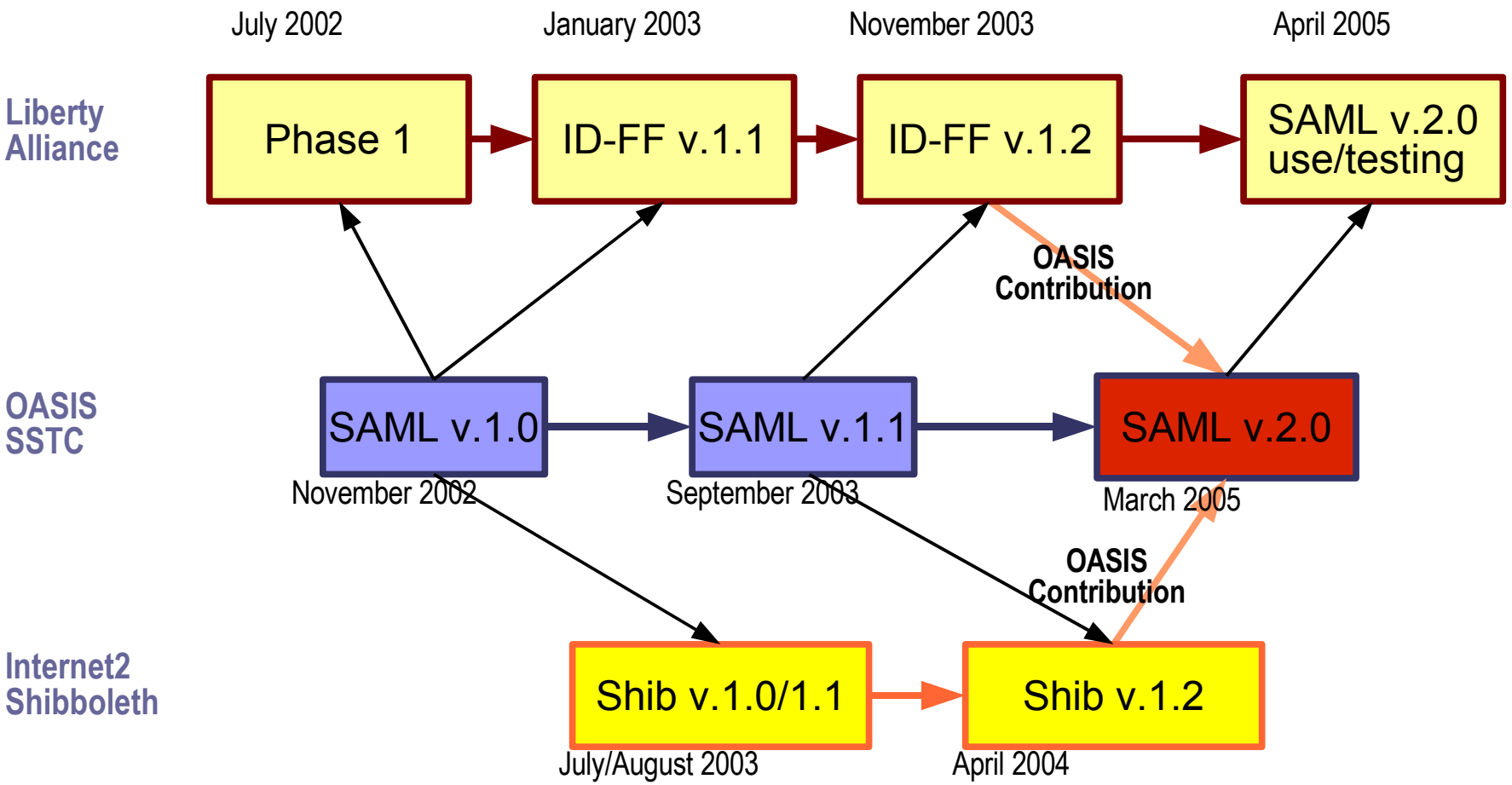
Liberty Alliance
What's After Federation

Fulup Ar Foll
Master Architect
Sun Microsystems

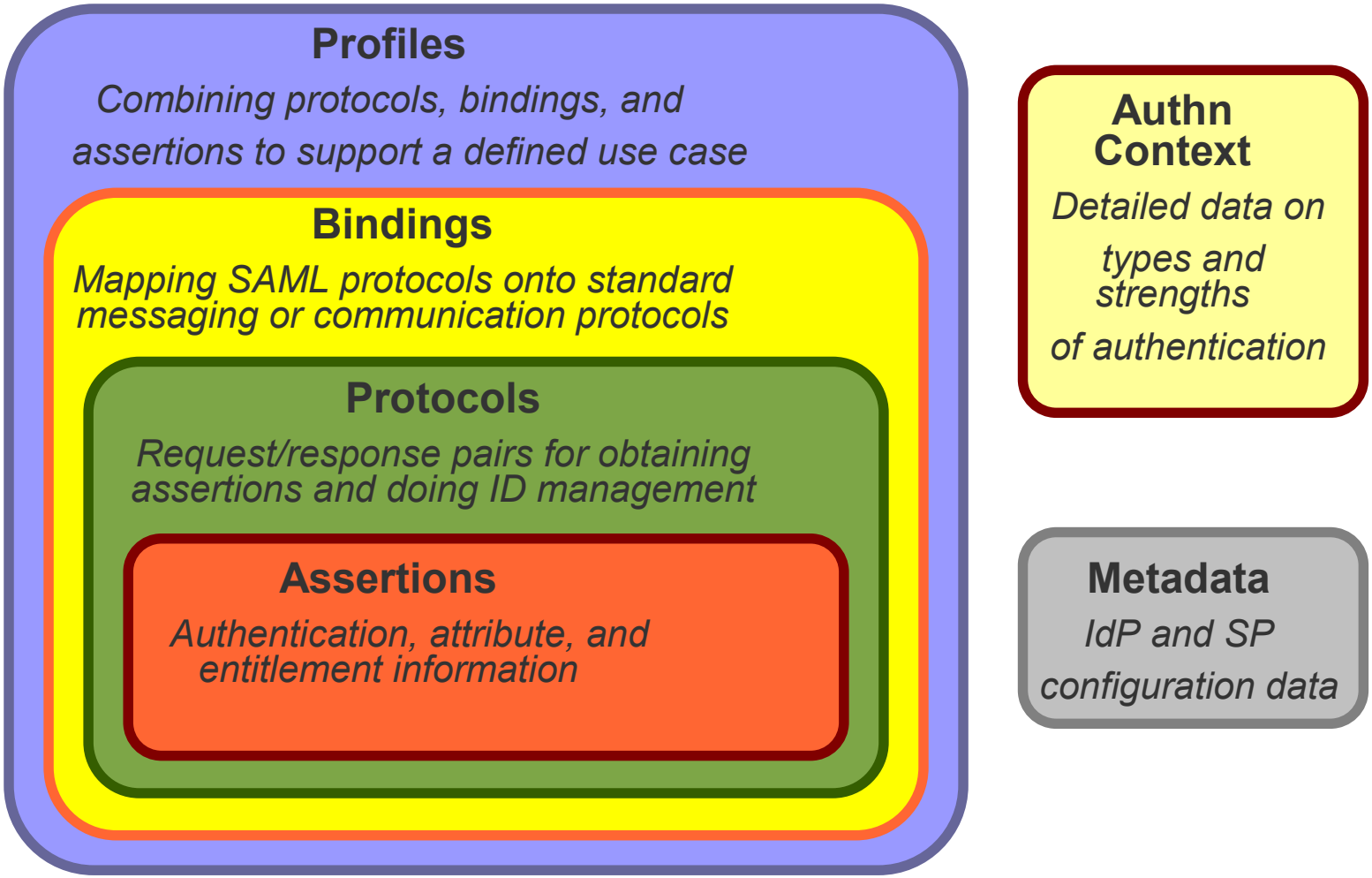
What's About Federation

- Federation of providers (CoT), a group of entities providing services who signed agreement, in order to make life of shared customers/users *(Principal)* more simple.
  - *accept Principal identity authentication to be done once per session (SSO) and by a shared authority (IDP)*
  - *Accept to provide service knowing only an "avatar" of principal identity (Opaque Handle/Federation Key). This non significant pointer on principal identity allowing service provider (SP) to know that "it is him" without knowing "who he is".*
- Federation: a weak link that allow to map a principal avatar identity used by a service provider to the effective principal identity know only from the authority of authentication (IDP).
- Federated Identity: The data/attributes at the service provider attached to a principal identity avatar.

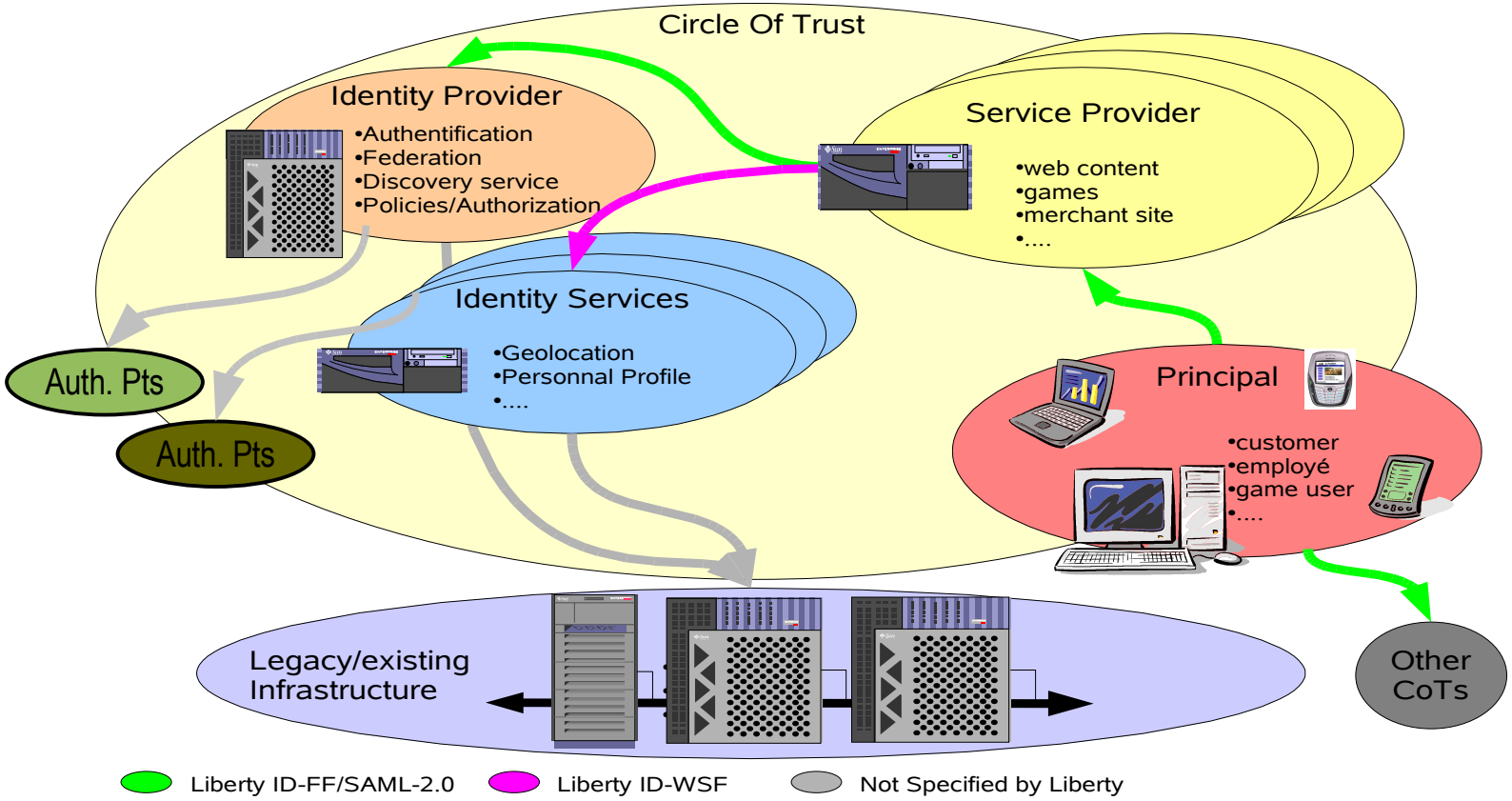
Standard and Convergence



OASIS SAML 2.0 Concepts



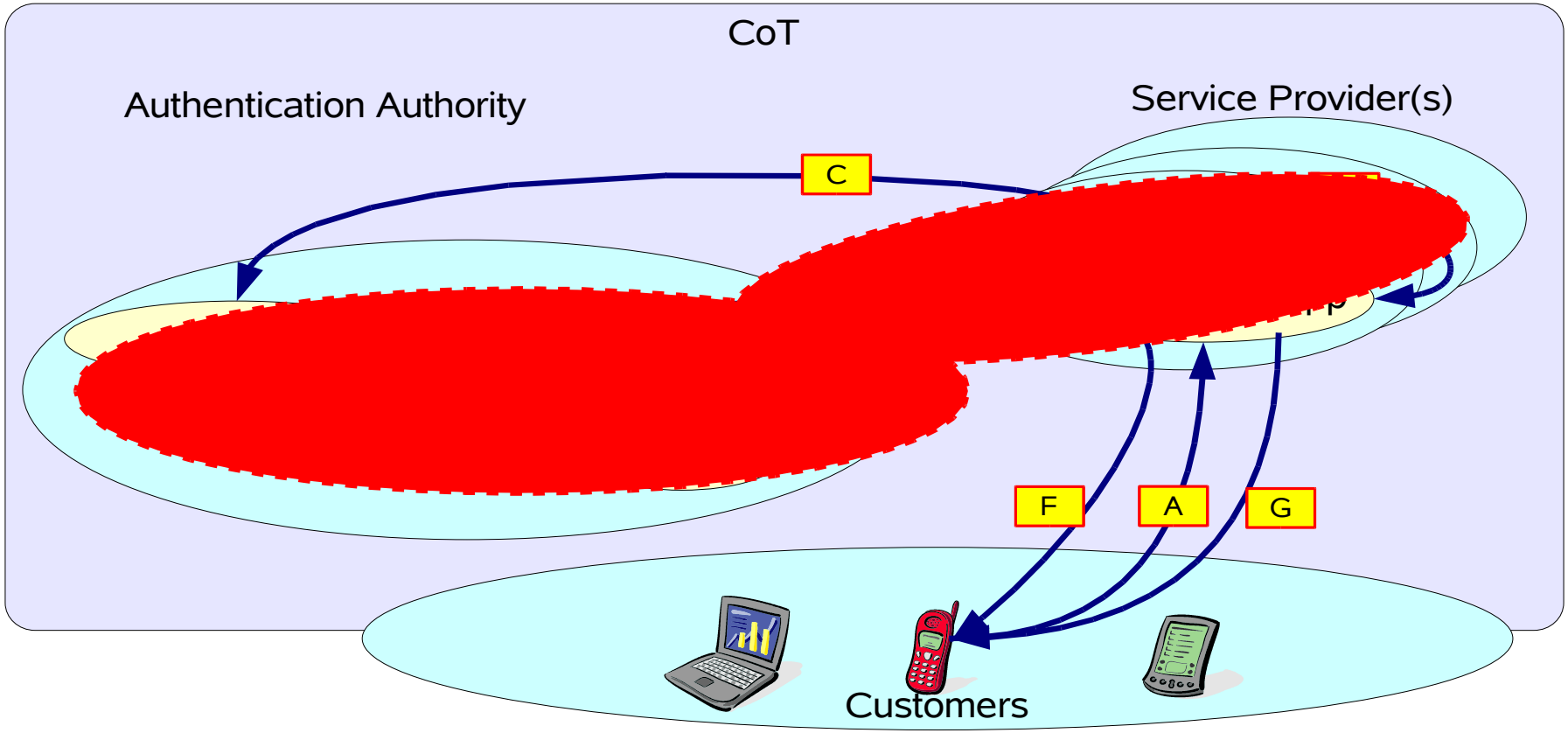
Global Liberty Architecture



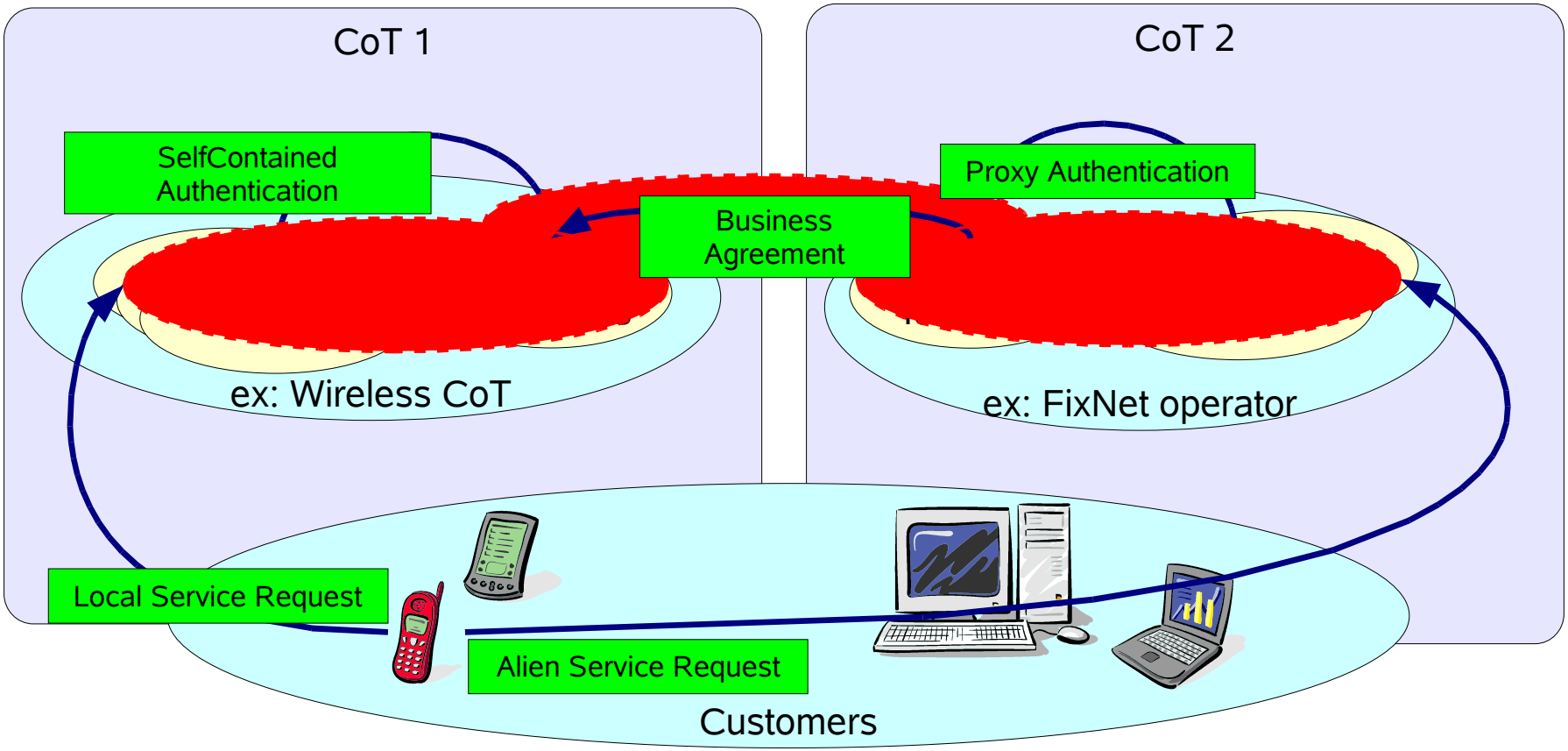
Liberty Technical Framework

- ID-FF (Identity Federation Framework)
  - Federation/Defederation
  - SSO *(single & simplified Sign On)* / SLO *(single logout)*
  - Authentication context & Attributes
  - Metadata
- ID-WSF (Identity Web Service Framework)
  - Authentication Service
  - Discovery Service
  - DST (Data Service Template)
  - Interaction Service
- ID-SIS (Identity Service Interface)
  - Personal profile, Geoloc, Presence, Contact Book, ...

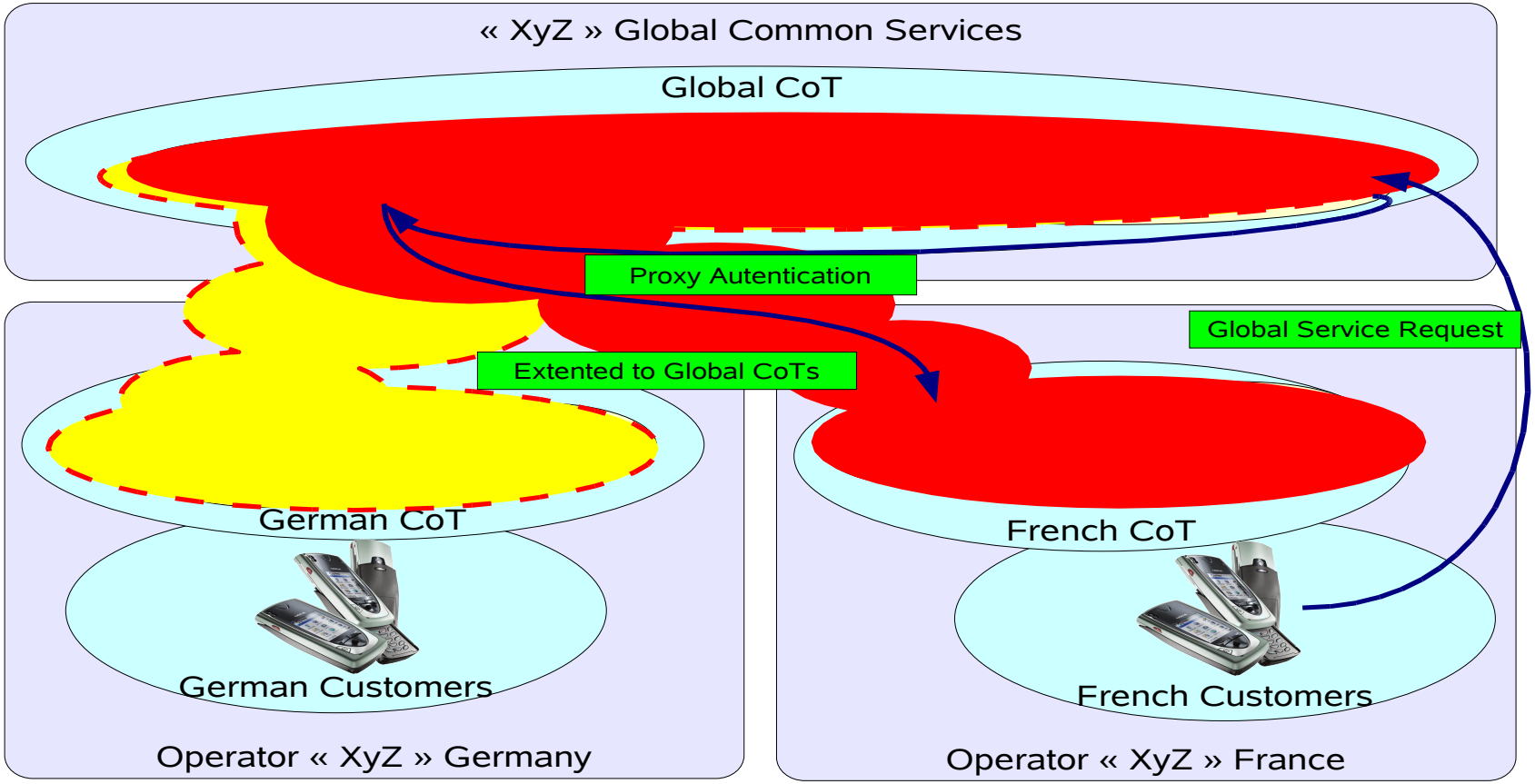
Basic CoT *(outsourcing of services)*



CoT/CoT *(proxy authentication)*



Shared CoT *(global shared Services)*



ID-WSF 2.0 (Public Draft 3)

- Features
  - Cross-user transactions
  - Asynchronous messaging
  - Subscription/Notification
  - Adoption of SAML2
- Components
  - Framework enhancements
    - Adoption of WS-Addressing
    - Multi-user invocation context
  - People Service
    - Who are my “friends”?

ID-WSF 2.0: Cross-User

- Extended Invocation Context to include:
  - Invocation Identity
    - Who is submitting the request
  - Target Identity
    - Who's resource is targeted in the request
  - Sender
    - Server sending the request
  - Destination
    - Server receiving the request

ID-WSF-2: People Service

- Identity Federation between *individuals*
  - Paul establishes a connection with Carolina
- Supports Invocation of another user's service
  - Carolina can access Paul's Calendar (w/permission, of course)
- Group (Collection) management
- Invitation model for cross-IDP federations

Why Choosing Liberty ?

- Fit your requirements:
  Free & Open standard, Privacy, Security, Interoperat
- An industrial reality:
  Certified products, Already proven in production
- You're not in a position of choosing:
  Costumer chooses for you !!!

Kravspesifikasjon for PKI i offentlig sektor Versjon 1.02 , Januar 2005

Krav 10.5.1 Autentisering

Det skal tilbys en ”Identity Provider” i henhold til Liberty Alliance spesifikasjoner. Løsningen skal beskrives. Det skal angis hvilke versjoner og overordnede funksjoner som støttes.

Requirements Spec. for PKI in Public Sector
Version 1.02 , January 2005

Requirement 10.5.1 Autentication

It shall be offered an ”Identity Provider” according to Liberty Alliance specifications. The solution shalll be described. It shall be indicated which versions and which high level functions are supported.

Access Control

SP is responsible for securing access.

For each SP, identify data needed for access control decisions and where it will come from.

- For individual consumers may come from user.
- For outsourcing scenario, data needed may be split between SP and IDP.
  - Attributes can be sent in a bulk feed.
  - SP application can use SAML
  - Can use provisioning/sync solution between SP and IDP to better leverage capabilities of an access management type of product.

Support

How to support someone you don't know ?

For each SP and IDP, identify potential user issues, and how support will be provided by SP and IDP.

- User cannot login, can't access app, data wrong,...
- Identify how users will report a problem
- Identify first responder, escalation paths
- Identify how each responder will
  - Be able to identify user's account
  - Be able to contact user later to ask more questions
  - Gets tricky if user has different ID at SP and IDP
  - User likely to forget SP ID when accounts federated

Logout

Local and/or Global logout both possible

- Bigger issue than it initially seems
- Providing just one may cause issues
  - Users do local logout, leave global session, walk away from browser
  - Users might avoid use of global logout thinking they have more work to do.
  - Best to support both, educate users on differences
  - If you must do just one, choose global logout

SSO expectations

Sign Sign One & Simplified Sign One

- Set expectation appropriately
  - Logins to hardware devices
  - Logins to networks (VPNs etc)
  - Logins to applications
  - Different levels of authentication (i.e. single versus dual factor)
- “Simplified Sign On” may be better term

Monitoring

- Obvious
  - Monitor HW, OS on all component servers (app, authN service, authZ service, storage)
- Proactive
  - Monitor CPU, number of connections, response time and set acceptability threshold values for each.
- Possible Glitch
  - Monitor federated login with synthetic transactions. IDP may be best positioned to do so if access to IDP is restricted.

Business Agreements

- Many other legal documents typically exist
  - Sales contracts, Purchase Orders, Statements of Work, Service Level Agreements, Contract approvals, Consulting Services agreements etc.
- Liberty-related agreements need to relate to other agreements
- Add Liberty-specific terms to existing SOW/SLA templates
  - Liberty compliance, adding/removing COT members, joining other COTs, federation, authN levels, session timeouts, adding/removing users, policy enforcement

Production Deployment

- There is a world of difference between doing this in a lab and the real world. Deploy and test as early as possible in the 'real' environment.
- Hardened environments
- Firewalls & firewall rules
- Network & Load balancers
- Router ACLs
- Certificates
- DNS and mappings

Liberty Summary

- A free standard focusing on:
  - *Privacy*
  - *Security*
  - *Interoperability*
- An industrial reality:
  - *Certified to latest spec products available*
  - *Already proven in production*
- Return of experience available
  - *Deployment paper*
  - *Consulting services*

Resources

- Java EE SDK
  - http://java.sun.com/javaee/downloads/
- Securing Web Services tutorial
  - http://www.netbeans.org/kb/55/amsecurity.html
- Liberty Alliance Project
  - http://projectliberty.org
- OpenSSO
  - http://opensso.dev.java.net
- Shameless Pat-promotion
  - http://blogs.sun.com/superpat

Liberty Alliance – What's Next

Fulup Ar Foll
fulup@sun.com