



# Person Lifecycle Management

This Draft Version 0.1 paper is a placeholder statement.

## Problem

Person lifecycle management covers the processes that manage an individual through the lifecycle from when they join, are operationally authenticated and assigned access and authorisation permissions, are then maintained (through perhaps several changes in roles through their lifecycle, and depart. This is historically the traditional long-term view of Person LM – through the point of when they join to when they leave.

In today's business collaboration world, where collaborative activities - with business partners, suppliers, customers, and staff and contract individuals - are increasingly required, these operations must be handled speedily and comprehensively.

Further, in the new world of collaborative activities in Cloud Computing, where collaborative activities may take very short times (of the order of minutes rather than months or years) business demands that collaborations must be speedily set up, and equally speedily closed.

The processes required include the management of individuals, including non-members of the managing entity. Such processes need to take into account the identity, personas, capabilities, reputation, and potential impact, of each of the individuals.

## Why should I care

Key issues for COA – to be added

## Recommendations/solutions

To be added

Primary source reference – proposed as ITIL / ISO 27002 (Section 8?)

## Background/rationale

Includes the following:

### Source of master data

Within an organisation there needs to be master source of user information, not only to act as an authoritative source for systems wishing to federate, but also ?? ...

### Authentication of individuals

The proliferation of accounts, log-in names and passwords (or stronger schemes) that a person has to deal with is expanding, at the expense of good security.

A stop-gap solution is the generation of private authentication solution - clubs whereby a group of interested parties can share and federate a single set of credentials. Such an example is TSCP (Trans-global Secure Collaboration Program) used by the military and aerospace companies.

Authentication of individuals, public schemes, clubs, strong authentication, personas,

Integrate with national identity scheme

Need to manage post employment (e.g. pensions, share schemes)

Vetting

Unused IDs –do not re-use.

Lockout – with regard to re-authorisations.

On-boarding / off-boarding of individual or group identities

Attributes

Scalability is an externalisation issue

How to federate with partners – sets of people (not all) in the partner

Role and use of Identity Brokers

Nature of relationships – this will indicate what type(s) of identity credentials are required, and selecting the one which has “skin in the game” (self-interest) to motivate assembling and maintaining accurate credentials.

## Challenges to the industry

Include the following:

### Strong personal ID

The concept of being able to manage a personal ID that can be re-used wherever you go is very attractive. A single strong ID can be set once, and then reused anywhere using an open standard set of API's, preferably with the ability to set a series of “persona” facets of you, with limited information that you choose to expose – e.g. you may choose / need to give different personas to your place of work vs. the tennis club.

Such current schemes lack the ability to integrate the level of strong authentication that many organisations require.

### The way forward

To be added.

---