Global Identity and Reachability Framework for Interoperable P2P Communication Services

Ibrahim Tariq Javed

TELECOM SudParis

Introduction

- Two types of Communication service delivery in market
  - The old fashioned federated delivery models, used by Telco operators.
  - The vibrant walled garden delivery models, used by OTT players.
- New emerging web services are confronting the traditional Telco operated communication services
- reTHINK project aims to propose a new web centric P2P service architecture having
  - WebRTC real time peer-to-peer communication capabilities
  - Secure, non-service-bound, privacy enabled identities
  - Global reachability with de-perimeterised services
  - Interoperability
  - QoS beyond best effort

Web Identity framework features

- A Trustworthy identity framework that has the following features:
  - Cross domain interoperable
    - Communicate with user identified in other services
  - Identity portability across service providers
    - Without losing identity details or contact lists
  - Identity decoupled from services provider
    - Use of Independent Identity Provider (IdP)
  - Global searchable
    - Searchable across the Internet, in any domain
  - Trust-enhanced identity features
    - IdP-certified identity
    - Complemented by Trust Engine

Hyperty Concept

- The distributed framework of reTHINK relies on a software concept:
  - **Hyperty** (Hyper linked entities): a module of software logic that is dynamically deployed in an endpoint browser runtime client.
  - It represents a 'live' user that can be contacted dynamically.
- The identity and support framework allows the discovery of hyperty instances downloaded from CSP

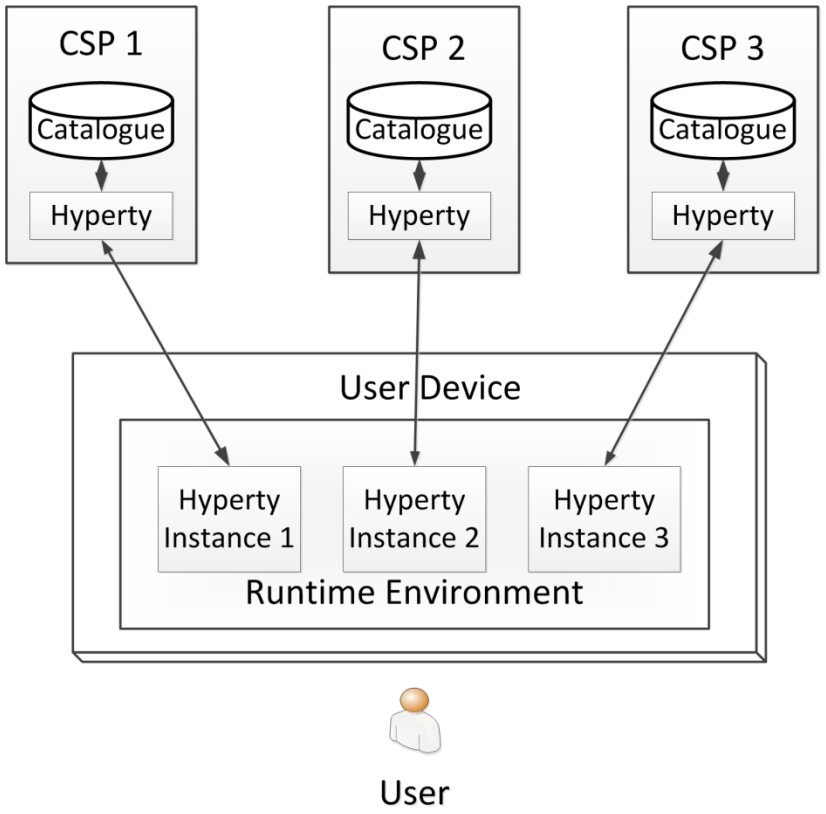

Fig 1: Hyperty Concept

Identity Support Functionalities

- The Identity and Support functionality within reTHINK framework are provided using four different component:
  1. Identity & Trust management
  2. Directories services
  3. Graph Connector
  4. Governance & Policy

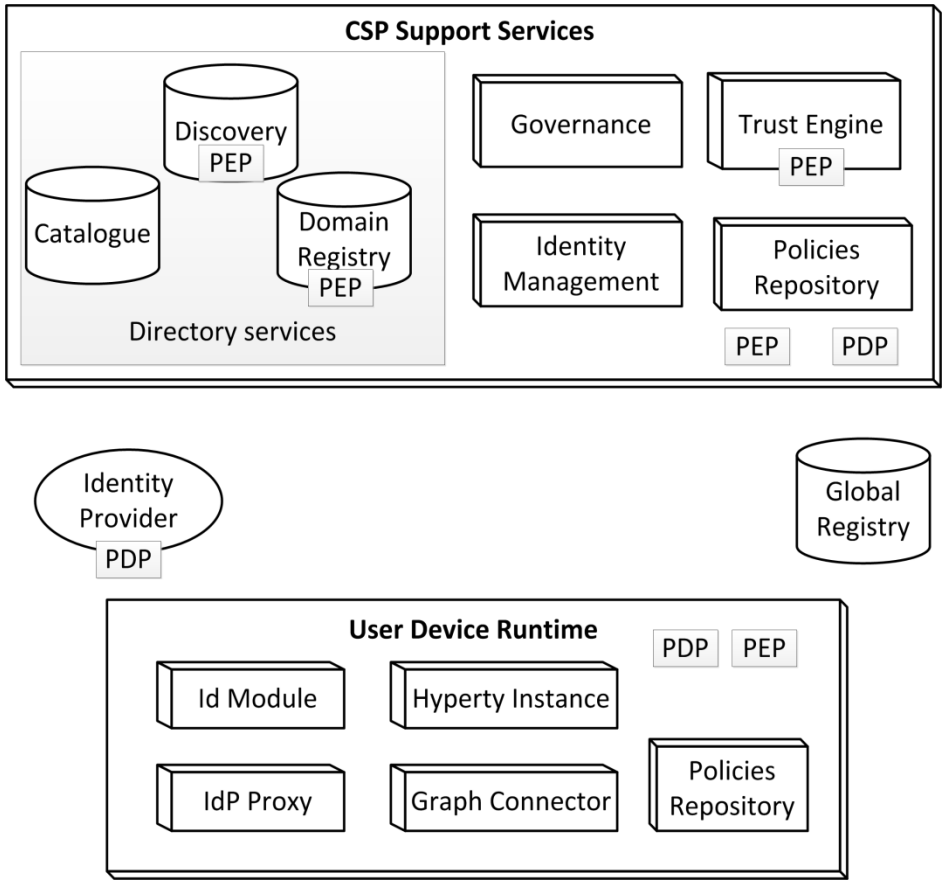

Fig 2: reTHINK functional architecture

Identity Management

- The Identity Management relies on:
  - Identity Provider (IdP):
    - Provide, manage and verify user identities.
    - Common standards such as OpenID Connect and OAuth
  - IdModule
    - Software module that preservers identity of users
    - Enable users to choose the adequate identity
    - Associates Hyperty instance with Identity
    - Support multiple Identity acquisition methods
    - Platform for IdP proxy execution

Trust Management

- The trust engine consists two basic modules
  - Authentication validation
    - The identity is verified from the issuing IdP
  - White and Black list:
    - Indicates whether identity is known for good or malicious behaviour
- Users can be displayed with Trust levels based on trust vectors
- Trust vectors involved in reTHINK trust engine are as follows
  - The caller is authenticated
  - The caller is already known
  - The caller is already known by another communication partner
  - The caller is not on a black list
- The decision to trust or not still relies with the user

Directory Services

- The Directory services include three main components
  1. Catalogue
     Provides list of available service functions provided by Hyperty of various CSP's
  2. Registry
     Provides information about available Hyperty instances for communication
  3. Discovery
     Used for finding users in various domains

Catalogue

- The Catalogue Service provides information about the Hyperties that are available
  - The Catalogue Service stores descriptors of Hyperties available for use.
  - This service is used by developers to find Hyperties to use in their own software, working as an App store.
  - It provides means for the runtime to obtain (download) the implementation of a Hyperty.

Registry Services

- Two types of identifier
  - Global Unique Identifier (GUID)
    - Domain agnostic
  - User Identifier (UserID)
    - Domain dependent identifier
- Registry service includes:
  - Global registry:

    Resolves user GUID to CSP specific User ID
  - Domain registry:

    Translates UserID to IP address of current Hyperty instance of user

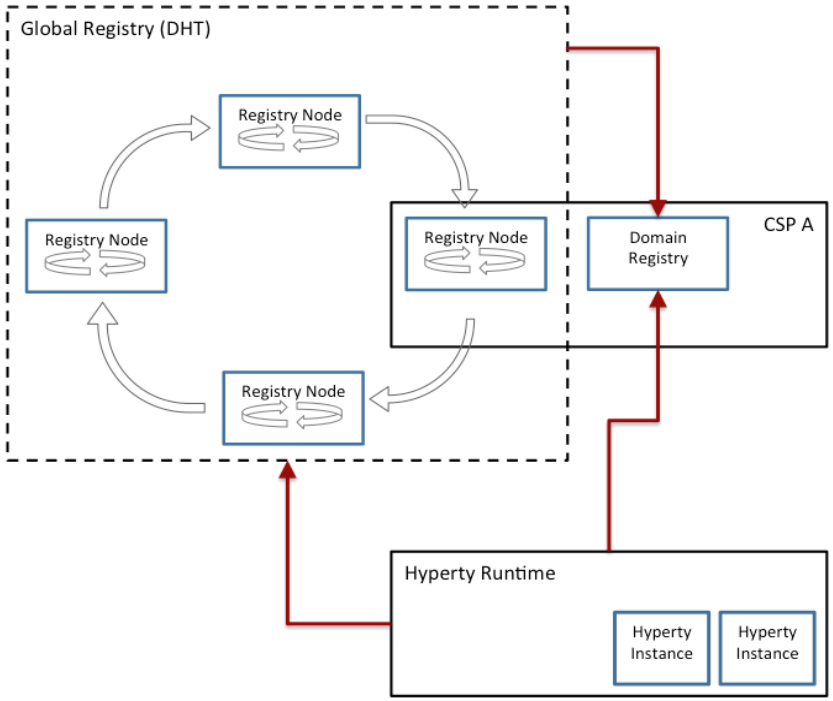

Fig 3: Global and Domain Registry

Discovery services

- How to find people across different networks or domains?
  - Communication beyond address
  - Search service based on what you already know
  - User oriented search engine for the discovery of GUID
  - Each user is free to create his own entry in the discovery registry and publish data
  - A trusted and reliable service needs to provide discovery service

Graph Connector

- Graph Connector is a local address book maintaining a list of known communication endpoints
  - A distributed, qualitative/quantitative-weighted social network
  - The graph will be stored in a distributed manner on the user device.
  - The graph can have named and weighted edges between vertices.
  - For Trust engine this graph can be used to estimate trust level between users that are not connected

Governance & Policy Management

- Classical PDP/PEP Policy repository structure is used
- Distributed among
  - End user devices
  - CSP infrastructure
- Policy are of two types
  - Policies defined by the CSP and accepted by the end user
  - Policies specific to the device local resources

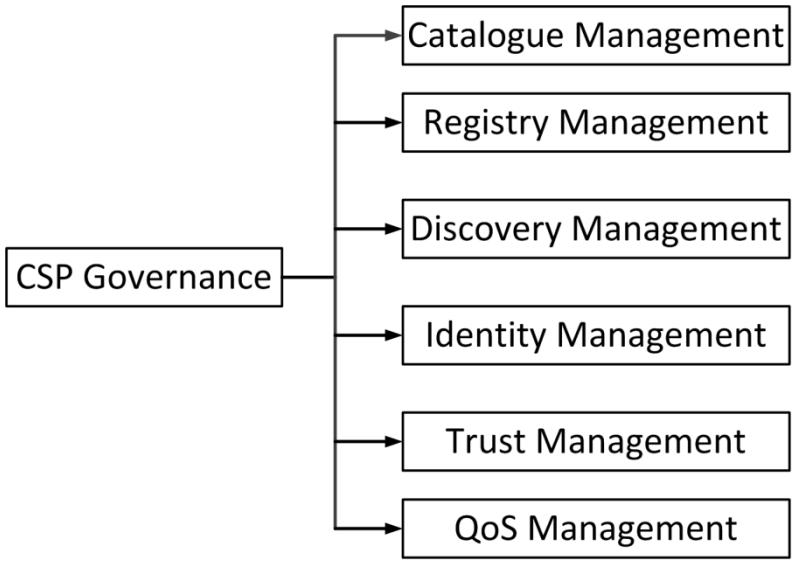

Fig 4: reTHINK functional architecture

reTHINK Call flow scenario

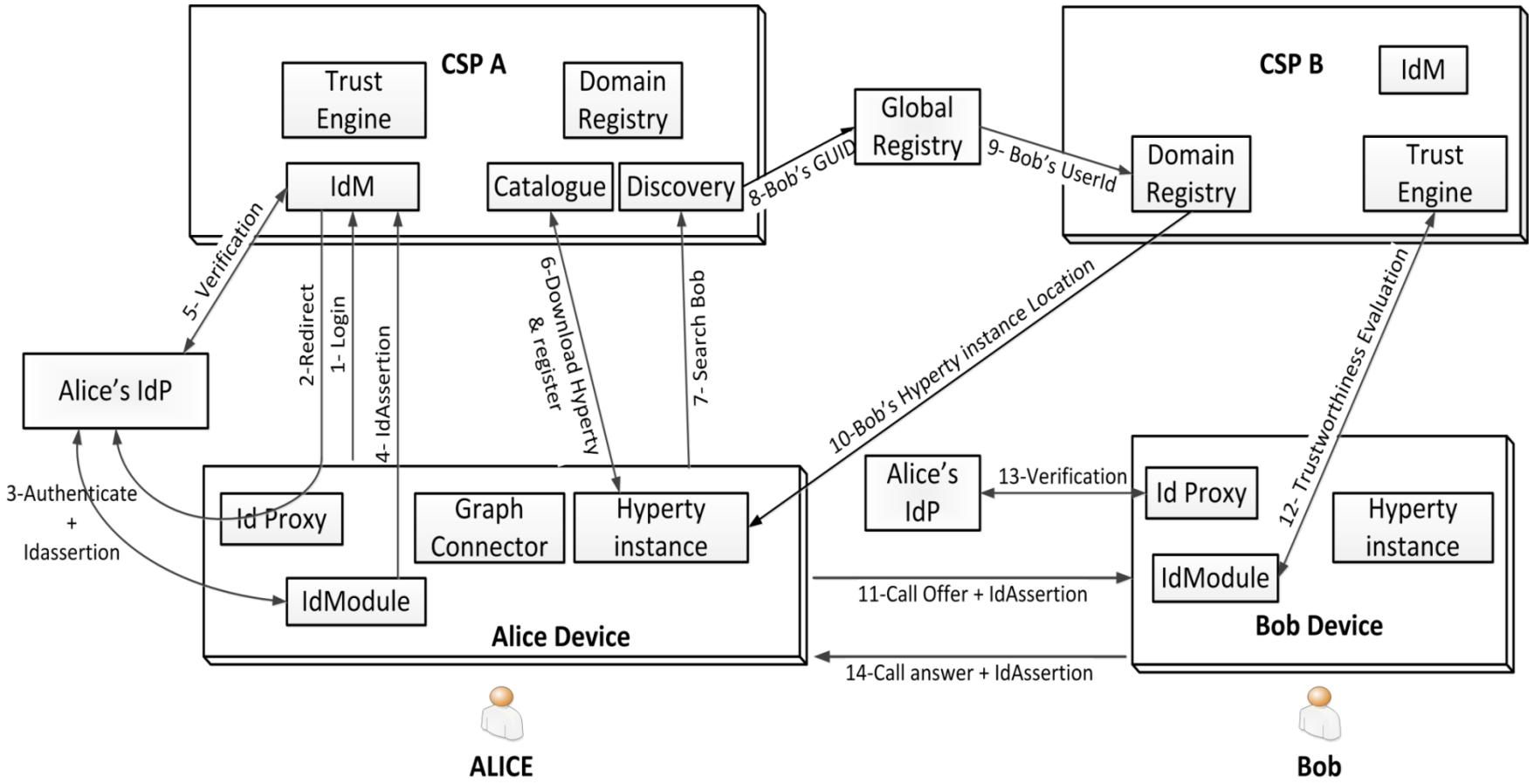

Fig 4: reTHINK call flow sequence

Conclusion

- The reTHINK framework allows endpoints to become a mesh of live hyperties to allow communication in a P2P fashion
- The framework includes directory services (registry, catalogue etc) and the use of two identifiers for locating and connecting to hyperty instances running in end user devices
- This paper explores
  - Peering identity
  - User registry and discovery
  - Social graph based facility
  - Trust engine
  - Governance of the edge based processing

Thank you!

TELECOM SudParis