## Аутентификация на основе справочной службы Active Directory

Процедуры авторизации и аутентификации в крупных организациях часто реализуются на основе распределенной справочной службы (см. главу . Это делает их надежными, производительными и удобными в использовании и управлении.

Как было отмечено выше, Windows обладает модульной системой аутентификации, при этом доменную аутентификацию обеспечивают два типа модулей - Kerberos и MSV_1.

Модуль MSV_1 поддерживает протокол аутентификации NTLM (версии 1 и 2), который использовался в доменах Windows NT и считается теперь устаревшим и используемым только для обратной совместимости с доменами, построенными на контроллерах или рабочих станциях Windows NT. Мы не будем рассматривать этот способ доменной аутентификации подробно, отметим только, что он использует так называемую «транзитную» (pass-through) аутентификацию, когда ресурсный сервер обменивается с аутентифицируемым пользователем словом-вызовом, но передает ответ пользователя для проверки аутентичности контроллеру домена, так как только контроллер домена знает пароли пользователей. Этот способ вносит задержки в процесс аутентификации, так как каждое обращение клиента к ресурсному серверу требует обращения к контроллеру домена. Механизм аутентификации Kerberos свободен от этого недостатка, так как квитанция на доступ к ресурсному серверу может использоваться многократно.

Kerberos- аутентификация в пределах одного домена не требует больших пояснений, так как ее схема в точности совпадает с описанной выше в разделе «Система Kerberos». Kerberos KDC в этом случае работает на контроллере домена, там же располагается база учетных данных пользователей и ключи ресурсных серверов. При логическом входе пользователя в домен происходит интерактивная аутентификация, при этом в качестве ресурсного сервера выступает компьютер пользователя, который должен быть членом домена. При успешной аутентификации пользователь получает доступ к своему компьютеру как пользователь домена, а также как член одной или нескольких групп домена – при условии, что данному пользователь и/или группам, в которые он входит, дано право логического входа в данный компьютер.

Сетевая (неинтерактивная аутентификация) при доступе пользователя к ресурсному серверу, отличному от компьютера, на котором он интерактивно работает, также происходит в точности со схемой, описанной в разделе «Система Kerberos».

В случаях, когда компьютер пользователя или ресурсный сервер находятся в домене, отличном от того домена, где был создана учетная запись пользователя, схема Kerberos-аутентификации немного усложняется. Как мы помним, аутентификационная информация пользователя – пароли – никогда не копируется в копии глобального каталога, а всегда хранится только в базе пользовательских данных того домена, к которому пользователь относится. Поэтому Kerberos-серверы различных доменов должны взаимодействовать в том случае, когда пользователь и ресурс находятся в разных доменах.

В качестве примера мы рассмотрим простой случай, когда имеется три домена, входящие в одно дерево. Эти домены показаны на рис. 16.12: корнем дерева является домен abc.ru, а листьями – домены moscow.abc.ru и orel.abs.ru. Между доменами существуют доверительные отношения «родитель-потомок», установленные автоматически при создании доменов-потомков. Важным фактом для рассмотрения междоменной Kerberos-аутентификации является то, что при установлении доверительных отношений создается разделяемый междоменный ключ, который хранится в базе Kerberos KDC каждого домена.

Рассмотрим отдельно случаи интерактивной и неинтерактивной многодоменной аутентификации.

### Интерактивная аутентификация

Боб является пользователем домена moscow.abc.ru, о чем говорит его имя bob@moscow.abc.ru. В рассматриваемом случае Боб выполняет логический вход с компьютера `dell12.orel.abc.ru`, являющегося членом домена `orel.abc.ru`, то есть чужого домена (см. рис.5.14).

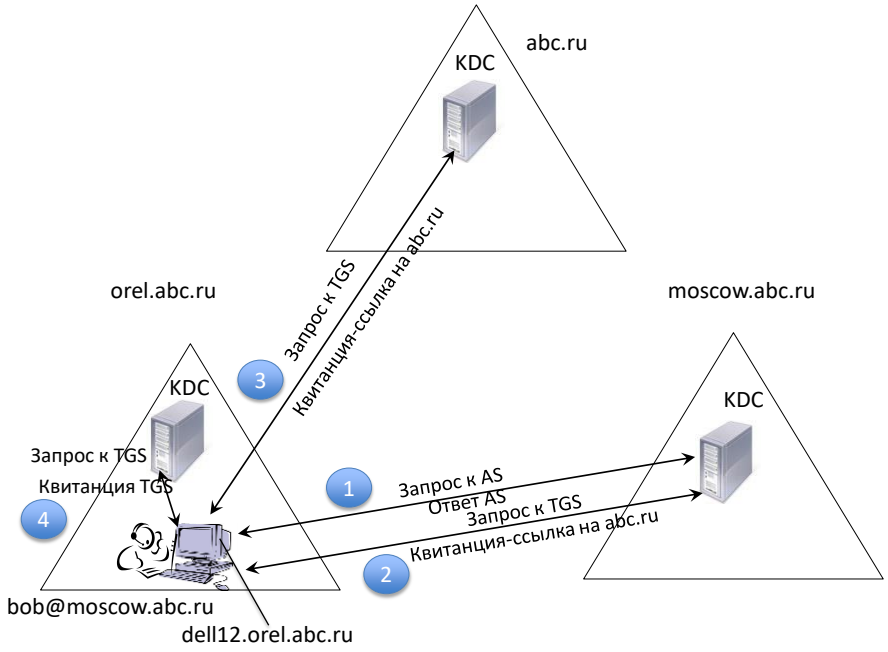


Рис. 5.14. Интерактивная многодоменная Kerberos-аутентификация

После ввода имени bob@moscow.abc.ru модуль Kerberos-аутентификации компьютера `dell12.orel.abc.ru` отправляет запрос на аутентификацию AS серверу домена `moscow.abs.ru`, так как только этот сервер хранит пароли пользователей этого домена `moscow.abc.ru`. Получив этот запрос, сервер AS направляет обычный ответ, в котором содержатся квитанция на доступ к серверу квитанций TGS и ключ сеанса, зашифрованные паролем пользователя.

Получив ответ AS, модуль Kerberos компьютера `dell12.orel.abc.ru` расшифровывает квитанцию и ключ сеанса, используя пароль, введенный Бобом.

Второй этап состоит в отправке компьютером `dell12.orel.abc.ru` запроса к серверу квитанций домена `moscow.abc.ru` за квитанцией доступа Боба к компьютеру `dell12.orel.abc.ru`. Сервер TGS домена `moscow.abc.ru` не может выдать такую квитанцию, так как ресурс находится не в его домене. Вместо этого он отправляет так называемую квитанцию-ссылку, которая указывает на домен `abc.ru` как на ближайший домен, с которым у домена `orel.abc.ru`, которому принадлежит ресурс, есть непосредственные доверительные отношения (а не транзитные). Квитанция-ссылка шифруется междоменным ключом, разделяемым доменами `abc.ru` и `moscow.abc.ru`.

Третий этап состоит в обращении компьютера `dell12.orel.abc.ru` с квитанцией-ссылкой к серверу TGS домена `abc.ru`. Этот сервер расшифровывает квитанцию-ссылку междоменным ключом и генерирует квитанцию доступа к компьютеру `dell12.orel.abc.ru`, зашифрованную ключом этого компьютера, вместе с новым ключом сеанса, а затем зашифровывает эту квитанцию старым ключом сеанса пользователя.

Четвертый этап является обычным для однодоменной схемы работы Kerberos – модуль Keberos-аутентификации пользователя расшифровывает квитанцию доступа старым ключом сеанса и передает ее вместе с аутентификатором пользователя, зашифрованным новым ключом сеанса, модулю Kerberos-аутентификации ресурсного сервера, в качестве которого выступает Kerberos-модуль компьютера `dell12.orel.abc.ru`. Последний расшифровывает квитанцию ключом, разделяемым с сервером квитанций TGS, и извлекает из нее новый ключ сеанса, с помощью которого расшифровывает аутентификатор.

### Неинтерактивная аутентификация

Этот случай иллюстрируется рис. 5.15, на котором представлены те же три домена, что мы рассматривали в предыдущем разделе, но на этот раз пользователь Алиса из домена `orel.abc.ru` работает за компьютером `com33.orel.abc.ru`, который также принадлежит этому домену.

*Первый этап*. Алиса уже аутентифицировалась для работы с этим компьютером (этот этап мы опускаем) и получила квитанцию на доступ к серверу TGS. Теперь ей нужен доступ к почтовому серверу `mail.moscow.abc.ru`, который находится в домене `moscow.abc.ru`. Сначала Алиса обращается за квитанцией доступа к почтовому серверу к серверу квитанций своего домена. Однако этот сервер не может ей выдать искомую квитанцию, так как ресурс находится за пределами его пространства имен. Поэтому он возвращает квитанцию-ссылку на сервер `abc.ru`, с которым у домена, которому принадлежит ресурс, есть прямые доверительные отношения.

*Второй этап*. Сервер TGS домена `abc.ru` возвращает квитанцию-ссылку на сервер TGS домена `moscow.abc.ru`, которому принадлежит ресурс `mail.moscow.abc.ru`.

*Третий этап*. Модуль Kerberos компьютера `com33.orel.abc.ru` отправляет запрос серверу TGS домена `moscow.abc.ru` на доступ к серверу `mail.moscow.abc.ru`. Сервер TGS может обслужить этот запрос и отправляет квитанцию на доступ.

*Четвертый этап*. Модуль Kerberos компьютера `com33.orel.abc.ru` отправляет серверу `mail.moscow.abc.ru` квитанцию доступа вместе с аутентификатором Алисы. Сервер `mail.msocow.abc.ru` проверяет аутентичность Алисы обычным для Kerberos способом.

При описании неинтерактивной аутентификации мы опустили подробности использования ключей, но читатель может дополнить этот пробел сам, пользуясь схемой интерактивного доступа.

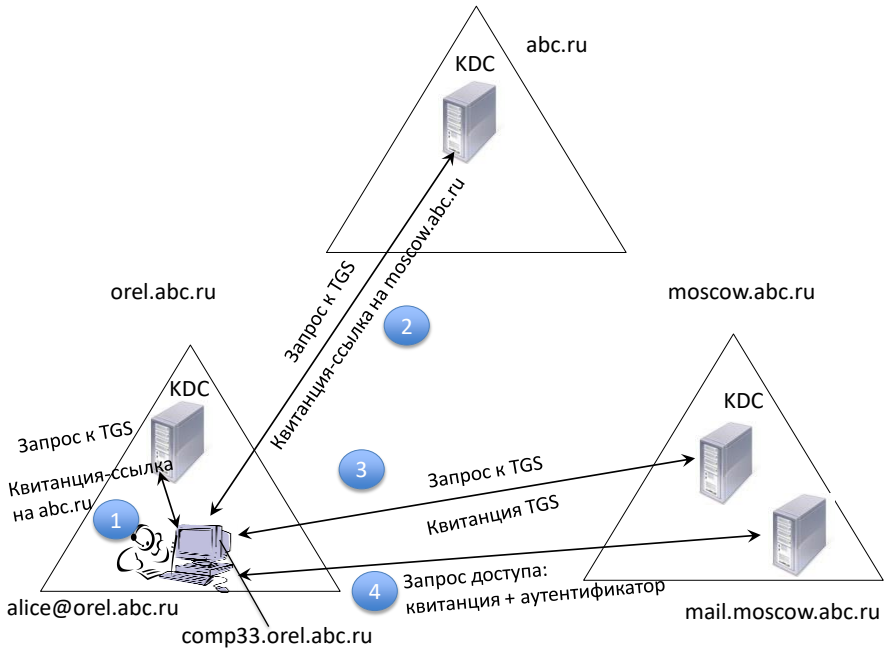


Рис. 5.15. Неинтерактивная многодоменная Kerberos-аутентификация

Реализация Kerberos в системе Active Directory использует фирменное расширение Micorsoft этого протокола, помогающее авторизации пользователей ресурсными серверами. Для этого квитанция на доступ к ресурсу включает ***сертификат привилегий пользователя (Privilege Attribute Certificate, PAC)***, который содержит идентификаторы групп, которым принадлежит пользователь, а также права пользователя.