TAS^3
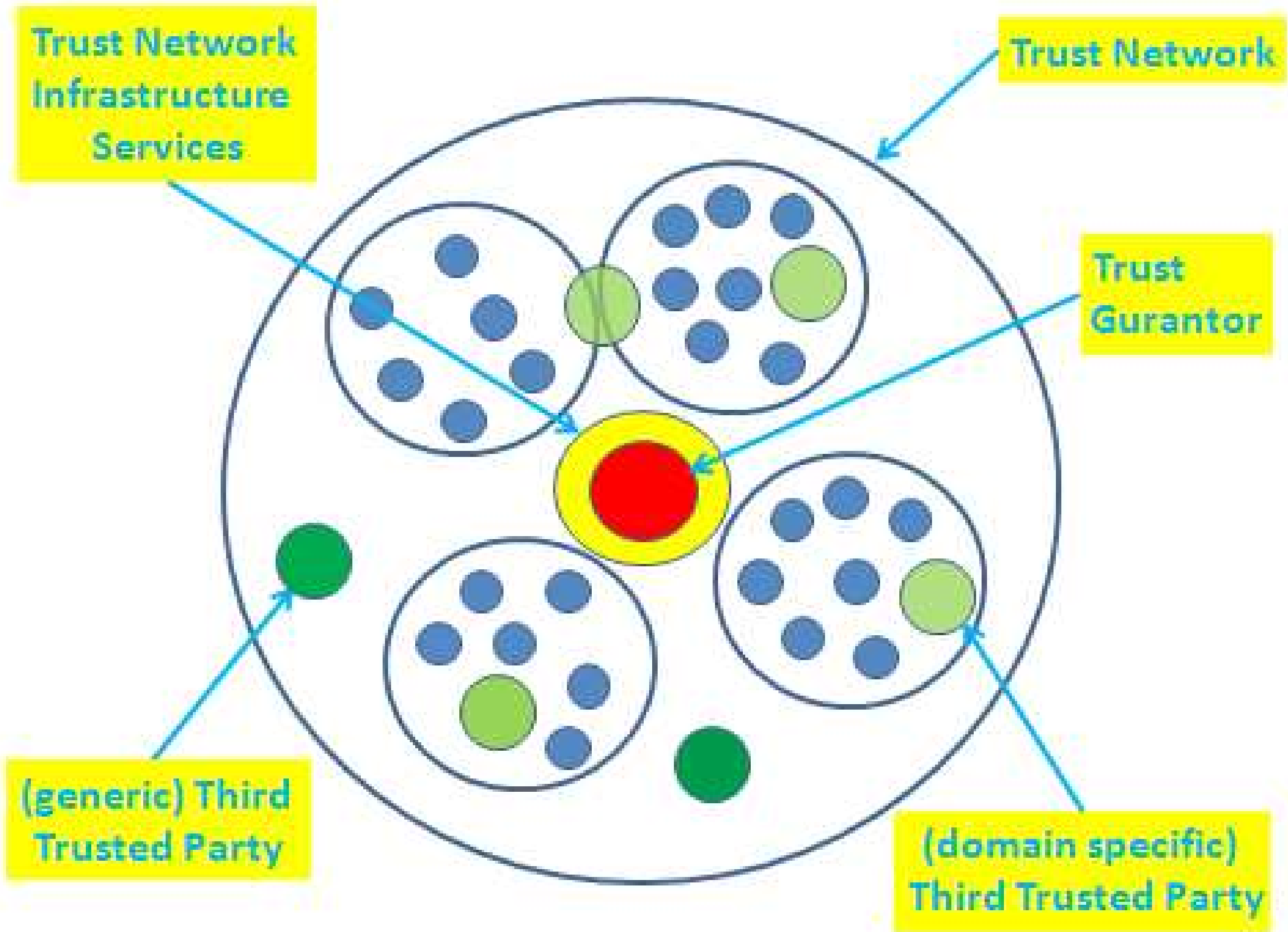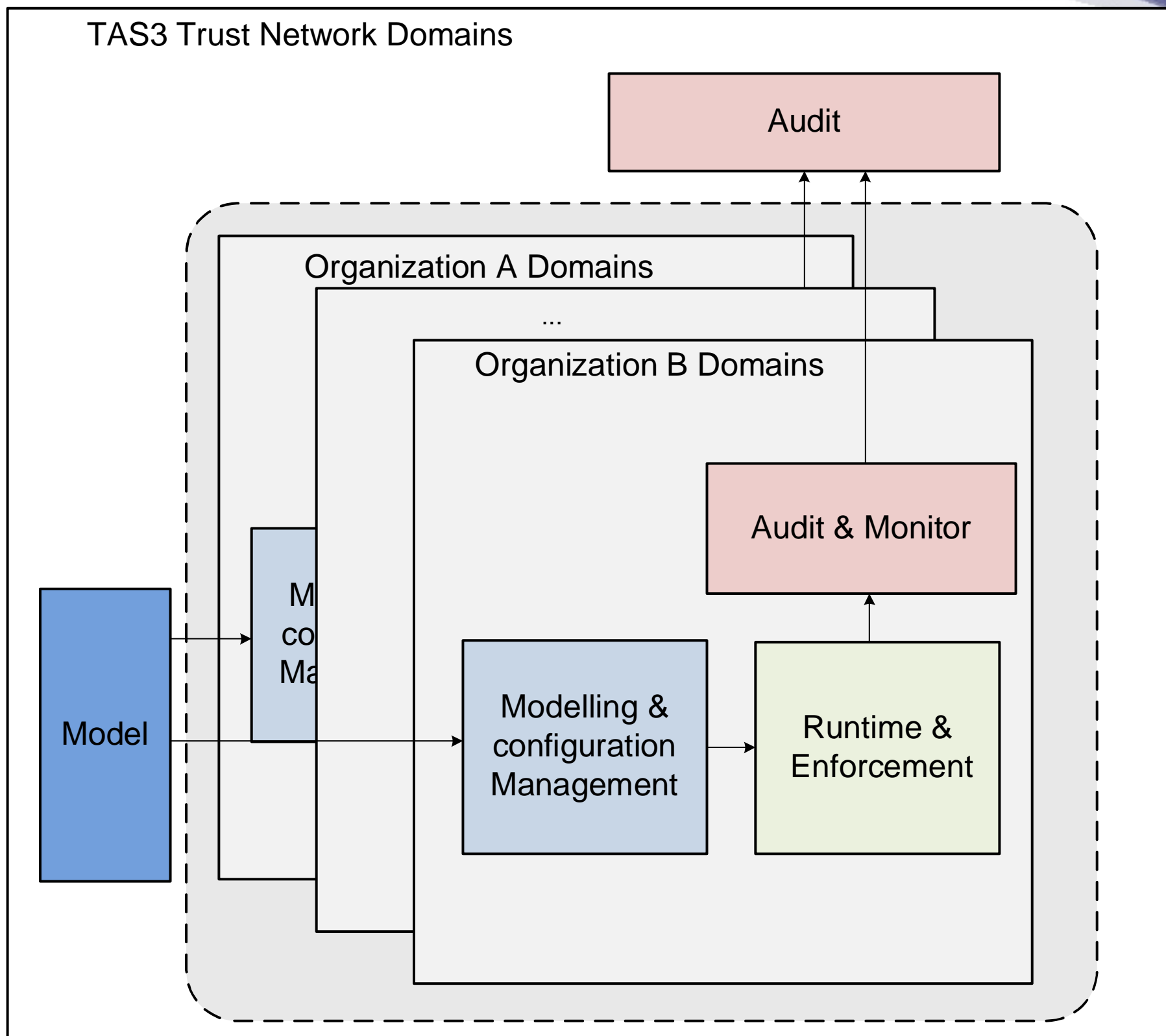# Trusted Architecture for
Secure Shared Services (with Privacy) and
Personal Data Store

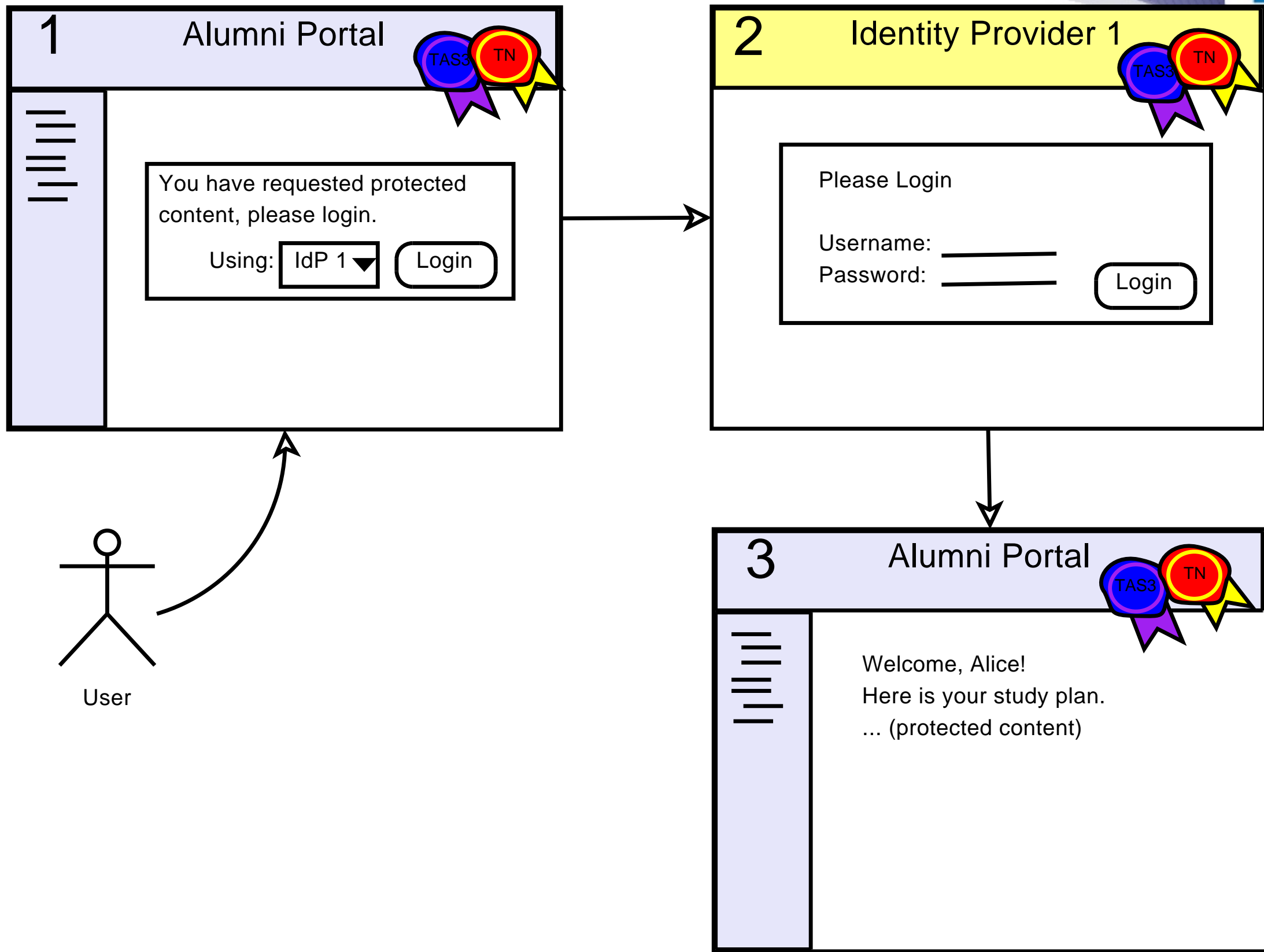Sampo Kellomäki (sampo@zxidp.org)

13. May 2011, EIC 2011, Munich

11

TAS^3 and Open Identity Trust Framework (1/2)

- TAS^3 specifies architecture both at Trust Framework and Technical Protocol Level
  - Ticks all columns of Rainer Hörbe's Trust Framework Capabilities: Identity, AuthN, Session, AuthZ, Accountablity, Privacy, User Control
- TAS^3 promotes the concept of "Trust Framework", but does not get to the level of definition that Open Identity Trust Framework does
- TAS^3 "Trust Network" covers many aspects of
  - Policy Setters
  - Trust Framework Provider
  - Trust Federation

TAS^3 and Open Identity Trust Framework (2/2)

- We foresee "Trust Convener" or Trust Network organizer that
  - Sets concrete policies, in broader context of policy setters (e.g. national law)
  - Has governance structure, usually with participation of members
  - Runs or outsources the "Trust Framework Provider" function
  - Runs or outsources the assessment and auditor functions
  - Is or specifies Trust Anchor
  - May run in some cases some core services such as IdP, Discovery, Audit, some aspects of Authorization, etc.

TAS^3 Intro and Vision

- EU FP7 research project runs until end of 2011
- Architecture
  - Identity Management, Authorization, and Audit plumbing
  - Holistic combination of existing technologies
- Std based profiles (SAML2, Liberty ID-WSF2, UMA, XACML2, ...)
- Reference implementation in open source (C/C++, PHP, Java, .Net)
  - `zxid.org` (Apache2 non-viral open source license)
- Vision of empowering users and building trust networks
  - Pair-wise pseudonymous: **uncorrelatable w/o user consent**
  - Internet of Subjects Foundation: **not-for-profit governance**
  - Competitive Svcs Market Place: **discover services you trust**
  - Delegation: **jobseeker to coach, represent organization**
  - Trust scoring and trust building: **make informed choices**
  - Privacy Preserving: **user in control, no unexpected correlation**

TAS³ Architecture Mini 2010

User is King

= Access Controll and Authorization

"Front Channel" SSO

Identity Provider (Authentication)

Web Site 1

Web Site 2

Self-audit Dashboard

"Backchannel"

O C T

Personal Service Discovery

Web Service 3

Web Service 4

Trust, Scoring, and Reputation

Web Service 5

Audit (comprehensive and ecosystemwide)

Governance & Interoperable Technology

TAS3 Architecture 2010
Component Overview v2.3

Web Browser or Fat Client
Client side app (e.g. AJAX)

Organization Domain

Modelling & Config. Mgmt
- Trust Network Mgmt Processes
- Config. Data
- Biz. Proc. Models
- Policies
- Modelling Tools
- Org. Level Ontology

Runtime & Enforcement

Payload Applications
- Front End (e.g. Web GUI)
- Business Process Engine
- Web Services

TAS3 User Tools
- User Audit Dashboard
- Policy Editor & Consent Management
- Delegation Settings

Core TAS3 Infrastructure
- Identity Provider
- Identity Aggregator
- Trust & Reputation

Core TAS3 Infrastructure Backchannel
- Authorization
- Delegation Service
- ID Mapper
- Ontology Handler
- Credentials & Policies Negotiator
- Discovery Registry

Event Bus
- Audit Events
- Management Events

Audit & Monitor
- (Audit Analysis)
- Online Compliance Testing
- (Operation Monitoring)

TAS^3 Intro and Vision

- EU FP7 research project runs until end of 2011
- Architecture
  - Identity Management, Authorization, and Audit plumbing
  - Holistic combination of existing technologies
- Std based profiles (SAML2, Liberty ID-WSF2, UMA, XACML2, ...)
- Reference implementation in open source (C/C++, PHP, Java, .Net)
  - `zxid.org` (Apache2 non-viral open source license)
- Vision of empowering users and building trust networks
  - Pair-wise pseudonymous: **uncorrelatable w/o user consent**
  - Internet of Subjects Foundation: **not-for-profit governance**
  - Competitive Svcs Market Place: **discover services you trust**
  - Delegation: **jobseeker to coach, represent organization**
  - Trust scoring and trust building: **make informed choices**
  - Privacy Preserving: **user in control, no unexpected correlation**

Empowering user to take control of his data
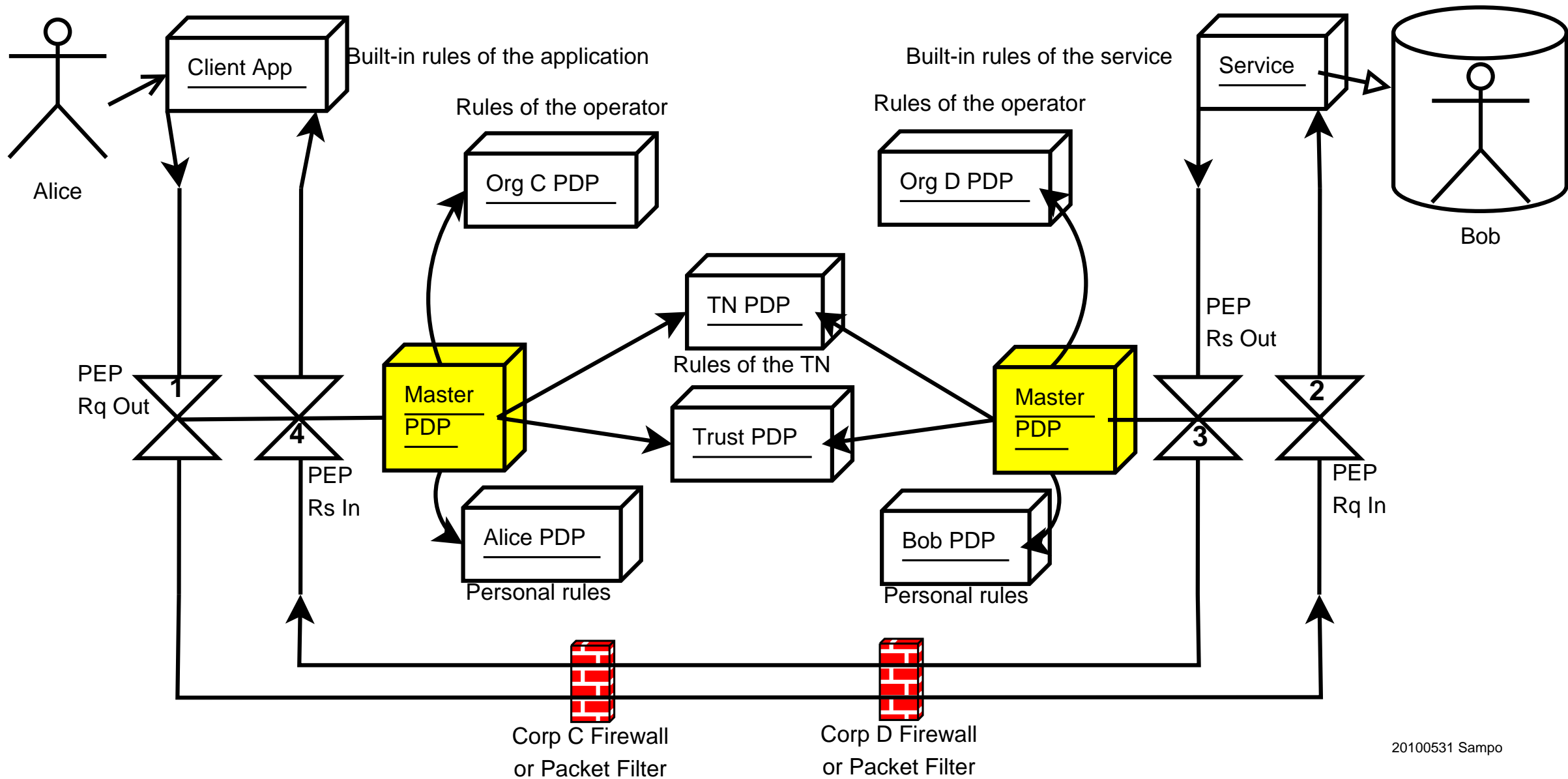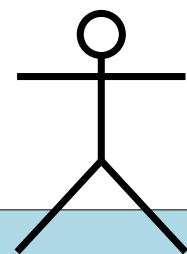
- Fully pair-wise pseudonymous design
  - Prevent correlation and collusion at all layers of deep SOA
- Model where user gives his data from his Personal Data Store
  - User well positioned to impose policies when releasing data
  - Only store data once, and in place that user chooses
- Personas, partial identities
- Privacy protection through noncorrelatability, access control, and sticky policies
- User self audit dashboard gives user visibility to use of his data
  - Independent means, to keep the service providers in check
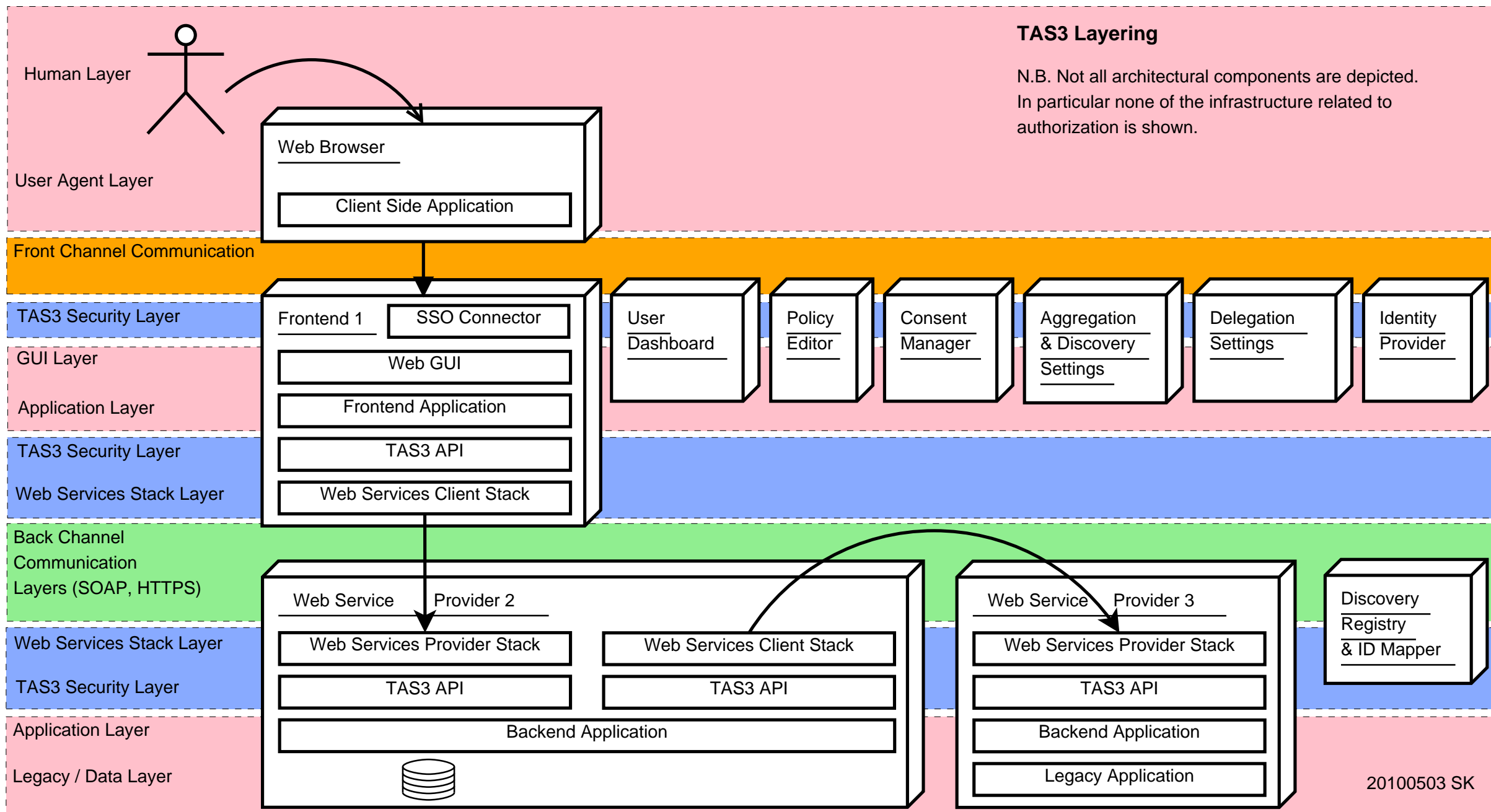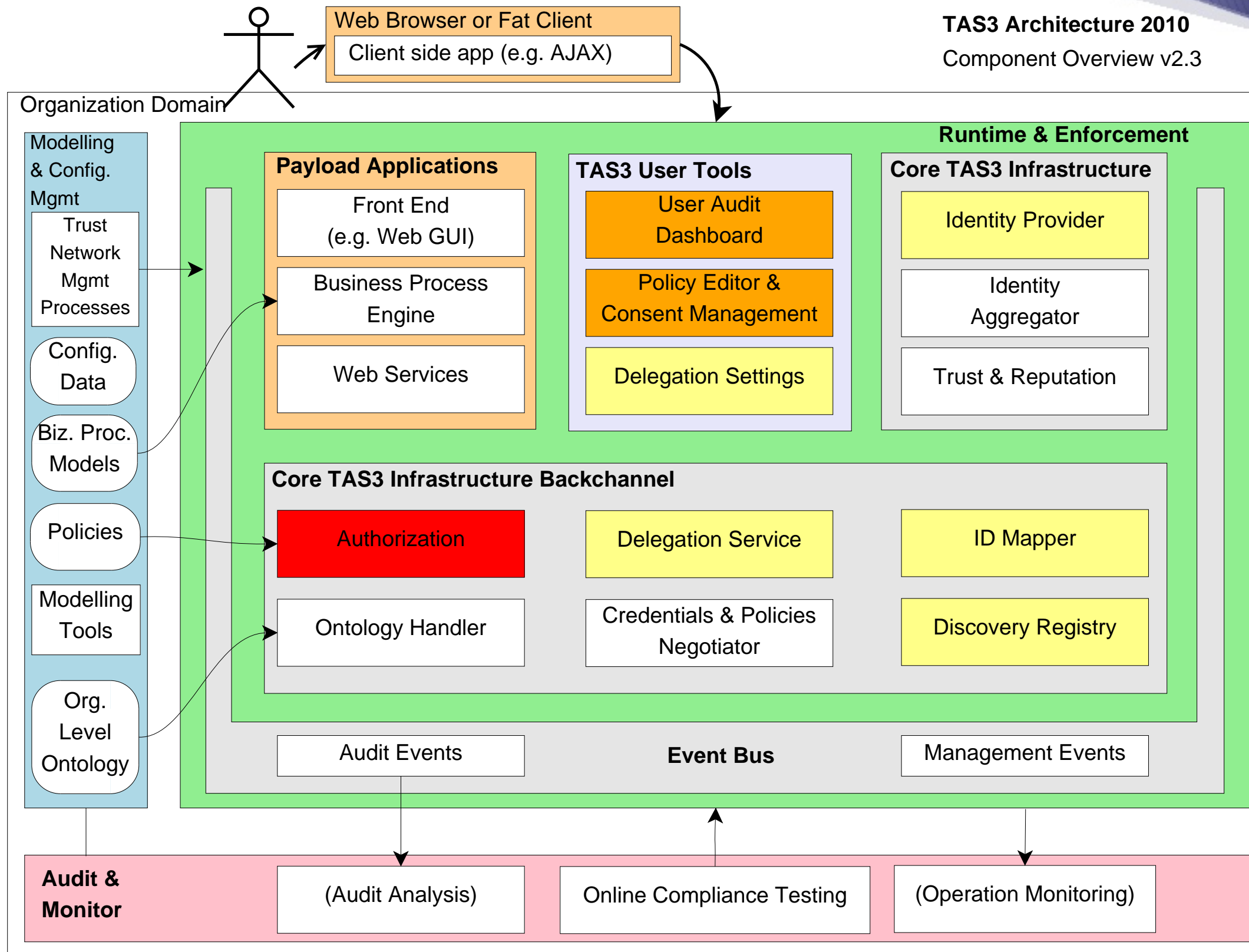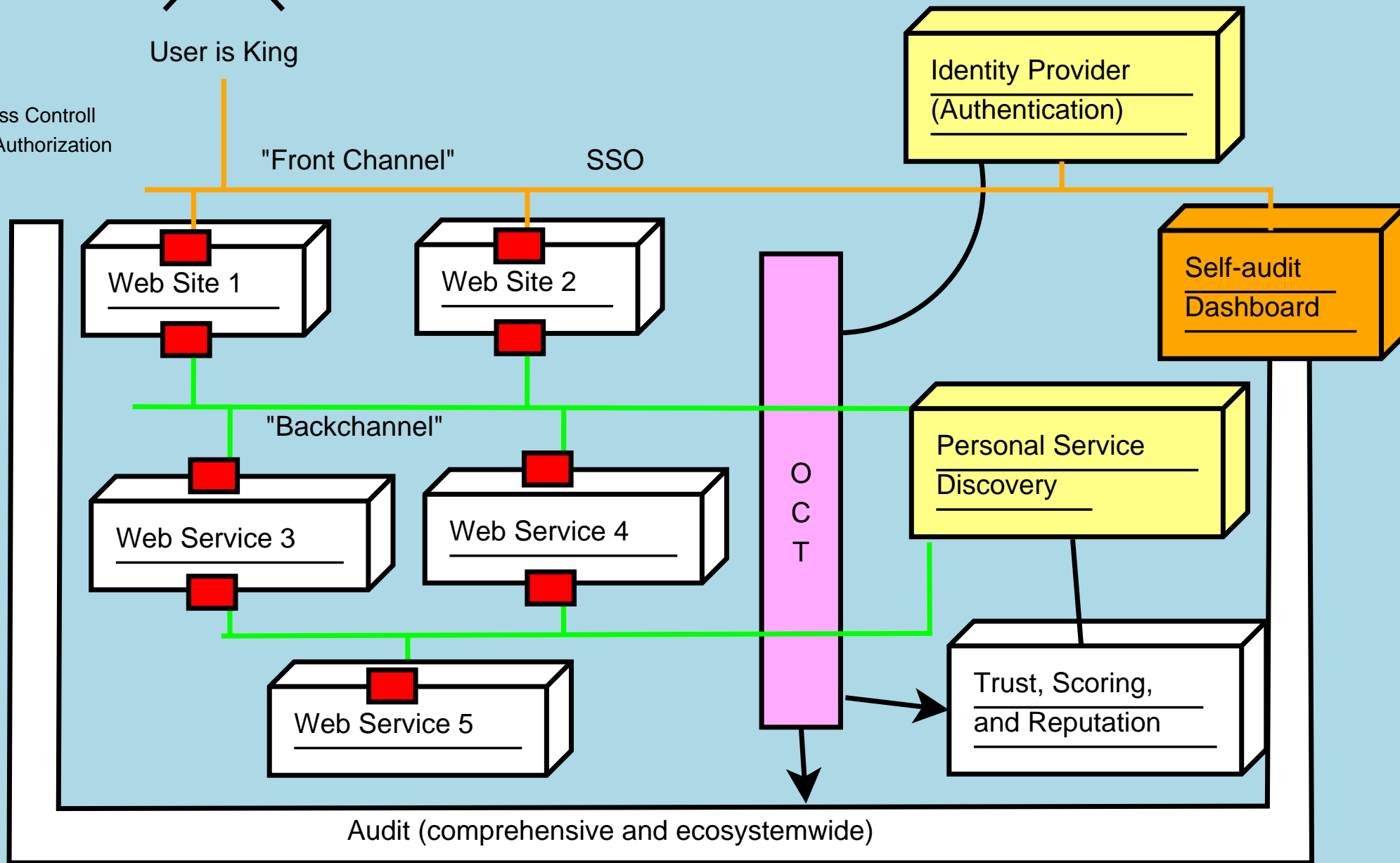- Digitally signed audit trail to ensure legal enforeability

TAS³ Architecture Mini 2010

TAS3 Layering

N.B. Not all architectural components are depicted. In particular none of the infrastructure related to authorization is shown.

Human Layer

User Agent Layer

Web Browser

Client Side Application

Front Channel Communication

TAS3 Security Layer

Frontend 1   SSO Connector

User Dashboard

Policy Editor

Consent Manager

Aggregation & Discovery Settings

Delegation Settings

Identity Provider

GUI Layer

Web GUI

Application Layer

Frontend Application

TAS3 Security Layer

TAS3 API

Web Services Stack Layer

Web Services Client Stack

Back Channel Communication Layers (SOAP, HTTPS)

Web Service   Provider 2

Web Service   Provider 3

Discovery Registry & ID Mapper

Web Services Stack Layer

Web Services Provider Stack

Web Services Client Stack

Web Services Provider Stack

TAS3 Security Layer

TAS3 API

TAS3 API

TAS3 API

Application Layer

Backend Application

Backend Application

Legacy / Data Layer

Legacy Application

20100503 SK

TAS3 Architecture 2010

Component Overview v2.3

Web Browser or Fat Client
Client side app (e.g. AJAX)

Organization Domain

Runtime & Enforcement

Modelling & Config. Mgmt

Trust Network Mgmt Processes

Config. Data

Biz. Proc. Models

Policies

Modelling Tools

Org. Level Ontology

Payload Applications
- Front End (e.g. Web GUI)
- Business Process Engine
- Web Services

TAS3 User Tools
- User Audit Dashboard
- Policy Editor & Consent Management
- Delegation Settings

Core TAS3 Infrastructure
- Identity Provider
- Identity Aggregator
- Trust & Reputation

Core TAS3 Infrastructure Backchannel
- Authorization
- Delegation Service
- ID Mapper
- Ontology Handler
- Credentials & Policies Negotiator
- Discovery Registry

Event Bus
- Audit Events
- Management Events

Audit & Monitor
- (Audit Analysis)
- Online Compliance Testing
- (Operation Monitoring)

XACML SAML profile with TAS3 Trust extensions

TAS3 Integration w/ZXID
20091016 SK

Liberty Federation Framework ID-FF SAML 2.0	Liberty Identity Service Interface Specifications (ID-SIS)
Enables identity federation and management through features such as identity/account linkage Simplified Sign-On, and simple session management.	Enables interoperable identity services such as personal identity profile, contact book, presence, and so on
	Liberty Web Services Framework (ID-WSF)
	Provides the framework for building interoperable identity services, permissions based attribute sharing, identity service description and discovery, and the associated security profiles.

Liberty specifications build on existing standards (SAML, SOAP, WS-Addressing, WS-Security, XML, etc.)

Figure 1: Liberty Alliance Architecture (for comparison of similarity).

TAS^3 Feature List

- Fully encrypted and digitally signed
- Per relationship authentication and identification (Pair-wise pseudonymous Id) plumbing for maximum non-correlation protection while identifying user to the SP and upon legal demand (can support correlation if requirement for it exists)
- Partial identities and personas
- Matching of pledges to acceptable policies
- Fully digitally signed audit trail with network level independent party as summary custodian.
- Transparency and end user visibility to the business processes and audit trail
- Per user discovery to support competitive services market place

TAS^3 Demo Highlights

1. SSO with pairwise pseudonyms

2. Web Service call with recursion, discovery, and pairwise pseudonyms

3. Invitation and Delegation

4. Visualization and user control of attribute release
   - Persona support

5. SP attribute requirement declaration

6. Matching pledges and obligations to acceptable policies

7. Obligations processing

8. User interaction widget
   - consent, policy editing
   - right of access

9. Discovery dialog

10. Regular authorization

11. Dashboard and audit bus

   - Audit drilldown

      - As a web service call

      - As an iFrame

12. Right of access

13. User intake

14. SP intake

15. PDS

TAS^3 Benefits (short)

- User as an equal stakeholder enables more equal opportunity to participate in Internet based Services Economy
  - Easier to innovate economic activity (individuals, SMEs)
  - New kinds of markets, expansion, get out of zero-sum-game
  - Ubiquotus use: becomes part of way of life and the way to do things, eliminating haphazard and confusing point-solution systems
- Solid layer
  - Avoid fraud, avoid data handling accidents, increase trust
    - **Increase usage and business**
  - EU Regulatory Compliance **on by default**
  - Non-repudiation, accountable: Tie-in to legal system, strong authentication
- Realistic and available now

- Standards based, reviewed, IPR safe, multivendor, plug and play
- Open source reference implementation available (`zxid.org`)
- Certification programs available
- Has been deployed in real world

TAS^3 Benefits (long): User

- User as an equal stakeholder enables more equal opportunity to participate in Internet based Services Economy
  - Control personal data - Even delete your data
  - Easier to innovate economic activity (self-employment, SMEs)
  - New kinds of markets, expansion, get out of zero-sum-game
- Life in high trust societies tends to be easier and more pleasant
- Easy (easier) to use technology that is adequately safe
- Ubiquitous use: becomes part of way of life and the way to do things, eliminate haphazard, confusing, point-solution systems
- Uniform user experience and data sharing practices lead to aware-ness and feeling of control (which feeling is based on real ability to control, not just impression)
- Awareness leads to responsible action, which minimizes unin-tended consequences

TAS^3 Benefits (long): Service Provider (B2C)

- Higher trust has network effect, enabling expansion
- Operate on internet scale
  - Reach new audiences and markets
  - Reach bigger audiences
  - Find and address smaller, niche, audiences and markets profitably (long tail)
  - New kinds of markets, expansion, get out of zero-sum-game
- Businesses can focus on business as the regulatory compliance is taken care of
- Practical technology that works: it interoperates and you can buy it from multiple vendors
- Lower costs from efficiencies
- Control your risks
- Save on user management (e.g. password reset)

TAS^3 Benefits (long): SP B2B and Enterprise Intranet / Extranet

- Practical technology that works: it interoperates and you can buy it from multiple vendors
- Standards based: expect partners to use the same technology
- Same technology works for intranet and extranet
  - fully flexibility to outsource internal functions or to bring external functions back in
- Good solution for post merger IT integration
- Same technology extends even to consumer market, if that is of interest
- Higher trust has network effect, internet scale: see previous slide
- Control your risks, regulatory compliance taken care of
- Save on user management and avoid duplicate identities (just use home organization ids)

TAS^3 Benefits (long): Societal (1/4)

- High trust society
  - Less waste in manual checking of credentials
  - Less opportunity for fraud, higher chances of being caught
    - Less energy wasted in trying to swindle
    - Less energy wasted in trying to prevent fraud
  - More aware, less gullible, users and citizens
- Citizen activation and empowerement
  - Life in high trust societies tends to be easier and more pleasant
  - Activated citizens are more likely to seek employment, especially officially
  - Lower barrier to self employment
  - More people earning salary and paying taxes, less people living on dole or gray economy

TAS^3 Benefits (long): Societal (2/4)

- Business stimulation
  - Focus on business: regulatory compliance taken care of
  - Lower costs from efficiencies, increase profits: more tax revenue
  - Higher trust has network effect, enabling expansion
    - more employment, more tax revenue
    - more corporate revenue
  - Create champions that operate on internet scale
- Possiblity to break up monopolies and increase competition
  - Federation model is ideal for taking big behemot internet con-glomerates and breaking them up to separate businesses
  - User experience, interoperation, and functionality can be main-tained in federation: remove barrier to break up monopoly
  - Levelled playing filed stimulates new business
  - Competition lowers prices

TAS^3 Benefits (long): Societal (3/4)

- Structurally and technically avoid adverse identity compromise scenarios
  - No need for fully centrally correlatable database from which a tyrant invader could pull out records for a religious group
  - No way to forget health records of millions in taxi, no need to transfer them that way either.
  - Make data on internet finally deletable in a controlled way
- Scalable legal system for digital age
  - Audit and evidence scales as well as any internet fraud scheme
    - System can not be inundated to avoid being caught
    - Likely hood of being caught prevents fraud up-front
  - Less crime means less cases and less workload
  - The workload that happes can be more efficiently processed as the evidence is already in standardized digital format.

TAS^3 Benefits (long): Societal (4/4)

- Lean government
  - Less need for menial paper pushing
  - Pass-on the savings and increased tax revenue to society
    - Pay down debt, Lower taxes
  - Politically controversial corollary: some jobs lost in govt
- Focus energies away from bureaucratic burdens (as these can be better automated)
  - Spend the released energies on *life*
  - Released time and good feeling leads to
    - quality time which stimulates internal market for high value goods and services
    - more resources for production and better productivity
    - more time and capacity to innovate to satisfy the created market opportunities

TAS^3 IPR Clean (1/3)

Per decisions of TAS3 General Assembly of 2010-09-13 (`TAS3_General_Assembly_minutes_2010_09_13_Leuven_V03.doc`), following declaration was made:

> "TAS3 architecture and specifications, as described in public deliverables D2.1, D2.4, and D7.1, are licensed free for implementation and use by anyone. Up to June 2010, TAS3 consortium partners do not hold patents nor will exercise patents that cover implementation and use of the TAS3 architecture and specifications of those deliverables. This license is only granted for the specific purpose of correct implementations of TAS3 specifications."

TAS^3 IPR Clean (2/3)

The OASIS and Liberty standards that TAS3 is based on have explicit IPR policies, administered by the respective standards organizations, that require Royalty Free licensing by those who participated in standards committees. This includes most major IT corporations.

Remember: open source is not sufficient for openness: royalty free IPR licensing is a requirement.

TAS^3 IPR Clean (3/3)

For further openness, it should be noted that ZXID, which is distributed under Apache2 open source license, is the Reference Implementation of the TAS3 Core Security Architecture, i.e. from software licensing perspective TAS3 is available in open source. Many other components of TAS3 are available in open source as well.

TAS^3 and FI-PPP (1/2)

TAS^3 Architecture (especially the core security architecture part) should be the privacy preserving Identity, Authorization, and Audit plumbing of the FI-PPP.

- Mature enough
  - based on well accepted and reviewed SAML2, Liberty ID-WSF (SOAP + WS-Security), and XACML technologies
  - unambiguous enough profiles and bindings to actually interoperate on wire
  - real life interoperation and certification programs available
  - multiple technology vendors, including open source, available
- Solid enough for high value work such as enterprise and eGovt
  - stood test of time, has not needed constant revising of specification (SAML2 stable since 2005, ID-WSF2 since 2006)

TAS^3 and FI-PPP (2/2)

- Has profile for Web 2.0 market: UMA, OAUTH, RESTful services
- Has profile for SAML2 with OpenID like trust model, so that OpenID can be avoided (due to uncertain security, spec stability, and IPR issues)
- IPR clean
- Holistic, addressing all important areas
- Acts as matrix to which new innovation plugs in

TAS^3 and IMS (Internet Multimedia System)

- IMS is an over arching vision and set of goals that needs to be populated with actual interoperable protocols
- Many TAS^3 components have seen good adoption in IMS context
  - SAML has been adopted
  - OMA adopted Liberty ID-WSF as identity web service recommendation
- Some IMS related research projects, such as SWIFT, used same technologies as TAS3 (e.g. SAML)

TAS^3 and PRIMELife, Master, SWIFT, Stork, ...

- TAS^3 is the concrete plumbing that the other projects need
- Partial identities and persona concepts are similar and mutually reusable
- TAS^3 acts as a matrix to which new innovation plugs in
  - PRIMELife partial identity and signing work
  - SWIFT partial identities
  - SWIFT audit concepts fit well with TAS^3 Dashboard and audit bus
  - Master compliance cockpit complemente well TAS^3 dashboard and may be able to share audit bus with TAS^3
  - Stork / eID can provide strong authentication with privacy preservation via Identity Providers
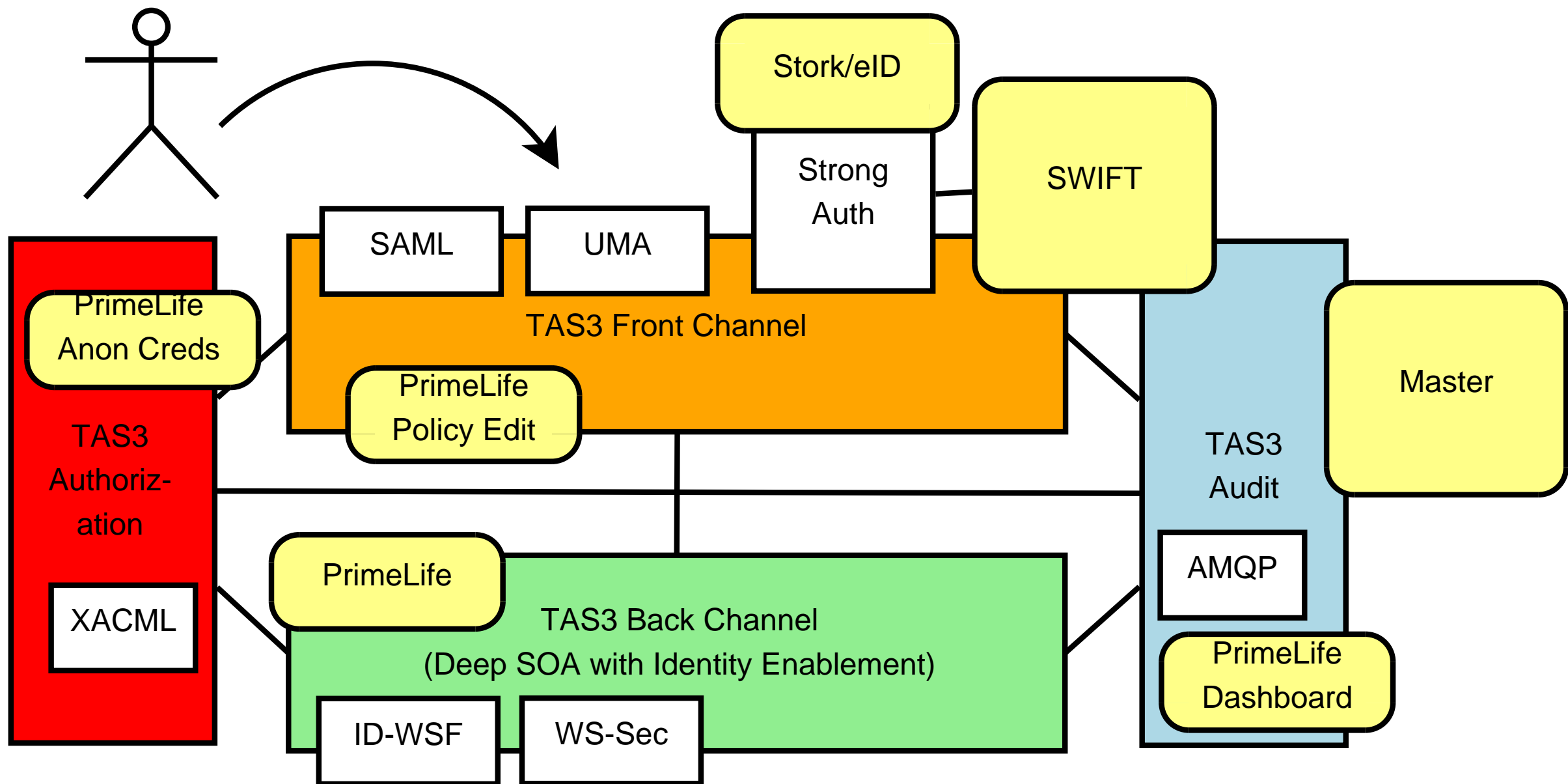
TAS^3 Architectural Assets

1. Validated flows and "plumbing" to make it feasible and achive per SP user authentication and identification while avoiding cor-relatability except upon legal request.

2. Automatic Compliance with EU Regulation wrt Right of Access, Rectification, and Deletion.

3. User control of policies relating to his data and the plumbing to pass these policies to ensure end2end trust.

TAS^3 Interoperability Profile Assets

1. Interoperable, multivendor, Single Sign-On (SAML2). Ability to use COTS (Common Off The Shelf) software.

TAS^3 Reference Implementation (`ZXID.org`) Assets

1. IdP and Discovery Service (SAML 2.0 and ID-WSF 2.0)

2. Frontend SP: mod_auth_saml for Apache httpd

3. SP: sso servlet for Java / Tomcat (frontend, WSC, WSP)

4. SP: PHP integration (frontend, WSC, WSP)

5. SP: Net::SAML perl integration (frontend, WSC, WSP)

6. SDK

Promotors of PDS

TAS^3 - Trusted Architecture for Securely Shareable Services
   Core Security Architecture

IoS - Internet of Subjects Trust Convener and Ecosystem Builder

ZXID Reference implementation of the TAS^3 Core Security Arch.

Core Standards

- OASIS SAML 2.0
- Liberty Alliance ID-WSF 2.0 & Data Services Template (DST) 2.1
- OASIS XACML 2.0 Access Control
- IoS and TAS^3: Personal Data Store (PDS) Specification
- Sector specific data schemas
- Personal Information metadata standardization still TBD

IoS 7 Rules

1. Personal Control

2. Searchability

3. Instant Social Networking

4. Ubiquity

5. Symmetry

6. Minimization

7. Accountability

Big 4 of Privacy Protection (Seda *et al.*)

1. Awareness: Self audit (dashboard), Identity mirrors

2. Confidentiality
   - Anonymity
   - Data minimality
   - Consent to release
   - Reputation based screening, Trust and Privacy Negotiation
   - Cryptographic protection
   - Avoidance of correlation handles (prevent illicit collusion)

3. Control
   - Intended purpose & Audience restrictions
   - Sticky policies
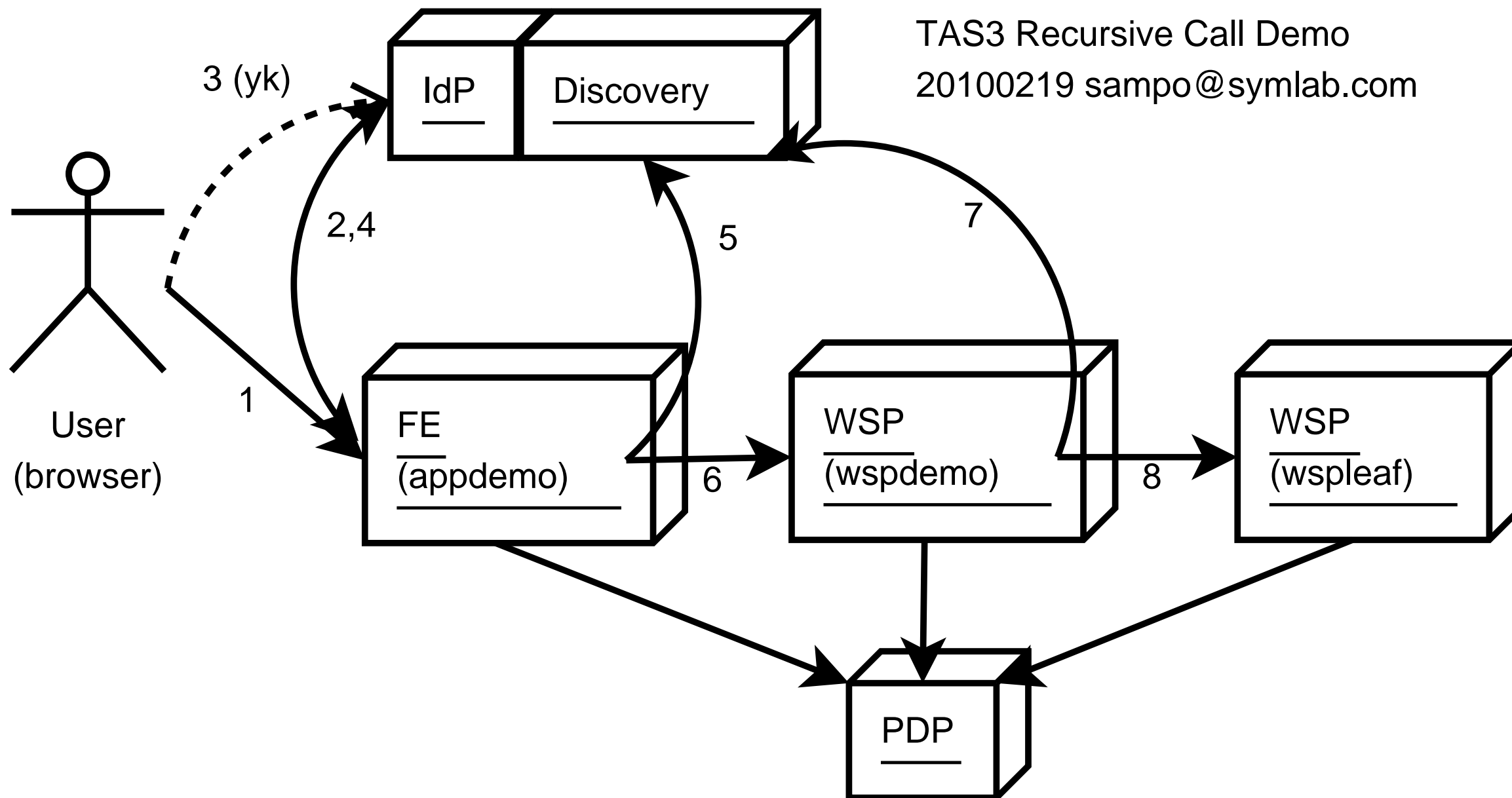   - Policy enforcement & Audit

4. Practise
   - Right to correct and delete, Right of response

- Transparency of practises and intents
- Trust and reputation feedback
- Send strong positive signal of your own

IoS Concepts

- IoS
  - IoS compliant Business Services
  - IoS Infrastructure
    - Dashboards
    - Shared WS: AIM, calendar, directories, harvesting, publication, ...
    - Personal data service(s) + dashboard (one or per service?)
  - Symmetry in providing services
    - Every user can become a Service Provider
- Personal - Communal - Public
- Separation of data from services
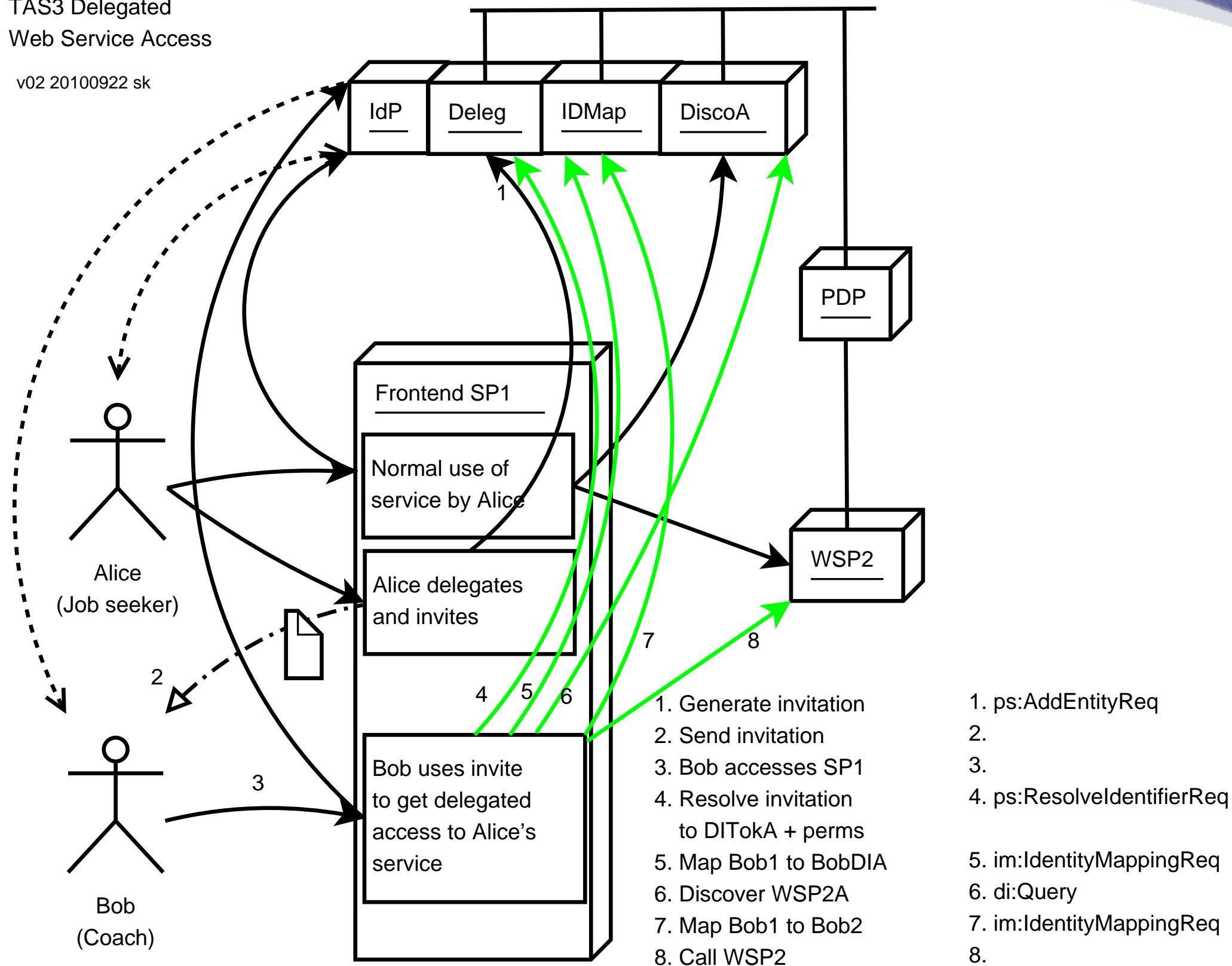- Mostly pull and as-needed communication (minimization)

TAS3 Recursive Call Demo
20100219 sampo@symlab.com

TAS3 Delegated
Web Service Access

v02 20100922 sk

IdP | Deleg | IDMap | DiscoA

PDP

Frontend SP1

Normal use of
service by Alice

Alice delegates
and invites

Alice
(Job seeker)

WSP2

2

4   5   6   7   8

Bob uses invite
to get delegated
access to Alice's
service

3

Bob
(Coach)

1. Generate invitation   1. ps:AddEntityReq
2. Send invitation   2.
3. Bob accesses SP1   3.
4. Resolve invitation   4. ps:ResolveIdentifierReq
   to DITokA + perms
5. Map Bob1 to BobDIA   5. im:IdentityMappingReq
6. Discover WSP2A   6. di:Query
7. Map Bob1 to Bob2   7. im:IdentityMappingReq
8. Call WSP2   8.

Delegation

1. Generate invitation
   - Assign invitation ID for management of invitation
   - Set up permissions for what resources invitee can access
     - The permissions can be keyed on invitee's identity, or
     - they can be keyed on the invitation ID

2. Send by out-of-band means, such as email or IM. The invitation will be formatted as a URL.

3. When Bob (being the invitee) clicks on the URL, he lands on Frontend site (alternatively Bob could land on WebGUI aspect of the Delegation server site)
   - The site forces Bob to SSO (if this did not happen, invitation would be a bearer token)

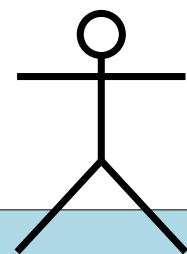4. The invitation is resolved to Discovery Token of Alice (the inviter)

- The token contains as an attribute the invitation ID (the token is encrypted so that only the discovery service of Alice can open it, therefore the invitationID itself does not become a correlation handle).
- Basically the discovery token of Alice would allow Bob to discover any service of Alice. As this is not desired, it is constrained by the permissions set at step 1.
- Problem: how does SP1 accessed by Bob know where Alice's Delegation Service is located? This would be obvious if the URL points to the Delegation service of Alice.

5. For Bob to be able to call Alice's discovery service (next step), Bob needs to present his own identity token to DiscoA. This is obtained by calling Bob's ID Mapping service.

6. Bob discovers Alice's WSP2. This is permitted by permissions.

7. For Bob to be able to call Alice's WSP2 (next step), Bob needs

to present his own identity token at WSP2A. This is obtained by calling Bob's ID Mapping service.

8. Call to WSP2A is made with Alice's token from step 6 as TargetIdentity SOAP header and Bob's token from step 7 as wsse:Security/Token.
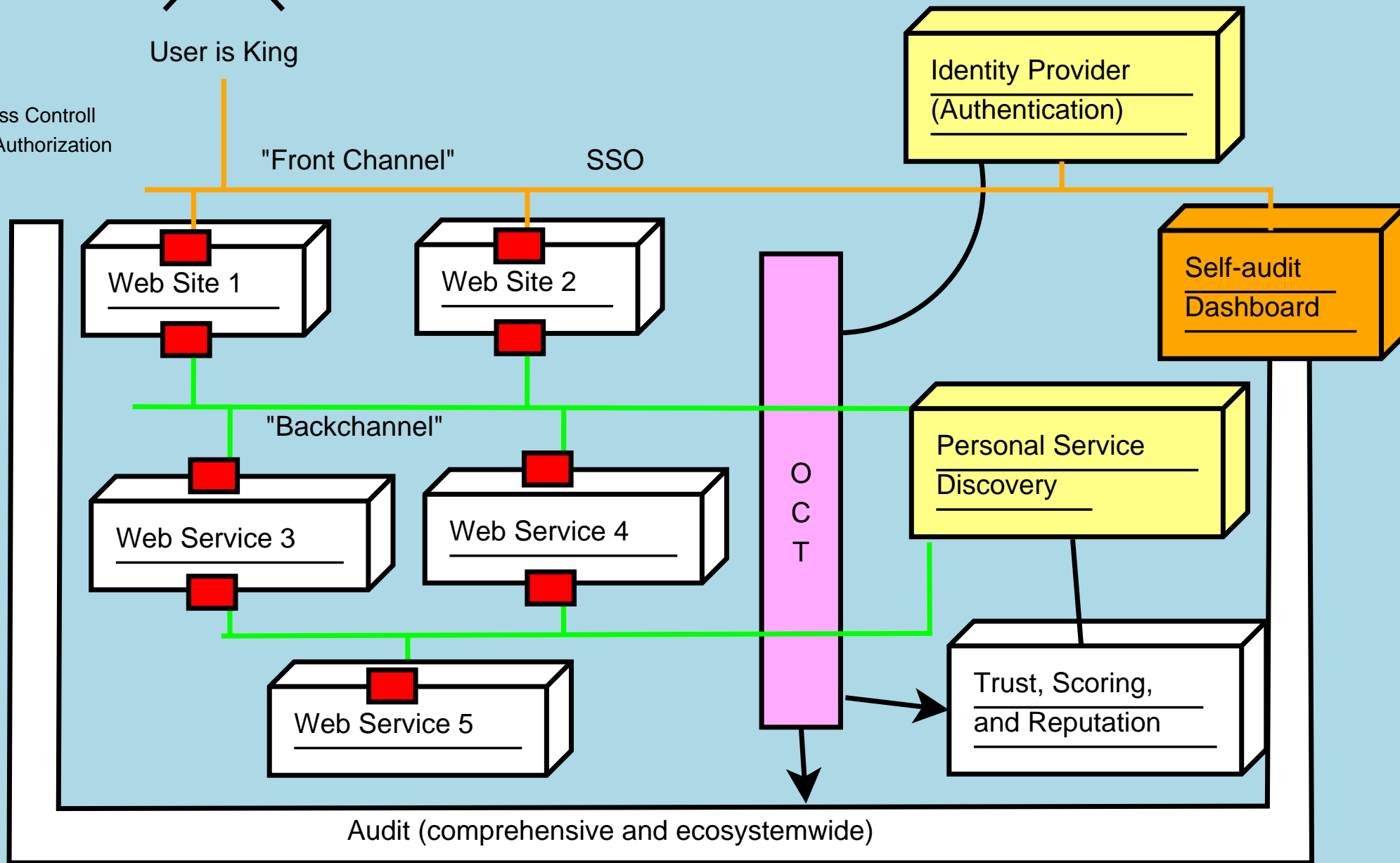
Ideally WSP2 would also have permissions indicating that the delegation from Alice to Bob is valid. This could be arranged by WSP2 making a call to Delegation service to confirm the delegation. Unfortunately such confirmation API is not specified by Liberty. We could invent an API. Another approach would be to at step 1 to provision the policies to PDP of WSP2.

TAS³ Architecture Mini 2010

User is King

= Access Controll and Authorization

"Front Channel"   SSO

Identity Provider (Authentication)

Web Site 1   Web Site 2

Self-audit Dashboard

"Backchannel"

Web Service 3   Web Service 4

O C T

Personal Service Discovery

Web Service 5

Trust, Scoring, and Reputation

Audit (comprehensive and ecosystemwide)

Governance & Interoperable Technology

TAS3 Architecture 2010
Component Overview v2.3

Web Browser or Fat Client
Client side app (e.g. AJAX)

Organization Domain

Runtime & Enforcement

Modelling & Config. Mgmt
- Trust Network Mgmt Processes
- Config. Data
- Biz. Proc. Models
- Policies
- Modelling Tools
- Org. Level Ontology

Payload Applications
- Front End (e.g. Web GUI)
- Business Process Engine
- Web Services

TAS3 User Tools
- User Audit Dashboard
- Policy Editor & Consent Management
- Delegation Settings

Core TAS3 Infrastructure
- Identity Provider
- Identity Aggregator
- Trust & Reputation

Core TAS3 Infrastructure Backchannel
- Authorization
- Delegation Service
- ID Mapper
- Ontology Handler
- Credentials & Policies Negotiator
- Discovery Registry

Event Bus
- Audit Events
- Management Events

Audit & Monitor
- (Audit Analysis)
- Online Compliance Testing
- (Operation Monitoring)

XACML SAML profile with TAS3 Trust extensions

TAS3 Integration w/ZXID
20091016 SK

Service

Service

Service

PDS

User

User's data is stored only once, in his PDS. User controls what Services see.

	Metadata	Pointers	Actual data (original format)
Data by me	Descriptions and annotations controlled by me.	Pointers to docs by me in other services, e.g. photos	Works of authoriship stored in PDS
Data about me	Descriptions and annotations controlled by me.	Pointers to docs about me in other services	Cached copies of docs about me and bearer certificates.

Index

Results

Launch a search

Instant
Social
Network
Custodian

User X

User A

PDS A

PDS B

PDS C

PDS X

N.B. "B" did not match search.

Each user's consent to be in result set is asked and ISN ID is passed.

v04 SK 20100908

Index

Instant
Social
Network
Custodian

Pseudonymity and
distribution through
Custodian ensures
privacy.

PDS A

PDS B

PDS C

PDS X

User X

User A

Any user
in ISN
can send
message
to all in
ISN.

v04 SK 20100908

Index

Request Peer Pseudonyms

Instant Social Network Custodian

Consent to move to peer mode is asked.

User A

PDS A

PDS B

User X

PDS X

Peer Pseudonyms are distributed
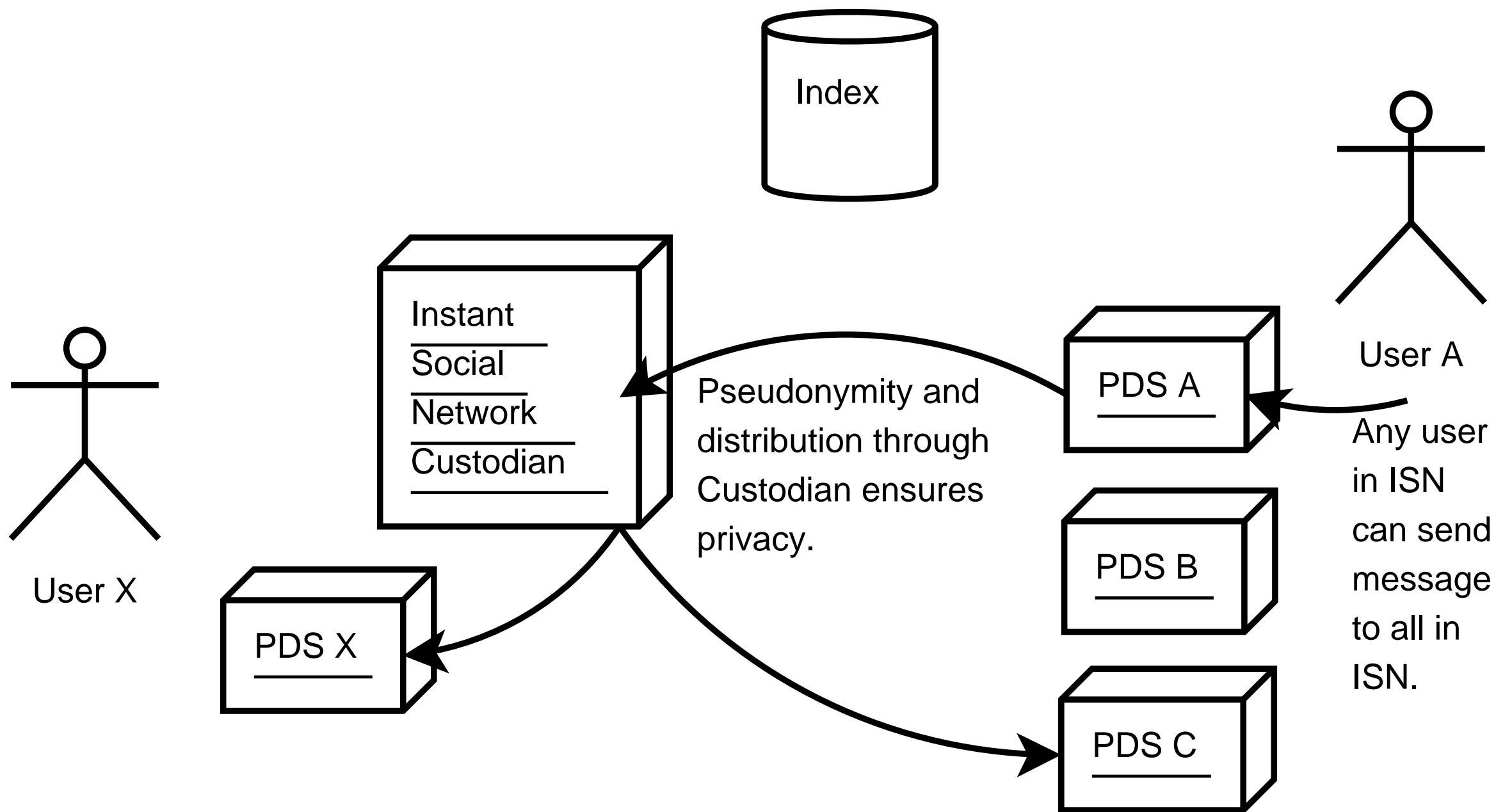
PDS C

Now peers can communicate directly without Custodian.
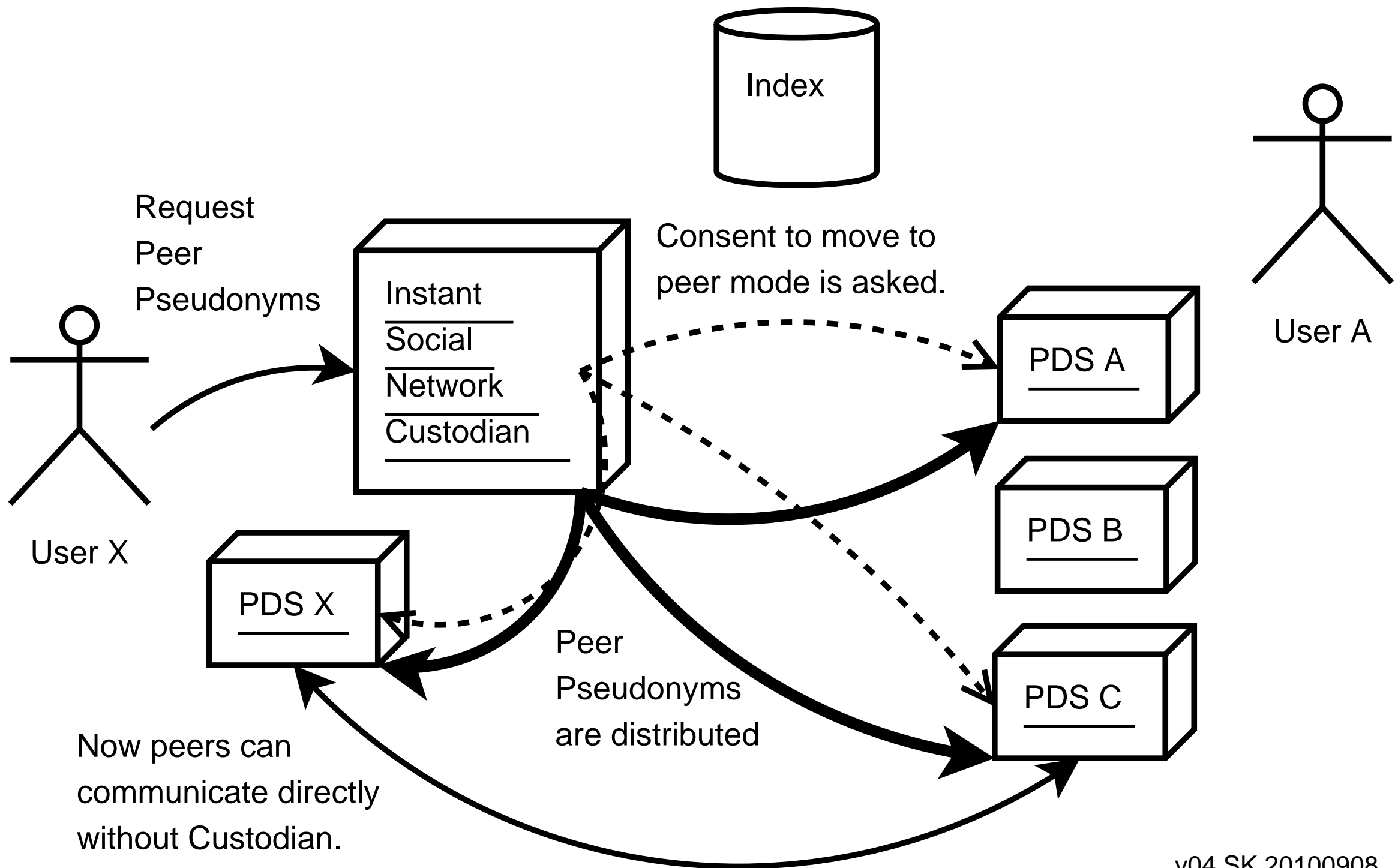
v04 SK 20100908

What is in Personal Data Store (PDS)?

- In
  - Core personal attribute data
    - cn / display name
    - language and other core preferences
    - core groups, tags, and roles
    - Age check?
    - Contact card, Shipping address / domicile
  - Personal documents at choice of user
  - Core social network (Social Data Store - SDS)
    - Contacts
    - Buddies and invitations and their permissions
    - Collaborative documents
  - Calendar data
  - Some audit records

- E-Portfolio / CV data
  - Degree certificates? Just references
- List of references to competencies
- Referees
- Personal Health Record? Copy of health records?
  - Possibility of managing personal doctor as member of your social network and keeping the records with him
- Fotos and videos
- Pointer to search, etc. Or discovery.
- Out (i.e. stored somewhere else)
  - Employee profile (maintained by employer's HR)
  - Per service preferences (maintained by each web site)
    - History or copy could be kept at PDS for backup
  - Shopping history (kept by each merchant), but copy could be kept at PDS for user's benefit

- Authorative health records
- Bookmarks
- Blogs

Services Provided by Personal Data Store (PDS)

- Attribute authority (for self asserted and long term signed creds)
- Personal Data Broker
- Agent / Privacy Manager
- Audit Dashboard
- Persona switcher
- Index, search, interaction with harvesting, connecting to queries
- Pico payment processor
- Anonymous message router
- IdP / Authentication Provider?
- Discovery?
- Personal Policy Decision Point (PDP)?
  - Kantara User Managed Access (UMA)
- Consent and Policy Editing

Approaches for Personal Data Store

- Ideal architecture permits plurality of approaches
  - Not all approaches are acceptable to consumers of identity, thus flag the nature of data source (i.e. assurance level) so that self-asserted is readily identified and can be rejected.
- User must have choice (and competitive market of providers or approaches)
  - Discovery or bootstrapping will be the key enabler
- Every user can be a service provider: peer-to-peer (C2C, C2B, B2C)
- Managed model
- Personally owned model
- Network side (cf. virtual wallet) vs. user's desktop or device
- Roaming, multiaccess, simultaneous sessions and authorities

Variants of Personally owned model

- Personally operated model: run it literally on your own computer or smart phone
- Hosted model: it is as if you owned and operated it, but you buy it as a service (e.g. OVH root servers, Google Gear)
- Browser plug-ins or CardSpace
- Personal fat clients

Managed Model: Pros & Cons

- Pro
  - Easier for technically uninterested
  - Well managed, more secure
  - Convincing authentication and authority
  - Nannying: ability to prevent users from doing stupid things or at least advice them
  - Systematic disaster recovery
  - Cheaper per unit
  - Business model: pay for utility, clear promoter
  - Easier to arrange alternate revenue from searches and aggrega- tions of data
  - User-not-present easy to support

- Contra
  - Loss of control and lack of influence / bargaining power against too big providers
  - Fat target and high impact of failure
  - Capital intensive
  - Offline use cases difficult to support

Personally Owned Model: Pros & Cons

- Pro
  - More tangible ownership and control of data
  - Offline use cases (except for rented/hosted cases)
- Contra
  - More difficult for technically uninterested (but rental/hosted approach can ease this)
  - Unconvincing authentication and authority
  - If you break it, you get to keep both pieces. Nobody to help.
  - No systematic disaster recovery
  - User-not-present difficult to support

User Centricity & Front Channel - Back Channel

- User centricity: user control. *Not about shifting bits through UA.*
- Front ch. doesn't really provide better guarantee than back ch.
  - User centricity requiring all traffic to pass through a browser is a *flawed* notion and does not address deep web services reality
  - May be easier to arrange for user interaction from back channel
- Back channel is often a *really* required and undisputed part of architecture: not supporting it, will only serve to exclude PDS from those architectures.
  - User interaction from back channel: difficult, not impossible
    - Interaction Service can be used to contact the user from deep in the call chain.
    - (TAS^3) business process aware Dashboard can be used to solicit user interaction and unblock a process that was stuck waiting for user input.

Available Standards and Stacks

- TAS^3 (SAML2 + ID-WSF) (deploy per user, if desired)
  - Fully pair-wise pseudonymous privacy protection
- FOAF style
  - Built-in assumption of globally unique ID and correlation handle
- Liberty Advanced Client aims at providing truly pseudonymous IdP and services from personally owned devices
  - Also supports disconnected model
- Higgins work?
- Skunkworks and new developments?

How to harmonize these so that Managed and Personally Owned, all the way to on-device, models can co-exist?

- TAS^3 decentralized + Liberty Advanced Client: an elegant solution

Applications

- Education
  - Mahara (work to separate database interface from rest of application / service)
  - Moodle (work to separate database interface from rest of application / service)
- Employment
  - Some matching / job seeker application, TBD
- Social networking
  - Wizi: ability to leverage core social network and profile
    - Nice iPhone app, good demo. But requires convincing CEO of a very busy company
  - Some sort of "contact kiss" application, TBD
- Other, Ideas?

Reality Check

- PDS and IoS infrastructure is a tall order, we can not have all of it on day one
- Initial core set of data?
- Initial core set features?
- Initial demonstration applications?

1. Moodle vs. Dokear

2. Mahara vs. Elgg

3. Universal CV

4. Wizi

5. TAS^3 and Kantara project web sites (Trac, Altassian Confluence)

6. Web Mail (pdmail)

7. Other?

PDS Data Priority List (London, Jan 2010)

1. Core contact card

2. E-Portfolio data

3. Audit records

4. Core social network

5. Core preferences, tags, and roles

6. Distribution of long term signed credentials from authorative sources, age check

7. Advanced social data store

8. Personal and and collaborative documents

9. Calendar data

10. Personal Health Record

PDS Feature Priority List (London, Jan 2010)

1. Discoverable, network side data store

2. IdP and Discovery support (even if not yet personally managed)

3. Audit dashboard

4. Agent / Privacy Manager / Personal Data Broker – first iteration

5. Index, search, interaction with harvesting, connecting to queries

6. Pico payment processor

7. Anonymous message router

8. Persona switcher

9. Personally owned PDS

10. Personal IdP, Discovery, service provider support

11. Better Audit dashb. / Agent / Privacy Mgr / Personal Data Broker

12. Personal Policy Decision Point

Requirements for PDS Software

We seek to convince *software developers* to implement PDS.

- Commercial (whether licensed or runs as SaaS model)
- Open source

Lets see what is included in such software...

1. Web Service

2. Web GUI

3. Supporting infrastructure such as
    - Databases
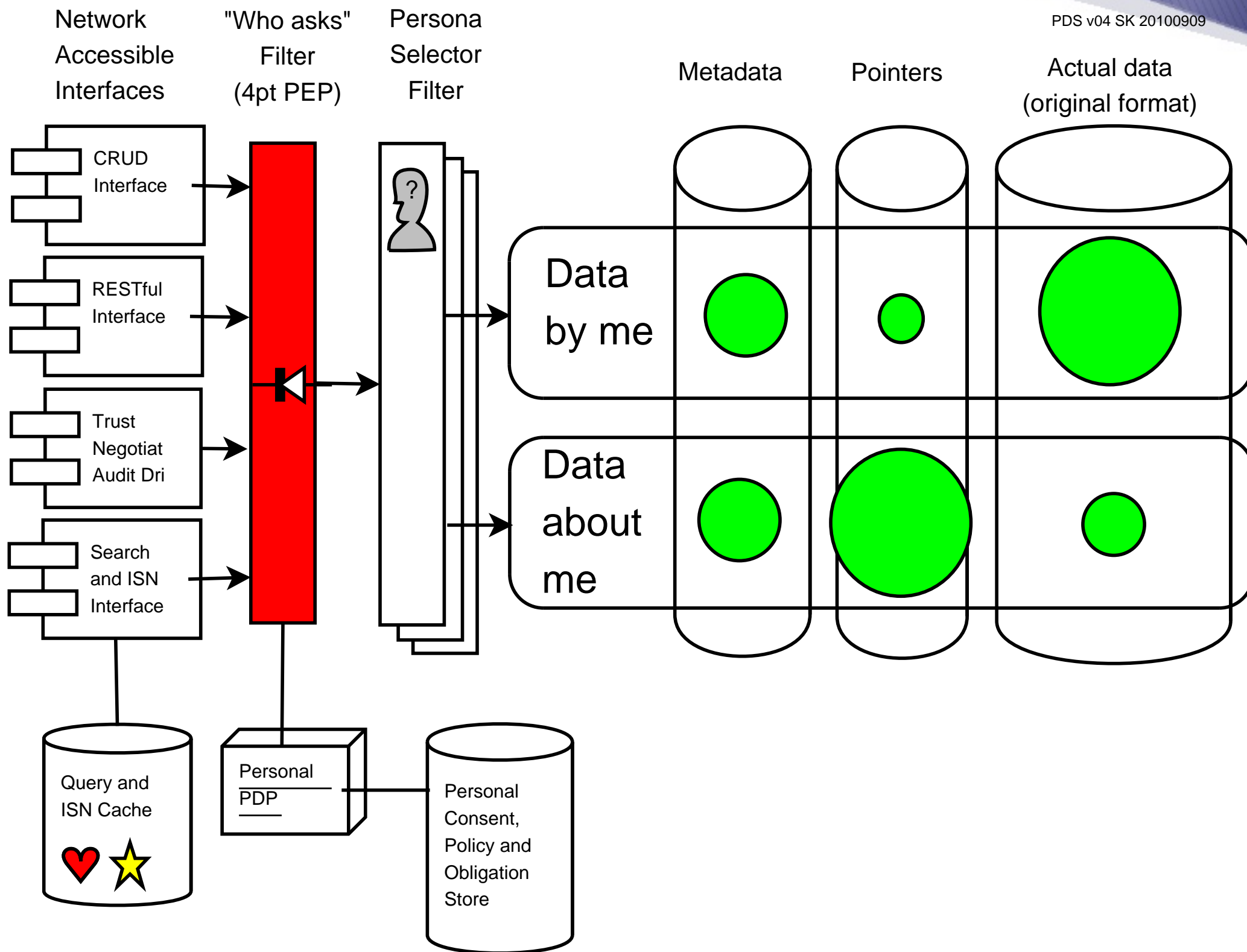   - PEPs and PDPs
    - Audit features

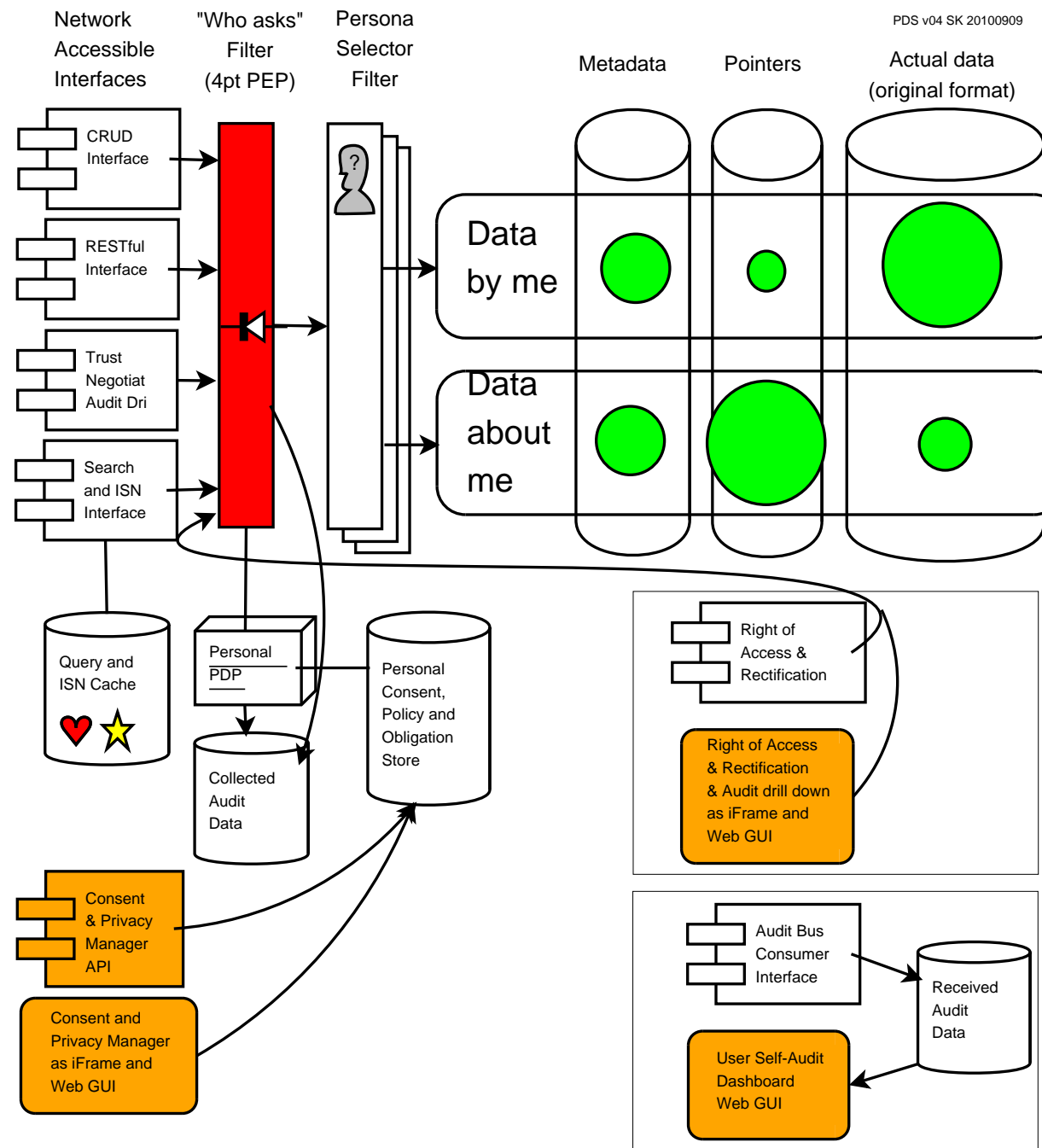   *Much of this is needed to be a* "TAS^3 Web Service"

PDS Technical Properties: Scope

1. TAS^3 web service, with full support for relevant TAS^3 features
   - Data access using Liberty Data Services Template (DST 2.1)
     - Service Type "urn:ios:pds:2010-05:dst-2.1"
     - CRUD methods, box carring, Subscriptions and Notifications
     - MTOM to preserve data in original format
   - Simple read-only data access (RESTful, SAML Attribute Query)
   - Distributed search responder (possibly part of R of CRUD)
   - Audit drill down as web service (to be specified)
     - Service Type "urn:tas3:audit:2010-06"

2. Web GUI (stand-alone, iFrame for data user, iFrame for Dashbrd)
   - At least basic privacy preferences management
   - Right-of-Access, Rectification, and Deletion
   - Audit drill down as GUI

Network Accessible Interfaces

"Who asks" Filter (4pt PEP)

Persona Selector Filter

Metadata

Pointers

Actual data (original format)

PDS v04 SK 20100909

CRUD Interface

RESTful Interface

Trust Negotiat Audit Dri

Search and ISN Interface

Data by me

Data about me

Query and ISN Cache

Personal PDP

Personal Consent, Policy and Obligation Store

Network Accessible Interfaces

"Who asks" Filter (4pt PEP)

Persona Selector Filter

Metadata

Pointers

Actual data (original format)

PDS v04 SK 20100909

CRUD Interface

RESTful Interface

Trust Negotiat Audit Dri

Search and ISN Interface

?

Data by me

Data about me

Query and ISN Cache

Personal PDP

Personal Consent, Policy and Obligation Store

Collected Audit Data

Right of Access & Rectification

Right of Access & Rectification & Audit drill down as iFrame and Web GUI

Consent & Privacy Manager API

Consent and Privacy Manager as iFrame and Web GUI

Audit Bus Consumer Interface

Received Audit Data

User Self-Audit Dashboard Web GUI

ID Map Delegation Discovery

Personal IdP SSO Attribute Mgmt

Personal Federation Database

Personal IdP, Discovery, and Delegation Managemet are optional features, applicable only to enthusiast users.

IoS PDS Special Requirement for ISN

To support *Instant Social Networking* (ISN) the PDS needs to provide:

- Special WAN indexable and anonymously (really anonymously, in some cases pseudonym may not be sufficient) searchable inter-face.

- If you are matched by a search, you gain equal rights to com-municate with the other members of the result set (anonymously and progressively revelaing details about yourself). This is *sym-metry.*

"WAN indexable" means indexable by Google and similar services.

This functionality is important for the business case of IoS, but is still in flux.

IoS Indexed, but, Distributed Search

One of the key elements of the business model of the Internet of Subjects is for the user to consent and accept to be found by searches of openended nature. The information you make available to such and other searches constitutes an important part of your "practise" of identity. We encourage legit players to strongly broadcast all their positive evidence.

PDS: TAS^3 Binding Features

- Fully discovery based
- Fully pair-wise pseudonymous
- Both Requester Token and TargetIdentity token support
  - Foundation for delegation support
- UsageDirective header with SOL1 expressions
- Integrated to audit bus (messages TBD)
- 4 point PEP with external PDP capability
- SOAP w/XML-DSIG now
  - eventual RESTful binding w/Simple Sigs

PDS Data: Labeling

- *By Me*
  - Original data, or
  - Pointers to places where there is data by me
- *About Me*
  - Pointers to places where there is data about me
  - Copies of data, with signatures intact, about me
- Version control or history feature (need guidance from IoS steering group re how sophisticated)
- **Persona** Support (perhaps as branches in version control?)
- Resource granularity *vs.* subresource granularity
  - Labeling and data schema granularity directly determines the possible access control policy granularity

PDS Data: Format

1. Metadata: RDF (XRD?) w/Turtle or N3 serialization *vs.* JSON
   - TBD soon, please provide feedback and suggestions
2. Pointer: `< EPR of server + identity + Local pointer >`

   EPR (URL + token) allows locating the server on the net

   Identity a pair-wise persistent pseudonym, essential to preven-tion of correlation and emergence of GUID for the resource

   Local pointer allows multiple resources under one identity

3. Original data:
   - Copy of the data in original format, signatures intact
   - Pointer to original source is kept
   - MTOM binary clean enveloping in protocol: data and sigs intact

PDS Data: Schema and Data Vocabulary

- PDS and metadata are schema agnostic at basic layer (no bias to any particular schema)
- Metadata schema standardization desired
  - Common vocabularies are easiest way to have interoperability
  - Some common basis
- Recommend schema standards for some immediately pertinent datasets, e.g.
  - ePortfolios

PDS spec (WIP)

Detailed specification by Sampo *et al.* is available as

```
draft-ios-pds-v01.pdf
```

Thank You! from PDS, IoS, TAS3, & ZXID

Sampo Kellomäki (sampo@zxidp.org)

+351-918.731.007

skype chat: sampo.kellomaki

`http://zxid.org/tas3/`