

Об интеграции средств аутентификации



Алексей САБАНОВ,
к. т. н.,
ЗАО «Аладин Р.Д.»

Для аутентификации пользователей и сервисов используются цифровые сертификаты X.509, своего рода «электронные паспорта». Одним из самых надежных способов при этом является строгая двухфакторная аутентификация. Первый фактор – смарт-карта, второй – знание личного PIN-кода. Для аутентификации пользователь и система должны предоставить друг другу действительные сертификаты и обменяться несколькими последовательными сообщениями, заверенными электронной подписью. Степень доверия к данному методу повышается, если связанный с сертификатом пользователя закрытый ключ хранится в защищенной памяти смарт-карты.

Такой способ аутентификации предоставляет возможность взаимной строгой аутентификации «информационный ресурс – претендент», при этом проверяются обе стороны, и, в частности, претендент может стать пользователем только в случае успешного прохождения им проверки подлинности с помощью защищенного обмена сообщениями.

К сожалению, в штате разработчиков приложений весьма редко встречаются специалисты по защите информации, и уж тем более наладно держать в штате софтверной компании специалиста по криптографии, даже если для

Абсолютное большинство корпоративных приложений требуют тех или иных способов аутентификации, перед тем как обеспечить доступ пользователя (или отказать в нем) к приложению (авторизовать) и непосредственно к данным, с которыми это приложение работает. Аутентификация – это сервис безопасности, который лежит в основе большинства решений по защите информации. Современные информационные системы предоставляют возможность аутентификации с использованием сервисов, предоставляемых PKI-инфраструктурой.

приложения необходим процесс встраивания электронной подписи или других сервисов PKI. В итоге за редким исключением мы имеем ситуацию, когда все вопросы, связанные с безопасностью, разработчики приложений с той или иной степенью надежности перекладывают на встроенные механизмы безопасности СУБД, операционной системы и (реже – или) средств удаленного или терминального доступа. Аналогично разработчики поступают и с аутентификацией. Как правило, даже в недавно выпущенных программных приложениях в качестве единственного фактора аутентификации используется

пароль. И это даже в том случае, когда в приложении может предусматриваться применение электронной подписи. В качестве итога в крупной организации обычно имеется следующий набор для решения задач аутентификации:

- одна или несколько сетей (сегментов) под управлением серверов Windows, Novell, Linux/Unix и другими, но чаще всего с PKI-совместимыми механизмами аутентификации пользователей корпоративной сети, например, на основе цифровых сертификатов;
- десятки приложений с разными механизмами и средствами аутентификации пользователей

мнение специалиста



Сергей РЯЗАНОВ,
заместитель генерального директора, ОАО «НИИАС» –
дочернее общество ОАО «РЖД»

Построение системы аутентификации и обеспечение доступа пользователей к корпоративным ресурсам являются сложными и объемными задачами. И чем крупнее компания, тем более нетривиальным может оказаться их решение. Как организовать процедуры аутентификации пользователей? Какие при этом использовать технологии? Как обеспечить комплексное управление доступом? Как интегрировать различные средства аутентификации? Все эти вопросы задают себе крупные и распределенные компании, реализующие проекты обеспечения информационной безопасности.

ОАО «РЖД» – одна из тех компаний, которые в числе первых внедряли системы аутентификации и обеспечения доступа пользователей в своих многочисленных подразделениях. В ходе проекта мы столкнулись именно с теми трудностями, о которых идет речь в статье. Нам пришлось обеспечивать защищенный доступ пользователей к многочисленным приложениям, внедренным в разные годы и основанным на технологиях разных вендоров. Интеграция систем аутентификации с современными и одновременно с унаследованными системами стала полномасштабной научно-технической задачей. От качества ее решения зависела эффективность функционирования ряда систем информационной инфраструктуры ОАО «РЖД», их безопасность и надежность. Опыт ряда наших проектов подтверждает успешность внедрения предложенного способа интеграции средств аутентификации – идти от удобства пользователя, обеспечивать ему как можно более полные возможности SSO с использованием единого носителя ключевой информации. Такой подход способен упростить реализацию проекта в крупных компаниях и сэкономить временные и финансовые ресурсы.

приложений, чаще всего с использованием пары логин/пароль.

Примером такой постановки задачи в упрощенном виде может послужить схема (см. рисунок). В сегментах корпоративной сети под управлением серверов производства Microsoft и Novell есть возможность организовать аутентификацию с применением цифровых сертификатов, однако в этих же сегментах сети имеется ряд так называемых унаследованных приложений, доступ к которым может быть организован только по паролям. Кроме того, можно использовать встроенные механизмы PKI к приложениям Microsoft, SAP и Oracle для организации современных и более безопасных способов аутентификации.

Как организовать процесс аутентификации пользователей для обеспечения доступа к необходимому набору приложений? Сколько должно быть центров сертификации (CA), предназначенных для выпуска сертификатов аутентификации? Как интегрировать различные средства аутентификации для удобства пользователей и прозрачности администрирования? Ответы на некоторые связанные с интеграцией средств аутентификации вопросы — цель данной статьи.

Аутентификация и управление доступом

Сама по себе аутентификация никогда не является самоцелью. Она нужна как фильтр (определение «свой — чужой») для предоставления доступа или отказа в нем. При решении задачи управления доступом зачастую понятия «аутентификация», «идентификация» и «доступ» путают или пытаются подменить одно другим. В частности, написать данную статью автора сподвигла публикация с таким же, как у предлагаемого материала, названием, в которой говорилось о необходимости создания мета-каталога на основе IAM (Identity & Access Manager) — как будет показано далее, это лишь малая часть задачи. Для начала определим основные понятия и их взаимосвязь.

Задача управления доступом пользователей (другими словами — администрирование) к информационным ресурсам системы

состоит из следующих основных составляющих:

- создание идентификаторов субъектов (учетных записей пользователей) и объектов (информационных ресурсов системы, находящихся на серверах) информационной системы;
- настройка определенных способов автоматической идентификации и аутентификации пользователей и объектов информационной системы;
- управление данными субъектов, используемыми для аутентификации (издание, смена, отзыв сертификата, смена паролей и т. д.) субъекта;
- управление правами доступа субъектов к объектам информационной системы.

Под средствами аутентификации будем понимать:

- серверы аутентификации и связанные с аутентификацией сервисы современных серверных операционных систем;
- LDAP-совместимые каталоги учетных записей субъектов;
- протоколы обмена;
- клиентские части (ОС, носители ключевой информации, ключевая информация, сертификаты и пароли субъекта и т. д.).

Напомним, что идентификация — процедура распознавания субъекта по его идентификатору. В процессе регистрации субъект предъявляет свой идентификатор системе, которая проверяет его наличие в своей базе данных (LDAP-каталоге). Простейшим примером идентификатора является учетная запись, содержащая логин пользователя. Субъекты с известными системе идентификаторами считаются легальными, остальные относятся к нелегальным. С идентификацией тесно связано понятие аутентификации.

Аутентификация — процедура проверки подлинности субъекта, выполняемая, как правило, с помощью криптографических преобразований и позволяющая достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует. Если для аутентификации претендент должен предъявить смарт-карту (или eToken) с записанным в ней цифровым сертификатом (а

в защищенной памяти смарт-карты — связанным с сертификатом закрытым ключом), на основе которого организован его доступ к информационным ресурсам, а принадлежность данной смарт-карты претендент подтверждает введением личного PIN-кода, то мы имеем дело с самой строгой двухфакторной аутентификацией. Цифровые сертификаты для доступа легальных пользователей должны выпускаться корпоративным центром сертификации (CA — Certification Authority), а в поле «назначение сертификата» указываются виды доступа (доступ к корпоративной сети, удаленный доступ и т. д.). Так создается внутри-корпоративная «доверенная среда», позволяющая делать аутентификацию строгой. К слову сказать, если на предприятии корпоративными политиками безопасности полностью запрещается использование паролей для доступа к информационным ресурсам, а разрешается только аутентификация по смарт-карте с размещенным на ней сертификатом доступа по протоколу Kerberos v.5 с опцией PKINIT, то это существенно повышает ее защищенность от атак извне. Напомним, что PKINIT (Public Key Initialization) — инициализация предаутентификации с использованием открытого ключа.

Разработчики системного программного обеспечения предоставляют такие возможности уже достаточно давно: первые версии с развитыми сервисами на основе PKI корпорация Microsoft выпустила еще в 2000 г. (Windows Server 2000), незначительно отставали от Microsoft такие производители, как IBM и Novell. Из производителей СУБД наиболее глубоко интегрированными с PKI являются сегодня серверы Windows и СУБД Oracle. Однако разработчики прикладных систем далеко не всегда готовы предоставлять такие сервисы аутентификации даже сейчас, в середине 2010 г.

Итак, аутентификация связана с задачей управления доступом только как цепь последовательных действий: перед тем как пользователю будут предоставлены права на доступ к определенным системам и данным, ему надо пройти процесс идентификации и аутентификации — чтобы доказать свое право на доступ. В случае успешного прохождения

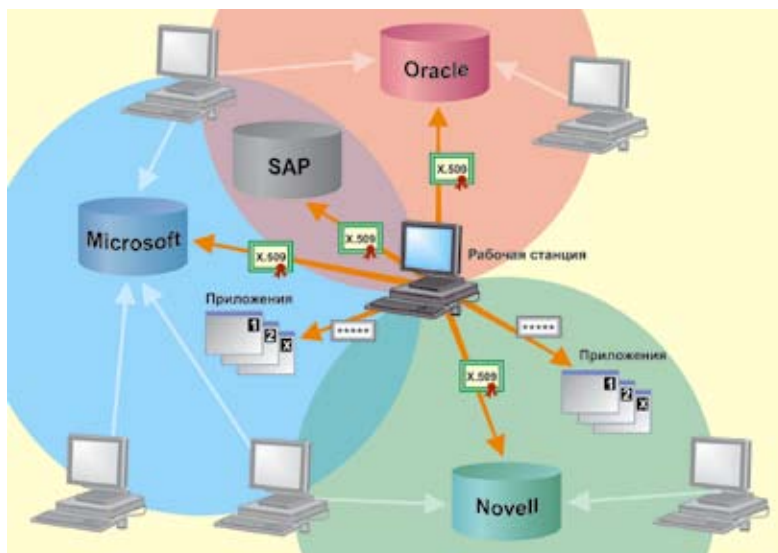
претендентом процесса аутентификации он становится легальным пользователем и получает доступ к корпоративной сети и всем необходимым для работы приложениям. Наилучшим решением по организации доступа является разворачивание корпоративного СА и настройка аутентификации пользователей только по предъявлению открытых ключей и цифровых сертификатов доступа, размещенных на смарт-карте пользователя. Подтверждение факта обладания смарт-картой осуществляется путем введения личного PIN-кода.

Управление доступом: путь создания мета-каталогов

О решении задач управления правами доступа написано не так уж много, причем авторы значительной части статей – системные интеграторы. К сожалению, большинство публикаций сводится к рекламе конкретных решений ряда производителей.

При совершенствовании системы управления доступом субъектов к информационным ресурсам вполне естественно желание сосредоточить в одном месте учетные записи всех пользователей не только корпоративной сети, но и бизнес-приложений. Интеграция учетных записей – это создание мета-каталога. Перед этим необходимо провести ряд трудоемких предварительных работ в виде «чистки» лишних записей (например, давно уволенных сотрудников), а заодно и минимизации прав доступа пользователей.

Де-факто наиболее распространенным способом управления доступом в приложениях является ролевое управление. Пользователю предоставляются права доступа к необходимым приложениям с соответствии с их служебными функциями. По правилам образования (обычно обезличенных) идентификаторов каждого пользователя, обладающего заданным набором ролей, составляется единый мета-каталог учетных записей сотрудников. Процедуру управления доступом можно автоматизировать. Такой подход для сбора всех учетных записей всех систем в один большой LDAP-



совместимый каталог разработан Microsoft, Novell, Sun Microsystems (ныне Oracle) и другими разработчиками. В качестве пользовательских средств аутентификации в продуктах названных производителей могут использоваться сгенерированные внутри смарт-карты закрытые ключи пользователей и размещенные на смарт-карте цифровые сертификаты, выпущенные корпоративным СА для доступа пользователя к информационным ресурсам. Эти мощные решения позволяют автоматизировать многие операции администраторов, в частности, достаточно оперативно менять ролевой доступ пользователя при изменении его служебного положения,

например, лишать доступа пользователя при увольнении и т. д.

Создание мета-каталога учетных записей – достаточно дорогое удовольствие как с точки зрения стоимости этого ПО от вендора, так и с точки зрения объема работ по упорядочиванию ролей (строк) с правами доступа каждого пользователя системы.

Одним из полезных следствий централизации управления доступом пользователей является возможность введения процедуры однократной аутентификации, так называемого SSO (Single Sign On), о котором чуть более подробно поговорим в следующем номере журнала. ■

Окончание смотрите в № 10, 2010 г.

Интеграция средств аутентификации крупной организации

мнение специалиста



Евгений КОЛЕСНИК,
начальник Управления по защите информации
Пенсионного фонда РФ

Каждое предприятие выбирает для себя наиболее оптимальное решение, исходя из существующих законодательных и нормативно-распорядительных требований, особенностей деятельности организации и необходимого функционала.

Для государственного учреждения таких масштабов, как ПФР, эта задача должна быть еще более тщательно проработана. При построении в ПФР централизованной системы контроля доступа и защиты информации мы отталкивались от наших первостепенных требований к обязательной защите ПДн, тайны пенсионных накоплений, обязательному шифрованию, защите каналов. При этом мы решили пойти именно по такому пути: попробовать осуществить SSO в информационные системы и системы защиты с точки зрения удобства пользователя. И не прогадали. Каждому пользователю выдан персональный носитель eToken, в защищенной памяти которого хранятся все секретные ключи, пароли, цифровые сертификаты, параметры доступа к необходимым приложениям и ресурсам с разными ограничениями для различных групп пользователей. Для повышения уровня безопасности разработаны регламенты и процедуры, которые пользователи соблюдают в обязательном порядке. По истечении трех лет успешной работы в ПФР РФ единой системы авторизации пользователей можем с уверенностью утверждать, что существующий способ организации процессов аутентификации является для нас оптимальным.