# Business Cases for CloudAuthZ

## Comments on Authorisation Problem for Independent Business Services

In the Clouds, it does not make sense creating a perfect technical solution if it does not sound feasible from commercial perspectives.

If Cloud technologies claim being service-oriented, they have to be compliant with all principles and concepts of service orientation. In this case, Cloud technologies including authorization/entitlement solutions must preserve “Knight’s Rules” of relationship in service-oriented ecosystem:

**A Service of my Service, is not my Service
A Consumer of my Consumer, is not my Consumer
A Partner of my Partner, is not my Partner
A Supplier of my Supplier, is not my Supplier**

This means that if a service/provider does not have an explicit Service Contract (OASIS SOA RAF, 2012) with a client/consumer/user, this one may have no access rights to that service and an identity of that consumer means nothing to the service.

If an intermediary service propagates \_its\_ consumer’s (user’s) identity to another service, the latter should act based on the permissions of the requestor (i.e. Service), not on the permissions of the propagated identity of initial consumer. The final service-provider has a trustful relationship with the immediate requestor and distrusts this request or on how it obtained somebody’s else identity.

Thus, a propagation of an end-user/consumer’s identity through a net of independent services is useless. Instead, if a service offers certain capabilities to its consumers, it must provide them on its own rights regardless whether it produces the results by itself or by engaging another service; all security concerns and control exist only between interacting services (otherwise, we are ‘opening doors’ to the use of stolen identities). If a service has no rights to certain functionality of an engaged service, owning an identity of those who have these rights does not change the service’s restrictions (“a **Consumer** of my **Consumer** is not my **Consumer**”).

## Business Cases

1. Client organisation (CO) has an authorization or an entitlement system or solution (ES) and works with one Cloud provider (CP) that does not have or is not covered by any ES



1. Client organisation (CO) has an authorization or an entitlement system (ES) and works with one Cloud provider (CP) that has its own ES (CES)



1. Client organisation (CO) has an authorization or an entitlement system (ES) and works with one Cloud provider (CP) that has does not have its own ES but is covered by a 3rd Party Cloud EC (PEC)



1. Client organisation (CO) does not have its own ES and works with one Cloud provider (CP) that does not have or is not covered by any ES



1. Client organisation (CO) does not have its own ES and works with one Cloud provider (CP) that has its own ES (CES)



1. Client organisation (CO) does not have its own ES and works with one Cloud provider (CP) that has does not have its own ES but is covered by a 3rd Party Cloud ES (PES)



1. Client organisation (CO) has its own ES and works with two or more Cloud providers (CP) that do not have or is not covered by any ES.



1. Client organisation (CO) has its own ES and works with two or more Cloud providers (CP) that have their own ES (CES).



1. Client organisation (CO) has its own ES and works with two or more Cloud providers (CP) that do not have their own ES but are covered by a 3rd Party Cloud EC (PES).



1. Client organisation (CO) has its own ES and works with two or more Cloud providers (CP), some of which do not have their own ES but is covered by a 3rd Party Cloud EC (PES) while some others have CES.



1. Client organisation (CO) has its own ES and works with two or more Cloud provider (CP), some of which do not have their own ES and may be clustered under an authority of the PES but different clusters may belong to different PES while some others have their own CES.



1. Client organisation (CO) does not have its own ES and works with two or more Cloud providers (CP), some of which do not have their own ES but is covered by a 3rd Party Cloud EC (PES) while some others have CES.



1. Client organisation (CO) does not have its own ES and works with two or more Cloud providers (CP), some of which do not have their own ES and may be clustered under an authority of the PEC but different clusters may belong to different PES while some others have CES.



1. Client organisation (CO) does not have its own ES, works with another organisation that has its own ES that, in turn, works with two or more Cloud providers (CP), some of which do not have their own ES and may be clustered under an authority of the PEC but different clusters may belong to different PES while some others have CES; the CO needs to access all mentioned Cloud providers.

