Use Case for eGov Provisioning Portal

Sampo Kellomäki (sampo@symlabs.com)

June 8, 2005

Abstract

A means to connect user's identity strongly to government provisioned data is needed. This connection should be independent of IdP and Discovery Service. A solution involving a trusted portal SP is presented.

1 Introduction

Some governments provide a domicile registry that authratively establishes official residence of the citizen. This is mainly important for taxiation, but the information is used for a number of other services are well.

As a case study of different government approaches to domicile registry, consider following figures.

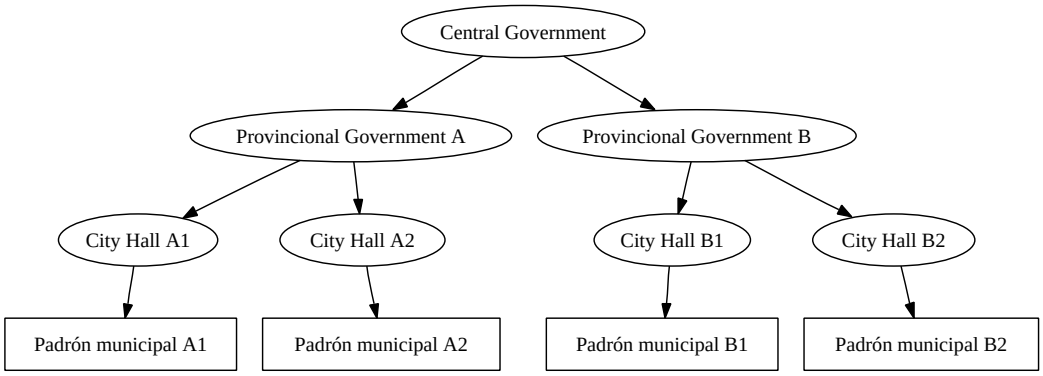

Figure 1: Spanish approach to the domicile registry is decentralized.

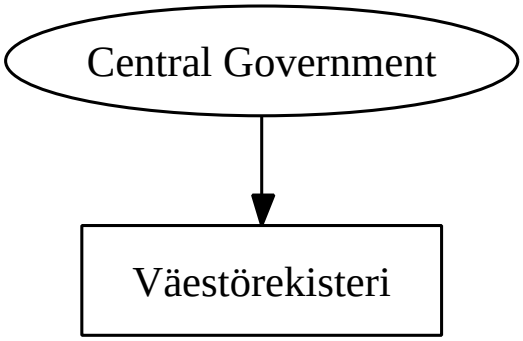

Figure 2: Finnish approach to the domicile registry is centralized.

While the central approach may be easiest from IT architecture perspective, it may not be acceptable from the police state avoidance perspective.

The domicile registry information can be conveniently represented as Personal Profile Identity Web Service, defined by the Liberty Alliance [**?**]. It is obvious that the government agencies that operate the domicile registries should be in the business of offering PP WSP.

There is only slight problem: there may be any number of personal profile services for any given citizen. How do we know which one represents the official domicile registry? The PP specification provides for domicile indicator (discovery option keyword).

Thus any government agency requiring domicile information can discover the (those?) PP service that provides this information.

However there is nothing to prevent a nongovernment PP from registering this indicator - unless this is prohibited by law from any other PP than the government. Essentially this is the requirement that discovery service must not accept rogue or nonofficial registrations. Since we are making such assumption about discovery service, this can be relied on. However, the original intent of the domicile indicator was not to indicate government authority. Thus it may be advisable to establish a new "official" indicator for this purpose.

2 eGov Domicile Registry Provisioning

2.1 Citizen Linkage Assumptions

- Linkage between online identity and physical (citizen) identity needs to be made by government agency.
- Its desireable that free market of IdPs exists and eGov should leverage it. Ideally government should not need to be an IdP.

2.2 Trust Assumptions

- IdP must be trusted at least to reliably authenticate the user, even if he is anonymous. This will require government enforced legal framework with sanctions and accountability for failing to perform this duty.
- Discovery service must be trusted not to permit rogue registrations. In particular it must not be possible to register a service without citizen's consent or official approval (and then we must trust the official - is this the slippery slope to the police state?).

Provided that the IdP and discovery services indeed satisfy the above requirements, then there is no reason why there could not be many of them.

2.3 Preconditions

- Citizen has already created an identity at IdP, however this identity is anonymous from government perspective
- Citizen has not been provisioned yet

2.4 Postconditions

- Discovery service will have a resource labelled as "official" for the citizen
- Anyone who can discover this resource can use (or even alter) official information

2.5 Linking Identity and Populating PP

1. Fed & SSO citizen, this gives NameID (pseudonym) to the SP (portal)
2. A proprietary technique (possibly involving a government officer) is used to check citizen's identity in a way acceptable to government and remember this linkage only for duration of the session at SP.
3. Submit new domicile information
4. Create PP resource in domicile registry assigned to citizen by the portal (based on government rules)
5. The PP resource is registered with "official" flag
6. The PP resource with "official" flag is discovered. Everything is standard business from here on.
7. Populate PP

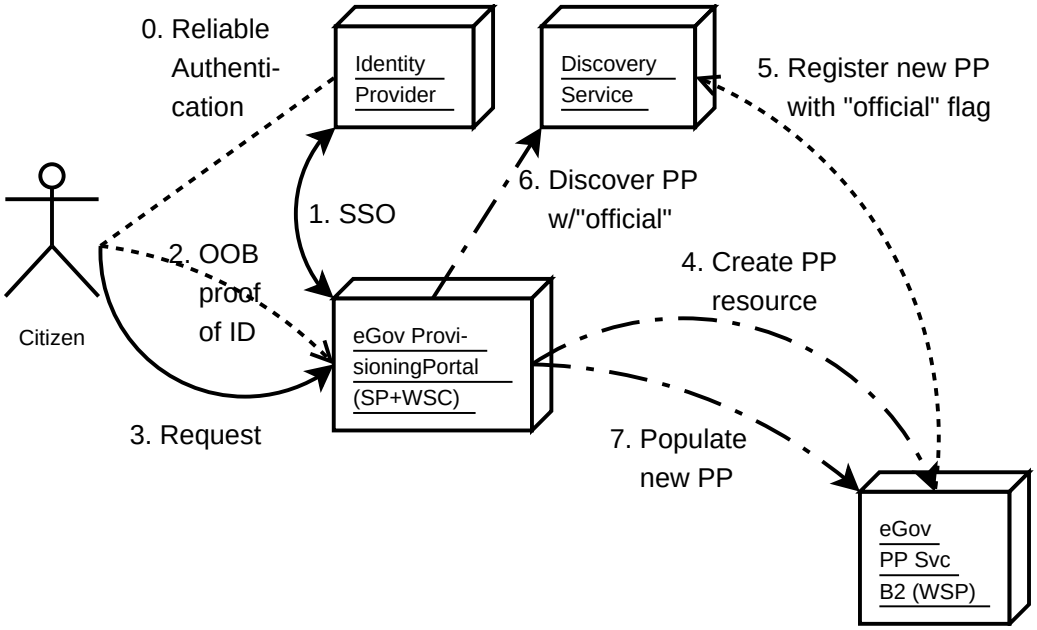

Figure 3: Linking citizen to eGov PP.

After the citizen linkage has been establish, using the official PP data as well as altering it consists of steps 1, 3 (submit whatever request), 6, and 7.

2.6 Ramifications

- While any SP (or web service at any level invoked by the SP) with whom the user uses his identity could theoretically access the eGov PP, the PP is expected to enforce access control based on how much it trusts the requesting WSC. Since there is a manageable number of government agencies, this is feasible.
- IdP, Discovery, or relying SPs need not know user's true identity as citizen
- No national ID number is relied on
- Government agencies operating as SP will use different NameIDs, thus preventing collusion by government about its citizens
- Even the provisioning portal can discard the linkage information as soon as the provisioning has been done
- There can be multiple entities offering each of the architectural components and many of these can come from free market

3 Copyright and Confidentiality