Liberty eGov Day, Brussels, April 2007

Sampo Kellomäki (sampo@symlabs.com)

1 Common eGov requirements

1. ID construction and allocation
2. Sector ID mapping (multi-agency data sharing)
3. Authentication
4. Mapping authentications across countries or domains
5. ID-WSF across countries or CoTs
6. Single Sign-On
7. Attribute sharing / Citizen account
8. Attribute usage policy
9. Consent
10. Withdrawal of identity from government

11. Non-repudiation
12. Audit and transparency
13. Document archival
14. Delegation
15. Creating Circles of Trust (CoTs) and their management
16. Operational issues
17. Risk sharing and assessment
18. Sharing systems with private sector
19. Government employee usage

2 Solutions

- The following solutions slides are based on informal discussions.
- General sense is that Liberty and SAML are highly applicable and at bit level there are no serious gaps.
- More work (profiling) is needing in applying the specs in uniform way across governments deploying eGov

2.1 ID construction and allocation

- SAML NameID format is flexible enough to support all cases
  - pseudonymous IDs
  - sector specific IDs
  - unique IDs (citizen number)
  - algorithmically derived (e.g. AT)
- Matter of country specific policy how to construct and allocate

2.2 Sector ID mapping (multi-agency data sharing)

- SAML NameID Mapping
- ID-WSF Identity Mapping Service
- Matter of country specific policy how to apply the above mechanisms and how the authorization to do the mapping is handled (legal privacy framework).
- Mon Service Public side steps the problem by having centralized eSafe service where user collects the documents that are needed in cross agency interactions
- Liberty framework in itself does not need mapping (or in few cases where it is needed, the result can be suitably encrypted so there is no privacy risk)

2.3 Authentication

- SAML is authentication method agnostic
- Country specific policies dictate what methods to use
- In medium term Liberty Strong Authentication Expert Group activity may produce relevant results

2.4 Mapping authentications across countries or domains

- SAML IdP proxying can support "clearing house" approach
  - Policy or legal framework to trust the clearing house
- If (but this is a big if) there was agreement about semantics of Authentication Contexts, then direct trust could happen
- Push EU to standardize Authentication Context semantics
- EU eID interoperability activity seems to have on its agenda addressing semantic interoperability (Fulup will be in next meeting)
- Electronic apostilla needed (but does not currently exist)

2.5 ID-WSF across countries or CoTs

- Direct calling is unmanageable and may be regulatorily difficult
- Proxying preferred (Sampo and Fulup have a straw man for doing this)
- Liberty may publish a white paper (Sampo to contribute first draft)

2.6 Single Sign-On

- SAML 2.0 (or ID-FF) is an existing standards based solution for this. Just use it.

2.7 Attribute sharing / Citizen account

- Personal Profile
- ID-DAP (conceptually LDAP with identities)
- Validation or attestation of attributes is not addressed very well in current specs
  - ACC (Attribute Collection Context) may be too basic
  - Vocabulary standardization for ACC enumerators
- SAML Attribute Authority that issues attribute assertions is a way to express this, but Liberty data protocols need adaptation to use assertions as data format.
  - Liberty plans to write ID-WSF profile for SAML Attribute Authority
  - As of today, anyone can define their own Data Services Template based service to pass attribute assertions

2.8 Attribute usage policy

- ID-WSF offers UsageDirective mechanism, but actual values that can appear as such directive require further standardization
  - Government or CoT should specify the allowable values and their semantics
  - Eventually EU regulation would be good way to standardize them so that cross country / CoT interoperability is ensured
- Liberty Identity Governance Framework (IGF) is current effort to standardize the values for usage directives
  - AAPML
  - PPEL

2.9 Consent (1/3)

- SAML and ID-WSF provide protocol fields for expressing consent
- Collection of consent is up to user interfaces
  - Opt-in and capturing consent from citizen
  - Consent may be given by a privacy commissioner (or similar authority) instead
- Consenting to civil servant (e.g. social worker) to access your records is similar to delegation
- ID-WSF Interaction Protocol to query user for consent
  - At service level (WSP)
  - At Discovery level
  - At People Service level
  - ID-CSM (Messaging) specification provides concrete support for contacting user, e.g. using mobile phone

2.9 Consent (2/3)

- In delegated use cases it may be necessary to route consent
  - Some operations attempted by child may need to be consented by parent
  - Other operations may be consentable by child himself
  - Register parent's Interaction Service in child's Discovery Service
  - Discovery Option to indicate that the registration corresponds to parent (or delegatee in general)
  - Other approach would be for the WSP to explicitly route the consent, perhaps based on querying People Service

2.9 Consent (3/3)

- Sometimes consent may need to be collected when user is not online
  - Use some back channel (e.g. ID-CSM messaging)
  - Wait until user comes online
  - Indicate pending status in dash board
  - Asynchronous response or Notification (in response to Subscription)
- Liberty to publish a white paper (Sampo to contribute first draft)

2.10 Withdrawal of identity from government

- SAML Federation Termination provides technical means
  - Unspecified whether federation termination will actually delete account (as opposed to just disconnecting from SSO framework)
  - Citizen may not be allowed to withdraw his electronic identity from some services or agencies
- SAML assertion query could be used as a method for checking validity of a session
  - Withdrawal of identity causes the validity check to fail
  - assertion query was not originally designed for this, perhaps it would be cleaner to extend SAML explicitly to support validity check
- WS-Trust Validate operation can also be used
- Online Certificate Status Protocol: similar check in PKI world

2.11 Non-repudiation

- SAML and Liberty protocols has plenty of digital signatures - just use them
- Attribute assertion is a non-repudiable attestation
- SSO + Server based digital signature protocols (DSS, Digital Signature Service)
  - Provides non-repudiation even if technically speaking user does not perform the signature
  - Norwegian legislation considers such "managed digital signatures" binding

2.12 Audit and transparency (1/2)

- Citizen must be able to see what operations or data accesses government has done or is process of doing at the moment
  - Opportunity correct or protest if flawed information enters a process
  - Way to inform citizen that some process is pending some citizen action, such as providing requested data
  - May be implemented as a dash board service
  - or may be a messaging system can provide transparency to government processes

2.12 Audit and transparency (2/2)

- Liberty Accounting Service
  - Provides mechanism to report / transport audit events
  - Attribute release already defined
  - eGov specific profile that describes the government specific privacy events needs to be written
  - Each country could write its own profile
  - EU regulation top standardize a profile across the board?

2.13 Document archival

- May serve audit purpose
- May serve inter-agency data exchange purpose
- Implementation as Liberty data service (e.g. Data Service Template based)
- French Mon Service Public eSafe is a good example of document archival service

2.14 Delegation

- ID-WSF 2.0 can express explicitly
  - Invoker's identity (who is doing operation)
  - Targeted identity (on who's behalf)
- People Service offers a good framework for capturing delegation relationship
- Parent-Child relationship
- Family relationship
- General power of attorney

2.15 Creating Circles of Trust (CoTs) and their management

- SAML metadata exchange protocol provides the technical solution
- PKI hierarchy and certificate revocation (OCSP) may help as well
- Every country will have to come up with regulatory or policy framework

2.16 Operational issues

- Corrections
- Fixing situations where none of the available options apply (e.g. in form filling)
- Fixing access control
  - Too strict (eGov service can not do its job) or
  - Too lax (privacy issue)
- It does not seem possible to standardize any management protocol. Every deployment will need to address this by themselves (perhaps using proprietary methods)

2.17 Risk sharing and assessment

- Cross agency
- Centralized?
- Between countries
- These are policy problems, the current protocols pass enough information for the decisions to be made.

2.18 Sharing systems with private sector

- Reduce cost
- Drive protocols that private sector should use vs. adopt the protocols that they chose?

2.19 Government Employee usage

- Generally the SAML SSO and ID-WSF are sufficient to address these use cases

3 Regulation Desired

For cross country interoperability reasons it could be desirable that some aspects of Liberty and SAML protocol exchanges were regulated (perhaps by EU)

- Authentication contexts
  - Common definitions and ranking across the board
  - Legal implications of trusting an authentication
- Electronic apostilla
  - Trusting authentications performed in different country
- eGov audit records: Common format (profile of accounting service)
- Attribute usage policy vocabulary (UsageDirectives) standardization
- Consent enumeration standardization

4 Liberty Tool Pack

- SAML SSO
  - Unique or
  - Sector based or
  - even pseudonymous IDs
- ID-WSF web services
  - discovery as authorization point
  - same ID properties as SSO
- ID Mapping Service or SAML ID Mapping
  - Connect sector based IDs
- People Service
  - act in role
  - delegation
- "Managed" Digital signatures based on strong SSO / DSS

- non-repudiation in the Norway sense

5 Acronym Expansion

ID-WSF Liberty Alliance Identity Web Services Framework

IdP Identity Provider (SAML role, asserting party)

SP Service Provider (e.g. web site) (SAML role, relying party)

CoT Circle of Trust: a group of SPs and the IdP(s) they trust

WSC Web Services Client

WSP Web Services Provider

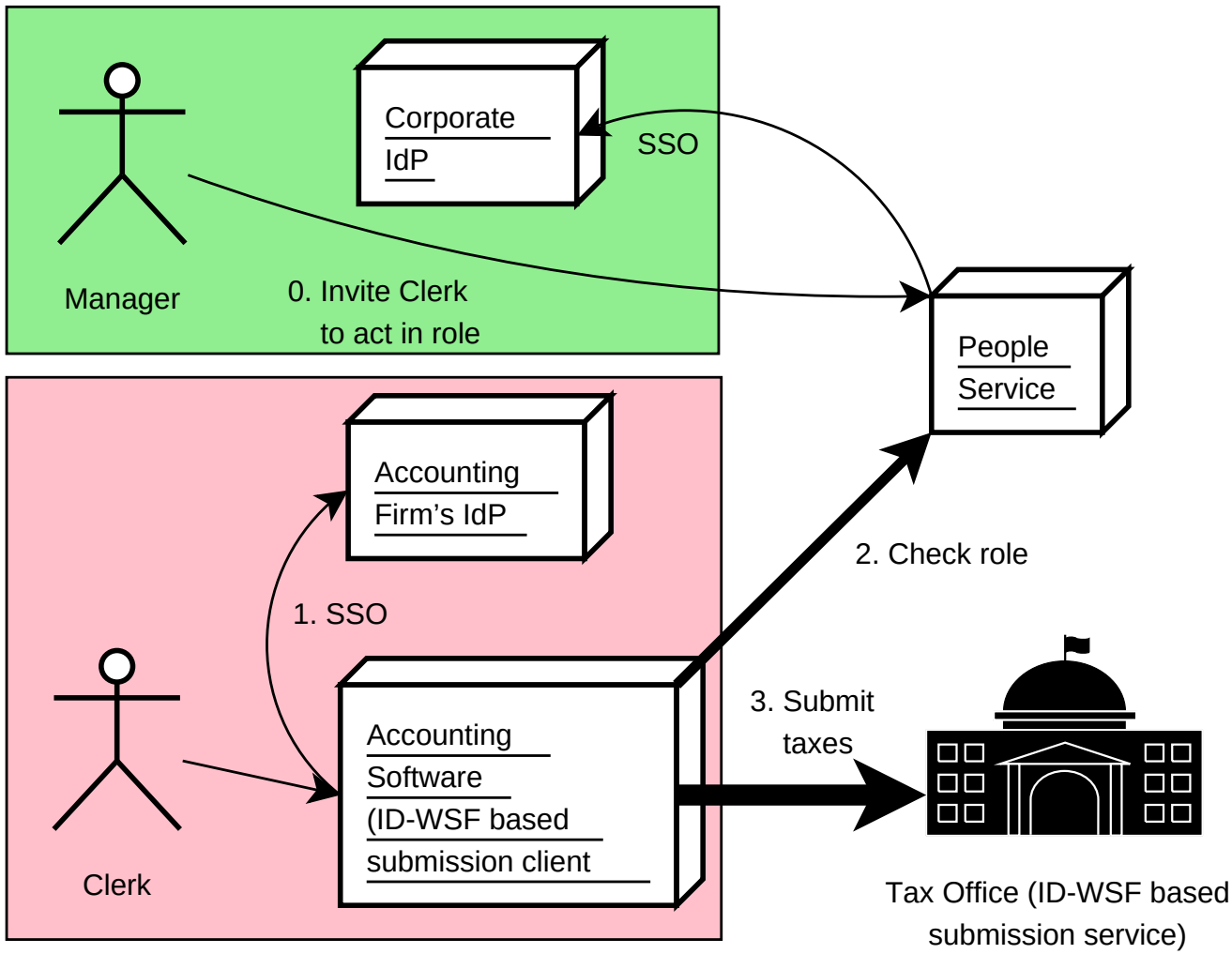
DS Discovery Service

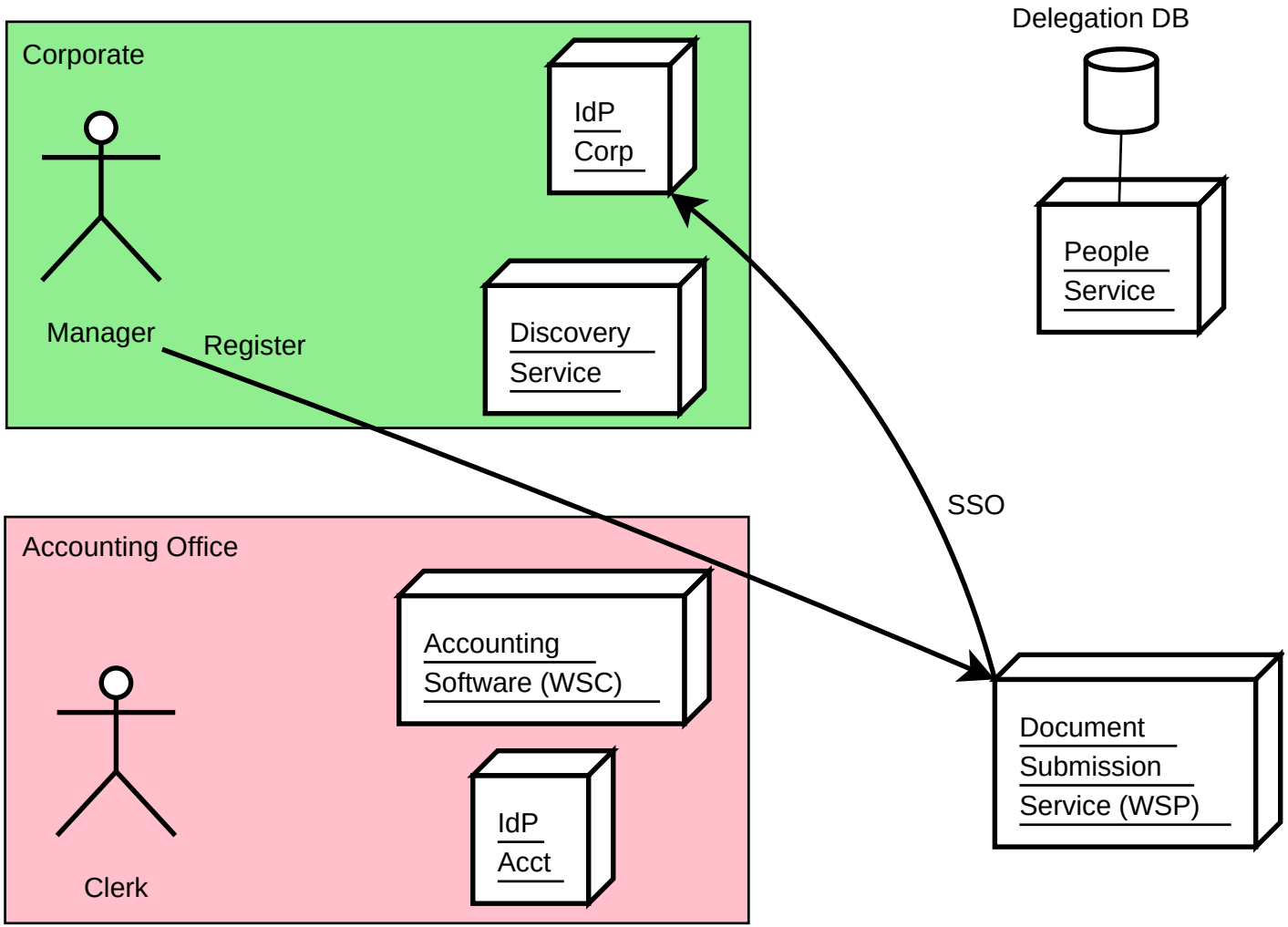
TokM Token Mapping Service

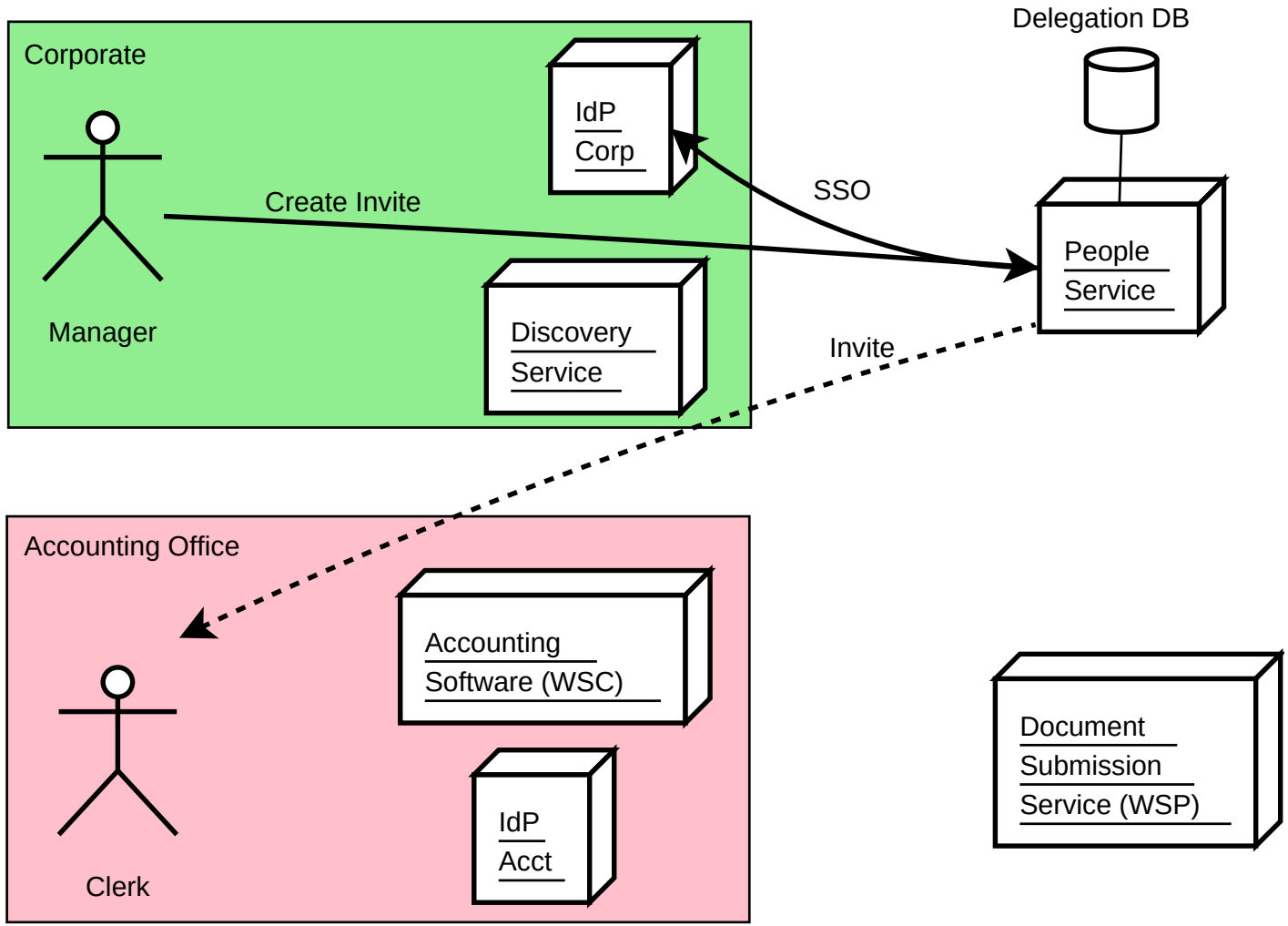
PS People Service

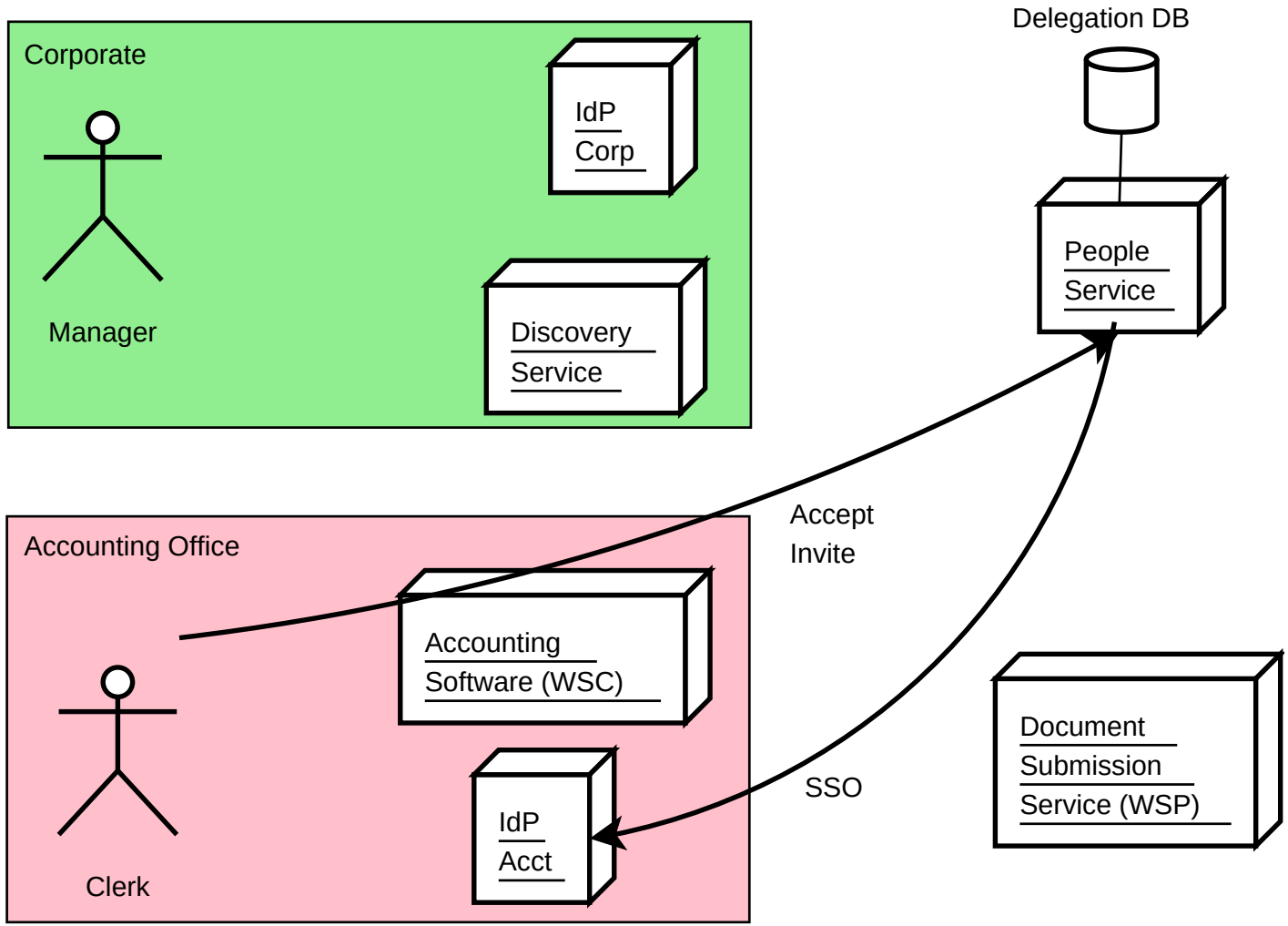
EPR End Point Reference (URL + metadata and possibly credentials)

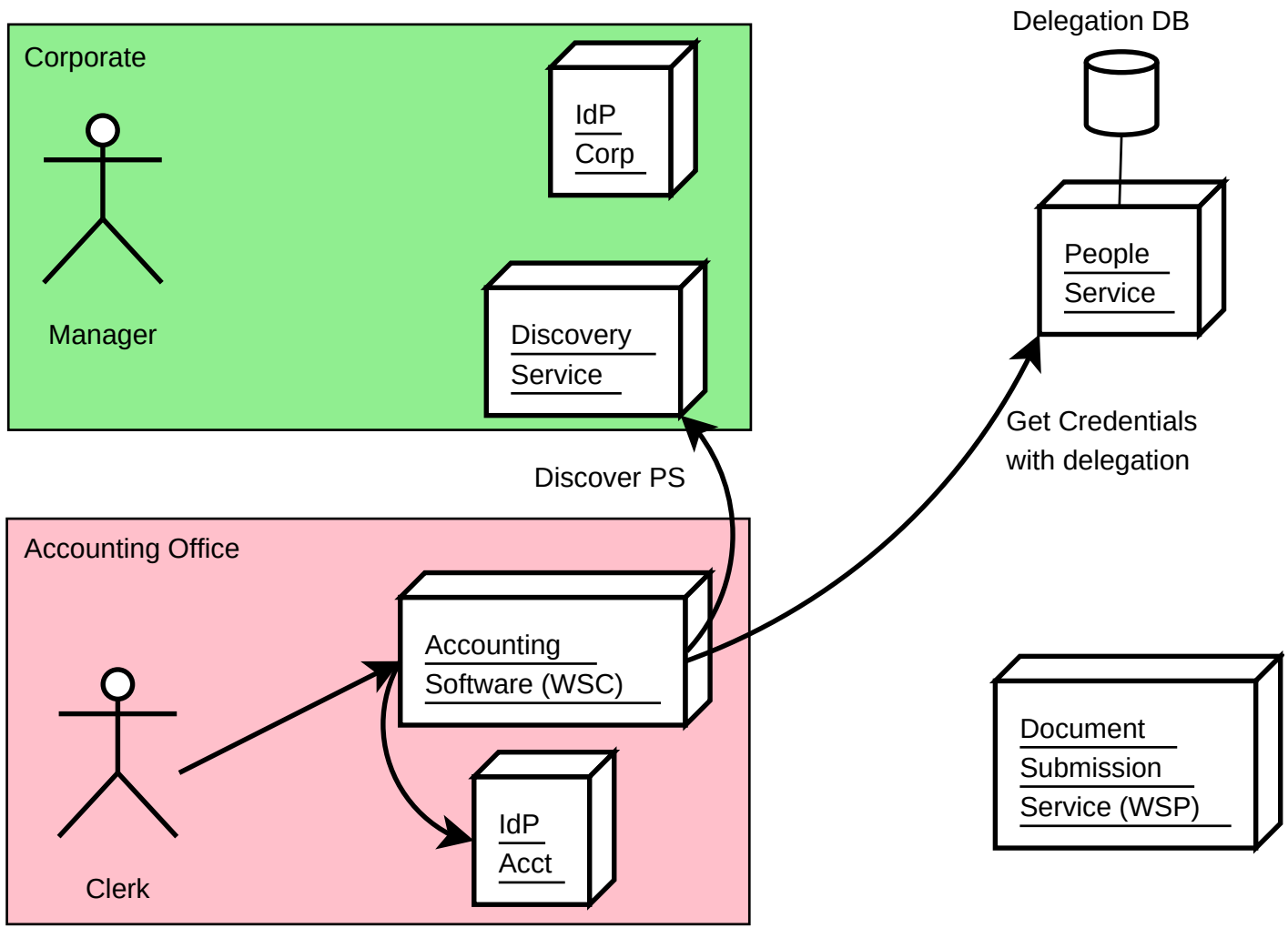
6 eGov delegation example

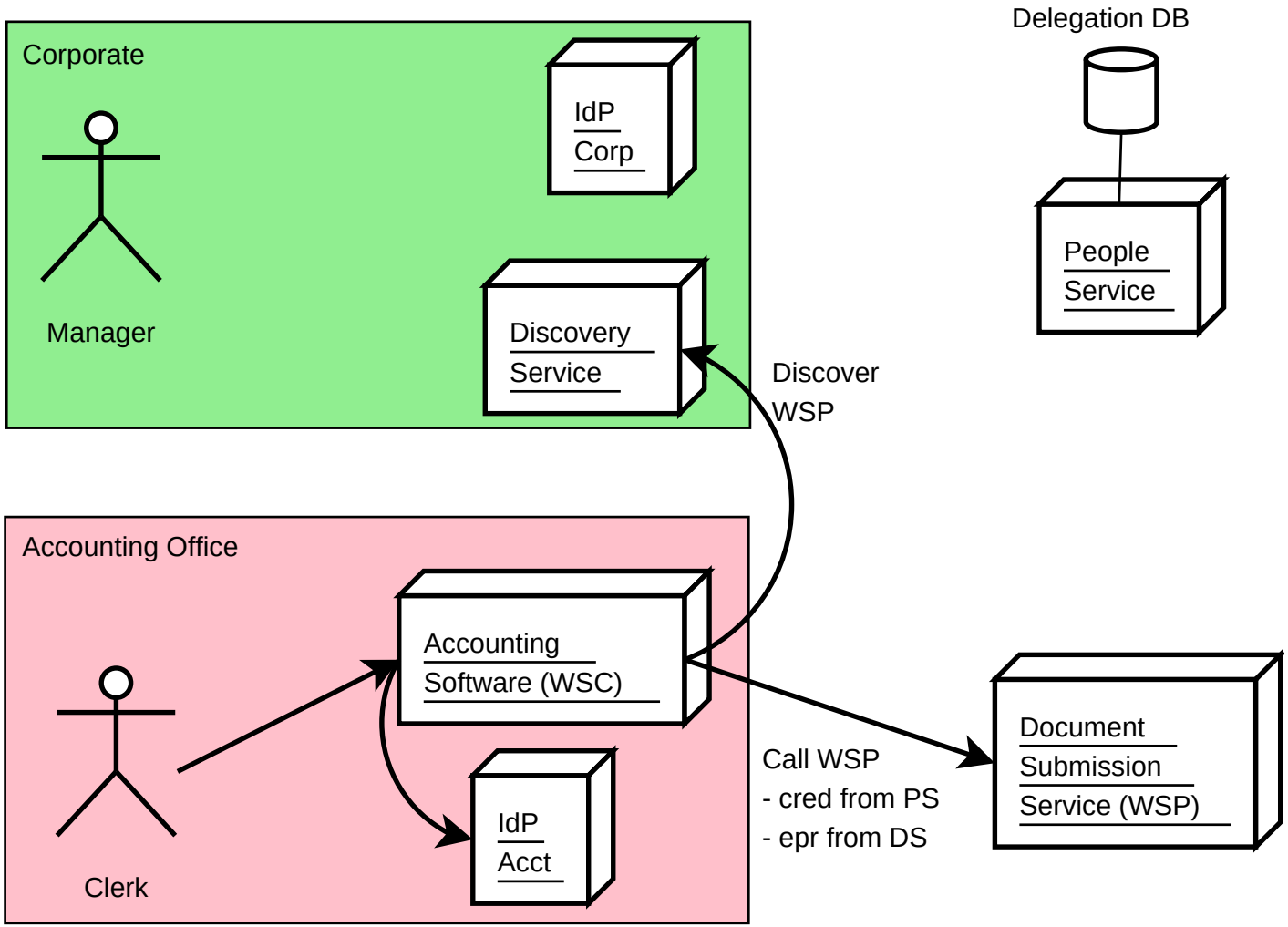



Corporate
IdP
Corp
Manager
Register
Discovery
Service
Delegation DB
People
Service
SSO
Accounting Office
Accounting
Software (WSC)
IdP
Acct
Clerk
Document
Submission
Service (WSP)


Corporate
IdP
Corp
Manager
Create Invite
SSO
Delegation DB
People
Service
Discovery
Service
Invite
Accounting Office
Accounting
Software (WSC)
Clerk
IdP
Acct
Document
Submission
Service (WSP)


Corporate
IdP
Corp
Manager
Discovery
Service
Delegation DB
People
Service
Accept
Invite
Accounting Office
Accounting
Software (WSC)
Clerk
IdP
Acct
SSO
Document
Submission
Service (WSP)

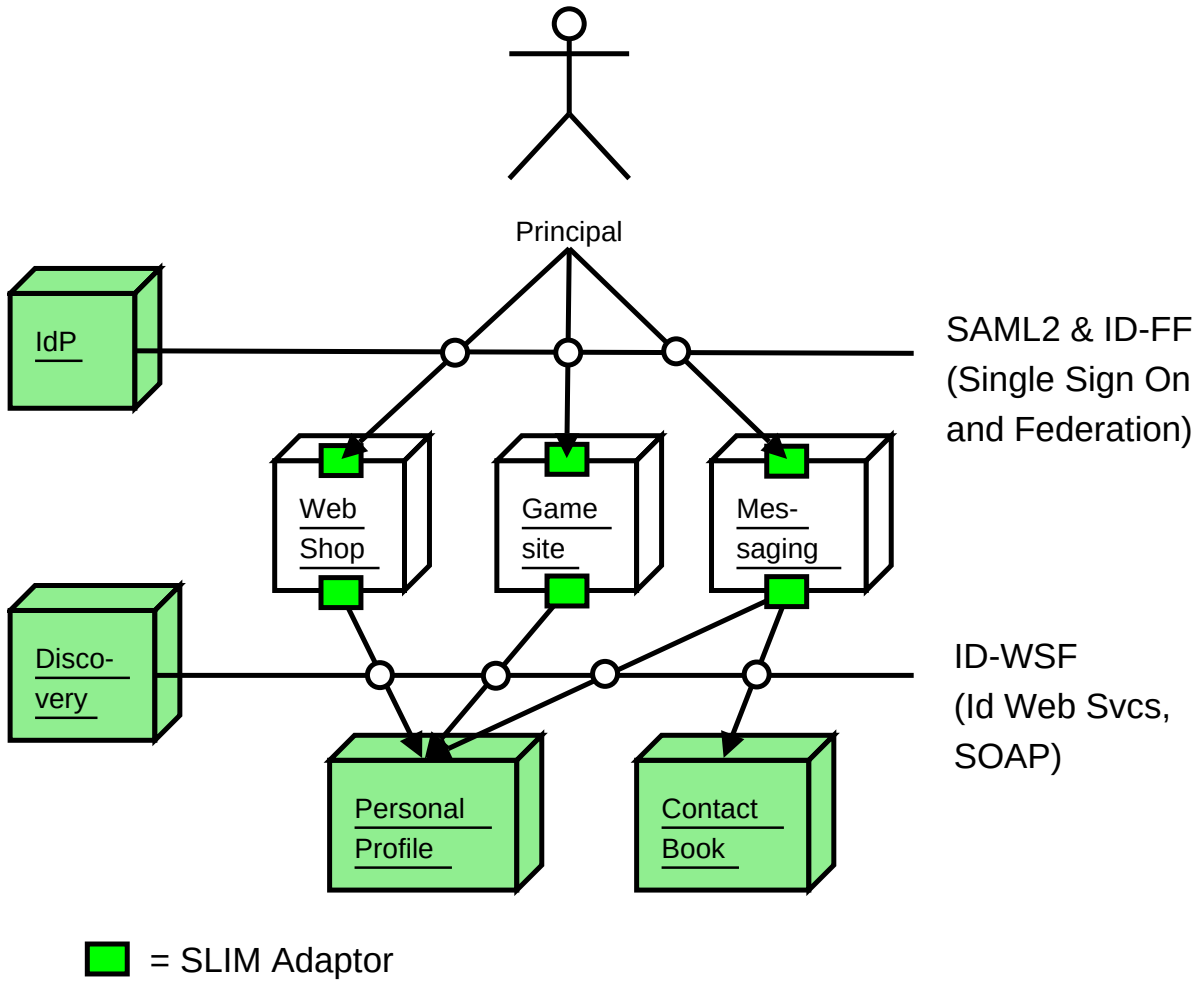

Corporate
IdP
Corp
Manager
Discovery
Service
Delegation DB
People
Service
Get Credentials
with delegation
Discover PS
Accounting Office
Accounting
Software (WSC)
IdP
Acct
Clerk
Document
Submission
Service (WSP)


Corporate
IdP
Corp
Manager
Discovery
Service
Delegation DB
People
Service
Discover
WSP
Accounting Office
Accounting
Software (WSC)
IdP
Acct
Clerk
Call WSP
- cred from PS
- epr from DS
Document
Submission
Service (WSP)

Thank you

Questions?

Sampo Kellomäki <sampo@symlabs.com>
+351-918.731.007


Principal
IdP
SAML2 & ID-FF
(Single Sign On
and Federation)
Web
Shop
Game
site
Mes-
saging
Disco-
very
ID-WSF
(Id Web Svcs,
SOAP)
Personal
Profile
Contact
Book
= SLIM Adaptor