4. Типовая служба ролей

4.1 Информация о службе

Наименование службы	Типовая служба ролей
Версия службы	1
Идентификатор службы	Для системы, использующей типовую службу ролей MoReq2010: 2f6d05c6-51e6-4a32-a7fc-c0a6883eb85b Для системы, использующей собственную службу: d945dcd9-dc2d-491d-965a-11ce936d044b

4.2 Обеспечение соответствия типовой службе ролей

4.2.1 Отсутствие общепринятого стандарта для ролей и разрешений

В данном разделе спецификаций MoReq2010 описывается типовая служба ролей и функциональные требования к ней, определяющая, каким образом осуществляется авторизация пользователей для выполнения функций в системе.

На момент публикации Moreq2010 не существует какого-либо распространенного стандарта, описывающего, каким образом осуществляется предоставление пользователям разрешений на работу с объектами в информационной системе. Распространенные модели, основанные на принципе «создание, чтение, обновление, удаление» слишком просты для использования в системах управления записями. В таких моделях, например, не проводится различия между полным и неполным удалением, а также отсутствует возможность создания остаточных объектов, что для систем управления записями является необходимым.

Ввиду отсутствия общепринятых стандартов поставщики разработали собственные подходы для контроля доступа пользователей к системам управления записями. Эти методы, во многих случаях обладающие высокой эффективностью, являются, как правило, связанными с конкретным приложением и не обеспечивают интероперабельности, так как модель одного поставщика может не совпадать с моделью другого.

4.2.2 Типовая служба ролей

Типовая служба ролей MoReq2010 представляет собой простую стандартизированную модель, предназначенную для систем управления записей и представленную в форме спецификаций. Все усилия были направлены на разработку нейтральной модели , основанной на понятиях, общих для большинства информационных систем — таких, как списки доступа или определения ролей.

В то же время типовая система ролей MoReq2010 описывает единственно возможный подход к контролю доступа и исходит из признания того факта, что этот подход может существенно отличаться от подходов, использовавшихся в системах управления записями ранее, что делает невозможным их тестирование на предмет соответствия настоящим спецификациям. Тестирование возможно только в случае их серьезной переработки.

Возникает сложная ситуация: типовая служба ролей вполне может быть использована в новых продуктах, тогда попытки приспособить ее к уже имеющимся на рынке продуктам могут оказаться неэффективными.

4.2.3 Подходы к тестированию и сертификации типовой службы ролей

По указанным выше причинам Форум по управлению жизненным циклом документов допускает два возможных подхода к тестированию на соответствие типовой службы ролей спецификациям MoReq2010.

A. В системе внедряется типовая служба ролей MoReq2010, а затем проводится тестирование на соответствие,

или

B. Система использует собственную модель, которая при этом должна соответствовать следующим критериям:

- должно быть подтверждено, что используемая модель обладает той же гибкостью и функциональностью, что и типовая служба ролей MoReq2010;
- она должна поддерживать интероперабельность; например, при экспорте списков доступа в формат XML, используемый в типовой службе ролей, должны сохраниться уровни доступа пользователей и групп к объектам, а также права на выполнение функций, которые будут экспортированы в другую систему управления записями.

4.2.4 Как обеспечивается соответствие альтернативным требованиям (типа B)

Для подтверждения уровня гибкости и функциональности, эквивалентного MoReq2010, в системе должна обладать следующими характеристиками:

- пользователь не может получить доступ к любому объекту в системе, не имея соответствующего разрешения, как индивидуально, так и в составе группы;
- в системе существуют множественные уровни доступа к объектам, конфигурируемые пользователями, в том числе и возможность по собственному усмотрению предоставлять разрешение на:
  - просмотр одних объектов с одновременным запретом на просмотр других;

    - выполнение одних функций с одновременным запретом на выполнение других.
- разрешение на доступ к объектам и выполнение функций может быть предоставлено как на уровне индивидуального объекта, так и на уровне набора объектов — например, агрегации записей;
- разрешение на доступ к объектам и выполнение функций может быть предоставлено в разных частях системы разными способами: например, должна существовать возможность предоставления пользователю разных прав на доступ к разным классами внутри одной и той же классификационной схемы;
- при создании нового объекта на него создается определенный набор прав по умолчанию: например, для новой запись, добавляемой в агрегацию, должен быть сформирован такой же набор прав, как и для всех остальных записей в этой агрегации;
- в системе существуют роли или права, которые не могут быть заблокированы владельцами определенных объектов, поэтому пользователи, имеющие эти роли или права, могут администрировать всю систему или ее часть.

При переводе метаданных из нативных форматов систем в формат метаданных MoReq2010 необходимо учитывать следующее:

- ни один пользователь не может получить в новой системе больше прав на доступ к объектам, чем в исходной системе;
- ни один пользователь не может получить разрешения на выполнение функций, которого у него не было в предыдущей системе;
- право, предоставленные группе пользователей, не может быть предоставлено каждому отдельному пользователю, входящему в эту группу;
- система управления записями должна во всех случаях, когда это возможно, осуществлять наследование в соответствии с MoReq2010 и избегать множественного повторения записей доступа для каждого экспортируемого дочернего объекта, когда возможно применить один набор записей доступа родительского объекта;
- поставщик должен описать алгоритм конвертации данных, используемый в системе управления записями, а также дать информацию и примеры того, каким образом экспортированные данные для ролей и списки доступа воспроизводят модель MoReq2010;
- поставщик должен обеспечить возможность включения схемы распределения доступа в полный тестовый отчет по своему продукту.

Дополнительные рекомендации и указания можно получить, обратившись в Управляющий совет MoReq через секретариат Форума по управлению жизненным циклом документов.

Далее будут представлены основные понятия и функциональные требования к типовой системе ролей MoReq2010.

4.3 Основные понятия

4.3.1 Определение ролей

Перед тем, как выполнить любую функцию по отношению к любому объекту, система должна проверить, обладает ли пользователь, запросивший выполнение функции, достаточными правами. Право на выполнение функций пользователи получают при предоставлении ролей.

Пользователь, подлинность которого установлена надлежащим образом, входящий в систему для выполнения функции в рамках имеющихся у него прав, называется авторизованным пользователем.

Так как одна и та же роль может быть назначена нескольким объектам, а также использоваться в нескольких системах управления записями, управление ролями осуществляется с помощью службы ролей. Определение ролей представляет набор определений функций, как это показано на рисунке 4a.

Определения ролей и определения функций могут быть связаны отношениями типа «многие ко многим»: с одной ролью могут быть ассоциированы несколько определений функций.

Термин «роль» обозначает набор функций, организованных логически таким образом, что право на их выполнение предоставляется избранным пользователям коллективно.

Выстраивание ролей подобным образом, с основой на взаимосвязанных наборах функций, является неотъемлемой чертой систем управления записями. MoReq2010 описывает очень много наборов функций, и было бы непрактичным приписывать их каждому пользователю или каждой группе отдельно.

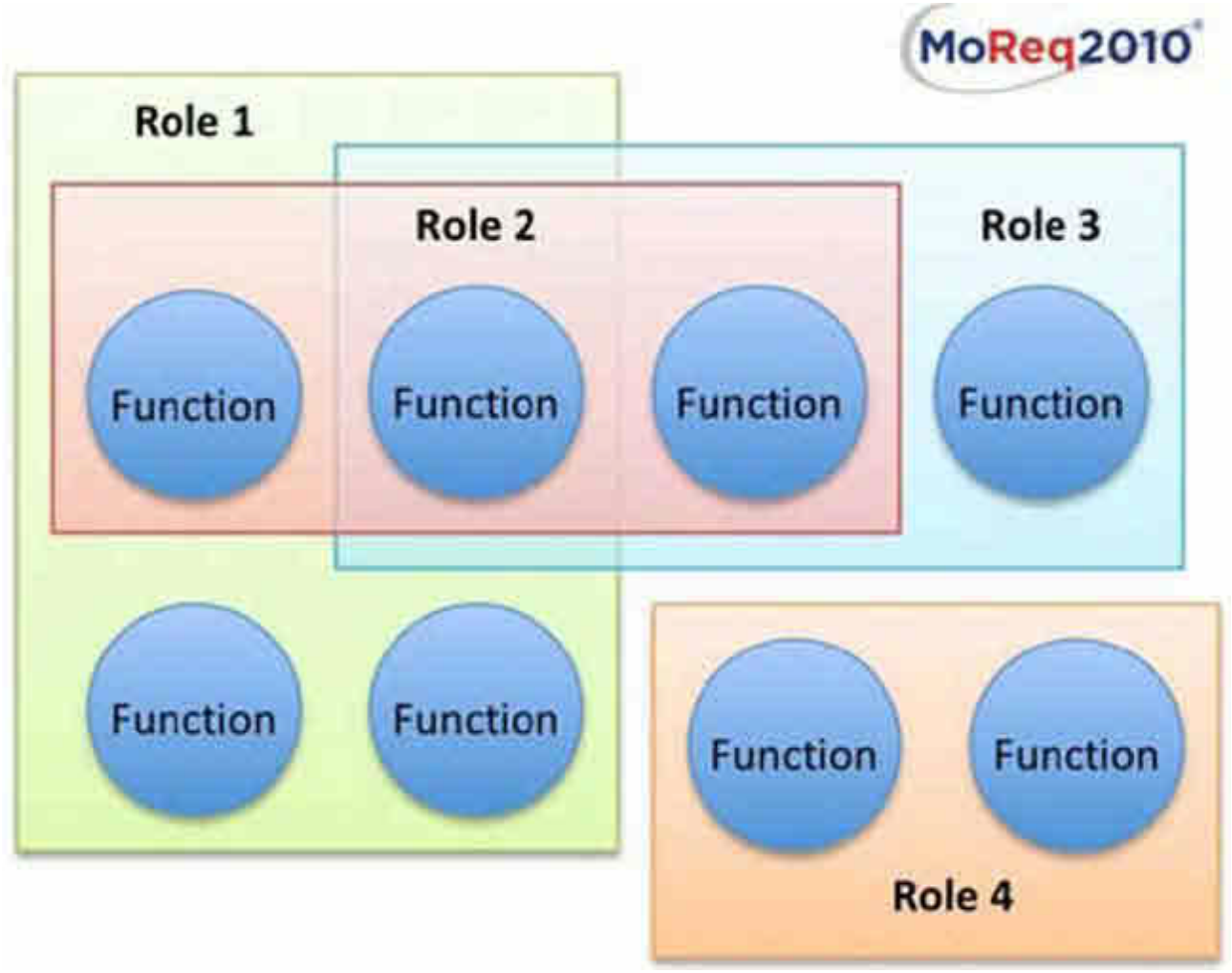


Рисунок 4а. Функции ассоциируются с ролями (каждая функция должна быть входить в состав по крайней мере одной роли).

4.3.2 Предоставление ролей

Роль может быть предоставлена как пользователю, так и группе относительно любого объекта системы, включая службы. При предоставлении роли создается запись доступа, в которой перечисляются пользователи или группы, а также предоставляемые им роли; затем она добавляется в список доступа соответствующего объекта.

Предоставление пользователю роли по отношению к объекту позволяет этому пользователю выполнять применительно к объекту все функции, указанные в определении роли.

При предоставлении роли группе каждый пользователь, являющийся членом этой группы, получает эту роль (см. **3. Служба пользователей и ролей**). Новые пользователи, вступающие в группу, автоматически наследует эту роль, тогда как пользователи, выходящие из состава группы, автоматически теряют все права в рамках данной роли; роль при этом не назначается каждому пользователю индивидуально.

Рекомендуется предоставлять роли группам, а не индивидуальным пользователям : таким образом проще управлять доступом к объектам, когда пользователи уходят из организации или меняют работу, не внося изменений в списки доступа для объектов системы.

Управление группами значительно проще и меньше подвержено ошибкам по сравнению с управлением ролями для каждого пользователя в отдельности.

На рисунке 4b показано, как пользователю или группе приписывается одна или несколько ролей по отношению к объекту, а в список доступа объекта добавляется новая запись. Каждый объект системы, равно как и каждая служба, обладает собственным списком доступа.

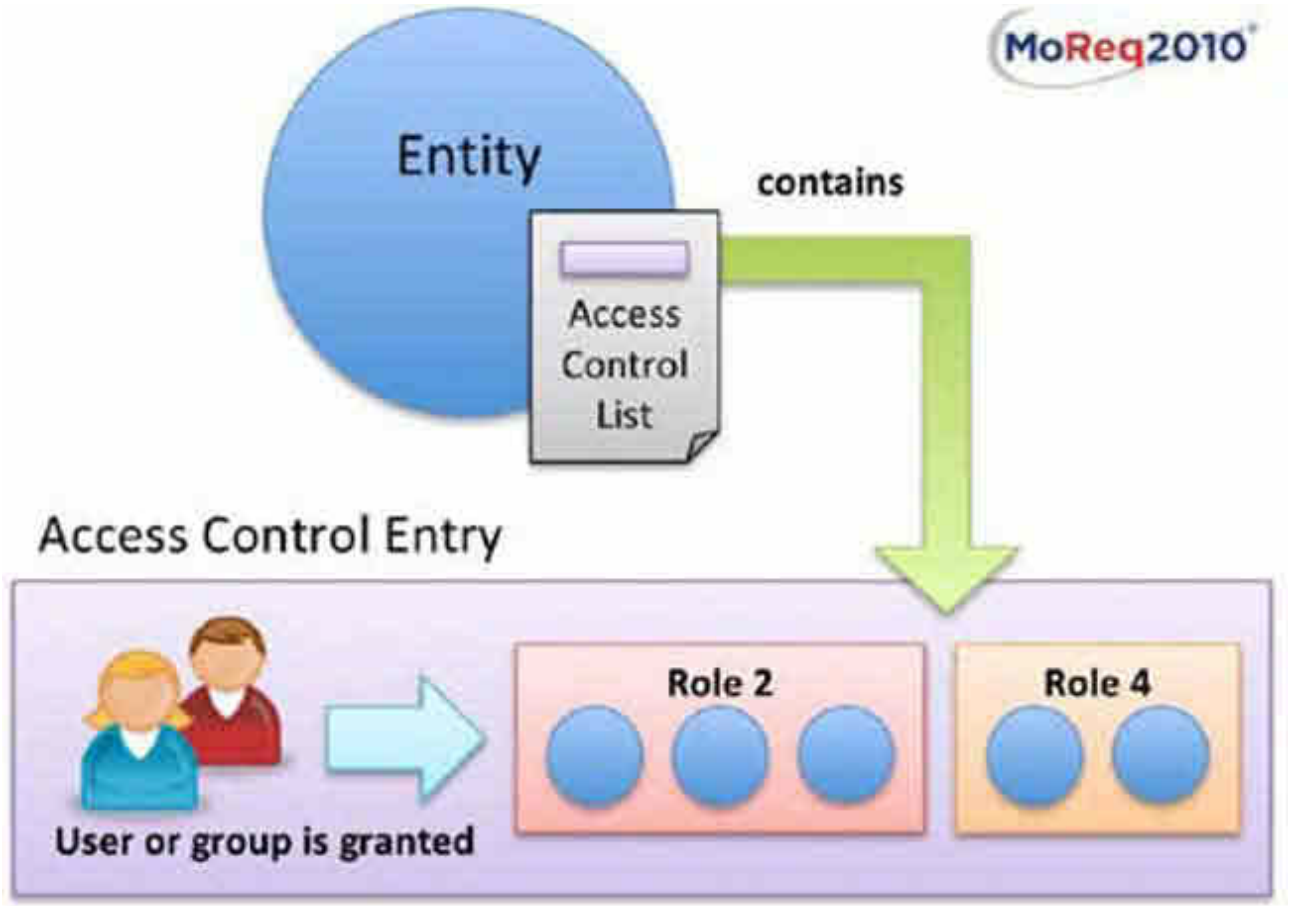


Рисунок 4b. Список управления доступом состоит из записей, связывающих пользователей или группы с ролями.

4.3.3 Наследование ролей

Помимо записей в списке контроля доступа объект может также наследовать роли, полученные пользователями и группами при работе с другими объектами. В функциональных требованиях MoReq2010 описаны ситуации, в которых осуществляется такое наследование. Как правило, если один объект является родительским по отношению к

другому, порожденный объект наследует список доступа родительского . Например, порожденная агрегация наследует от родительской агрегации, равно как и запись. Существует обстоятельства, при которых один объект может наследовать из множественных источников; подробнее об этом см. в **4.3.5 Множественное наследование .**

Наследование является одним из важных механизмов управления большими системами записей, в которых предоставление ролей по отношению к отдельным объектам оказывается непрактичным.

Для некоторых ролей в случае необходимости наследование может осуществляться не по стандартной модели. MoReq2010 предусматривает, чтобы в каждый список доступа был включен флажок наследования ролей, показывающий, были ли унаследованы родительские роли порожденными объектами.

Если в списке доступа убран флажок наследования ролей, то будут автоматически наследоваться только лишь административные роли.

4.3.4 Административные роли

В MoReq2010 выделяется два типа ролей:

- административные роли и
- неадминистративные роли.

Тип роли описывается в ее определении.

Административная роль, предоставленная по отношению к службе в целом или к любому родительскому объекту, всегда применяется по отношению к объектам, являющимся порожденными по отношению к этой службе или объекту. В этом случае для административных ролей флажок наследования не устанавливается.

Неадминистративные роли наследуются порожденными объектами только тогда, когда в списке контроля доступа порожденного объекта разрешено наследование ролей.

Наглядный пример приведен на рисунке 4c. Роль2 является административной, а роль 4 — неадминистративной. Для порожденного объекта 1 установлен флажок «Включать унаследованные роли», и поэтому он наследует как роль2, так и роль4. Однако для порожденного объекта 2 такого флажка не установлено, и поэтому он наследует лишь роль 2, являющуюся административной.

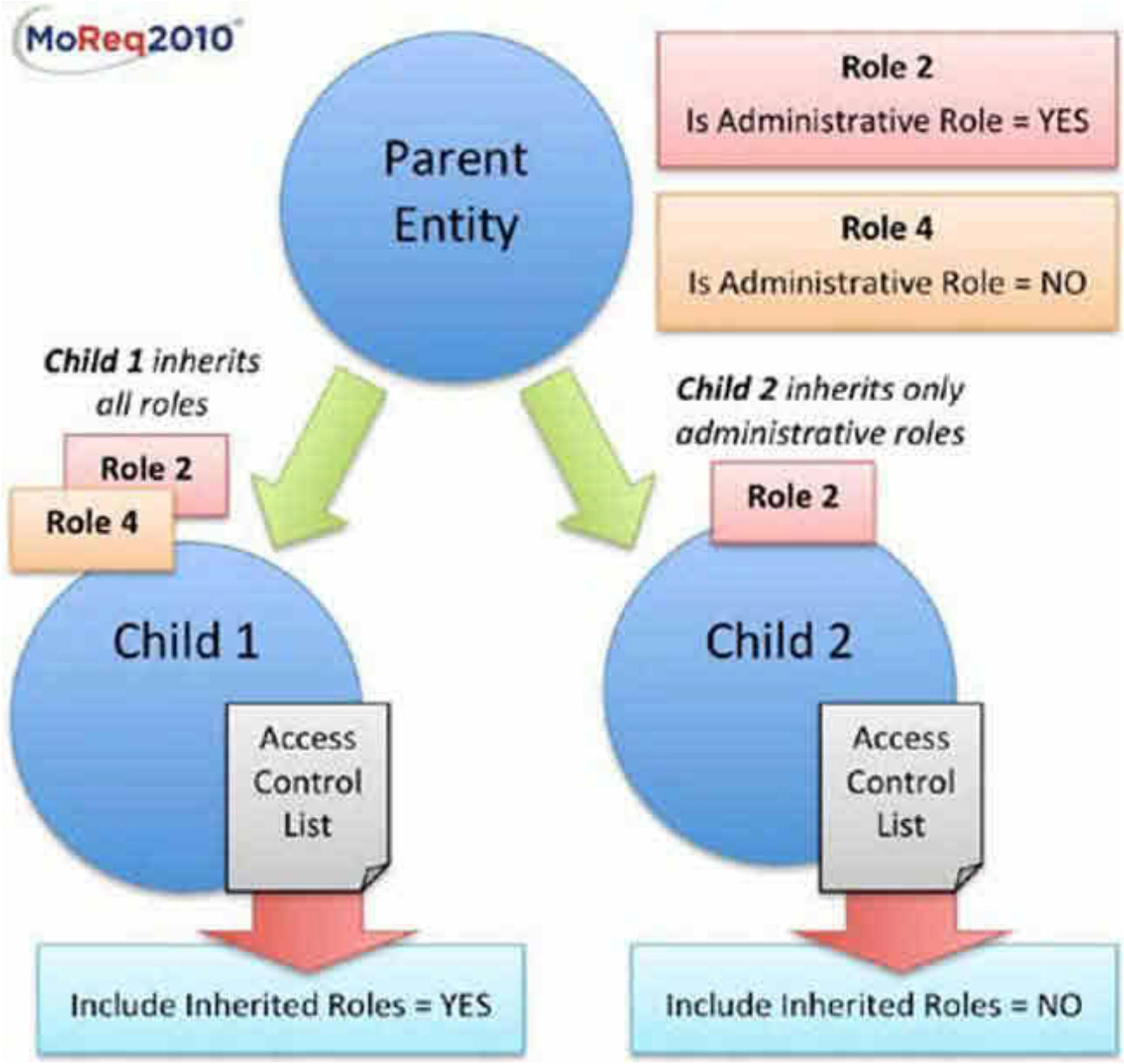
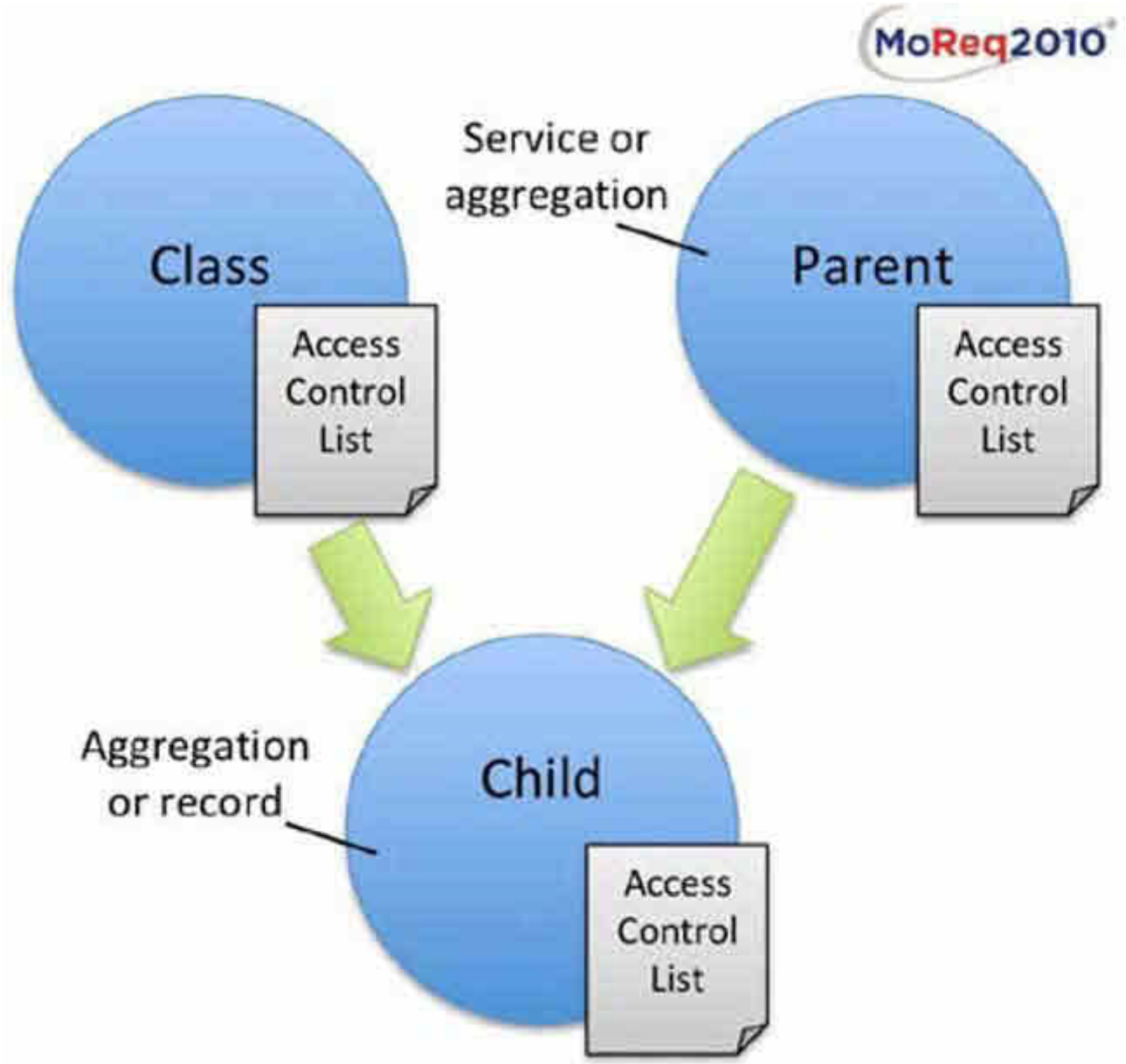


Рисунок 4c. Административные роли наследуются всегда, независимо от того, установлен ли флажок наследования ролей.

4.3.5 Множественное наследование

Как уже было указано выше, в настоящих спецификациях предусмотрены случаи, когда один объект наследует роли от нескольких объектов.

Например, агрегации и записи, поддерживаемые службой записей, унаследуют от родительской агрегации список доступа, а также классификации. Это показано на рисунке 4d. В этом случае порожденный объект унаследует от родительского как роли, так и классы. Естественно, если наследование ролей отключено, то порожденный объект унаследует только административные роли.



4d . - Иногда списки контроля доступа могут наследоваться из более чем одного источника.

4.3.6 Предзаданные роли

Очень часто системы управления записями устанавливаются с заранее установленной поставщиком по умолчанию системой ролей — это делается для удобства организации клиента, которая получает в этом случае возможность немедленно приступить к использованию системы. В таком случае некоторые из предзаданных ролей могут быть изменены или даже полностью (если они не были использованы) или частично удалены авторизованным пользователем, тогда как другие предзаданные роли могут быть защищены поставщиком и оставаться неизменными в рамках одного решения по управлению записями.

4.5 Функциональные требования

R4.5.1 Система должна позволять авторизованному пользователю создавать роли, обладающие по крайней мере следующими метаданными:

- системный идентификатор;
- метка времени создания;
- дата/время происхождения;
- индикатор административной роли;
- метка времени начала использования;
- название;
- описание;
- ограничительная помета;
- идентификатор определения функции;
- метка времени удаления.

Каждая роль также обладает:

- историей событий (см. **2. Системные службы**);
- списком доступа для роли;

и также может обладать

- контекстуальными метаданными (или их эквивалентом, см. **7. Типовая служба метаданных**).

*В зависимости от подхода, используемого в системе для создания **7. Типовой службы метаданных**, механизм, с помощью которого осуществляется добавление элементов контекстуальных метаданных к системным объектам, может различаться.*

*Обратите внимание на то, что предзаданные роли поставляются как часть системы управления записями, а не создаются пользователями, однако они обладают теми же метаданными, что и роли, созданные пользователями (см. **4.3.6 Предзаданные роли)**.*

R4.5.2 Система должна позволять авторизованному пользователю изменять название, описание и ограничительные пометы роли, равное как и ее контекстуальные метаданные.

*Обратите внимание на то, что данная функция не может быть применена к предзаданным ролям, установленным в системе по умолчанию (см. **4.3.6 Предзаданные роли)**.*

R4.5.3 Система должна позволять авторизованному пользователю придавать роли статус административной/неадминистративной, но только в случае, если роль не была включена ни

в одну из записей доступа.

После того, как роль была использована, уже невозможно изменить ее статус с административного на неадминистративный, и наоборот — это может иметь непредсказуемые последствия для объектов, по отношению к которым была предоставлена роль, а также к их порожденным объектам.

*Обратите внимание на то, что данная функция не может быть применена к предзаданным ролям, установленным в системе по умолчанию (см. **4.3.6 Предзаданные роли)**.*

R4.5.4 Система должна позволять добавлять определения функций к активным ролям и удалять их, обеспечивая при этом ассоциацию каждого определения функции по крайней мере с одной ролью.

В противном случае могут появиться функции, которые никогда не будут выполнены. Определения функций добавляются во время использования активных ролей.

Определения функций не могут быть добавлены к остаточным (резидуальным) ролям и, соответственно, удалены из них. Остаточные (резидуальные) роли могут сохранять отсылку к определениям функций, которые были связаны с ними на момент удаления

*Обратите внимание на то, что данная функция не может быть применена к предзаданным ролям, установленным в системе по умолчанию (см. **4.3.6 Предзаданные роли)**.*

R4.5.5 Система должна позволять авторизованному пользователю полностью удалять роль, ни разу не включенную ни в один из списков доступа, при условии, что каждое определение функции все время ассоциировано по крайней мере с одной активной ролью.

При первом включении роли в запись доступа система должна установить метку времени начала использования.

*Обратите внимание на то, что данная функция не применяется к предзаданным ролям, являющимся частью системы по умолчанию. (см. **4.3.6 Предзаданные роли)**.*

R4.5.6 Система должна позволять авторизованному пользователю осуществлять частичное удаление роли, которая уже была включена в запись доступа при условии, что каждое определение функции все время ассоциировано по крайней мере с одной активной ролью.

После начала использования роль уже может быть удалена не полностью (как это описано в R4.5.6), а лишь частично. После частичного удаления сохраняется остаточная роль. Остаточная роль не дает пользователям прав на выполнение функций.

*Обратите внимание на то, что данная функция не применяется к предзаданным ролям, являющимся частью системы по умолчанию. (см. **4.3.6 Предзаданные роли)**.*

R4.5.7 В соответствии с R2.4.22 и в дополнение к R2.4.11, система должна позволять авторизованному пользователю просматривать роли и определения функций по крайней мере следующими способами:

- просматривать в службе ролей роли и их метаданные;
- просматривать в службе ролей определения функций и их метаданные;
- переходить от роли к определениям функций, включенным в эту роль, и просматривать их метаданные;
- переходить от определения функции ко всем включающим его ролям и просматривать их метаданные.

*Значение термина просматривать указано в **13. Глоссарий.***

R4.5.8 Система должна автоматически создавать для каждой службы или группы служб (R2.4.1), а также для каждого системного объекта (в случаях, когда это необходимо) список управления доступом, обладающим следующими метаданными:

- индикатор наследования ролей (M14.4.43)

Каждый список управления доступом также включает:

- записи доступа для каждого объекта.

*Список управления доступом представляет собой структуру данных (ее детальное определение приведено в **D14.3.2**) содержащую записи доступа, определяющие, какие именно пользователи и группы могут получать доступ к объектам в рамках конкретных ролей. Каждый список управления доступом является неотъемлемой частью объекта; каждому объекту принадлежит единственный список управления доступом.*

Списки управления доступом применяется в MoReq2010 как к объектам, так и к службам, поэтому могут быть унаследованы всеми объектами в службе. Список управления доступом для службы записей наследуется только корневыми агрегациями. Таким образом, например, обеспечивается возможность предоставить группе пользователей административный доступ к классификационной схеме внутри службы классификаций. Если в организации используются две службы классификаций , то управление службами может осуществляться двумя группами независимо друг от друга, и у каждой из служб будет собственный список управления доступом.

Необходимость наличия списков управления доступом для большинства типов объектов прописана в других требованиях. Например, требованием R2.4.2 для модуля системных служб, требованием R2.4.10 для типов объектов, требования R2.4.12 для определений функций; аналогичным образом в службе пользователей и групп — требованием R3.4.1 (для пользователей) и требованием R3.4.8 (для групп).

В базовых службах MoReq2010 только списки управления доступом, записи доступа, события и компоненты не имеют собственных списков управления доступом. Обратите внимание на то, что в состав метаданных списков управления доступом не входит отдельный системный идентификатор, так как список управления доступом принадлежит объекту и является его неотъемлемой частью. Индикатор наследования ролей, таким образом, включается в состав метаданных каждого объекта, имеющего список контроля доступа.

Значение индикатора для службы не имеет никакого значения, так как службы не наследуют списков управления доступом.

Индикатор наследования ролей означает лишь то, что объект унаследует только списки управления доступом для административных ролей. Наследование административных ролей не может быть заблокировано.

R4.5.9 Система должна позволять авторизованному пользователю просматривать списки управления доступом и содержащиеся в них записи.

Данная функция является отдельной от общих метаданных объекта.

R4.5.10 Система должна позволять авторизованному пользователю изменять список управления доступом к объекту, изменяя таким образом значение индикатора наследования ролей, а также добавлять, изменять и удалять записи доступа со следующими метаданными:

- идентификатор пользователи или группы и
- идентификатор роли.

Записью доступа называется структура данных, включенная в список управления доступом. Записи доступа всегда ходят в какой-либо список.

Каждый объект может иметь только одну запись доступа, относящуюся к конкретному авторизованному пользователю или группе. Каждая запись должна быть снабжена идентификатором пользователя или группы и по крайней мере одним идентификатором роли. Добавляя запись в список управления доступом, авторизованный пользователь предоставляет определенным пользователям и группам право на выполнение функций по отношению к объекту и его порожденным объектам. Удаляя запись из списка, авторизованный пользователь лишает определенных пользователей и группы этого права. Изменяя запись доступа, авторизованный пользователь может увеличить или уменьшить число ролей, тем самым расширяя или сужая набор функций, применяемый по отношению к объекту и его порожденным объектам.
В ситуации, описываемой требованием R2.4.15, в соответствии с R2.4.13, при добавлении, изменении или удалении записи доступа в истории событий объекта всегда создается новое событие.

R4.5.11 Система должна позволять пользователю выполнять любую функцию по отношению к любому объекту при условии, что эта функция включается в активную роль, предоставленную пользователю или любой активной группе, членом которой является этот пользователь, в особенности по отношению к этому объекту, включая роли, наследуемые от службы, родительского объекта или класса (если таковые имеются).

Специфические правила наследования, используемые в типовой службе ролей, выглядят следующим образом.

- *корневые агрегации осуществляют наследование от службы записей и от своих классов;*
- *порожденные агрегации наследуют роли от родительских агрегаций и их классов;*
- *компоненты используют списки управления доступом для записей, к которым они принадлежат (собственных списков управления доступом они не имеют);*
- *указания о запрете на уничтожение наследуют роли от службы графиков удаления;*
- *графики удаления наследуют от службы графиков удаления;*
- *объекты наследуют роли от службы, к которой они принадлежат;*
- *определения функций наследуют роли от службы, к которой принадлежат связанные*

с ними объекты;

- *группы наследуют от службы пользователей и групп;*
- *определения элементов метаданных осуществляют наследование от службы метаданных;*
- *записи наследуют от родительской агрегации и собственного класса;*
- *роли наследуют от службы ролей;*
- *шаблоны наследуют от службы метаданных;*
- *пользователи наследуют от службы пользователей и групп.*

Наследование объектом ролей от его службы, родительского объекта или класса зависит от значения индикатора наследования ролей. Административные роли наследуются всегда, тогда как неадминистративные роли будут наследоваться только в случае, если установлен флажок наследования ролей.

При получении роли группой пользователи, входящие в ее состав, наследуют роль в течение всего время, пока они остаются членами группы, а группа остается активной. Пользователи не наследуют ролей, назначенных удаленным группам.

В этом требовании разъясняется значение понятия «авторизованный пользователь». Не имеет значение, каким именно образом осуществляется авторизация пользователя и сколько именно существует способов такой авторизации.

R4.5.12 Система должна предоставлять активному пользователю возможность получать информацию о том, выполнение каких функций по отношению к любому объекту ему разрешено.

Метод, с помощью которого осуществляется обратная связь с пользователями, зависит от используемого в системе интерфейса (см. R2.4.6)

R4.5.13 Система должна позволять авторизованному пользователю создавать отчет с информацией о том, какие именно функции имеет право осуществлять по отношению к объектам системы выбранный пользователь и каким образом эти функции определены.

Помимо права на получение отчета, авторизованный пользователь должен иметь право на просмотр объекта и его списка управления доступом.
Отчет должен включать:

- *все функции, на выполнение которых по отношению к определенному объекту пользователь имеет право;*
- *для каждой функции — активные роли, включающие эту функцию, в которых может выступать пользователь;*
- *для каждой активной роли — список путей, посредством которых они могут быть предоставлены пользователю, включая членство в активных группах и наследование ролей от родительского объекта*

R4.5.14 Система должна предоставлять авторизованному пользователю возможность создавать отчет, содержащий информацию об определениях функций, принадлежавших конкретной роли на конкретную дату и время.

В отчете должно быть указано, относятся ли введенные дата и время к периоду до создания роли или к периоду после ее уничтожения.

R4.5.15 Система должна позволять авторизованному пользователю искать и находить:

- объекты, в списки доступа которых включена конкретная роль;
- объекты, в списки доступа которых включены конкретные пользователи или группы.

Пользователи могут искать и находить объекты, на просмотр списков доступов которых они обладают достаточными правами (R4.5.9). Авторизованный пользователь может искать как объекты в системе, по отношению к которым была назначена роли, так и пользователей и группы, которым была назначена роль. Более подробную информацию см. в ***10. Служба поиска и отчетов.***