Secure registrar identification & authorization

A future scenario
Registrars self-service panel

typically used for

- provisioning of programmatic interfaces (EPP)
- manual management of clients domain names
- billing
- ..
Password don’t cut it

- The dependency upon domain names increases
- The attackers are more sophisticated and persistent
- Only a password between an attacker and potentially thousands of high-value domain names
- Generally, the risks are too high
- Risks has to be managed in a scalable, economically feasible and sufficiently secure way
Alternatives to password

- registry-issued tokens
- national e-authentication (eID) scheme
- ...
eIDAS

- EU regulation for national eID schemes
- Very little focus on private-sector use of eID
- One step forward, two steps back
- National eID’s may work nationally
Registry-issued tokens

- hard one-time (connected) password token
- hard one-time (air-gap) password token
- soft token in smart phone
Registry-issued tokens

- Generally high costs for managing
- Should be tied to an individual (not a group)
- Users can handle one or two, not twenty
A federated identity approach

“A federated identity in information technology is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems”

wikipedia
In the registrar context

A registrar’s representative, which can be securely identified by one registry, can be securely identified across all participating registries.
How does it work?

Hi, I am Anna. I represent the registrar Foo-reg.

Registry A
Identity Provider

Provides assertion

Registry B
Service Provider

Authenticates

Makes claim
How does it work?

Hi, I am Bert. I represent the registrar Bar-reg.

Registry A
Service Provider

Provides assertion

Hi, I am Bert. I represent the registrar Bar-reg.

Makes claim

Registry B
Identity Provider

Authenticates
How does it work?

- Each participating registry provides a trusted authentication and authorization service to the federation.
- A registrar's employees would use one of these services to authenticate to any participating registry.
From a registrars’ perspective

- Will select one registry which can identify and vouch for its employees
- At least one individual will go through a process to prove authority for representing the registrar (Authorized Representative)
- This individual can then add co-workers for different roles
From the registries’ perspective

- Will implement a common policy ("trust framework") for identification and authorization
- Maintains a database over verified registrars, co-workers and authorizations
- Authenticates users and issues tickets ("assertions") upon requests from other participants in the federation
How are the registrars’ Authorized Representatives identified?

- Can use a national eID scheme to determine the authority to represent the registrar, or
- May perform proofing of identity and authority conforming to the requirements of the trust framework, to issue their own credentials.
The Registrar’s Authorized Representative

- Once authority has been verified, can add co-workers to different roles (only), using a Security Control Panel provided by the registry.
- Co-workers can be provided two-factor tokens through the Authorize Representative, or
- Co-workers may use the national eID scheme.
- Is accountable for the co-workers.
Security Control Panel

- Used by the registrars Authorized Representative for
  - Management of role assignments
  - Used to issue and revoke co-workers tokens
  - The registry will only have to verify the identity and authority of one or two individuals, provides scalability
one registry

verifies

authorized representative

issues credential

assigns roles

co-workers

proves authority

another registry

the federation
Scalability and convenience

- Only the Authorized Representative requires proofing
- All other identities can be issued instantly through the Authorized Representative
- The registrar will be able to select the registry which can most conveniently verify the Authorized Representative
- More than one registry provides freedom of choice
Catches?

- Has this technology been proven to work?
- Is it expensive?
- Does it provide protection of personally identifiable information?
- Will it work with the new EU regulation (eIDAS)?
- What about registrars outside of Europe?
Liability?

- Each registry will be liable to follow the policy (the “trust framework”)
- If the protocol is followed, that party is not liable for damages incurred
- The federation does not free the relying registry from responsibility to act upon suspicious activity
What needs to be done?

- A trust framework
- Technical specs
- Agreement upon a pre-defined set of roles
- Joint development of the registrar identification and authorization system (“RIAS”)
RIAS?

- Provides interface for Authorized Representative to manage co-workers roles
- Holds and maintains the identity and authorizations database
- Ties two-factor tokens to co-workers
- Identifies registrars co-workers and issues assertions
- (optionally) Integrates with national eID structure
RIAS could be the same system instantiated across all federation members, with minor adaptations.

- Guarantees interoperability
- Significantly reduces costs for development and testing
- Can be extensively tested for security vulnerabilities and quality assurance
- Reduces lead-time
fredrik@kirei.se