всегда можно поменять на живые деньги. Но для юридических лиц система WebMoney Transfer предоставляет более продуманную и гибкую ***состыковку с «живой» бухгалтерией****. Поэтому система WMT распространяется быстрее и является по сути первой (и единственной) Российской платёжной системой, получившей распространение за рубежом.*

Например, уже сейчас в России возможна оплата телефонных счётов МТС, Билайн, Мегафон и МГТС прямо через WebMoney Transfer. Всё это говорит о стремительной популяризации системы WMT, поэтому в качетсве темя для доклада было сделано предпочтение в пользу этой системы.

Общее описание системы WebMoney Transfer

WebMoney Transfer – это учетная система, с помощью которой все желающие могут обмениваться универсальными учетными единицами: титульными знаками WebMoney (WM). Система открыта для свободного использования всеми желающими в любой точке земного шара.

WebMoney Transfer не является системой «электронной валюты» в общем понимании, так как она не оперирует электронными эквивалентами денег. В WMT нет понятия «электронная банкнота» - в электронных кошельках пользователей хранятся лишь записи о количестве средств. Контроль за каждой валютой принципиально невозможен.

Клиентами системы являются продавцы и покупатели товаров и услуг. С одной стороны, это Web-магазины, с другой - пользователи Интернета, не имеющие возможности или не желающие использовать альтернативные методы расчетов (кредитные карты и т.п.) из-за длительности трансакций, низкой безопасности, риска возврата совершенных платежей и т.п.. Фактически покупатели и продавцы никак не различаются в рамках системы WMT. Сервисы WMT предоставляют способы перевода средств с одного WM-кошелька на другой, плюс ряд дополнительных услуг коммуникации.

С помощью WebMoney Transfer можно совершать мгновенные безотзывные трансакции, связанные с передачей имущественных прав на любые товары и услуги, создавать собственные web-сервисы и сетевые предприятия, проводить операции с другими участниками, выпускать и обслуживать собственные расчетные инструменты.

Все транзакции (взаимодействия) клиентов системы осуществляются через открытые интерфейсы единого центра сертификации https://w3s.webmoney.ru, (сами файлы скриптов доступны на https://w3s.webmoney.ru/asp/). Для обращения к интерфейсам используется порт 443. Далее, после объяснения некоторых основнях понятий, будут приведены краткое описание одного из интерфейсов на центре сертификации (исключительно в качестве примера).

WM-кошелёк

Регистрация в системе, а также управление средствами осуществляются с помощью клиентской программы WM KEEPER.
С помощью программы WM KEEPER вы можете осуществлять мгновенные расчеты в WM с другими клиентами системы, оплачивать товары и услуги в Сети, конвертировать WM в активы с переводом на банковские счета, а также обсуждать с партнерами условия торговой сделки по встроенной в программу WM KEEPER защищенной системе обмена сообщениями.

Получить WebMoney на кошелек вы можете:

- переводом из любого банка (в том числе Сбербанка РФ), а также почтовым переводом на расчетный счет одного из официальных агентов системы (сумма перевода будет автоматически конвертирована в WM и зачислена на указанный вами кошелек);
- с помощью WM-карты пополнения (для Z-кошельков) – юридическим гарантом услуги «WM-карты пополнения кошельков» является ОАО «Альфабанк»;
- от других участников системы в обмен на товары, услуги или наличные деньги.

Хранящиеся на вашем кошельке WebMoney находятся в вашем полном распоряжении и в любой момент – круглосуточно и ежедневно - могут быть использованы вами для расчетов. При необходимости вы сможете снять WebMoney с кошелька и перевести на указанный вами банковский счет с одновременной конвертацией в соответствующую валюту.

См. также: Список тарифов на операции с WM.

Виды валют

Транзакционным средством в системе служат титульные знаки WebMoney (WM) нескольких типов, хранящиеся на электронных кошельках их владельцев:

- WMR – эквивалент RUR – на R-кошельках,
- WME - эквивалент EUR - на E-кошельках,
- WMZ – эквивалент USD – на Z-кошельках,
- WM-C и WM-D – эквивалент USD для кредитных операций – на C- и D-кошельках.

При переводе средств используются однотипные кошельки, а обмен WM-R на WM-Z производится в обменных пунктах, которые должны регистрировать своё предпринимательство в системе WMT так же, как и другие продавцы услуг и товаров.

Ещё один способ обмена WM-валют – использование для обмена различных типов WM (WMZ, WMR, WME) автоматической интернет-биржи между участниками WMT по взаимным договоренностям. Биржи действуют по принципу автоматического подбора встречных заявок, выставляемых владельцами WM-кошельков. Обмен производится по курсам, устанавливаемым самими участниками обмена.

Безопасность транзакций

При использовании WebMoney Transfer WM-средства передаются между пользователями через Интернет. Открытая архитектура Интернета требует строгих мер безопасности во избежание попыток перехвата информации о торговой сделке.

Рассмотрим некоторые меры безопасности, примененные в WebMoney Transfer:

1. Для входа в программу WM Keeper необходимо знание уникального 12-значного WM-идентификатора пользователя, его личного пароля, а также места расположения на диске компьютера файлов с секретным ключом и кошельками (рекомендуется хранить их на дискетах или других портативных носиьелях информации).
   - WM-идентификатор (имя пользователя в системе) - генерируется автоматически, уникален для каждой регистрации участника и необходим для входа в программу WM Keeper и проведения сделок в системе WebMoney Transfer.
   - Пароль - назначается пользователем и необходим для входа в программу WM Keeper и осуществления сделок в системе WebMoney Transfer.
   - Перевод и получение WM-средств осуществляется только между однотипными кошельками участников системы.Для проведения сделки необходимо сообщить партнеру номер WM-кошелька, после чего он сможет отправить средства на ваш WM-кошелек. При этом никто не сможет снять деньги с вашего WM-кошелька с удаленного компьютера.
   - Невозможно сделать перевод с кошелька, на котором нет средств (этой защиты лишена, например, система оплаты с помощью кредитных карт).
2. Все сообщения в системе передаются в закодированном виде, с использованием алгоритма защиты информации подобного RSA с длиной ключа более 1024 бит. Для каждого сеанса используются уникальные сеансовые ключи. Поэтому в течение сеанса (времени осуществления трансакции) никто, кроме Вас, не имеет возможности определить назначение платежа и его сумму.

3. Никто не сможет совершить никаких денежных операций, основываясь на реквизитах Ваших прошлых сделок (этой возможности лишена, например, система оплаты с помощью кредитных карт). Для каждой сделки используются уникальные реквизиты (увеличивающийся счётчик транзакций, время тразакции), и попытка использовать их вторично немедленно отслеживается и гасится.
4. Устойчивость по отношению к обрывам связи. Если любая операция в системе не была успешно завершена по причине обрыва связи, то система не учитывает данную операцию.
5. Все процессы, совершаемые в системе - хранение WebMoney на кошельках, выписка счетов, WM-расчеты между участниками, обмен сообщениями - выполняются с использованием алгоритма кодирования, эквивалентного RSA, с длиной ключей не менее 1024 бит, что определяет высокую устойчивость системы ко взломам и обрывам связи. Для каждой транзакции назначаются уникальные сеансовые реквизиты, и попытка их повторного использования мгновенно отслеживается и пресекается. Если та или иная операция не была успешно завершена, она не учитывается системой.

   (***Примечание:*** *Компания «КИТ», разработчик и владелец системы WMT, ограничилась лишь фразой «…с использованием алгоритма кодирования, эквивалентного RSA…». В какой мере эта «эквивалентность» проверена и кем подтверждена – неизвестно, так как сам алгоритм можно разобрать лишь декомпилировав программные средства, распространяемые в рамках системы. Компания «КИТ» проигнорировала многие запросы официальных лиц, прессы и обычных пользователей, и оставила без внимания просьбы открыть наконец этот алгоритм. Насколько мне известно, эта информация до сих пор является закрытой*)

Подобное сочетание личных настроек и случайным образом генерированных идентификаторов программы гарантирует невозможность несанкционированного использования программы и получения доступа к Вашим средствам.

Идентификация

При регистрации участнику WebMoney Transfer присваивается 12-значный WM-идентификатор, необходимый для работы в системе. WM-идентификатор служит уникальным обозначением участника.

Владелец WM-идентификатора самостоятельно назначает пароль и определяет место для хранения файлов с секретным ключом и кошельками. По своему желанию он может вносить в информационные поля программы данные о себе и при необходимости изменять их, открывать и закрывать доступ к своим данным для друих пользователей.

Помимо идентификации пользователей при помощи WM-идентификатора, в системе осуществляется аутентификация на основании секретного ключа и пароля к нему. Секретный ключ не должен передаваться третьим лицам (по Сети), поскольку является собственностью владельца WM-идентификатора. Наличие ключа служит гарантией того, что его владелец сможет подтвердить права на управление своим WM-идентификатором. Таким образом, владельцем WM-идентификатора в системе всегда признается тот, кто владеет секретным ключем и паролем.

Для удостоверения личности владельца WM-идентификатора в системе действует WM-аттестация (см. далее).

Каждый WM-кошелек имеет свой уникальный номер в системе (12-значный с префиксом, обозначающим тип кошелька).

Анонимность

При желании, с помощью настроек программы WM Keeper, вы можете сделать ваши персональные сведения недоступными для других клиентов WebMoney Transfer (имя, фамилия, E-mail, почтовый адрес, номера банковских счетов и т.п.).

Из информации, используемой при сделках, другая сторона не может получить указанных сведений о вас. Ваши партнеры, любые частные, государственные, финансовые, коммерческие, контролирующие структуры находятся от вас на "безопасном" расстоянии. Все транзакции происходят лишь с использованием идентификаторов кошельков и пользователей – персональные сведения при этом не передаются.

Однако если позднее ваш торговый партнер потребует от вас указания некоторых из вышеперечисленных личных сведений, и вы согласитесь с этим требованием, то настройки программы WM Keeper позволят легко сделать их доступными.

Сертификация

Цифровые подписи и сертификаты (общие сведения)

В целях обеспечения безопасности передачи документов многие Web-приложения требуют подкрепления электронного документа цифровой подписью. Метод цифровой подписи основан на использовании алгоритмов асимметричного шифрования. Такие алгоритмы (RSA, Diffie-Hellman) подразумевают наличие пары ключей – открытого (публичного) и закрытого (секретного, приватного). Предположим, необходимо переслать документ по безопасной электронной почте и поставить под ним цифровую подпись. Для этого документ обрабатывается специальной хэш-функцией, а полученное в результате значение (условно его можно назвать "контрольной суммой" или сверткой, далее: хэш-значение) зашифровывается закрытым ключом отправителя и пересылается вместе с документом. Это и есть цифровая подпись. Получатель использует открытый ключ отправителя для того, чтобы извлечь хэш-значение из цифровой подписи. Подпись считается подлинной, если извлеченное из нее хэш-значение совпадет с результатом повторного хэширования полученного документа.

Также, если необходимо закрыть информацию от несанкционированного просмотра при передаче через Интернет, передаваемый документ кодируется с использованием открытого ключа получателя, и раскодировать его сможет только получатель - владелец закрытого ключа. Таким образом, необходимо передавать открытые ключи пользователей неискаженными.

Чтобы удостовериться в том, что открытый ключ не искажен и действительно принадлежит тому, за кого выдает себя отправитель, существует механизм цифровых сертификатов. Доверенное третье лицо – уполномоченный по выдаче сертификатов (Certification Authority – CA) – заверяет электронной подписью соответствие между открытым ключом и именем (идентификатором) его владельца. Подписанные таким образом данные (открытый ключ, идентификатор владельца и некоторые другие связанные с ним атрибуты) и представляют собой цифровой сертификат. Генерация цифровых сертификатов регламентируется стандартом X.509.

Необходимо сразу отметить, что у владельца сертификат с открытым ключом (далее: цифровой сертификат) может храниться в персональном компьютере вместе с закрытым ключом. Такой сертификат будет называться персональным цифровым сертификатом. В программах электронной почты персональные цифровые сертификаты и закрытые ключи часто называют «цифровыми удостоверениями».

Любой цифровой сертификат пользователя или сертификат Web-узла сопоставляет некоторые идентификационные данные с открытым ключом. Закрытый ключ, дающий возможность расшифровать послание или поставить цифровую подпись только его владельцу, хранится в персональном цифровом сертификате. Посылая свой сертификат посторонним лицам, пользователь фактически передает им свой открытый ключ, благодаря чему они могут посылать указанному пользователю зашифрованную информацию, расшифровать и прочитать которую может только владелец персонального цифрового сертификата (закрытого ключа).

Цифровая подпись, которой подписана какая-либо информация (сообщение, документ или даже сертификат), является электронной идентификационной картой этой информации и пользователя, пославшего ее. Она сообщает получателю, что данная информация действительно пришла от определенного пользователя и не была испорчена или «подделана» посторонними лицами.

Чтобы получить возможность посылать зашифрованные или подписанные цифровой подписью сообщения, пользователю нужно получить персональный цифровой сертификат и настроить Web-браузер на работу с этим сертификатом. Защищенный Web-узел (название которого начинается с «https») при посещении его пользователем автоматически посылает ему свой сертификат.

Персональные цифровые сертификаты

Для защиты, идентификации и передачи данных при Интернет-соединениях в WebMoney Keeper Light edition используются персональные цифровые сертификаты и протокол SSL (Secure Sockets Layer). Протокол SSL, являющийся в настоящее время стандартом де-факто, используется наиболее распространенными программными продуктами для World Wide Web (в том числе браузерами Netscape и Microsoft Internet Explorer) для работы в защищенном режиме HTTPS (HTTP Secure). SSL гарантирует безопасное подключение к Web-узлам и серверам приложений (сервер WebMoney Keeper Light edition является сервером приложений).

Персональный цифровой сертификат удостоверяет владельца WM-идентификатора (WM id), подтверждая, что тот кто получил WM id и сгенерировал у себя закрытый ключ к нему, тот и управляет этим WM id. Идентификация обеспечивается путем применения закрытого ключа, хранящегося только у владельца персонального цифрового сертификата WebMoney Keeper Light (так как в процессе регистрации закрытый ключ создается на компьютере пользователя и не передается по сети).

Таким образом, для пользователя системы WebMoney важным моментом при его регистрации в системе является сохранение в надежном и безопасном месте его закрытого ключа (а также создание его резервной копии).

Персональные цифровые сертификаты могут быть использованы для отправки закрытых и подписанных сообщений по электронной почте, обеспечивая достоверность передаваемых сообщений и документов. Чтобы воспользоваться этой возможностью необходимо установить в программе почтовом клиенте персональный цифровой сертификат (см. описание используемой почтовой программы).

Персональные цифровые сертификаты могут быть выданы на основании полученного клиентом аттестата (см. далее). При этом подтвержденные данные о пользователе системы (по его выбору) будут записаны в сертификат для отображения и контроля всеми участниками (тем самым обеспечивая пользователю системы большее доверие со стороны его корреспондентов).

Иерархия аттестатов WebMoney Transfer.

В системе WebMoney Transfer разведена иерархия «аттестатов доверия» пользователей. Покупатель в интернет-магазине может проверить аттестат доверия продавца – его наличие и уровень доверия. Недовольные покупатели могут повлиять на аттестат доверия нерадивого продавца. Система WM-аттестации существует поверх стандартной системы цифровых сертификатов в Internet, регламентированной стандартом X.509.

Аттестат регистратора (1 уровень)

Аттестат регистратора является аттестатом 1го уровня. Он выдается участнику WebMoney Transfer центром технической поддержки и аттестации системы (АНО "ВМ-Центр") при обязательном личном присутствии аттестируемого (или доверенного лица компании).

- Для частных лиц необходимо предьявить паспорт, контактную информацию и подписать договор с Центром аттестации на ведение аттестационной деятельности в системе. В договоре будут определены правила и порядок выдачи регистратором персональных аттестатов, а также ответственность регистратора.
- Для юридических лиц необходимо назначить ответственного сотрудника компании, который будет заниматься аттестацией. Порядок получения аттестата для него такой же как и для частных лиц.

1. Основное назначение аттестата регистратора заключается в том, что его владелец становится официальным аттестатором системы и получает право выдавать WM-аттестаты 2го уровня (персональные аттестаты).
2. Помимо этого владелец аттестата первого уровня имеет все полномочия аттестатов нижлежащих уровней – 2го и 3го.

Прилагается список регистраторов, обладающих аттестатами 1 уровня, доступный для зарегистрированных пользователей WMT. Услуга получения аттестата 2го уровня предоставляется аттестаторами за плату порядка 5-10 WMZ.

Персональный аттестат (2 уровень)

Персональный аттестат является аттестатом 2го уровня. Он выдается участнику WebMoney Transfer официальным регистратором системы (владельцем аттестата регистратора первого уровня) в следующих случаях:

- в личном присутствии аттестируемого (или доверенного лица компании) у регистратора с предьявлением ряда удостоверяющих документов и заявления на аттестацию
- по почте (обыкновенной НЕ email) с предьявлением ксерокопий ряда удостоверяющих документов

1. Основное назначение персонального аттестата – удостоверение ответственности «продавца». Администрация WMT рекомендует получить песональный аттестат на ресурс, сервис или интернет-магазин, использующий систему WMT.
2. Помимо этого, владелец персонального аттестата обладает правом выдавать аттестаты доверия (3го уровня).
3. Владелец аттестата 2го уровня обладает также и всеми полномочиями аттестата 3го уровня.

Владелец персонального аттестата лишается права на аттестационную деятельность в системе в случае, если персональные данные хотя бы одного, аттестованного им участника оказались недостоверными при их проверке центром аттестации.

Существует список ресурсов, обладающих аттестатами второго уровня, лоступный для зарегистрированных пользователей WMT. Получения аттестата 3го уровня предоставляется пользователями из этого списка за плату порядка 1-5 WMZ.

Аттестат доверия (3 уровень)

Аттестат доверия является аттестатом 3го уровня. Он выдается участнику WebMoney Transfer владельцем персонального аттестата под его личную ответственность на основании предоставленных ему паспортных и контактных данных аттестируемого, гарантированно соответствующих действительности (личная встреча, нотариальное заверение, выдача аттестата близким и знакомым под личную ответственность).

Владелец аттестата доверия не имеет права на аттестационную деятельность в системе и не может участвовать в партнерской программе Центра аттестации. В последствии он может получить персональный аттестат (после прохождения процедуры, соответствующей 2 уровню аттестации).

Название аттестата ДОВЕРИЯ, говорит само за себя. Персональный данные о владельце аттестата доверия не проверяются ни нотариусами ни официальными представителями Центра аттестации. Данные о владельце аттестата доверия, в отличие от других аттестатов, всего лишь записываются со слов участников системы, имеющих персональный аттестат.

1. Аттестат доверия позволяет обезопасить себя от потери или повреждения электронных ключей или кошельков. В случае наличия аттестата его владелец в любой момент сможет восстановить управление над аттестованным идентификатором, предъявив свой паспорт.
2. Аттестат доверия позволяет вести кредитную деятельность в системе, например выдавать кредиты или получать их. Без аттестата заведение кредитных кошельков и кредитная деятельность в системе невозможны. Хотя для ведения кредитной деятельности администрация WMT рекомендует получить персональный аттестат 2го уровня.
3. Позволяет участвовать в различных партнерских, спонсорских и прочих программах (например в BXOD.COM). Наличие аттестата гарантирует владельцам программ отсутствие возможности множества регистраций с вымышленными и виртуальными данными от имени одного человека. Для ведения подобной деятлеьности достаточно иметь аттестат 3го уровня, хотя рекомендуется получить персональный аттестат 2го уровня.

Подробнее об аттестатах можно посмотреть: Перечень открытых документов, которыми регулируется аттестационная деятельность в системе WMT.

Пример работы с https-интерфейсом WMT.

Ипользование Цифровой Электронной Подписи (ЦЭП) в рамках WMT.

Все транзакции для операций с WM-валютой проходят через центральный сертификационный сервер https://w3s.webmoney.ru, транзакция по проведению какой-либо операции адресуется соответствующему этой операции интерфейсу. Все интерфейсы доступны по URL https://w3s.webmoney.ru/asp/. Используемый при запросах к серверу порт - 443. Имена файлов интерфейсов и параметры запросов приведены в описании каждого интерфейса. Подробные описания всех https-интерфейсов приведены на официальном сервере системы. Разберём один подробнее в качестве примера.

Предположим, покупатель хочет приобрести некий товар в интернет-магазине. Он устанавливает с магазином защищённое https-соединение. Это значит, что общение покупателя с продавцом проходит в зашифрованном виде, открытым ключом является сертификат магазина, выданный им по протоколу X.509 в рамках системы ресурсов WMT. Предположим, что покупатель заполнил в интернет-магазине некую форму, указал свои WM-реквизиты (номер кошелька), подтвердил размер выплаты. Сервер составляет https-запрос к интерфейсу выписывания счёта клиенту https://w3s.webmoney.ru/asp/Invoice.asp по следующей схеме:

Интерфейс 1. Выписывание счета от одного участника (магазина, web-ресурса) другому участнику (покупателю, клиенту) системы

Для того чтобы выписать счет любому пользователю системы WebMoney Transfer необходимо выполнить следующий https-запрос:
https://w3s.webmoney.ru/asp/Invoice.asp?SL=LoginOfStores& SP=PurseOfStores& CL=LoginOfCust& IN=OrderID& D=Desc& AD=InvAddress& A=Amount& E=Experation& P=Period& RN=RequestN& SS=SignStr

В параметрах данного запроса передаются реквизиты счета, который необходимо выписать:

- SL=LoginOfStores - это параметр, указывающий WM-идентификатор web-ресурса. Здесь вы должны вместо LoginOfStores указать идентификатор WM Keeper, который вы установили для использования на Web-ресурсе. Этот параметр может выглядеть так: SL=123234743554;
- SP=PurseOfStores - это параметр, указывающий кошелек Web-ресурса. Здесь вы должны вместо PurseOfStores указать WM-кошелек Web-ресурса, на который будут приходить средства от покупателей в оплату за покупки. Этот параметр может выглядеть так: SP=Z349727391047;
- CL=LoginOfCust - этот параметр определяет покупателя. Здесь вы должны указать WM-идентификатор покупателя, которому необходимо выписать счет. Этот параметр может выглядеть так: CL=143567890432;
- IN=OrderID - этот параметр определяет номер счета (номер заказа) на Web-ресурсе (в магазине). Номер генерируется вами самостоятельно и хранится в базе Web-ресурса (магазина, сервиса) - по этому номеру в дальнейшем будет определятся состояние счета (оплачен или нет). Номер должен иметь целочисленное значение и может выглядеть так: IN=123;
- D=Desc - этот параметр определяет описание товара, на который выписывается счет. Параметр должен быть произвольной строкой от 0 до 255 символов и может выглядеть так: D=Покупка доступа в Интернет - 4 часа провайдер Россия-Онлайн;
- AD=InvAddress - этот параметр определяет адрес доставки товара. Данный параметр передается Web-ресурсу покупателем. Если товар онлайновый, то адрес можно оставить пустым. Параметр должен быть произвольной строкой от 0 до 255 символов и может выглядеть так: AD=PIN доступа (будет выслан вам по внутренней почте);
- A=Amount - этот параметр определяет сумму счета. Данный параметр формируется Web-ресурсом. Указанная в параметре сумма выставляется для оплаты покупателю. Параметр должен быть числом с плавающей точкой (разделитель - .) и для десяти с половиной может выглядеть так: A=10.5 . Незначащие нули в

конце и точка, если число целое, должны отсутствовать, например, 10.50 - не верно, 10.5 - верно, 9. - не верно, 9 - верно);

- E=Experation - этот параметр определяет срок действия счета. Параметр формируется Web-ресурсом. В течение указанного здесь количества дней с момента выписывания счета покупатель может оплатить данный счет. Если указать здесь 0, то счет не будет иметь срока действия, и его можно будет оплатить всегда. Параметр должен быть целочисленным значением от 0 до 255 и может выглядеть так: E=0;
- P=Period - этот параметр определяет срок действия протекции сделки. Параметр формируется Web-ресурсом. Он определяет максимальный срок протеции сделки при оплате счета. Если указать здесь 0, то счет не будет иметь срока протекции (оплата должна быть произведена покупателем без протекции сделки). Параметр должен быть целочисленным значением от 0 до 255 и может выглядеть так: P=0;
- RN=RequestN - этот параметр является уникальным возрастающим числом. Параметр формируется Web-ресурсом и должен быть всегда больше такого же параметра, указанного в предыдущем запросе. Параметр нужен для исключения повторных запросов. Лучше всего формировать этот параметр из текущего года, месяца, дня, часа, минуты, секунды и сотых секунд на WWW-сервере Web-ресурса. Параметр должен быть целочисленным 16-ти разрядным значением и может выглядеть так: RN=2000022312121200;
- SS=SignStr - этот параметр является цифровой подписью запроса. Он гарантирует то, что именно ваш Web-ресурс выписал счет (а SSL-соединение защищает только трафик, но не обеспечивает идентификации). Для того чтобы сформировать цифровую подпись счета необходимо воспользоваться объектом WMSigner, который доступен для свободного распространения(доступны скомпилированные версии для NT, Unix под платформу Intel и в исходниках).

//Формирование строки парметров, которую необходимо подписать при выполенении Интерфейса 1
var PlanStr = '' + OrderID.toString() + LoginOfCust + PurseOfStores + Amount.toString() + Desc + InvAddress.toString() + Period.toString() + Experation.toString() + RequestN

На выходе после процесса цифровой подписи будет получена 132 (или 133)-символьная строка (SignStr), которую необходимо передать в данном параметре SS.

После выполнения запроса будет возвращена строка с информацией о том, что счет выписан в следующем формате:

WMInvId:номер - это уникальный номер счета в системе WebMoney Transfer - вы можете сохранить этот номер в базе данных вашего Web-ресурса (этот номер гарантированно уникален), и тогда проверка состояния счета (оплачен или нет) по этому номеру будет происходить быстрее, чем проверка по OrderId (собственному номеру счета Web-ресурса).

Если при выполнении запроса произойдет ошибка, то будет возвращено сообщение формата: Error:номер ошибки

Как видно из приведённого описания, после того как запрос составлен, все важные (значащие) параметры составляются в единую строку и затем подписываются электронной подписью при помощи программного средства WMSigner. WMSigner – модуль, осуществляющий подписывание электронной подписью длиной 132 бита по стандартной схеме RSA+MD4. Код модуля WMSigner на нескольких языках программирования, а также уже готовие программные модули, доступны для свободного скачивания в **соответствующем разделе официального сайта**.

Электронная подпись передаётся вместе с запросом в качестве одного из параметров. В подписываемые поля входит также уникальный (для данного магазина/ресурса/продавца) номер запроса requestN. Подобная электронная подпись обеспечивает аутентификацию продавца на сервере сертификации и исключает возможность воспроизведения записанного диалога третьей стороной.

Такой параматр как электронная подпись присутствует во всех транзакциях к интерфейсам WMT, что в купе с использованием сертифицированных https-соединений образует довольно серьёзную криптозащиту системы. Как правило, электронному подписыванию подлежат

все параметры запроса, имеющие отношение к самоё финансовоё операции, плюс идентификаторы запросов (во избежание имитации).

На официальном сервере системы доступны подробные описания следующих https-интерфейсов:

- **Интерфейс 1. Выписывание счета от одного участника (магазина, ресурса) другому участнику (покупателю) системы**
- **Интерфейс 2. Проверка состояния выписанного ранее счета (оплачен или нет)**
- **Интерфейс 3. Перевод средств с одного кошелька на другой**
- **Интерфейс 4. Перевод средств с одного кошелька на другой с протекцией сделки**
- **Интерфейс 5. Проверка выполнения операции по переводу средств между кошельками**
- **Интерфейс 6. Отправка сообщения произвольному WM-идентификатору по внуренней почте WMT**
- **Интерфейс 7. Идентификация и аутентификация клиента - владельца WM Keeper Classic на стороннем сайте**
- **Интерфейс 8. Получение информации о принадлежности кошелька WM-идентификатору**
- **Интерфейс 9. Получение доступной информации о текущем владельце WM-идентификатора (текущая заполненная информация "О себе", наличие аттестации, открытая аттестационная информация)**

В совокупности https-интерфейсы WMT предоставляют разработчику интернет-магазинов (и других платных web-ресурсов) огромную свободу в изобретении сценариев взаимодействия покупатель-продавец. Например, большое распространение получила схема оплаты товаров с протекцией сделки – в условиях взаимного недоверия покупателя и продавца товара с предоставлением услуги доставки. В таком сценарии покупатель не отдаёт сумму WM продавцу, а как бы кладёт её на общий стол, резервирует. Окончательная передача WM от покупателя к продавцу происходит только после доставки товара курьером по месту назначения. Если курьер по какой-либо причине не доставил товар, то выделенные средства через указанный покупателем период времени («период протекции сделки») снова автоматически переходят в кошелёк покупателя.

Используемая литература

1. Официальный сайт WebMoney Transfer в России: **www.webmoney.ru**
2. Официальный сайт WebMoney Transfer в мире: **www.webmoney.com**
3. Интернет-портал WM-ресурсов: **www.webmoneyworld.com**
4. Официальный сайт поддержки WMT в Украине: **www.wmcenter.com.ua**
5. Статья Андрея Шипилова «Три кита», посвящённая обзору российских платёжных систем: **http://www.ibusiness.ru/offline/2001/147/6803/index.html**
6. Конференция портала **www.void.ru**
7. Материалы переписки со службой поддержки **support@webmoney.ru**