Identity governance toolbox

Piotr Cofta (piotr@cofta.eu)

20.07.2011

Executive summary

Working identity governance is a matter of compromise, but it is worth exploring how such a compromise may be reached. For public projects, the triangle of cost-choice-coverage provides a handy reference model to discuss pros and cons of different policies, and demonstrates how they can be build. This document discusses the generic structure of identity governance policies for the public provision of government services. It provides two examples of possible, complete yet imperfect polices: the 'big government - small people' and the 'small government - big people' ones.

Introduction

There is a large number of potential identity governance schemes for the public identity systems, each with their respective pros and cons. While they may differ, they always have to address the tension between three basic constraints of any public project: cost-choice-coverage.

Therefore it is worth examining options for identity governance policies using those three constraints as a reference. Such an analytical approach reveals possible conflicts as well as opportunities, and may lead to a governance propositions, that better manages its inherent conflicts. It is intentionally contrasting, highlighting differences.

This analysis is conducted from the perspective of an identity system for the public provision of government services. Therefore this analysis may not be directly applicable to other identity systems (e.g. for the internal usage of the government), and is not relevant to systems financed by the industry. Such systems tend to be constrained by another triangle, of cost-quality-time, not discussed here.

Constructing a governance policy

Public projects are often found caught in the triangle of constraints of cost-choice-coverage, shown on Fig. 1.

Every project can easily disregard two constraints and focus entirely on serving the chosen one, leading to one of three one-factor policies. It is also possible to satisfy any two out of three constraints with the appropriate two-factor policy.

However, there is not a single, coherent policy that can satisfy all three constraints. If the three-factor policy is needed (and usually it is), it is best served by the uneasy combination of the one-factor and the opposite two factor policies. One of those policies will be the

dominant (major) one, and the other will be the minor one, compensating for deficiencies of the major one.

On Fig. 1. major constraints are located at vertices of the triangle, complemented by one-factor policies that best suits them (for identity systems). Two-factor polices are listed along edges of the triangle. Three-factor policies can be located anywhere along altitudes of the triangle, with two of those policies marked with large black and white dots.

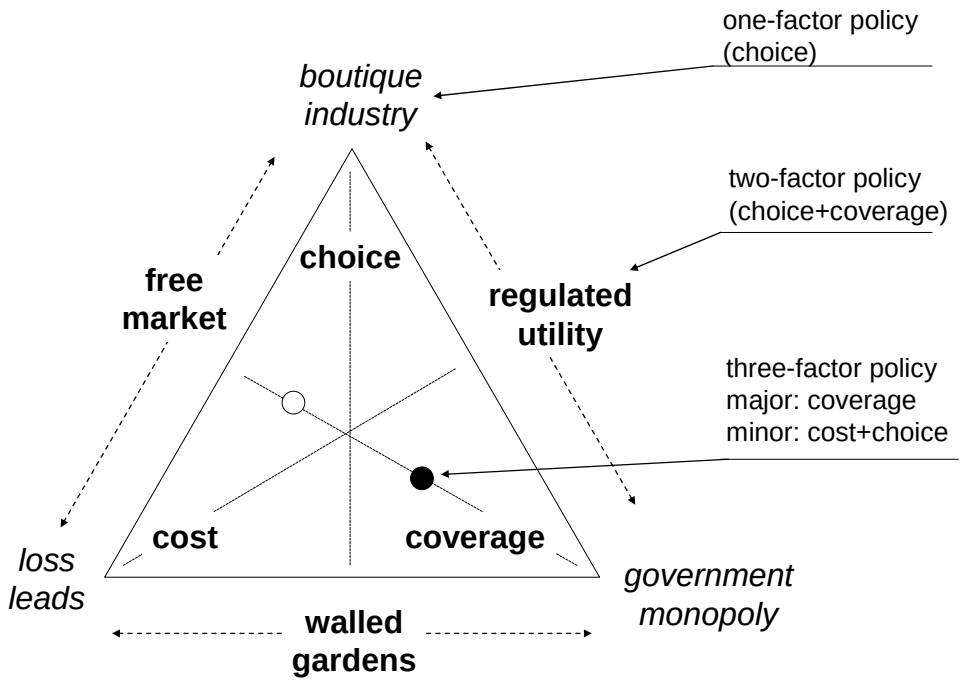

Fig. 1. The triangle of constraints

This paper proposes a systematic approach, discussing:

- constraints and one-factor policies that satisfy the chosen constraint
- two-factor policies that satisfy two out of three constraints
- the construction of three-factor policies

This paper intentionally does not provide any recommendation regarding the best or the preferred policy, but it indicates implications for various choices.

Constraints and one-factor governance policies

Public projects are constrained by the triangle of cost-choice-coverage For the purpose of public identity projects (identity systems for the public provision of government services), those constraints can be detailed as follows:

- Low **cost**. Their large sizes, public oversight and limited resources make public projects particularly sensitive to the issue of cost, even if eventually such a cost can

be hidden in taxation or budgetary spending. For identity management projects, low cost usually imply that the scheme should be self-financing.

The cost constraint can be best met by positioning identity projects as a **loss lead**, where the cost to set-up and operate the scheme is recovered through future savings. However, concentrating on cost alone may lead to solutions that do not provide choice (as choice brings additional cost) or coverage (as some fraction of the population is very expensive to serve). Further, focusing on loss lead may lead to the relaxed attitude regarding privacy and potential function creep.

- Wide **choice**. The necessity to cater for the variety of circumstances (disability, legal status, privacy concerns) leads to the constraint of a wide choice, in this case of a wide choice of identity providers and identity credentials.

  Choice itself is best served by the **boutique industry** where several independent providers can deliver a wide range of solutions. If unchecked, choice alone lead to social exclusion (as boutiques cater only for those who can afford the choice), and high cost (as there is little space for the economy of scale).

- Universal **coverage**. Public projects should deliver a near-universal coverage, both for individuals (covering the target group, e.g. the nation), and for service providers (covering all services that are in scope).

  Disregarding other constraints, universal coverage is best served by the **government monopoly**, where the government sets and enforces necessary standards and procedures. Monopoly alone leads to the loss of choice (as the solution that is convenient for the monopoly is preferred), and growing cost (as the non-existent competition does not keep the cost in check).

Two-factor governance policies

It is interesting to consider policies that cater for two constraints. Using Fig. 1. as a guide, one can see that there are three possible solutions, located along edges of the triangle. Each policy has certain implications on the identity governance, identity assurance as well as on the choice of identity management technologies.

Regulated utility

The combination of coverage and choice leads to the policy that positions identity system as a regulated utility. The government retains some of its monopoly, but - instead of directly operating the identity scheme - it is licensing its operation to commercial operators. UK telecommunication market can be used here as a reference.

- Governance. Licensing of identity providers is in place, with appropriate oversight. Participations is voluntary, operators and individuals enter into the agreement only if they see benefits. Individuals can holds multiple credentials. Licence agreement

stipulates the coverage as well as the choice. Cost structure is left to the market, possibly capped by agreements.

- Assurance. Criteria for identity assurance are set by the government, and are likely to relate to regulatory or legal requirements, not technical ones. There may be certain international harmonisation of assurance levels, if necessary.

- Technology. Minimum technical requirements are mandated by the licence agreement, but otherwise operators are free to deploy their own technologies. There is a certain guarantee of identity portability, but not of technical portability.

Regulated utility is not a low cost solution. Operators treat it as the commercial operation on its own, not as a loss lead. High entry barriers makes competition harder, thus reducing the pressure on cost. Voluntary contribution leaves the government to foot the bill for the part of the population that is most expensive to serve.

Note also that the government does not hold a fully enforceable monopoly on identity, as contrasting with other utilities. The creation and destruction of identities (such as births and deaths) are socially embedded, and the government cannot deny them. Further, the government often cannot refuse public services solely on the basis of the lack of an appropriate identity credential.

Free market

The combination of cost and choice (but not coverage) leads to the policy of an identity free market, where operators can compete on the identity market with a minimal government intervention. The government can capitalise on an availability and choice, at a competitive price point, and can exercise it bargaining buying power. There is no established free market for identity operators, but there is an established free market for identity technologies that can serve as an example.

- Governance. The free market is mostly self-government through voluntary agreements. Minimum requirements (e.g. safety) are enforced through the legal system. The government has its role in the market creation, stimulating the competition and allowing access to the market.

- Assurance. Schemes and voluntary and tend to be based on technology and risk. Operators may stress the technology side, while service providers may stress risk related to the acceptance of particular technologies. There are certain agreements in place.

- Technology. Technical progress is rapid, and one can see that there are several technologies looking for problems to address. Open standards with proprietary lock-in dominate the market. Operators innovate on top of established technologies by creating solutions that provide added value.

Free market does not guarantee coverage, as operators tend to pick areas that maximise their benefits. This may lead to the 'identity divide: those that can afford it are showered

with identity solutions, those that are in need may not gain access to any solution. certain governmental intervention may be required.

Walled gardens

The combination of cost and coverage (but not a choice) leads to the policy that encourages walled gardens - large operators who cater for their respective public. They may have a near-universal coverage within the population they address. They deployed identity systems for their own purpose, so that the operation of those systems is considered a loss lead. It may be even that they share the same underlying technology or standards. The government positions itself as a user of existing identity systems. Internet social networks, or large retailers can serve as a model.

- Governance. Legal oversight is the primary governance regime. Operators are mostly left to themselves, for as long as their operation does not interfere with legal requirements. The government is seen by them as one of several customers that can use their identity systems.

- Assurance. Each operator is likely to develop its own assurance criteria, on the basis of their own development path, and their business model. If there is any agreement, it is a fragile one. If the government require a different assurance model, it should develop and upkeep its own mapping.

- Technology. Technological choices are made by operators, and there is a tendency to re-purpose existing technologies. If interoperability or portability is legally required, it is likely to be at the lowest common denominator only.

This governance model is particularly aggressive towards privacy and choice. Walled gardens recover their investment because they are able to lock the individual in and to re-purpose their identity-related information.

Three-factor governance policies

Referring back to Fig. 1., the construction of a three-factor policy is a matter of choice. Any one-factor policy can be combined with the opposite two-factor policy to produce the three-factor one. One of those policies have to be the dominant (major) one, while the other (minor one) has to compensate for deficiencies of the first one.

Three-factor polices tend not to be consistent, because there is no consistent way to address all three constraints. If they are promoted as a universal panacea for all three constraints, they may disappoint. Therefore it is important to clearly identify what is the major and what is the minor policy.

There is a large number of possible three-factor policies, but for an illustration two are described below in more details.

Example 1: big government, small people

The following description provides and outline of the policy that is indicated by the large block dot on Fig. 1. This policy is dominated by the constrain of a coverage, while remaining constraints of cost and choice are less pronounced. It can be viewed as the heavyweight government regulation imposed on the market.

- It is the duty of the government to provide coverage, while providing reasonable choices at a relatively low cost. Thus the governance should be a mix of a government monopoly and a free market approach.
- The government should act as an issuer of identity credentials, and assure low cost through competitive bidding. If possible, credentials should be provided free or at the cost that is means tested.
- The government should define assurance in terms of legal liability, but it should provide the mapping of its requirements that are understood by the industry, specifically in terms of technologies.
- The government should allow other operators to register with the scheme, and should accept credentials issued by them, if found suitable. Those operators will be subject to a governmental oversight with regard to government-accepted credentials, but otherwise they will be free to innovate.
- The government should allow other service providers to accept government-issued credentials, and provide means to assess the risk associated with such an acceptance. Service providers may be charged for the usage of credentials.

Example 2: small government, big people

Following is the outline of the alternative policy, indicated on Fig .1. by the white dot. This policy is dominated by joint constraints of cost and choice (thus empowering people), while the constraint of coverage is less pronounced, limiting the role of the government. This 'small government - big people' combination lends itself to policies shaped by the free market with a minimal government intervention.

- It is the duty of the government to provide a choice of identification methods while containing the cost. Thus governance policies should be formed as a mix dominated by a free market approach, complemented by the government monopoly.
- The government should open its identity market for a competition, by publishing its minimum requirements and standards. Any operator should be allowed to issue credentials that are accepted by the government, albeit at a varying risk level. Any service provider should be allowed to accept such credentials.
- Cost, means of payment, quality of credentials, the reputation of issuers and risk should be determined by the market. The government should not impose its own standards.
- The government should define its identity assurance requirements in terms of risk and technology, i.e. in terms that are understood by the industry.
- Operators should be allowed to charge for the issuance of credentials as well as for their acceptance. The government should not interfere with the pricing.

- The government should create an agency that serves those who are unable to receive a credential from one of commercial operators. The operation of this agency should be subject to the rules of a market for as much as possible.

Recommendations

While there is no perfect policy for identity governance, there is a systematic way to create a satisfactory one. Therefore:

- It has to be accepted that the single, consistent policy cannot satisfy all three constraints of cost-choice-coverage, but an inconsistent policy can.

- The government should decide about its priorities with regard to the identity governance, defining its primary constraint (or a pair of constraints) and its secondary one.

- The identity governance policy should reflect those priorities. Any communication regarding the policy should clearly indicate those priorities.

- Two exemplary policy outlines: 'big government - small people' and 'small government - big people' should be used to test the current political climate.

- Decisions regarding identity assurance and technologies for identity management should follow the choice of a policy, not vice versa.