ICT Project Guidance

Persons, Identities,   
Groups, Roles,   
Permissions and Obligations

Author:

Sky Sigal, Solution Architect

## Description

A reference document describing the interrelated elements required to correctly model persons relating, collaborating, and developing resources together.

## Contents

[Description 1](#_Toc146284703)

[Contents 2](#_Toc146284704)

[Introduction 4](#_Toc146284705)

[Impact 5](#_Toc146284706)

[Resolution 5](#_Toc146284707)

[Outcome 5](#_Toc146284708)

[Entities 6](#_Toc146284709)

[Person Management 6](#_Toc146284710)

[Person 6](#_Toc146284711)

[Person’s Attributes 6](#_Toc146284712)

[Identity 7](#_Toc146284713)

[Identity Attributes 7](#_Toc146284714)

[Names 8](#_Toc146284715)

[Identity Profile 8](#_Toc146284716)

[Attainment 9](#_Toc146284717)

[Personal Relationship Management 10](#_Toc146284718)

[Identity Relationship 10](#_Toc146284719)

[Relationship Profile 10](#_Toc146284720)

[User Groups and Group Role Management 11](#_Toc146284721)

[Application 11](#_Toc146284722)

[Invitation 12](#_Toc146284723)

[Acceptance 12](#_Toc146284724)

[Responsibility 13](#_Toc146284725)

[Obligation 13](#_Toc146284726)

[Assignment 13](#_Toc146284727)

[Person Group Role 14](#_Toc146284728)

[Group 14](#_Toc146284729)

[[Person] Group 15](#_Toc146284730)

[Person Group Profile 15](#_Toc146284731)

[Resource Management 15](#_Toc146284732)

[Resource 15](#_Toc146284733)

[[Resource] Group / Folder 15](#_Toc146284734)

[Folder Role 16](#_Toc146284735)

[Folder Permission 16](#_Toc146284736)

[Resource Role 16](#_Toc146284737)

[Resource Permissions 16](#_Toc146284738)

[User and Group Discovery and Communication Channels 16](#_Toc146284739)

[Channel 17](#_Toc146284740)

[Location 17](#_Toc146284741)

[System, Tenancy and Organisation Management 18](#_Toc146284742)

[[Tenancy] Group 18](#_Toc146284743)

[Tenancy Profile 18](#_Toc146284744)

[System 18](#_Toc146284745)

[[Organisation] Group 18](#_Toc146284746)

[User 19](#_Toc146284747)

[User Digital Identity 19](#_Toc146284748)

[User [System] Profile 19](#_Toc146284749)

[User Security Profile 20](#_Toc146284750)

[System Group Role 20](#_Toc146284751)

[System Group Permission 20](#_Toc146284752)

[Account Management 20](#_Toc146284753)

[Contractual Elements 21](#_Toc146284754)

[Agreement 21](#_Toc146284755)

[Outcome 21](#_Toc146284756)

[Tasks 21](#_Toc146284757)

[Use Cases 21](#_Toc146284758)

[System Design 22](#_Toc146284759)

[Frameworks 22](#_Toc146284760)

[Authentication and Authorisation Module 23](#_Toc146284761)

[Decision Considerations 23](#_Toc146284762)

[In-System Role Management 23](#_Toc146284763)

[Organisations as Systems 23](#_Toc146284764)

[PersOrg and IdentityGroup 24](#_Toc146284765)

[Code Sets 24](#_Toc146284766)

[Code Set influenced system logic 24](#_Toc146284767)

[Personal information, Archiving, Virtual and Physical Deletion 25](#_Toc146284768)

[Data Hub Correlation Identifiers 25](#_Toc146284769)

[Implementations 26](#_Toc146284770)

[Appendices 27](#_Toc146284771)

[Appendix A - Document Information 27](#_Toc146284772)

[Images 27](#_Toc146284773)

[Tables 28](#_Toc146284774)

[References 28](#_Toc146284775)

[Review Distribution 28](#_Toc146284776)

[Audience 28](#_Toc146284777)

[Diagrams 28](#_Toc146284778)

[Terms 28](#_Toc146284779)

## Introduction

Systems to facilitate the collaboration of Persons to develop and release Resources for consumption by end Users cannot be effectively designed, developed and developed, if the subject matter is not correctly modelled first.

Original naïve modelling of the relationships and grouping of Persons was designed to map relatively ideal conditions: nuclear families composed of un-divorced and married Caucasians with fixed male or female sex and gender, referred to with tri-partite (given, middle, sur) names developed using Latin characters without diacritical marks (i.e., without umlauts, macrons, etc.), with single identities, in a single context, employed by one enterprise, with no concurrent employments.

Issue

The world has proven to have always been more complex than the above model.

People are statistically more often than not unmarried or divorced and non-Caucasian, with naming patterns that change per cultural locale, who may require sex alignment or realignment, may present an identity and gender that differs from their biological constraints, may or may not be adopted within potentially extended families within which designated caretakers may be parents, grandparents, aunts and uncles, or none of the above, and have legal guardians, and may be employed by multiple organisations concurrently in a gig-economy.

Software to assist with the automation of interactions within the above-described contexts has not kept up.

Cause

The reason for this is due to a combination of issues:

* A majority of stakeholders on a project may believe that their past experiences and observations are sufficient and unbiased so as to inform their intuitive understanding of the elements involved, without further analysis or verification.
* System development stacks are commercial in nature and focus on delivering features and simplicity to meet their core customer base (enterprises) most common development workloads[[1]](#footnote-2). Enterprises, with a rigid hierarchical organisation of internal roles requires but a limited subset of human interaction modelling.   
  The simple modelling of an enterprise context is a key reason for the evolution of siloed Groups within organisations, disassociation from their exterior user base, negatively impacting quality of service.
* The majority of “enterprise grade” systems are considered mature *because* they have been around for a while. This age in turn implies they were originally developed using system development stacks in an era prior to the rise of the need for systems to manage hiring of non-male Caucasians, who are provide flexible consulting and collaboration in a gig economy.
* As the modelling of Persons and Users is a foundational aspect of system development on which almost all other system operations depend, there is risk and associated resistance to change to change these sublayers after a software has been deployed for use by end users.

## Impact

The impact is that the software procured to assist with interactions, consulting and collaboration and feedback between Persons, does not meet expectations, requiring development and use of workarounds. The work arounds are often manual. The work arounds often influence, extend and perpetuate poor practice[[2]](#footnote-3).

## Resolution

A resolution to the above involves developing a clearer understanding of the elements required to model interactions and grouping of Persons, to better inform the analysis of requirements for procurement and/or custom systems design.

The elements of a more capable model, intended for influencing analysis and subsequent design decisions, are described next in this guidance document.

## Outcome

The outcome of People and relationships and Roles within Groups, both within and beyond the boundaries of organisations and groups, enables subsequent automation of tasks required to develop and distribute quality resources for feedback. that can be acted upon to iteratively improve value for both provider and consumer.

# Entities

The following catalogue lists the logical entities required to define, design, develop and deliver a system capable of managing multiple collaborating organisations and groups, and persons with Roles within them.

### Person Management

All systems involve Persons to some degree, as either direct Users of the system, or simply related to information within the system.

A certain number of basic elements are needed to model a natural Person in a usable way.

#### Person

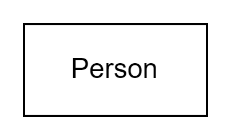


Figure : Person element

A *natural* Person is a Person one that is unique, distinct from all other Person’s, irrespective of Identities they are known by.

Natural Persons are distinct from *juridical* Persons (legally recognised groups or organisations), covered lower down.

#### Person’s Attributes



Figure : Person Attributes

An individual Person[[3]](#footnote-4) will have attributes, some that are considered immutable and don’t change.

For example, a person’s place and date of birth are factual attributes that are unchangeable (when correctly ascertained[[4]](#footnote-5)) - even if there have been several attempts to do so)[[5]](#footnote-6).

Traditionally a person’s biological attributes at birth (e.g., a person’s weight) were classified as immutable -- but the number of attributes that are immutable, versus changeable is diminishing. For example, eye colour at birth is known to change over time. The same applies to natural hair colour. Or having hair.

The same applies for a person’s Sex. While traditionally immutable and classifiable as a male, female, or intersex (e.g.: a hermaphrodite with dual chromosomes). reassignment surgery has made this physical attribute changeable in some countries[[6]](#footnote-7).

Note:  
A Person’s sex is an attribute that is distinct from an Identity’s Gender, covered next.

#### Identity



Figure : Identity element(s)

A Person may have multiple Identities over time.

A well recognised example is of a Person using one Identity -- built around their birth or adopted family’s surname -- until they become married, when then take on their partner’s surname and some other aspects they wish to share (e.g., convert to a shared religious denomination).

A Person often has multiple concurrent identities, based on their Role in different Groups. For example, a person may be “Mom” in a family context, “Ms Smith” in a formal role work context, and simply “Beth” among a friend context or Group.

An Identity may even be retired and restored. For example, a married Person may return to a class reunion where they will restore a retired identity they had before they were married.

#### Identity Attributes



Figure : Identity Attributes

All Identities of a Person will inherit base Person Attributes (date of birth, eye colour, sex, etc.) that are common to all Identities, but will have additional attributes specific to the Identity itself.

For example, while the physical body may be of male Sex, they may identify as having a female Gender.

They will always have at least one attribute, an Identifier or Name to differentiate between Identities.

#### Names

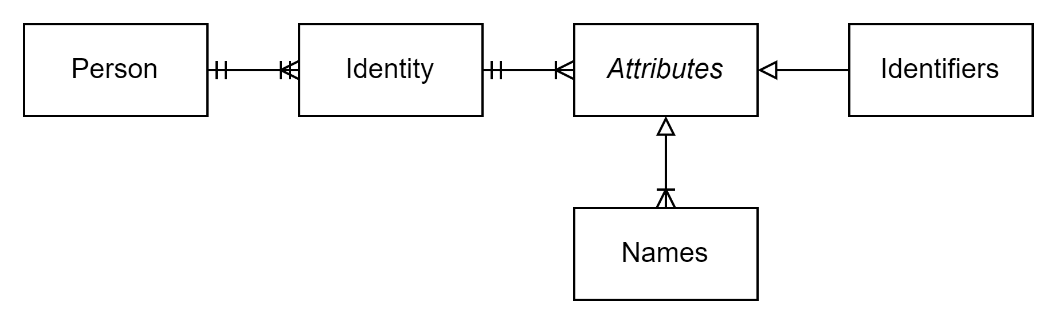


Figure : Identity Names

An Identity can have multiple Name Identifiers.

A person can be identified with “Mom”, “Mrs. Smith”, and “Dear”.

While not globally unique, they are sufficient to identify an Identity within a Group.

Whereas most identifiers will identify the authority that issued the identifier, Name identifiers may have no authoritative source identified (e.g., “Mom”).

While legacy systems may expect one of the names to be defined as an official name, this is now considered flawed logic, as Person may have multiple legal names, and use different ones in different contexts. For example, It is relatively common for a Chinese person to have a regional (e.g., Hong Kong) name as well a formal mandarin name, both in Chinese *hanzi*, *kaishu*, etc, as well as latinised equivalents of these names. They may have been given a name when studying English, which has become one they are known by (“Ben”), not counting any nicknames (“Benny”). The name they used on their English based identity papers may be any one of those 4 or more.

#### Identity Profile

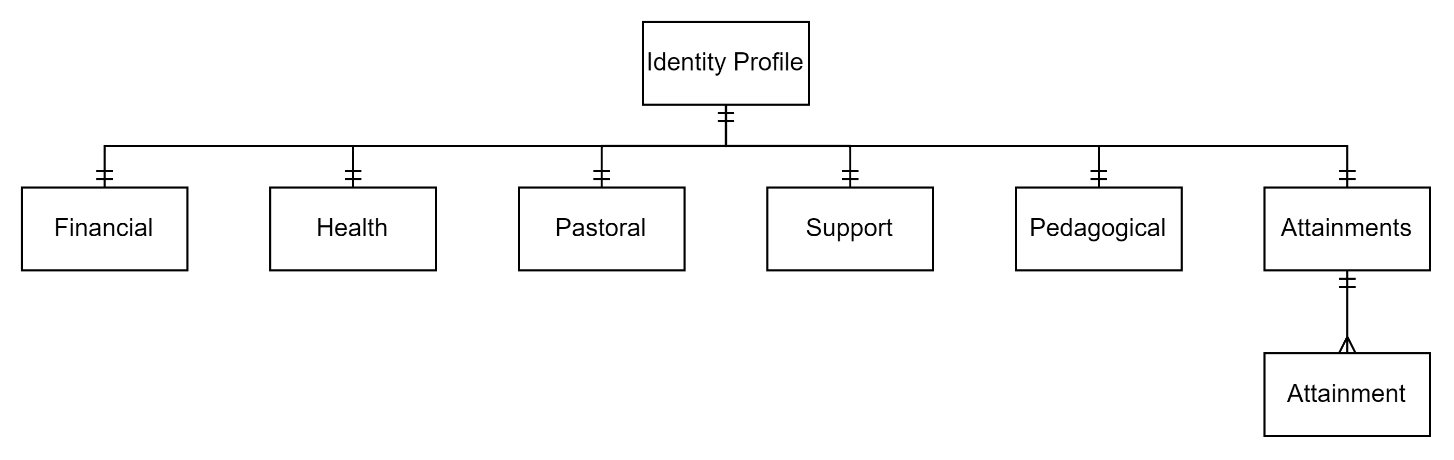


Figure : Identity Profile

An Identity has an associated Profile, which is a collection of richer information about an Identity organised into distinct sub-Aspects. The exact number needed will vary depending on system design.

Common identity Aspects would include:

* **Demographics:** classification information (race, ancestry, religion, etc.)
* **Health**: physical, mental, and medical notes
* **Pastoral**: behavioural information and incidents, student voice (interests, aspirations, goals), transition notes, support and interventions
* **Pedagogical**:
* **Assessments**: information about their measurable progress via Assessments through course material, curricula, etc.
* **Attainments**: the qualifications the Identity has attained. Note that Attainments is common to many types of Identities (Learners, Teachers, Professionals, etc.) not just and can be used as information to inform decisions to engage with them.
* **Financial**: information about financial situation and funding.
* **Etc**.

#### Attainment

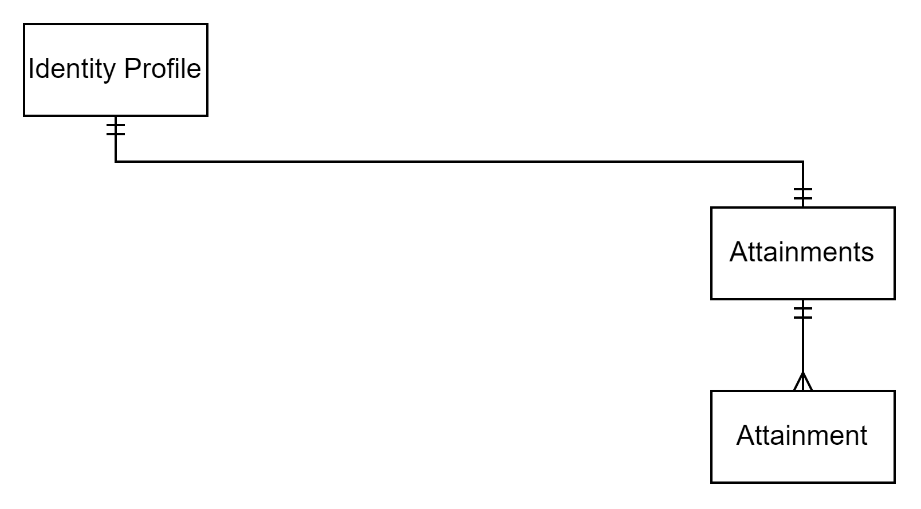


Figure : An Identity's Individual Attainments

An Attainment is a summary of a person’s attainment (e.g., national exams, teacher qualifications, etc.), and a reference to the authority that issued the qualification, possibly even a digital record of the attainment itself[[7]](#footnote-8).

Attainments may expire and need re-certification, hence Attainments should be linkable in some followable way.

Consider the use of or coexistence with Open Badges[[8]](#footnote-9).

### Personal Relationship Management

Persons, via their Identities, are related to other Persons in a myriad of ways.

#### Identity Relationship

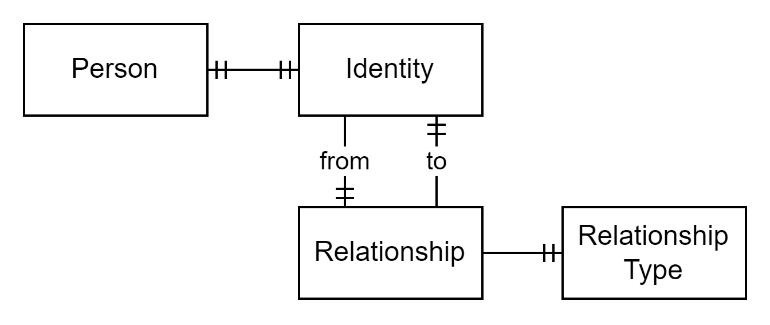


Figure : Identity Relationship

An Identity can be related to another Identity in one manner or another. For example, one Identity can be a Friend (or “Mother”, “Caretaker”, “Classmate”, “schoolmate”, etc.) to another Identity.

Relationships are sometimes to Identities of Persons within the same Group (“Brother”, “Classmate”, etc.), and sometimes to Identities of Persons in parent or parallel groups (“Relative”, “Cousin”, “Schoolmate”, etc.).

Relationships are directional and paired: one defining that one is a parent of a child, and the other defining they are the child of the parent.

A Relationship may also require the issuing of an invitation and acceptance to accept Privileges and/or Consents that come with the Relationship.

#### Relationship Profile

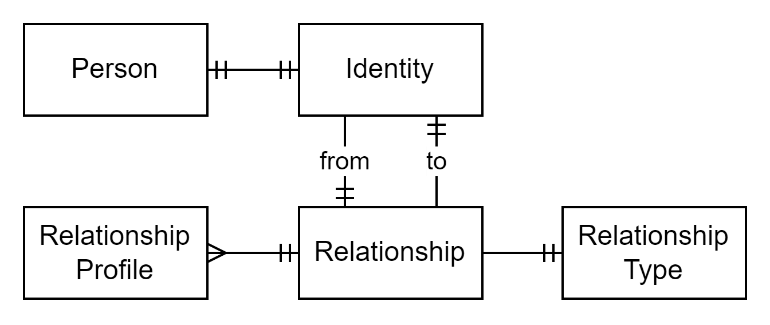


Figure : Relationship Profile

A relationship may be related information that is not shared with any other Persons.

A Relationship Profile is used to attach Relationship specific Attributes.

Note:   
If the attributes were to be shared beyond the relationship, it might be more appropriate to include them in Profile that belongs to one’s relationship to a whole Group.

### User Groups and Group Role Management

Beyond one-to-one relationships, Persons belong to Groups, and have Roles within them.

#### Application

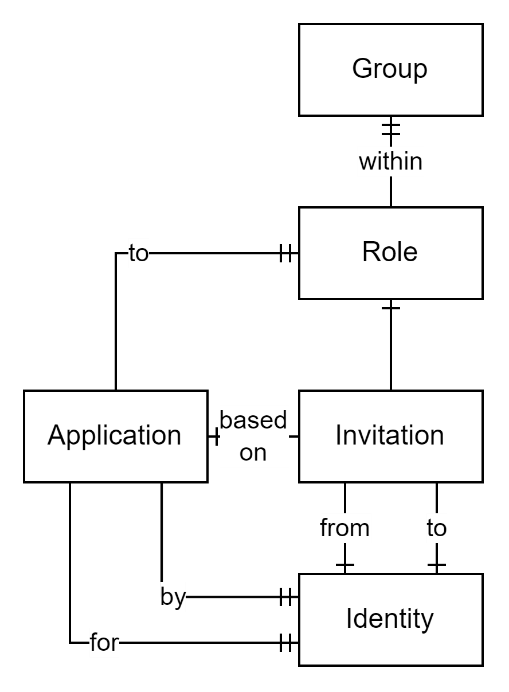


Figure : Application for a Role in a Group

A Person may apply to be invited to a Role within a Group. The application is handled by a Manager of the Group who has been allocated the Permission to manage Applications.

An Application is not necessarily required to initiate an Invitation.

#### Invitation

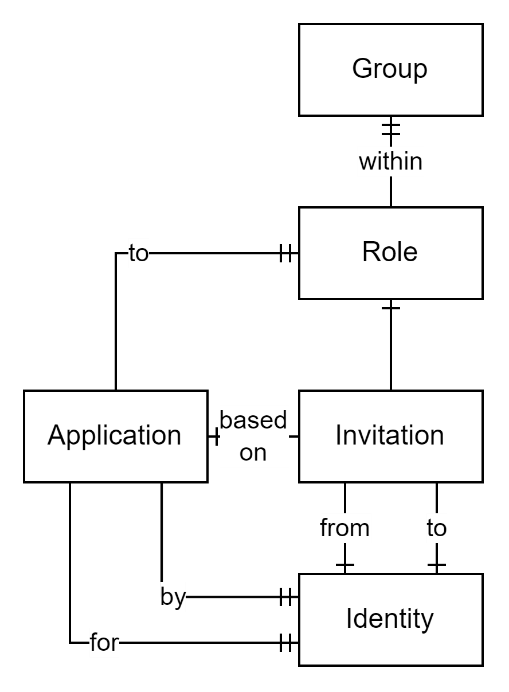


Figure : Group Role Invitation

After considering an Application to a Role, if any was received, an Identity with a Role that permits it to do so can Invite another Identity to Accept a defined duration/term (From/To) Role within a Group.

#### Acceptance

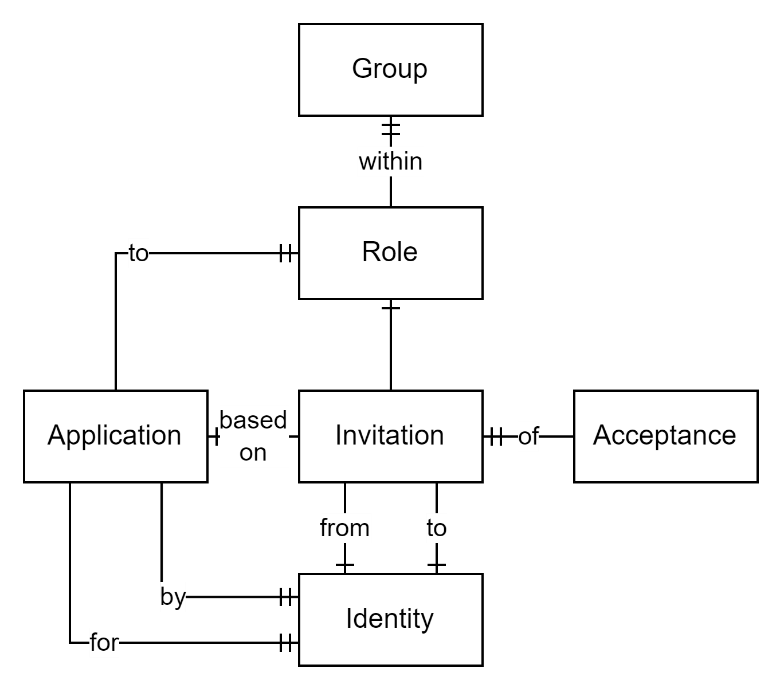


Figure : Acceptance of Invitation to a Role within a Group

An Invitation to a Group permits a User to presented for review a specific version of Responsibilities associated to a Role’s Permissions before signalling back acceptance of the Role.

#### Responsibility

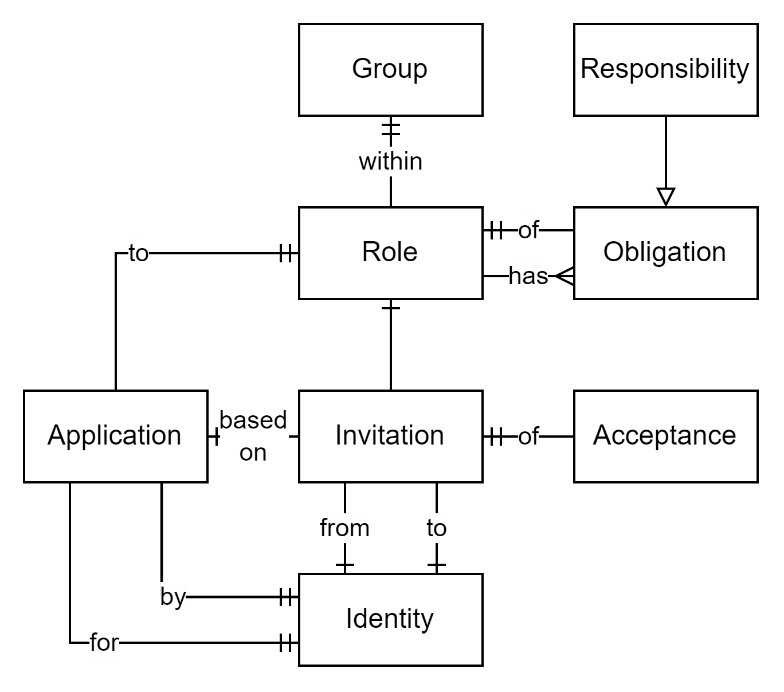


Figure : Role Responsibilities

The Obligation must be Accepted before being given the Permissions associated to a Role to which one is invited.

#### Obligation

Both Responsibilities and Duties are both subtypes of Obligations.

The difference is that a Responsibility comes by accepting Roles, whereas Duties are Obligations that come from joining or having been joined to a System.

#### Assignment

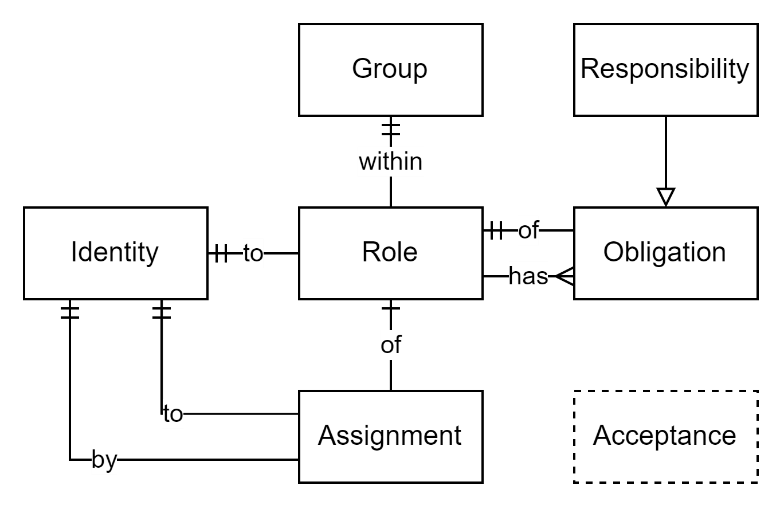


Figure : Group Role Assignment

It is considered poor practice to Assign a Person a Role in a Group rather than by providing choice and Acceptance via an Invitation – but it does happen by changes in context (“became in charge, by default”, “unplanned parenthood”, etc.).

#### Person Group Role

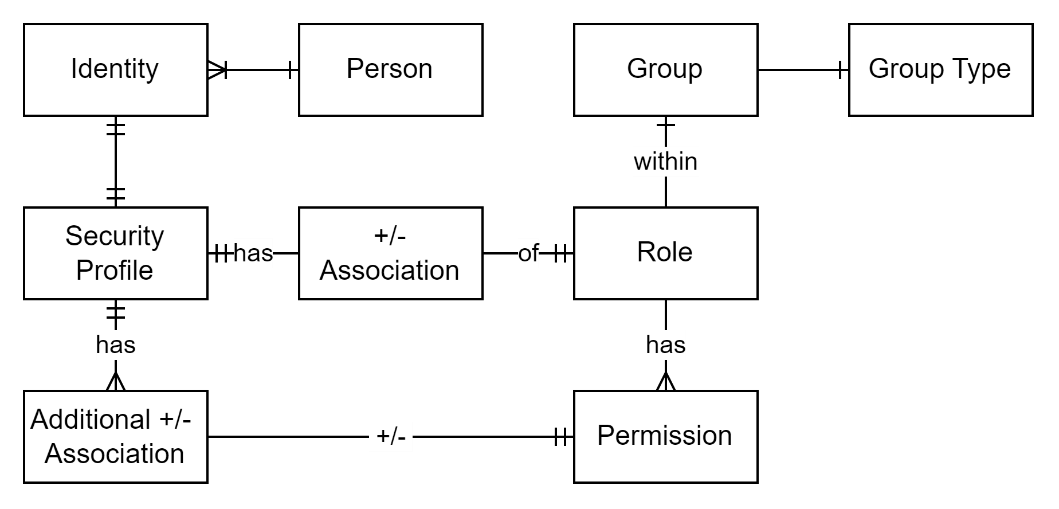


Figure : Group Role

All Persons are associated to one or more Groups by Accepting an invitation to a termed Role within a Group. The name used for the Role is context domain specific (e.g., “Mom” in a family domain, “Boss” in a work domain).

Roles always have start and end dates that can be any time in the future. It is poor security practice to assign for a role association to be open ended.

#### Group

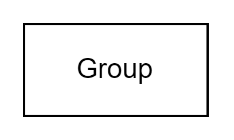


Figure : Group of Person Identities

Groups can be developed for at least the following use cases:

* Systems,
* Tenancies,
* Organisations,
* People,
* Whānau/[Extended] Families, being a subtype of People,
* Resources (i.e., a “Folder”).

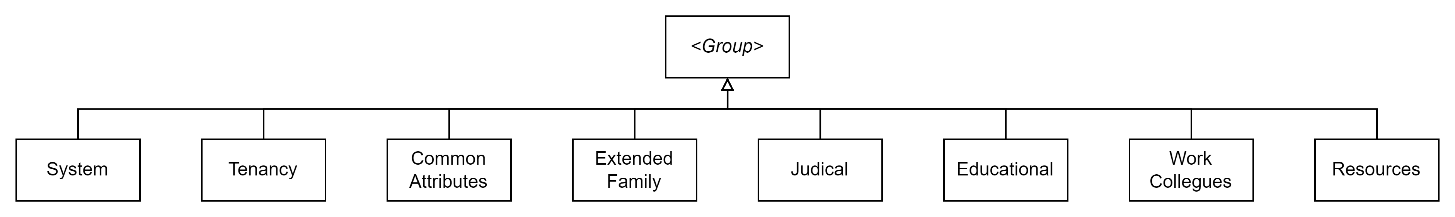


Figure : Example Group Types

#### [Person] Group

Groups are collections of Persons who have Accepted the Responsibilities that come with accepting the Permissions associated to a Role to which they have been invited.

Groups can be developed for any purpose, only limited by system needs. For example, Groups can be developed to represent Family, Friends, Colleagues, Common Characteristics, Interests or Concerns, Cohorts, Enrolment, Classes, etc.

Persons can have Roles in many Groups simultaneously. For example, a Person can be a Mother in a Family Group, while also having a Manager role in a work context Group.

Whereas People are not nestable, Groups are (e.g., State, University, School, Department).

#### Person Group Profile

A group may have information shareable by members of the Person Group.

Note:  
Whereas Group Profile may be merged with the Group, it is considered poor practice to not disambiguate between the two (most operations don’t need access to Group Profile information, just knowing who’s in a Group).

### Resource Management

Groups of Users are developed to spread the load of managing Resources.

#### Resource

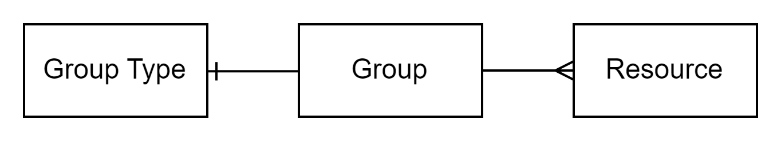


Figure : Resource

A resource is a system record, that describe something (e.g., a Sales Record, bank xfer), or is metadata summarising associated media (image, etc.).

#### [Resource] Group / Folder

Resources can be grouped dynamically (by common traits) or virtually within a logical folder.

A Folder is very similar to a Group, except that it is containing Resources rather than Persons.

Folders can be hierarchically nested.

A Folder, and all its child Folders and Resources, can be linked to a Person Group (as the Group’s common Resources) or Person (as their personal Resources).

#### Folder Role

A Person can be Assigned or Invited to Accept a Role [of Folder Permissions] in a Folder, and its child nested Folders and Resources.

#### Folder Permission

Folder Permissions provided a Person the ability to Browse the displayable Summaries of Resources in the Folder, and do not automatically grant Permissions to the Resources within the Folder (although that is commonly the default configuration of a system).

#### Resource Role

Each type of Resource has associated Roles, that enable part of a Resource Lifecycle’s management Roles specific to the Type. Type specific Roles could include one or more of the following, Owner/Accountable, Creator, Contributor, Reviewer/Commentor, Approver, Maintainer, Consumer.

#### Resource Permissions

A Resource Role is nothing much more than a logical set of Resource type specific Permissions. They type specific instances of classic Create, Update, Comment, StateChange permissions.

Note:  
It is still common for system analysts to make a distinction between Groups and Organisations, but we submit there is none, beyond juridical entities having identifiers specific to organisations (e.g., business/tax identifiers) under their Group Profile.

### User and Group Discovery and Communication Channels

People and Groups are searched for to Communicate with them.

When there are no usable communication Channels, or no response, the Person or Group has to be physically Located.

#### Channel

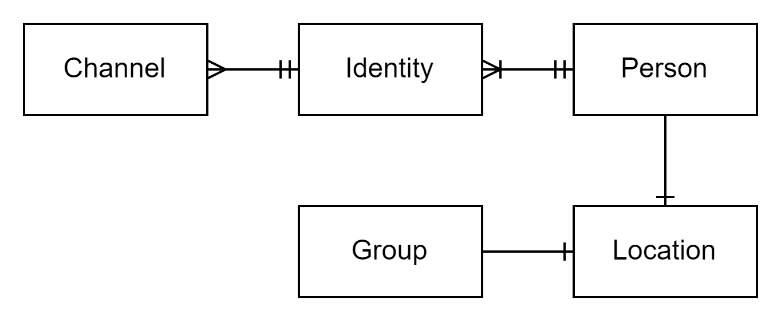


Figure : Group and Identity Channels

Both person’s and groups are contactable via multiple Channels. Whereas the Postal system was the most used channel 20 years ago, times change, and cellular and/or email system-based channels are now preferred communication channels for Persons and Groups. [[9]](#footnote-10)

In other words, a Channel has an indication of what system they belong to (Postal, Phone, Twitter, etc.) and a means for storing the system specific identifier[[10]](#footnote-11).

Note:  
a postal address is a communication Channel and not a Location, as it can be at different location than the group or person itself, without specifying a different Location (e.g., a postal box).

#### Location

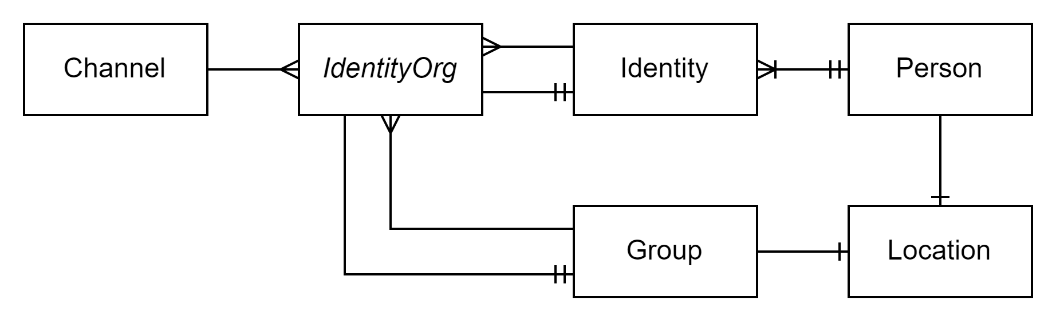


Figure : Group and Person Location

Persons and Groups can have associated physical Locations defined using GPS and even possibly elevation.

Entities cannot be in more than one place at once, therefore can only have one Location. This does not stop an Organisation Group being able to define multiple buildings (sub Groups), each having their own Location.

### System, Tenancy and Organisation Management

#### [Tenancy] Group

Tenancies are logical separations of groups from other organisations.

It is still common for system designers to keep accounts separate into distinct tenancies, in different physical storage data bases. The legacy design of entrusting security to the data tier rather than keeping it in the system’s logical tier is no longer considered best practice because it removes the ability of Persons, such as Consultants, having roles in two different organisations or tenancies, or sharing resources across organisations, without duplication and loss of full lifecycle management[[11]](#footnote-12).

Hence Tenancies are Groups -- but flagged so they cannot be nested under any other group than a Group of type *System*.

#### Tenancy Profile

A Tenancy has settings specific to itself and can be the just a Group Profiles.

#### System

All Tenancies are hosted within the System.

Note:  
A recommended design approach is to make a top group be for the automated System itself. This avoid having to make a separate mechanism for defining and assigning System Roles and Permissions.

Individual Tenancies become direct children of the System Group.

#### [Organisation] Group

An Organisation is no more than a specific type of Group.

Organisations can be nested within other parent Groups (e.g., “Car Manufacturing”, “Education Providers”, “Communities of Learning”, etc.).

But being an Organisation, they have autonomy in that they are the top of a chain of authority (i.e., Roles) and are not affected by Roles of Groups they are added to[[12]](#footnote-13).

#### User

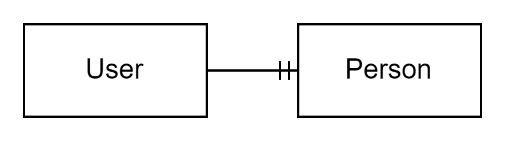


Figure : User

A User is a Person who is authorised to uses a system.

All Users are Persons, but not all Persons are Users.

For example, a Learner may be a Person, who is a User, and the system may record caretaker (“Mother”) associations between the User’s Person and other Persons (Parents, Caretakers) who are not authorised to be Users of the system.

#### User Digital Identity



Figure : User Digital Identity

A User may be associated to one or more external Digital Identities, developed by external 3rd party Identity Providers (IdP) to represent Users they recognise.

Most systems will only allow one Digital Identity per User, but they should allow multiple. For example, a User may be able to sign in using their externally defined personal or employment Microsoft Account identity, or Google Account identity. A contractor may be coordinating work across multiple organisations and have a choice of organisation managed digital identities to sign in with.

An external digital identity, from the point of view of a system, is a token representing a User of a different system, that it can trust as being associated to a User in this system.

#### User [System] Profile

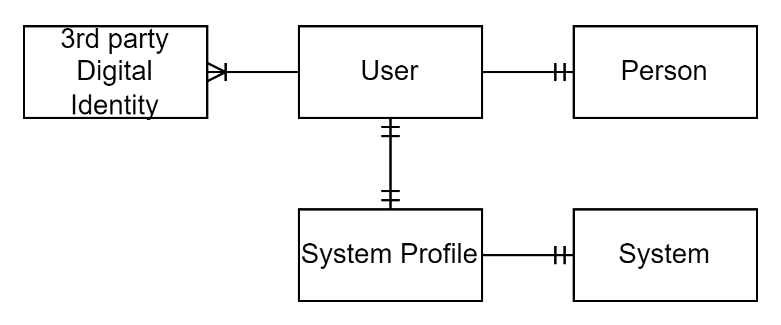


Figure : User System Profile

A User will have a System Profile to manage the User’s personal preferences as to how to use a system.

It is common but considered poor practice to limit flexibility by merging a User entity with their User Profile as a single logical entity.

Common user session settings in a User System Profile might include their default user interface language, interface layout (left to right, or right to left) and presentation styling (font, background, foreground, etc.) considerations.

A System Profile would also cover settings made available by Modules enabled or disabled by a User’s Account.

#### User Security Profile

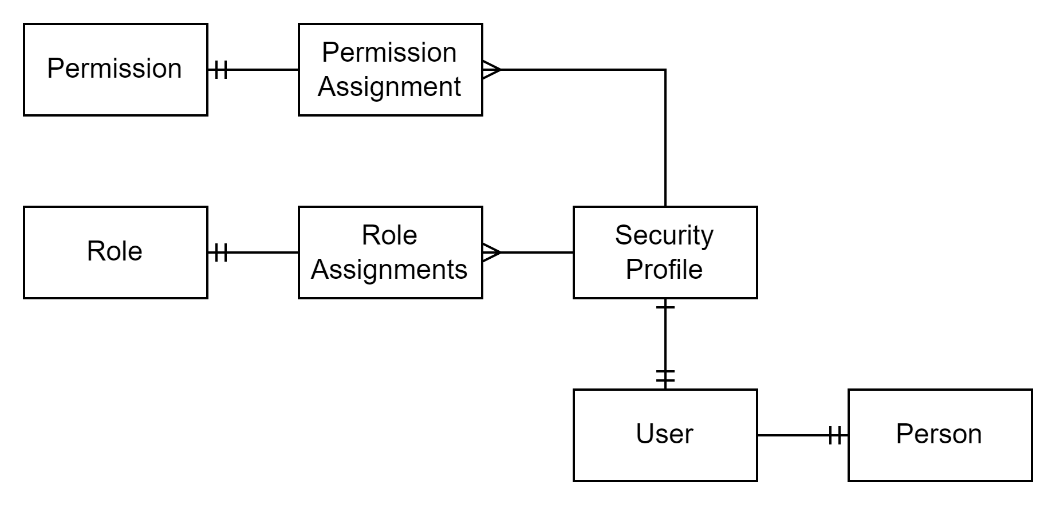


Figure : User Security Group

All users of a system have an associated security profile, to which is associated their System wide Roles and its System wide Permissions.

There is an argument to consider a Security Profile being an aspect of a Person and not a User, as Persons, to develop their security profile even before they become a system User.

#### System Group Role

*If a System Group is not developed, System Group Roles and permissions will require being developed, to be assigned to a User’s Security Profile.*

A User will have a System wide Role (“Admin”, “User”).

A System Role is a named logical group (e.g.: “Admin”) of System Permissions usually limited to an entity type (“\*-READ”).

#### System Group Permission

A System Role is a collection of System Permissions.

### Account Management

Accounts are distinct from Tenancies and Users. The logical entities to map them, their relationship to System Features, and the roles required to be mapped to system Users (Owner, Bill Payer, SysAdmin, User, etc.) are even if they are easily modellable using Groups again, the subject matter is beyond the scope of this document.

### Contractual Elements

While elements required to support Group Role allocation to Persons, the subject of Agreements and Contracts were not included till now.

#### Agreement

An Agreement is an element between two parties that are either natural Persons or Groups, to capture each parties agreed Responsibilities, Outcomes, and associated Tasks.

Agreements can be bilateral, or unilateral (where only one party makes a promise to deliver outcomes.

Agreements are more effective when the Outcome is defined, and not just Tasks.

#### Outcome

An Outcome is a recognised outcome. To remove ambiguity, Outcomes should be *measurable*.

#### Tasks

An Agreement may also specify the Tasks expected to deliver the Outcome.

## Use Cases

The above model can be demonstrated to enable the following common use cases:

* Including in Groups the Persons who are not Users of the system.  
  This permits stakeholders (e.g. Parents of Learners enrolled at a school) being informed of group progress by an email channel, even though they don’t use the system themselves.
* Permitting Signalling to Persons who are not Users, of secure reports exist in the system for their perusal.   
  This permits Persons (e.g., Parents) being made aware of a confidential resource (e.g., a Term Report) being available for them to access, even though they have not yet used the system. The conversion to a User can be done seamlessly.
* Permitting Persons to accept Roles in a system after they have consciously reviewed Obligations of the role and its associated Permissions. The Acceptance permits having an Auditable trace of their understanding and acceptance of their Obligations. The Obligations should be Versioned to permit auditability of the acceptance of a specific Obligation.
* Permitting signalling to Users as they signed in that the Terms and Conditions and/or Role obligations have been updated. This is enabled by having a reference to specific versions of Obligations, but not the latest.
* Permitting a Role to be assigned to a Person, with the ability to Add an additional specific Permission Association that restricts o one or more of the Permissions that were defined in the Role. This permits a person be given the same role as another person (e.g., Accountant), adjusting for them to have a few less permissions (e.g.: an Assistant Accountant may not be permitted to sign off on cheques), rather than having to develop a specific Role for Assistant Accountant.
* Permitting a general Role being assigned to a Person, adding one or more specific Permissions that were not defined in the Role. Maybe it’s a Temporary allocation while someone else is on holiday.
* Permitting the inviting of Persons to accept a role at the beginning of term (in the future), for a fixed duration (one year). A notification could be triggered a month before the end to signal to a manager that they could review at this arrangement, and optionally extend it (e.g., another year).   
  This ensures that system access and role allocations are not open-ended, mitigating a quite common security issue and potential risk.
* The ability to develop longitudinal information about a Person, with the capability to cater for one or more Identities changes over time. An example may be that a Person started with an Identity of being male before identifying as a female gender, or vice versa.
* The ability for a Person to have an Enrolled Role in one or more education providers groups, while having a Mother Relationship to another Person currently Enrolled in another education provider Group, while having an employed Role in one or more Organisations type Groups -- any one potentially being an education provider.

## System Design

### Frameworks

The above-described framework is more capable, and necessarily more complex than those that come with by default with development frameworks, irrespective of the development language.

It is important to recognise and understand the impact from the fact that Development Frameworks are developed with the following objectives:

* To be easy for new users to be able to create something relatively quickly.
* To be able to develop the most common types of systems.
* By their largest consumer base, enterprises.

These frameworks are therefore not focused on delivering a solution to meet:

* Other development needs (e.g.: game development)
* Other types of consumers (gig-economy system developers)

Additionally, the frameworks are designed to increase uptake, by decreasing a need for training, education or skill to produce something. They are not there to make one a better developer.

#### Authentication and Authorisation Module

Developers who wish something more will be required to put in the work to develop a replacement for the framework’s baseline/entry-level authorisation and authentication modules.

### Decision Considerations

The above-described concepts are sufficient to understand elements required to design mature information systems, even non-automated ones.

However there remain design aspects that are left for further exploration if so desired.

#### In-System Role Management

There was a school of design to extract Authorisation logic from systems and instead manage it externally as a central Enterprise service. Part of the drivers were to reduce the cost of developing authorisation logic in each system, and part of the logic was The approach was based on an incorrect analysis of the problem, and a muddling of multiple concepts, including business role, system role, permissions, state change signalling, and reporting requirements.

While non-trivial to develop, services require their own authorisation system to allocate permissions, and then control operations based on permissions received.

The logic they use to allocate roles and permissions to users can be *influenced* by information gained from external services (e.g., HR Role title, which in most cases would not be exactly equivalent to system roles).

#### Organisations as Systems

Organisations are Systems in their own right, with their own Duties.

A design decision is required to define whether Systems by default can inherit Roles from parent Systems, or whether there is a difference between Organisation Systems, which must inherit parent all-of-System Roles.

#### PersOrg and IdentityGroup

There is considerable amount of design history associated to the use of a PersOrg entity for use by both Natural Persons and Juridical Persons (Organisations).

There are conditions where one must be capable of referencing *both* types. An example, in NZ, is when an Organisation has a Trustee Role within a Trust Organisation.

While this approach is more correct than implementing two distinct types of Roles, one for Persons, one for Organisations, implemented naïvely, the approach can introduce a long list of undesirable design issues[[13]](#footnote-14).

An approach that performs correctly is to develop PersOrgs as joining objects referenced from Group Roles, such that PersOrg have a Type flag to define what kind of entity it is referring to, and fields to point to the target Person or Organisation.

While PersOrgs have merit, there is more flexibility and accuracy to instead use a joiner that is an IdentityGroup, Permitting the provision of roles to non-juridical Groups, as well as be more precise as to what Identity.

It also implies that some fields are common to both natural Persons and Juridical Persons to facilitate reporting without requiring secondary queries to data sources for these attributes. A preferred complete and formal Name[[14]](#footnote-15) would be expected to be considered as one of these attributes.

#### Code Sets

The above catalogue listed top elements, and didn’t discuss the Reference Entities required:

* PersOrgType [Natural | Juridical]
* GroupType [System, Juridical, Family, Social, Resource Folder]
* RelationType [Ancestor, Great-Grant, Grand, Parent, Sibling, First Cousin, Second Cousin, Removed, Half siblings, Child, Extended Family]
* Group RoleType [ Employed, Enrolled, Teacher, Learner, Member, Informed, etc.]

Guidance on the development of Reference Data system entities is available in another Guidance document on the subject matter.

#### Code Set influenced system logic

Figure : Group Type

The *type* can dictate logic that is applied. For example, Person Groups do not permit Persons to be directly associate to them, but do permit Roles be associated, which in turn permit defining the Person. They also permit other groups of type Folder to be associated to the group.

#### Personal information, Archiving, Virtual and Physical Deletion

Guidance is available separately on the correct and legal manner to remove information from circulation and use.

#### Data Hub Correlation Identifiers

Guidance is also available separately on capabilities required to develop *data hubs* to facilitate interchange of data between multiple local systems of authority.

# Implementations

The above described logical elements can be developed using a relational database.

The following is a diagram of example schema.

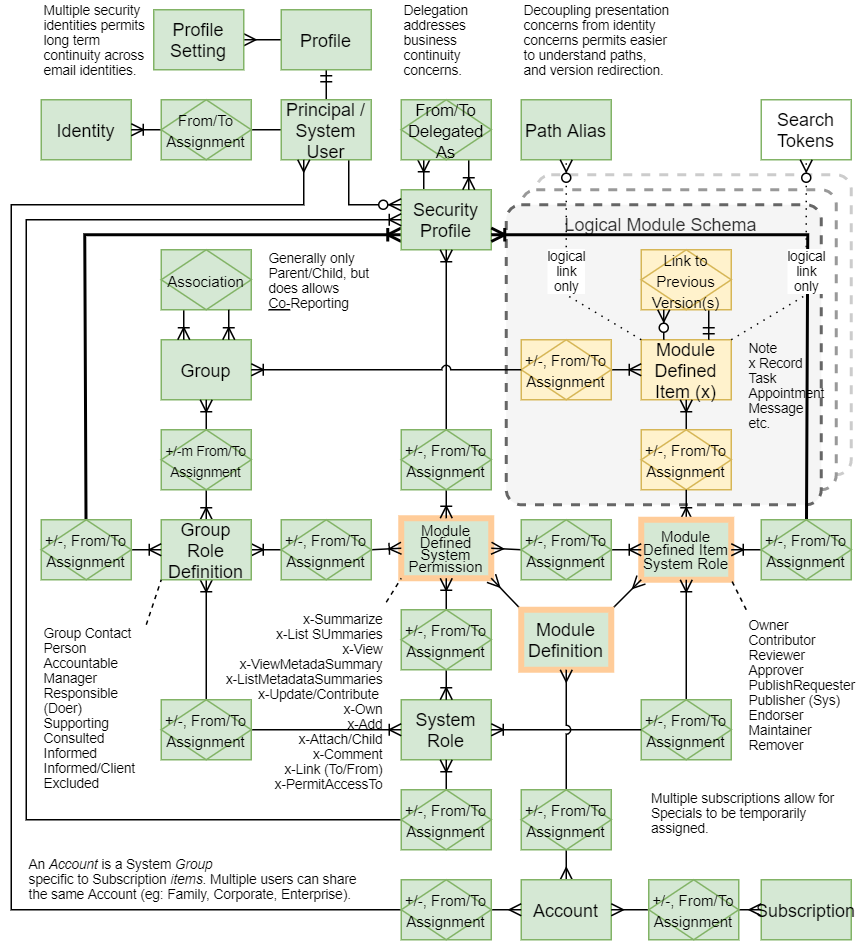


Figure : Example System Entity Relational Diagram (ERD)

Appendices

Appendix A - Document Information

### Images

[Figure 1: Person element 6](#_Toc146031830)

[Figure 2: Person Attributes 6](#_Toc146031831)

[Figure 3: Identity element(s) 7](#_Toc146031832)

[Figure 4: Identity Attributes 7](#_Toc146031833)

[Figure 6: Identity Names 8](#_Toc146031834)

[Figure 7: Identity Profile 8](#_Toc146031835)

[Figure 8: An Identity's Individual Attainments 9](#_Toc146031836)

[Figure 9: Identity Relationship 10](#_Toc146031837)

[Figure 10: Relationship Profile 10](#_Toc146031838)

[Figure 11: Application for a Role in a Group 11](#_Toc146031839)

[Figure 12: Group Role Invitation 12](#_Toc146031840)

[Figure 13: Acceptance of Invitation to a Role within a Group 12](#_Toc146031841)

[Figure 14: Role Responsibilities 13](#_Toc146031842)

[Figure 15: Group Role Assignment 13](#_Toc146031843)

[Figure 16: Group Role 14](#_Toc146031844)

[Figure 17: Group of Person Identities 14](#_Toc146031845)

[Figure 18: Example Group Types 15](#_Toc146031846)

[Figure 20: Resource 15](#_Toc146031847)

[Figure 21: Group and Identity Channels 17](#_Toc146031848)

[Figure 22: Group and Person Location 17](#_Toc146031849)

[Figure 23: User 19](#_Toc146031850)

[Figure 24: User Digital Identity 19](#_Toc146031851)

[Figure 25: User System Profile 19](#_Toc146031852)

[Figure 26: User Security Group 20](#_Toc146031853)

[Figure 19: Group Type 24](#_Toc146031854)

[Figure 28: Example System Entity Relational Diagram (ERD) 26](#_Toc146031855)

### Tables

### References

**There are no sources in the current document.**

### Review Distribution

The document was distributed for review and input as follows:

|  |  |
| --- | --- |
| Identity | Notes |
| Amy Orr, Data Domain Architect |  |
| Roger Govind, Security Specialist |  |
| Trish Jenkins, Security Specialist |  |
| Josh Xie, Business Analyst |  |
| Jaleh Edwardson, Business Analyst |  |
| Archana Sahani, Business Analyst |  |
| Dijana Sneath, Business Analyst |  |
| Derek Wenmoth, Digital Education Strategist |  |

### Audience

The document is technical in nature, but parts are expected to be read and/or validated by a non-technical audience.

### Diagrams

Diagrams are developed for a wide audience. Unless specifically for a technical audience, where the use of industry standard diagram types (Archimate, UML, C4), is appropriate, diagrams are developed as simple “box & line” monochrome diagrams.

### Terms

Refer to project Glossaries.

##### Juridical

: recognised under law as having the capacity of the potential to act legally and constituted either by a collection or succession of physical persons or a collection of properties.

1. either solely internal staff facing or external customer facing, rarely both -- and most definitely not to assist *other* (potentially competing), organisations. [↑](#footnote-ref-2)
2. Paper forms may be developed with instructions to fill in the “First, Middle and Last name, without Accent” -- because the system cannot handle more appropriate input. [↑](#footnote-ref-3)
3. A Person can be a either a Natural individual or Juridical (group) Person. [↑](#footnote-ref-4)
4. [Home Office to introduce scientific methods for assessing the age of asylum seekers - GOV.UK (www.gov.uk)](https://www.gov.uk/government/news/home-office-to-introduce-scientific-methods-for-assessing-the-age-of-asylum-seekers) [↑](#footnote-ref-5)
5. [Emile Ratelband, 69, told he cannot legally change his age - BBC News](https://www.bbc.com/news/world-europe-46425774) [↑](#footnote-ref-6)
6. [Change the sex/gender on a birth certificate | New Zealand Ministry of Justice](https://www.justice.govt.nz/family/change-the-sexgender-on-a-birth-certificate/) [↑](#footnote-ref-7)
7. Modern digital solutions include referencing Open Badges which perform the same function. [↑](#footnote-ref-8)
8. [Home | IMS Open Badges](https://openbadges.org/) [↑](#footnote-ref-9)
9. If it’s not WhatsApp, Snapchat, or a myriad of other new channel options appearing regularly. [↑](#footnote-ref-10)
10. All modern Channels can be stored in a single value. Post is an exception in that it can either be stored as a single value with line formatting in it, or using a number of fields if it needs to be later searched on (e.g.: to find Persons by City or State) [↑](#footnote-ref-11)
11. A;; wj [↑](#footnote-ref-12)
12. Except the top All-Of-System Group [↑](#footnote-ref-13)
13. Organisations don’t have Given and Surnames, nor have Health aspects, for example. [↑](#footnote-ref-14)
14. Possibly a dynamical attribute. [↑](#footnote-ref-15)