Identity Federation & Web-Services Technical Use Cases for Mobile Operators

Fulup Ar Foll

Master Architect
Global Expertise Center
Sun Microsystems

Fulup@Sun.com

Sun microsystems

Liberty Marketing Answer

- IS a member community delivering technical specifications, business and privacy best practices
- IS providing a venue for testing interoperability and identifying business requirements
- IS developing an open, federated identity standard that can be built into other companies' branded products and services
- IS driving convergence of open standards

Liberty toward customers

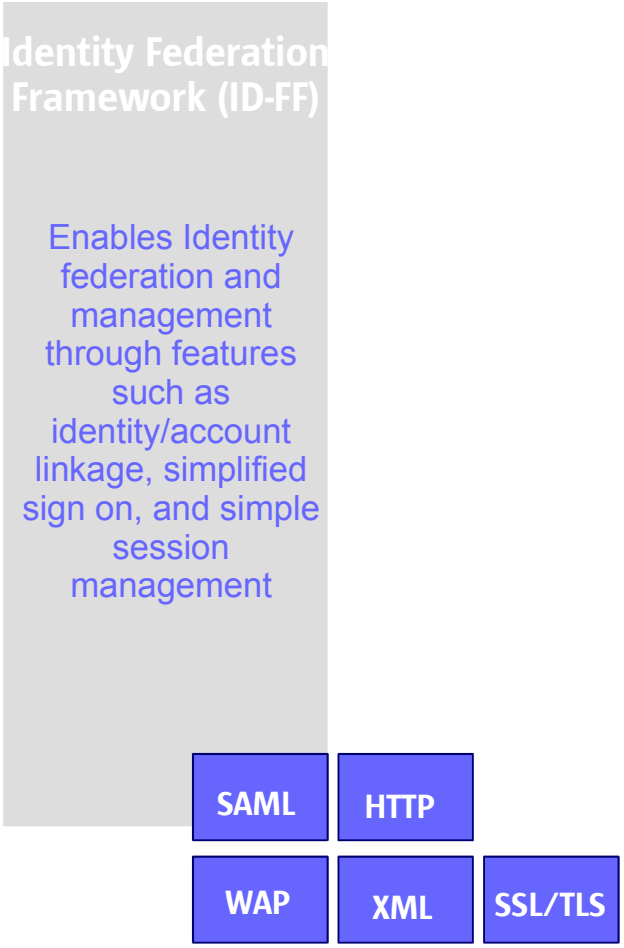
- Option for medium term architecture strategy
  - Web Services SOA framework.
  - Loosely couple identification.
  - Commercial softwares stack.
- Solution path to some short term issues
  - Outsourcing of application
  - Easier integration of partners
  - Extend panel of services
  - An answer to some security concerns

Liberty from Technology

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

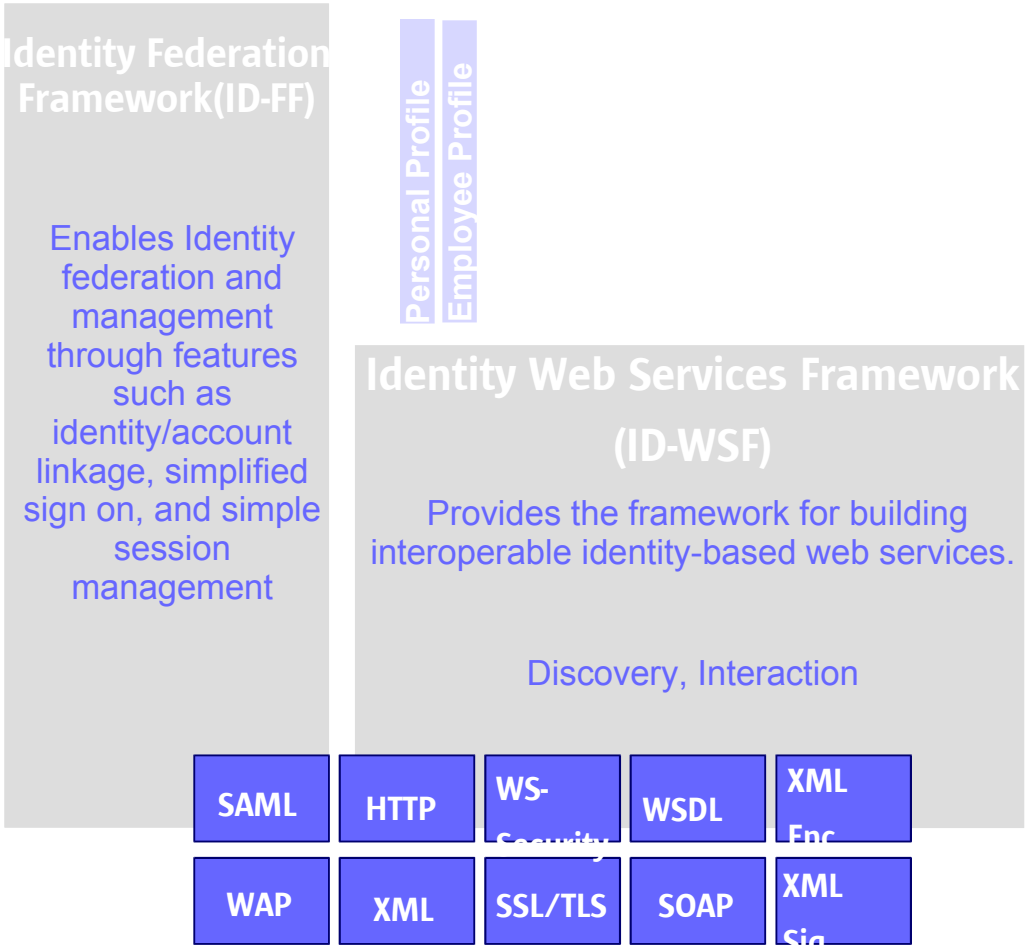
A constellation of venues

Federation Framework



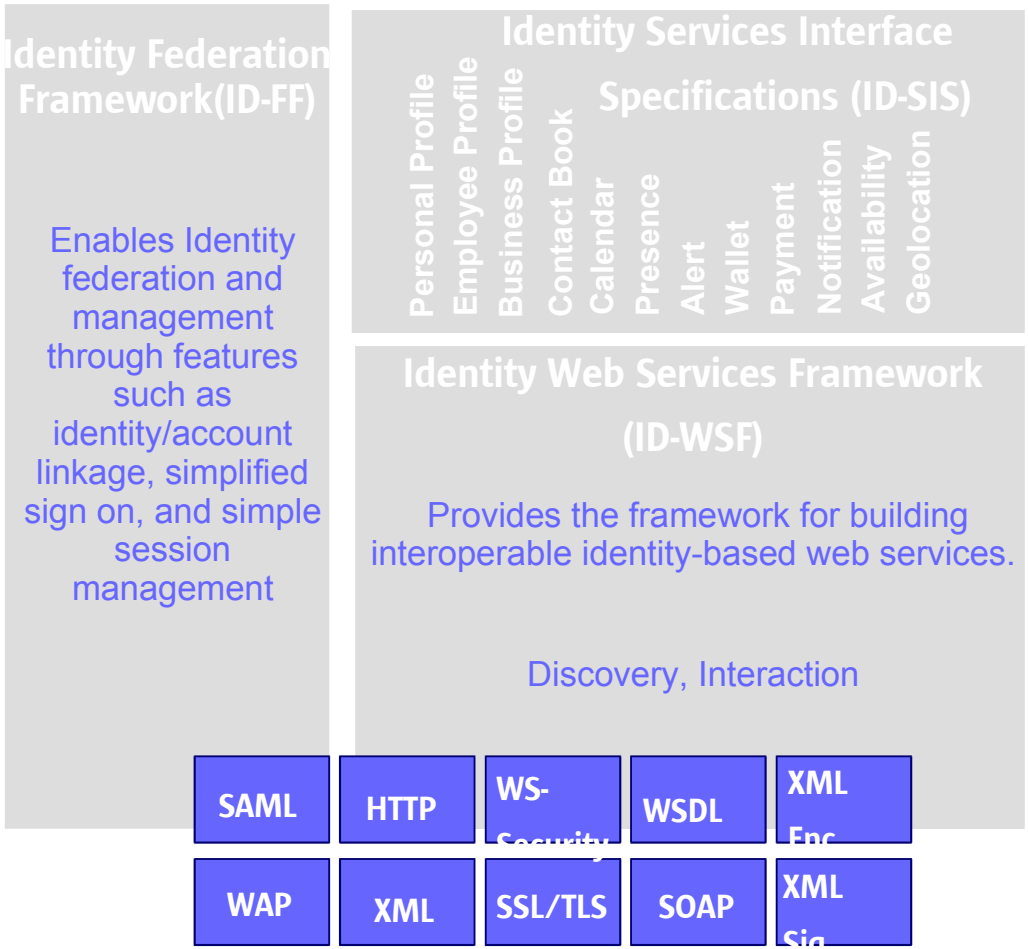
- Spec. Released 7/02
  - Browser and WAP profiles
- Opt-in
- Single Sign-on and Log out
- Profiles for “thin” clients
- Submitted to OASIS SAML TC
- RSA Interop. Event 4/03
  - AOL, Communicator Inc, Ericsson, HP, Jabber, Mycroft, NeuStar, Nokia, Novell, NTT, Ping ID, Phaos, PostX, SchlumbergerSema, Sigaba, Sun, Symlabs, Trustgenix, Vodafone, Waveset

Web Services Framework



- Permission based attribute sharing
- Services Template
- Personal & Employee Identity Profiles
- Released Nov `03
  - Available for public download
- Already supported in 5 implementations

Services Interface Specification



- Interface and data schema
- Horizontal or vertical
- Defined in parallel
- First service tracks:
  - Contact Book
  - Geolocation
  - Presence

ID-WSF: Discovery Service

- Registry for services associated with an identity
  - Registration and Lookup services
  - Resource Offering (RO) describes services
    - Service Endpoint
    - Resource Identifier at the service
    - Security Mechanism
- Translates and protects tokens (as necessary to allow one entity to safely communicate with a second entity)
- Multiple providers of the same service
- Chaining of services
- Data specific discovery
  - Retrieve the wallet service that has a credit card
  - Retrieve the profile service that has an age

ID-WSF: Authentication Service

- Bootstrap to Discovery Service
- SASL Based SOAP Authentication
  - General purpose authentication exchange mechanism
  - Existing defined support for multiple mechanisms
    - CRAM-MD5, PLAIN, X.509, SECURID, etc.
  - Extensible for future methods/mechaisms

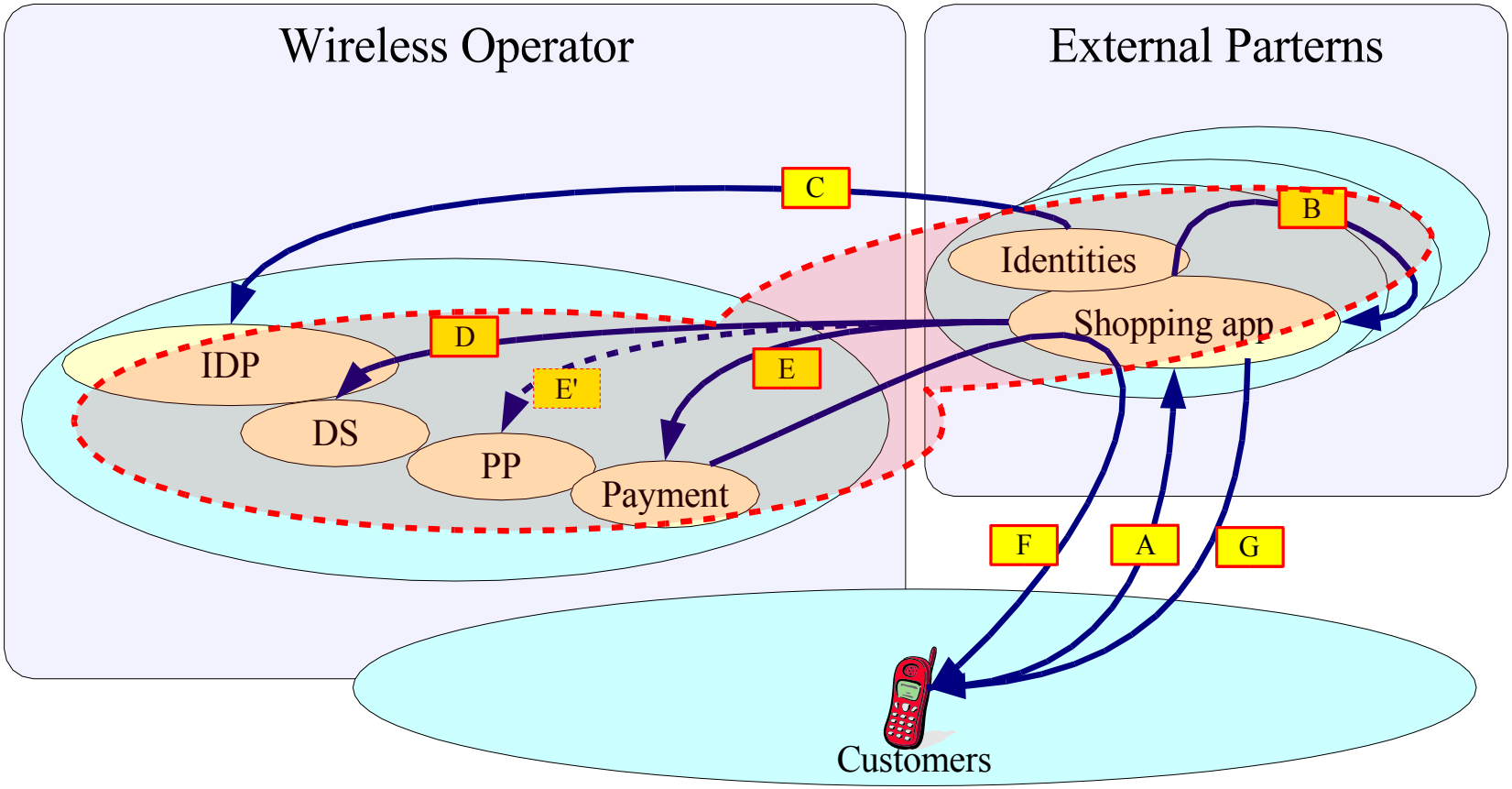
ID-WSF: Data Service Template

- Data Service Template (DST) provides generic mechanisms for interacting with data services
- Data Service Template provides protocols for the query and modification of data attributes related to a Principal that are exposed by a data service.
- Defines some guidelines, common XML attributes and data types for data services.

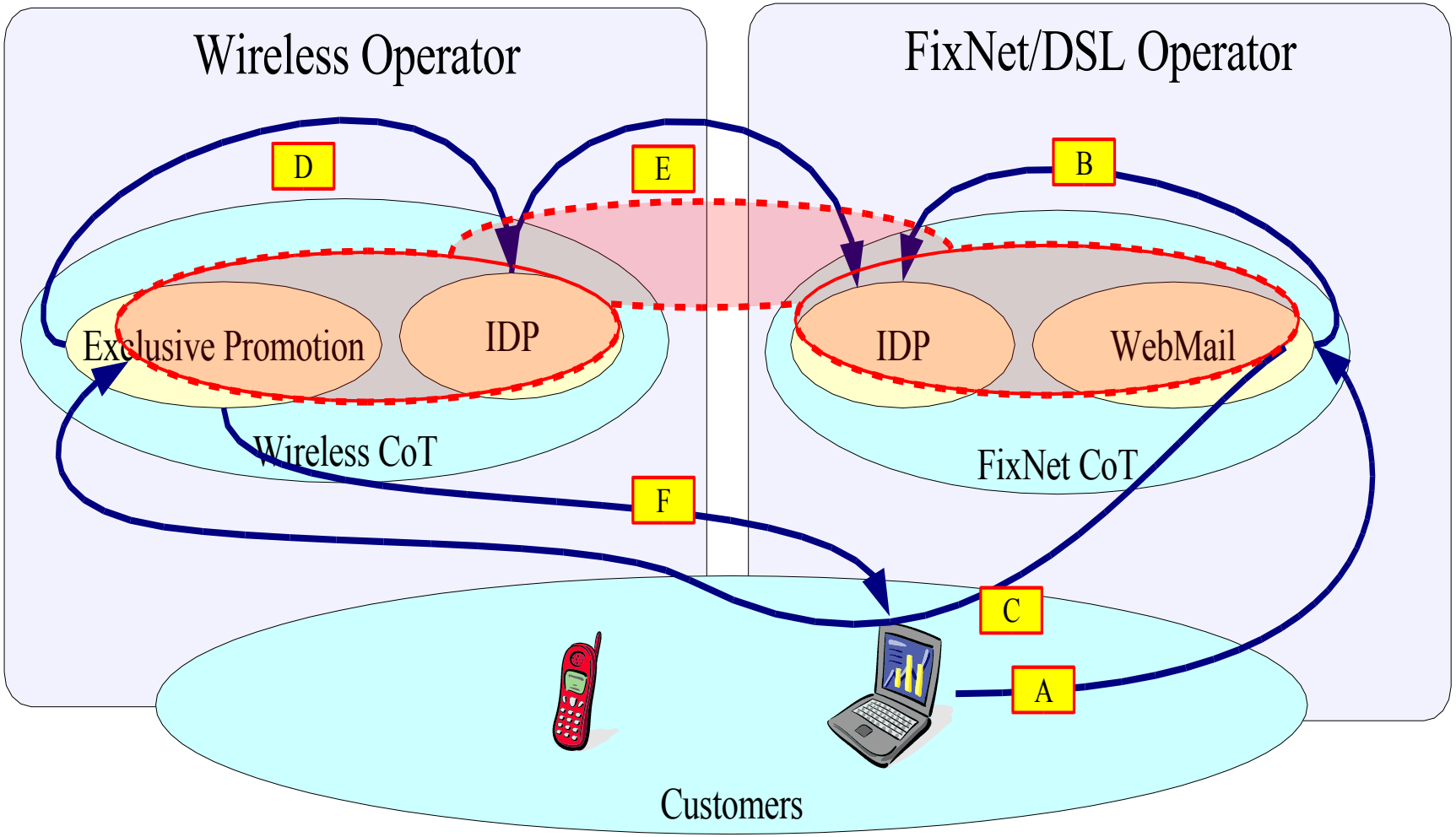
ID-WSF: Interaction Service

- Enables WSP Interaction with User
  - Typically WSP does not have direct user access
  - Real-time consent, data, and/or decision Collection
- Multiple Methods
  - Allow trusted party (SP) to interact
  - Request that SP re-direct user's browser to WSP
  - Direct interaction without involving SP

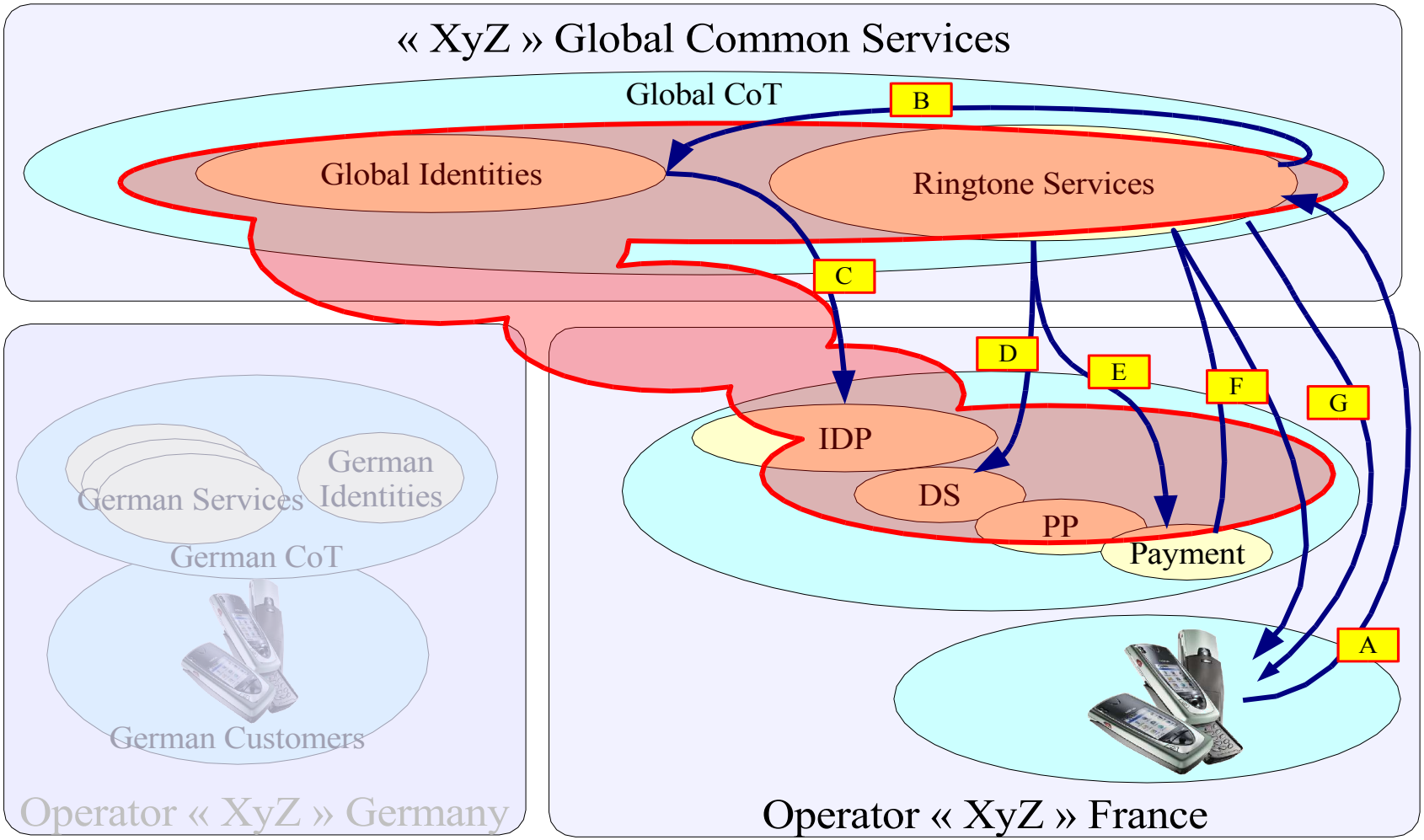
Basic CoT *(outsourcing of services)*



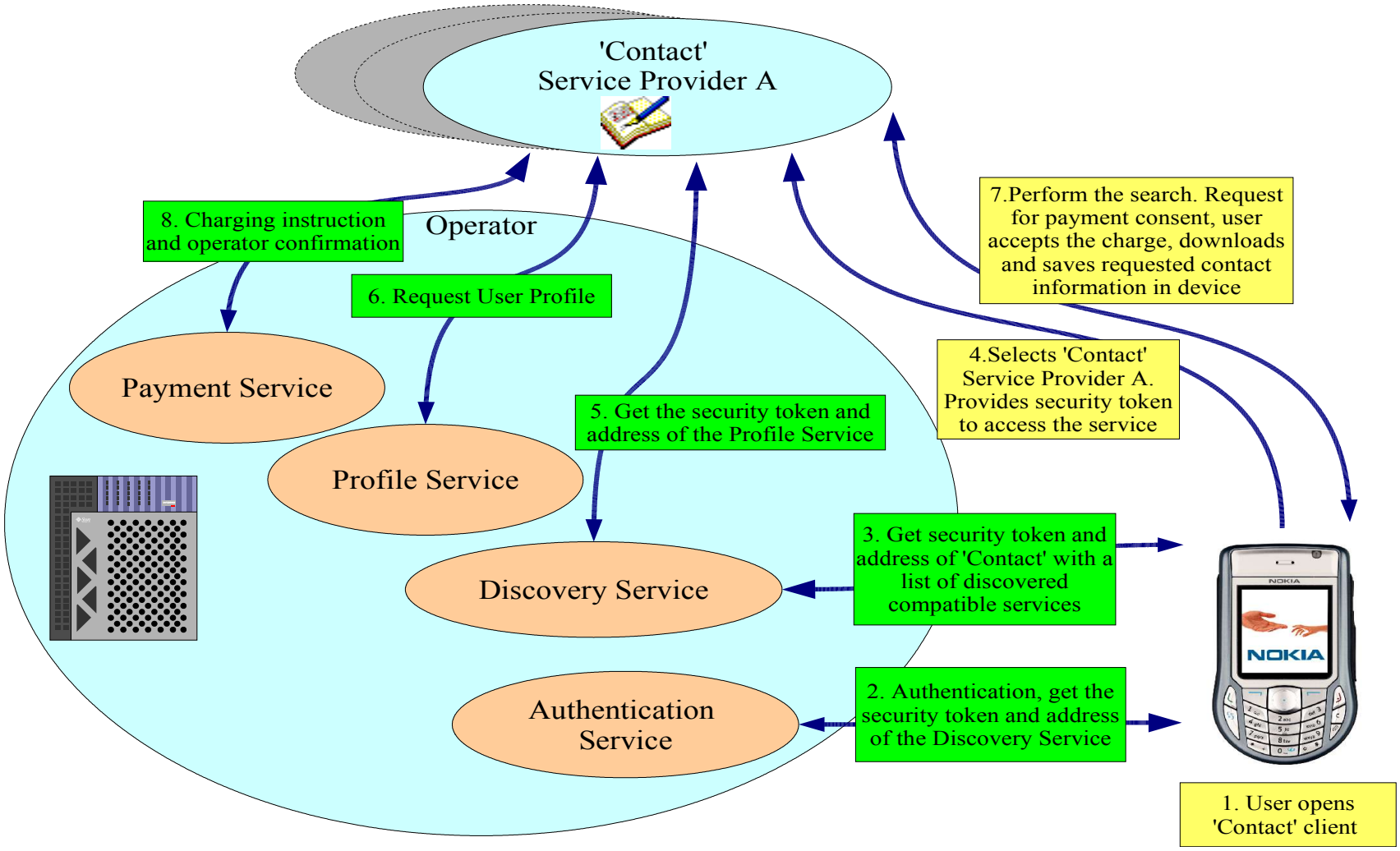
CoT/CoT *(proxy authentication)*



Shared CoT *(global shared Services)*



Embedded Web-Services



Most of High Added Value Web Services need identity

- **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

Web services have all the classic security requirements

- **Authentication:** Participants in a message exchange recognize each other and the creators of the content
- **Authorization:** Actions on resources are checked against permissions
- **Auditing:** Participants have a record of what happened
- **Integrity:** Message content wasn't altered inappropriately in transit
- **Confidentiality:** Content is protected from prying eyes
- **Non-repudiation:** A message sender can't refute that they sent it
- **Trust:** Participants have agreed to work together

Trust and technology

- Trust is only partially a technical problem
- Federated identity networks depend on working agreements
- Liberty offers best-practices material to assist this, in addition to metadata exchange protocols for the technical angle

Liberty enabled products & services

Communicator (available)
Computer Associates (Q4*)
DataKey (available)
DigiGan (Q3*)
Ericsson (Q4)
Entrust (Q1 2004)
France Telecom (Q4 2003)
Fujitsu Invia (available)
Gemplus (TBD)
HP (available)
July Systems (available)
Netegrity (2004)
NeuStar (available)
Nokia (2004)
Novell (available)
NTT (TBD)
NTT Software (available)
Oblix (2004)
PeopleSoft (available)
Phaos Technology (available)
Ping Identity (available)
PostX (available)
RSA (Q4)
Salesforce.com (TBD)
Sigaba (available)
Sun Microsystems (available)
Trustgenix (available)
Ubisecure (available)
Verisign (Q4*)
Vodafone (2004)
WaveSet (available)

Liberty Summary

http://www.projectliberty.org

- A free standard focusing on:
  - Privacy
  - Security
  - Interoperability
- An industrial reality:
  - Certified products available
  - Already proven in production

http://www.projectliberty.org/resources/whitepapers/Nokia_Sun_US_2812.pdf