



From UseCases to Specifications

Fulup Ar Foll

Liberty Technical Expert Group

Master Architect, Global Software Practice

Sun Microsystems

Why Identity Related Services ?

- **Basic:** Performed without regard to who's doing the asking or using the results
- **Identity-enabled:** Offers personalization when given access to identity details
- **Identity-enabling:** Exposes identity details to other services

Why Choosing Liberty ?

- x **Fit your requirements:**

Free & Open standard, Privacy, Security, Interoperability



- x **An industrial reality:**

Certified products, Already proven in production

- x **You're not in a position of choosing:**

Customer 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 Authentication

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

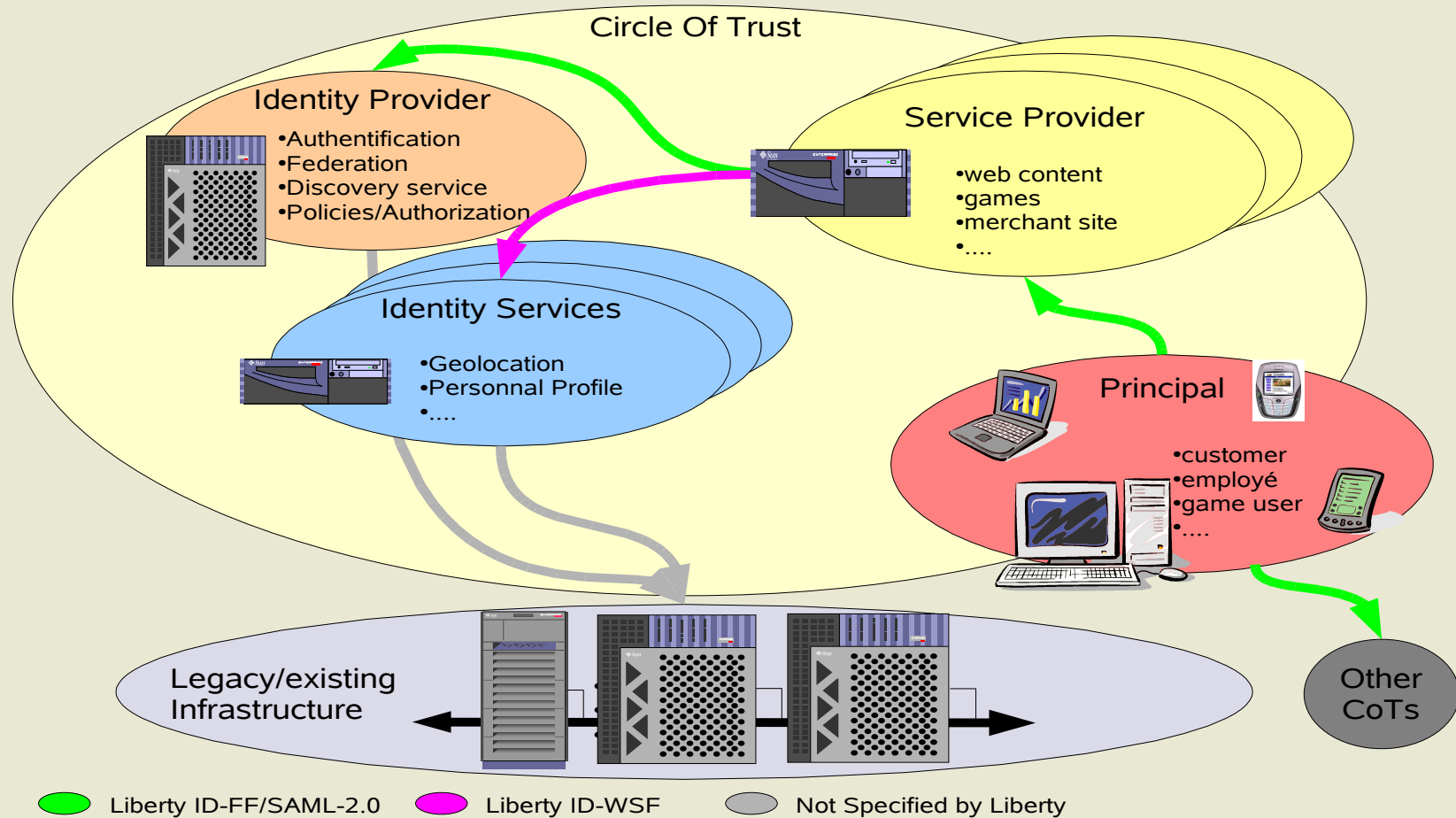
What's About Federation

- **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.

Liberty is not a concept but an existing Today Technology Reality

- SOA (Service Oriented Architecture) Framework
 - Identity Provider (IDP) Circle of Trust (CoT)
 - Services provider /consumer (SP – WSP/WSC)
 - Discovery (DS), Invocation (DST)
 - Terminology
- Set of specifications
 - Network protocols
 - Messages syntaxes
- Certification process

Global Liberty Architecture



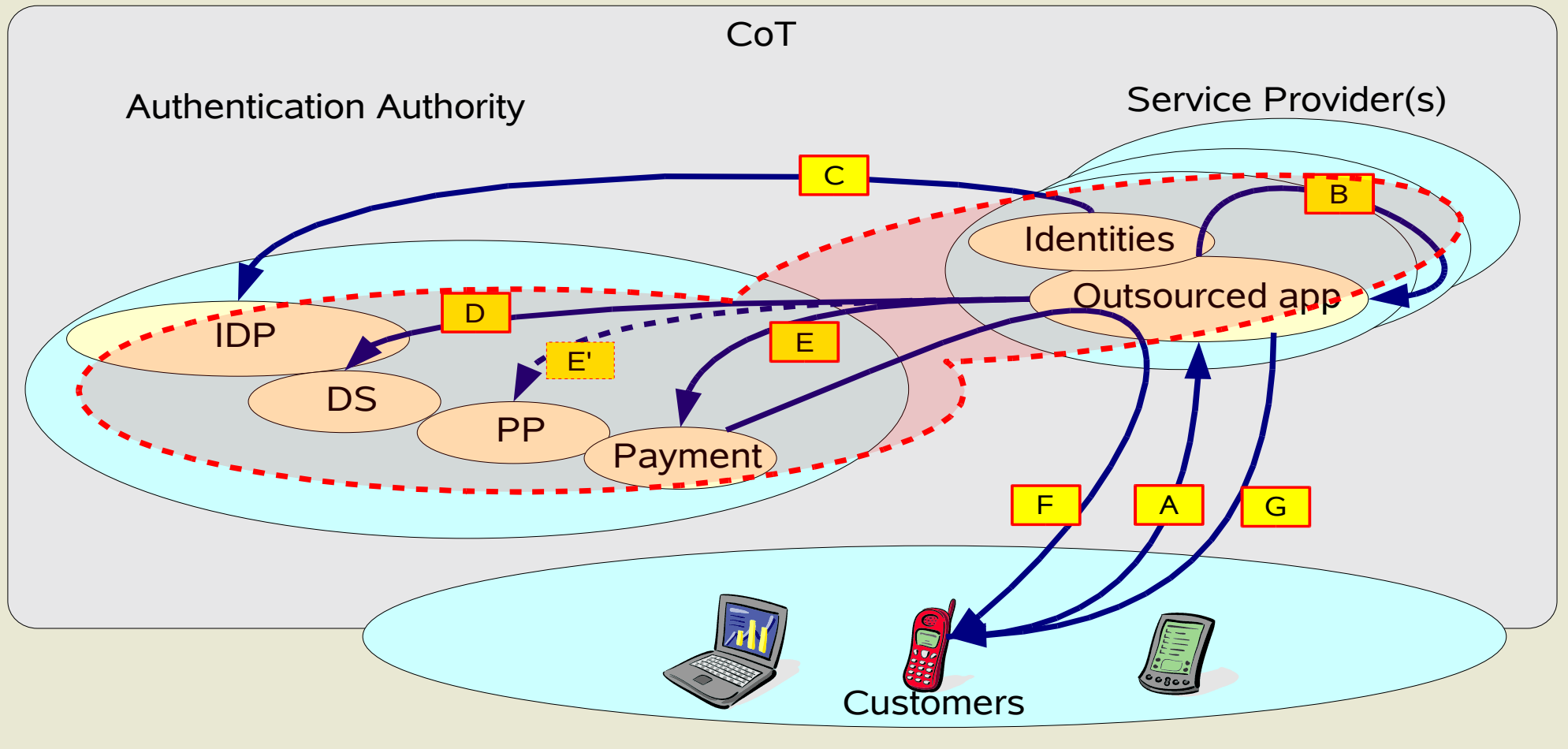
Liberty Standard and the others



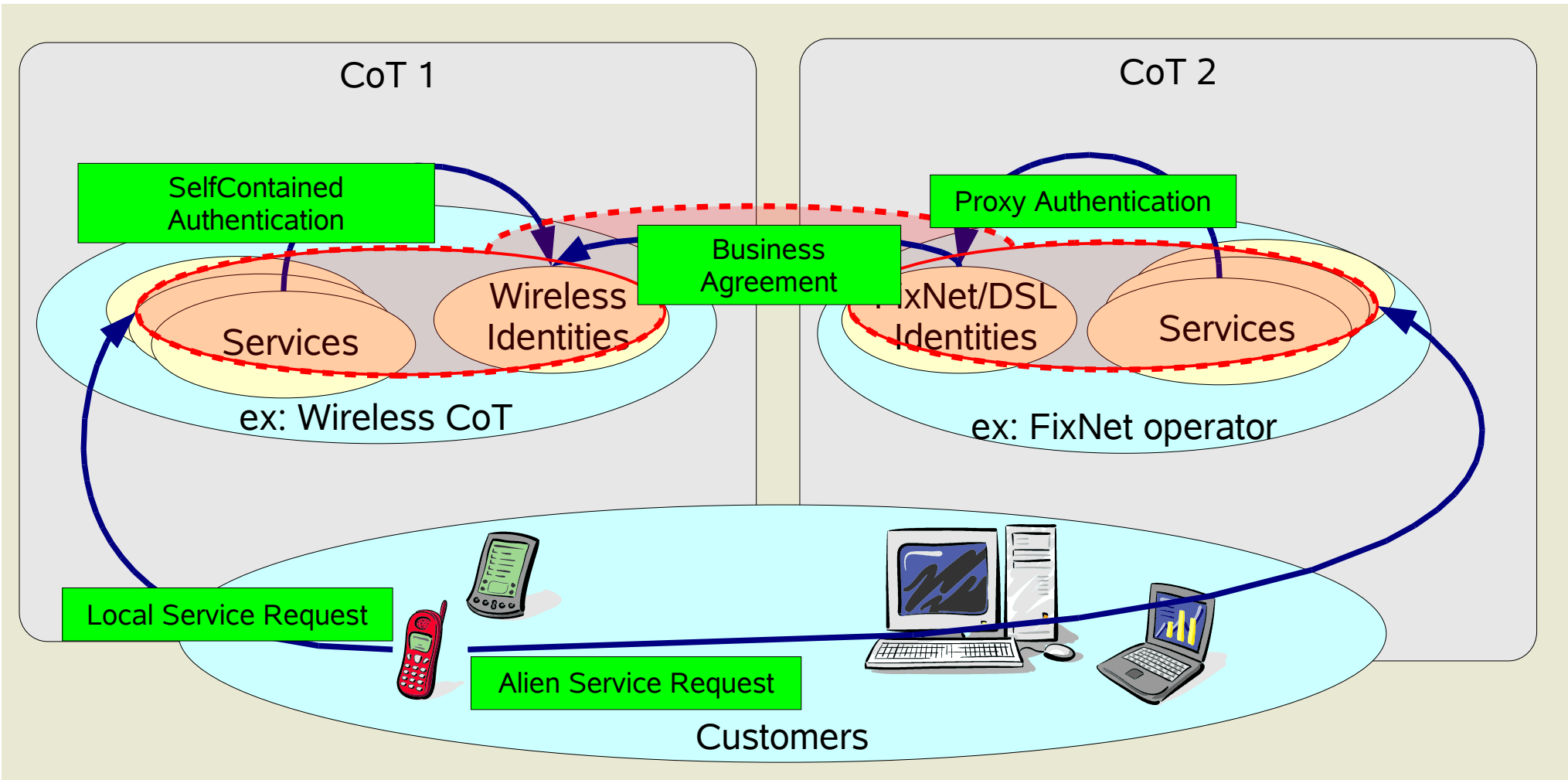
Liberty Technical Framework

- 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, ...

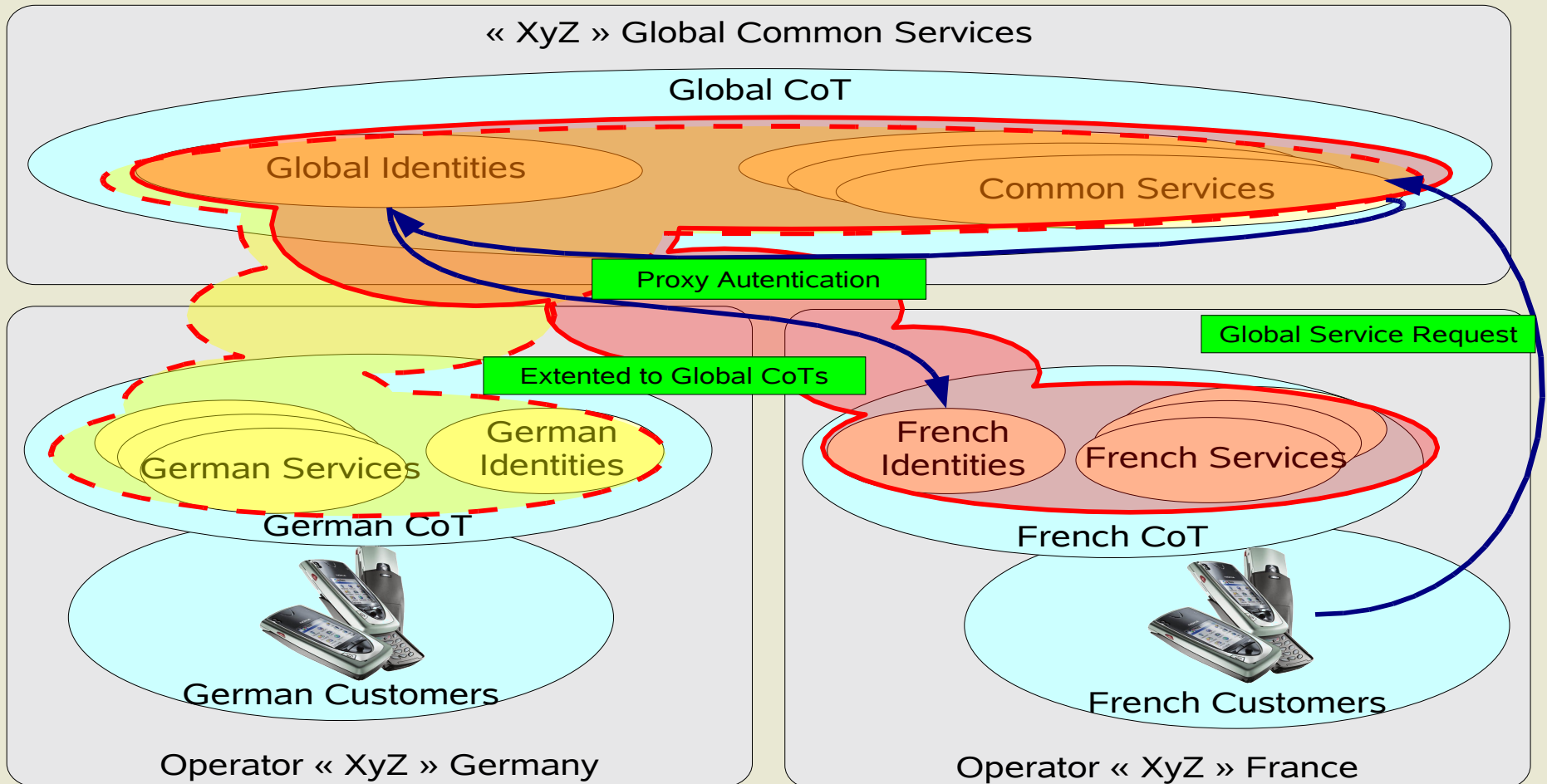
Basic CoT (*outsourcing of services*)



CoT/CoT (*proxy authentication*)



Shared CoT (*global shared Services*)



The End

fulup@sun.com