

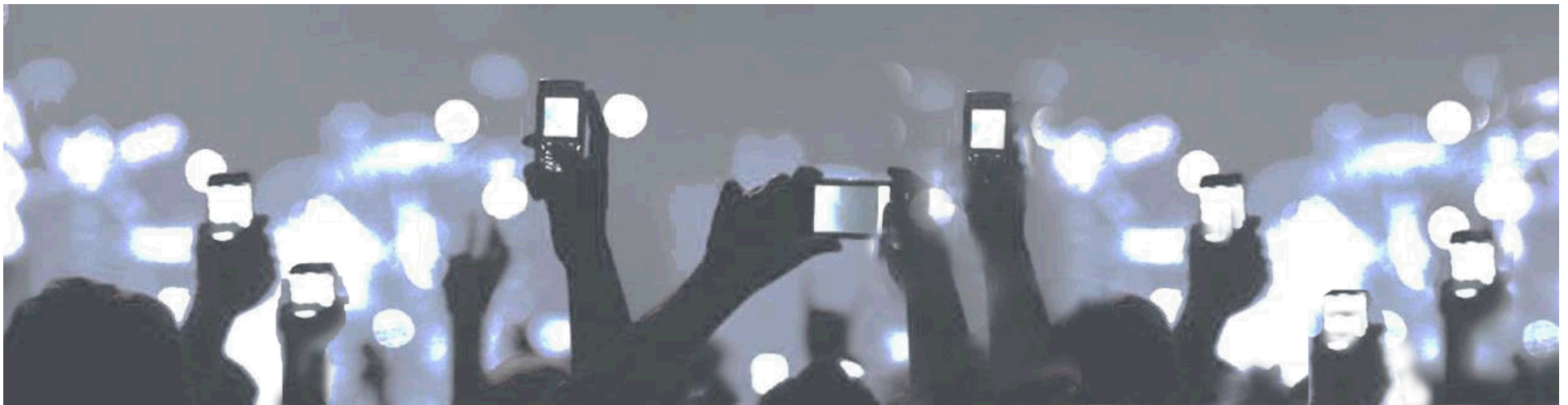


Trustful hyper-linked entities in dynamic networks

reTHINK / 5G

Open Portable Trusted Identity for Services

JM Crom, Orange
Brussels, April 6th 2016





reTHINK positioning within 5G



➤ Web-centric approach to design 5G Service Architecture

- In the context of 5G being a *holistic end-to-end network infrastructure*, reTHINK project results are relevant for end-to-end service delivery and thus are very likely to impact and be impacted by architectural decisions

➤ Web Identity management for 5G transformation

- One focus of the reTHINK work is the design and development of security and portability features, relying on trusted third party *user-selected identity providers*.
- The emphasis on identity management and the expected impact on convergent, multi operator services relying on trusted identity providers, suggests that the result are of significant importance in the context of the future 5G infrastructure.



reTHINK Identity in 5G



- Identity for the Internet of Everything
 - connecting human beings, digital services & things
 - reconciling 2 faces of identity: authentication and reachability

- user-centric approach
 - for choice of identity of service, etc.
 - trust information for better empowerment
 - distributed architecture: close to the user

- will be demonstrated in several scenarios
 - Enterprise Conversational
 - Smart Contextual Assistance
 - My City



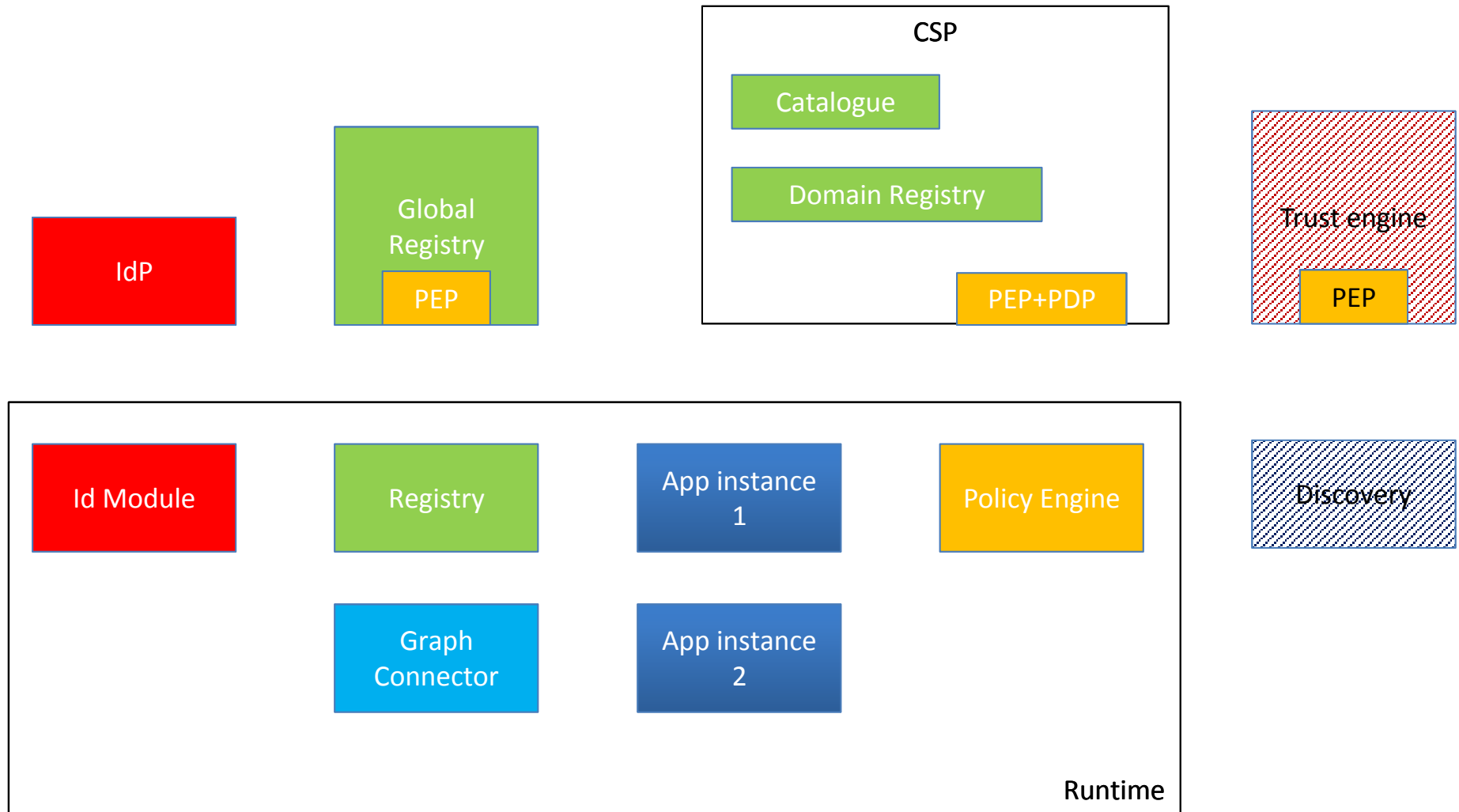
reTHINK Global Identity and Reachability Framework



- 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 service providers
 - use of Independent Identity Provider (IdP)
- Globally searchable
 - across any domain
- Trust-enhanced identity features
 - IdP-certified identity
 - complemented by Trust Engine



reTHINK Support services: the big picture





reTHINK components



- **Registry**
 - to guarantee portable reachability (i.e. independently of IdP/CSP choice)
 - GUID (Global User Identifier) as a portable reachability address
 - generated and under control of the user
 - Global Registry to associate GUID to registered CSPs
 - Domain Registry at each CSP to manage live service sessions (hyperty instances)
- **Catalogue**
 - for CSP to manage available services (hyperties)
- **Discovery Service**
 - to provide multi-domain search engine for users and things
- **Graph Connector**
 - to provide an address book and to build a distributed social network
 - to generate and/or store GUIDs
- **Identity Module & Identity Provider**
 - to authenticate users and provide identity tokens for peers
 - to check identity tokens
- **Trust Engine**
 - to evaluate trust value of a conversational session
 - to provide trustworthiness to end-users
- **Policy Engine**
 - to apply security policies on the client runtime and an CSP side



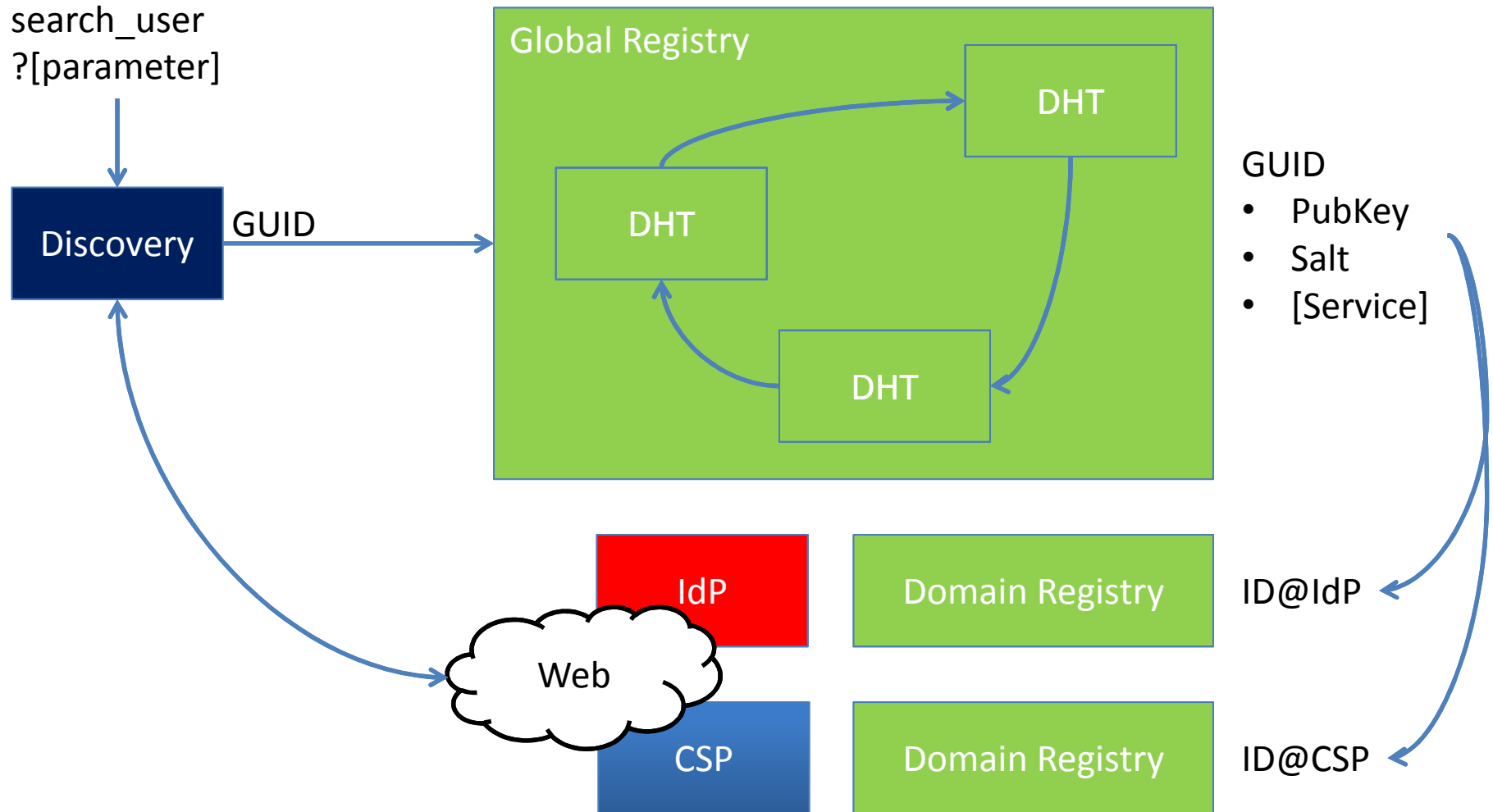
Portability & Reachability



- A global user-managed identifier
 - spans across multiple domain
 - created by the user
 - associated with domain accounts (IdPs & CSPs)
- published in a distributed Global Registry
 - on top of which discovery services may be built
- used as the seed of a distributed social network
 - implemented through GraphConnector



Portability: Registry & Discovery





Identity & Trust



- user control his identity through local Identity Module
 - chooses his Identity Provider to authenticate himself and get identity tokens for peers
 - also checks received identity tokens
- 2 basic trust modules
 - authentication validation: checks a given identity token against the issuing IdP and provides an indicator, that the identity is authenticated or not

| anonymous | not authenticated | authenticated | trusted |
|-------------------------|--------------------------|--------------------------|---|
| no identifier displayed | any identifier displayed | identifier authenticated | identifier is authenticated and trusted |
| — — | ✓ 🔒 | ✓ 🔒 | ✓ 🔒 |

- white-/black-list: indicates whether the given identity is already known for good or malicious behaviour
- should be extensible to innovative features
 - calculations based upon social relationships
 - based upon GraphConnector: a distributed, qualitative/quantitative-weighted social network that takes care of “like” 👍 and “dislike” 👎
 - usage of specific policies



reTHINK for 5G



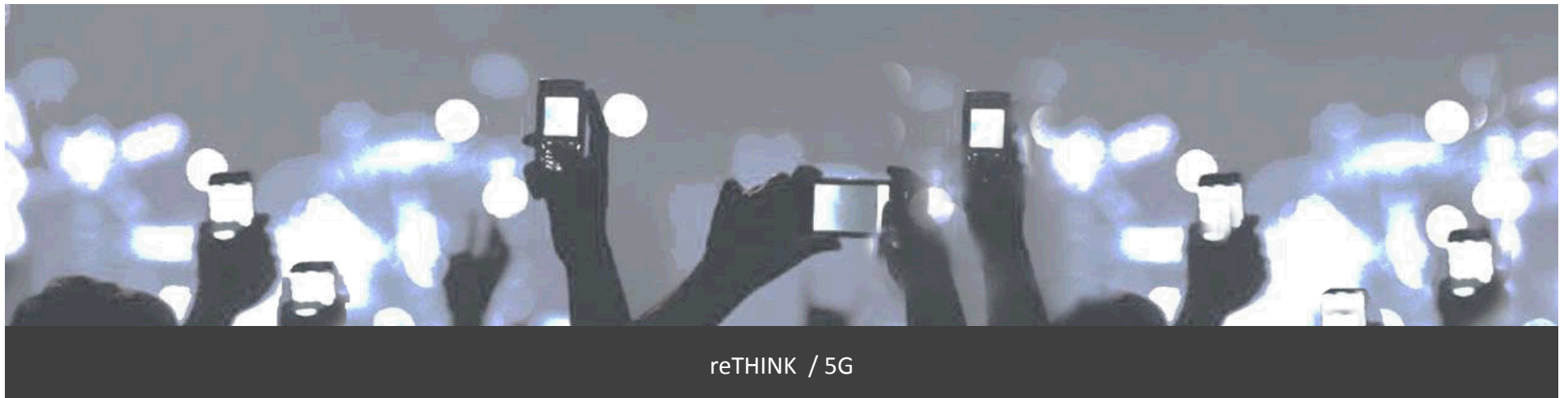
- reTHINK envisions to overcome the main challenges of traditional Telco and OTT models by providing a new web centric P2P architecture
- reTHINK devolves the communication session management to the endpoint

- The aim of reTHINK identity & reachability framework is to have
 - Non-service-bound Identities
 - Cross domain interoperability
 - Globally searchable and reachability
 - Portability
- This is achieved using a set of specialized components (support services)
 - Identity & Trust management
 - Directory services
 - Graph connector
 - Policy & governance



Thank You!

jeanmichel.crom@orange.com





Changing the DNA of Telcos and Webcos



A new GENOME: Good Enough Network of Moving Endpoints

- It is a change of DNA for Telcos
 - Position services between VoLTE and VoIP
 - Unlicensed, non-territorial, quick to launch
 - Independent identities
 - Adopt 'Good Enough' QoS service
 - Accept 3rd party software downloads to devices
- It is a change of DNA for Webcos
 - Independent identities
 - Interworking with non-subscribers
 - Collaborative QoS routing with SLA

