Держи золотой ключик

Управление жизненным циклом ключевых носителей

Для обеспечения высокого уровня информационной безопасности компании предпочитают применять строгую аутентификацию с использованием смарт-карт и токенов, которые необходимо учитывать и контролировать.

Автор: Денис Гундорин, руководитель направления инфраструктурных решений ИБ, Департамент информационной безопасности Softline

Осознавая неспособность парольной аутентификации обеспечить необходимый уровень безопасности в условиях современных требований к информационной безопасности, компании все чаще внедряют IT-системы на основе цифровых сертификатов и инфраструктуры открытых ключей (Public Key Infrastructure, PKI). Эти системы позволяют применять технологии электронной подписи, строгой аутентификации и шифрования данных и, таким образом, эффективно решать проблемы, возникающие при использовании парольной аутентификации.

Что это?

PKI представляет собой совокупность различных средств, предназначенных для управления ключами и цифровыми сертификатами пользователей, программ и других элементов IT-системы.

В основе PKI лежит ассимметричное шифрование, при котором для шифрования данных и/или проверки электронной подписи (ЭП) используется открытый ключ, передаваемый по открытому (незащищенному) каналу. Расшифровка сообщения и генерация ЭП выполняются с использованием закрытого ключа, который, в отличие от открытого ключа, хранится в тайне (как правило, в защищенной памяти смарт-карты).

Помимо шифрования, с которым обычно ассоциируют технологию открытых ключей, системы на основе PKI обеспечивают конфиденциальность информации и контролируют ее целостность, а также позволяют идентифицировать пользователей и ресурсы, к которым они обращаются.

Главный компонент

Это удостоверяющий центр, который выпускает сертификаты открытых ключей, удостоверяет их подлинность и сопровождает выпущенные сертификаты на протяжении всего жизненного цикла. Поэтому выбор удостоверяющего центра является одним из важнейших вопросов при внедрении PKI-системы.

Card Management System

Использование PKI-системы требует наличия у сотрудников персональных носителей ключевой информации, на которых хранятся закрытые ключи шифрования и цифровые сертификаты. Соответственно, возникает необходимость учета и контроля таких носителей. Однако базовый инструментарий удостоверяющих центров не ориентирован на управление смарт-картами пользователей и позволяет выполнять только ос-

Indeed Card Management является единой точкой предоставления доступа в сеть и приложения.

Система управления ключевыми носителями должна легко интегрироваться в IT-инфраструктуру компании, поддерживать различные удостоверяющие центры и ключевые носители.

новные операции работы с сертификатами. Поэтому другим важным вопросом при внедрении PKI-системы является выбор системы управления ключевыми носителями (Card Management System, CMS).

Такие системы обеспечивают централизованное управление ключевыми носителями и хранящимися на них сертификатами на протяжении всего их жизненного цикла, позволяя учитывать и контролировать использование смарт-карт, автоматически выполнять выдачу, перевыпуск и отзыв цифровых сертификатов, а также осуществлять аудит событий системы.

Система управления ключевыми носителями должна легко интегрироваться в IT-инфраструктуру компании, поддерживать различные удостоверяющие центры и ключевые носители. Желательна также возможность интеграции CMS-системы с системой управления логическим доступом, что существенно упрощает процедуры предоставления и получения доступа к данным.

Конечно, Indeed!

На российском рынке этим требованиям в достаточной мере соответствует решение Indeed Card Management, разработанное компанией Indeed ID и предназначенное для эффективного решения задач, связанных с применением инфраструктуры открытых ключей в масштабах предприятия.

Система позволяет управлять жизненным циклом ключевых носителей и вести учет используемых СКЗИ, автоматизировать процессы управления сертификатами пользователей, выполнять резервное копирование ключевой информации, а также предоставляет сотрудникам механизм самообслуживания для оперативного решения основных задач использования ключевых носителей и осуществляет журналирование и аудит действий администраторов и пользователей.

Ориентированная на работу с различными ключевыми носителями, данная система поддерживает широкий спектр смарт-карт и USB-ключей различных производителей, позволяя при этом использовать любые их сочетания в рамках одной инфраструктуры. Благодаря этому можно свободно выбирать модели ключевых носителей, оптимально подходящих по стоимости и функциональности для решаемых задач и условий работы компании (следует отметить, что не все CMS-системы, предлагаемые на рынке, предоставляют такую возможность).

Система поддерживает удостоверяющие центры Microsoft CA, КриптоПро УЦ 1.5 и КриптоПро УЦ 2.0. Поэтому внедрение данной системы подходит для государственных учреждений, госструктур и организаций, тесно взаимодействующих с ними, а также для других инфраструктур, где требуется ГОСТ-шифрование.

Кроме того, система Indeed Card Management может быть интегрирована с системами управления логическим доступом Indeed Enterprise Authentication и Indeed Enterprise SSO этого же разработчика, что позволяет синхронизировать жизненные циклы смарт-карт и учетных данных пользователей. В момент выпуска ключевого носителя администратор имеет возможность сразу сконфигурировать SSO-профиль пользователя, благодаря чему сотрудник, получая ключ от администратора, уже имеет все необходимое для полноценной работы. В таком сценарии работы Indeed Card Management является единой точкой предоставления доступа в сеть и приложения.

В завершение следует отметить, что помимо возможностей данная система отличается выгодной схемой бессрочного лицензирования, не требующей ежегодной оплаты использования системы, и бесплатной поддержкой в течение года после покупки лицензий.

В основе PKI лежит ассимметричное шифрование, при котором для шифрования данных и/или проверки электронной подписи (ЭП) используется открытый ключ, передаваемый по открытому (незащищенному) каналу.