

Краткое ознакомительное руководство по криптографии с открытым ключом

Существует два вида криптографических систем: симметричные (с одним секретным ключом) и асимметричные (с парой ключей – открытым и личным). Симметричные системы используют один и тот же секретный ключ для проведения операций шифрования и расшифровки, а асимметричные системы – личный и соответствующий ему открытый.

В симметричных системах существует проблема надежной передачи секретного ключа защищенным способом: обе стороны, обменивающиеся информацией, должны знать этот ключ.

В отличие от симметричных систем, в асимметричных системах используется пара связанных друг с другом ключей – открытый (свободно передается по сети) и личный (хранится в секрете у владельца) ключ. Зная открытый ключ, практически невозможно определить соответствующий ему личный. Таким образом, открытый ключ можно свободно передавать по сети и публиковать в общедоступных местах.

Личный ключ используется для расшифровки полученного сообщения, которое было зашифровано соответствующим открытым ключом получателя. Абонент грид-сети должен держать личный ключ в секрете, чтобы прочитать полученное сообщение мог лишь тот, кому оно адресовано. Достаточно часто личный ключ хранится на носителе в зашифрованном виде и расшифровывается только на время произведения каких-то действий, требующих знания личного ключа. Таким образом, асимметричные алгоритмы шифрования помогают обеспечить конфиденциальность при передаче сообщения от одного субъекта другому.

С помощью личного ключа субъект может подписывать передаваемое сообщение, подтверждая тем самым, что именно он является автором письма. Получатель проверяет данную подпись соответствующим открытым ключом. Неотрекаемость от подписи гарантируется тем, что подписать документ можно, только владея личным ключом. В случае, если письмо было перехвачено, то, не зная личного ключа, невозможно изменить документ так, чтобы подпись осталась неизменной. Поэтому подпись с высокой степенью достоверности свидетельствует, во-первых, о неизменности подписанного документа, во-вторых, что выработавший ее субъект знает личный ключ.

Асимметричные системы обеспечивают аутентификацию субъекта, которая сводится к доказательству владения им соответствующим личным ключом. Получатель, проверяя подпись полученного документа с помощью открытого ключа отправителя, может установить личность владельца личного ключа, которым был подписан документ.

Функции обеспечения надежной связи открытых ключей с субъектами выполняет удостоверяющий центр (УЦ).

УЦ – специальная организация, обладающая полномочиями выпускать цифровые сертификаты. УЦ позволяет аутентифицировать субъект, который владеет данным сертификатом. Подлинность связи между открытым ключом и информацией, которая идентифицирует субъекта, является важным элементом безопасности при передаче сведений, в особенности отнесенным к государственной тайне. При шифровании документа открытым ключом получателя субъект должен быть уверен, что владельцем открытого ключа является личность, которому адресовано письмо.

В качестве идентификаторов абонентов грид-среды используются цифровые сертификаты X.509. Все участники грид-среды (физические лица, службы и сервера) владеют X.509 сертификатами открытых ключей, используемыми для аутентификации. В сертификате, подписанном личным ключом УЦ, что гарантирует его подлинность, указаны идентификатор владельца (отличительное имя) и соответствующий открытый ключ (именно это связывает владельца с ключом), срок действия сертификата. Сертификат также содержит сведения о владельце открытого ключа, например, информацию, которая его дополнительно идентифицирует. Таким образом, выдавая сертификат, издатель удостоверяет подлинность связи между открытым ключом абонента и информацией, которая его идентифицирует. Персональные сертификаты в формате X.509 выдаются на длительный срок (один год и один месяц) в результате процедуры изначальной проверки подлинности абонента. Применение сертификата для аутентификации предполагает использование личного ключа, который обычно хранится в зашифрованном виде на системе пользователя и защищен паролем, который надо предъявлять при каждом его использовании.

Правила и процедуры, используемые УЦ при выпуске и управлении сертификатами, описываются в документе “Политика применения сертификатов и регламент УЦ”. Документ содержит максимально подробное и точное описание операций политики сертификации УЦ. Участникам грид-среды необходимо ознакомиться с особенностями работы УЦ и его требованиями к абонентам.