Open mustard seed

Patrick Deegan, Ph.D.
ID3

ID3
idcubed.org

OpenSocial FSN (draft) August 8, 2013

Open Mustard Seed (OMS) Introduction

- The OMS Trustworthy Compute Framework (TCF) extends the core functionality of Personal Data Stores, in the form of RESTful APIs to provide:
  - Federated, single-sign on for a user's devices and clients via OpenID Connect- system managed identity provider
  - User, persona, group (identity) management
  - Data access control and sharing
  - On-demand compute resources for data analysis and real-time feedback
  - Infrastructure deployment and management
    - VM provisioning
    - Framework bootstrapping
    - Portals, Applications, e.g. Ride Share

Goals of OMS

- integrate group-based functionality and access-control
- Provide developer and user support for powerful identity management
  - Implementation of ‘personas’ follows The Jericho Forum’s Identity, Entitlement & Access Management (IdEA) Commandments.
  - A Group for a particular App instance are defined as a set of personas
  - Group is built when another user accepts a valid invitation to join
  - Acceptance initiates automatic deployment of necessary APIs and persona “registrations” in each others respective Identity Provider

Enabling Trust

- Trusted Application Bundles (TAB) contain instructions for how to deploy and maintain applications and further include provisions for enforcing:
  - What data is collected, accessed, stored, logged, etc.
  - The policies and access control mechanisms by which this data is protected
  - How groups are formed, governed, managed, and evolved
  - How users interact and share information
  - Hosted front-end web client deployment

Personas

- Regulatory compliance
  - Verifiable pseudonym – when relying party presents sufficient conditions/claims, attributes that can attest to specific truths about the identity of the individual can be unlocked
  - Anonymous is ‘base’ persona, augmented by attributes, either 3rd party or internally verified
  - All tied back to core identity
  - Cannot re-link back to core identity

Motivation: Identity

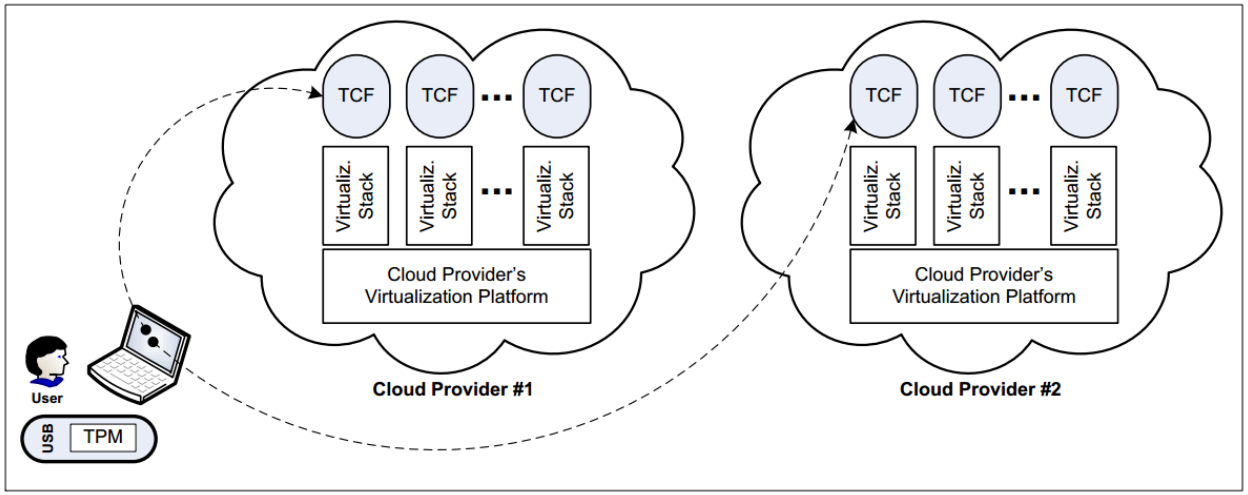
- You don’t know who you’re talking to
  - Authenticate everyone’s identity (OpenID Connect)
- It is presently difficult to trust people you may not “know”, especially when they present claims/attributes
  - Rely on trusted 3rd parties for verification
  - System maintains trust metrics
- It is presently difficult to administer and maintain secure password policies for people in systems that implement permission based access control on shared resources
  - Provide organic authentication via collected data that doesn’t require any human in the loop to administer and maintain policy (biometric, etc.)

Motivation: Private Resources

- People have highly sensitive data that are difficult to share and protect
  - Personal Data Stores are mapped to APIs that Encapsulate access control as defined by deployable Application Bundles
- It is presently difficult to federate or provide access to private resources from the user's perspective
  - Only share specific things under certain conditions to certain people, determined a priori via developer specifications in TAB
- It is presently difficult to federate or provide access to private resources from the site administrators perspective
  - Provide zero-knowledge solution from site administrators perspective, total user control

Virtualization Reality

- Enabling participants to “manage” such a distributed system, in a realistic way, requires a system with low coordination costs
- Trusted Compute Cells (TCCs)
  - Personal, Portal, and Group types
  - Meet TCF specifications (packaged to allow code signing, etc.)
  - Deployed in a scalable manner or shut down as needed



App Deployment Pattern

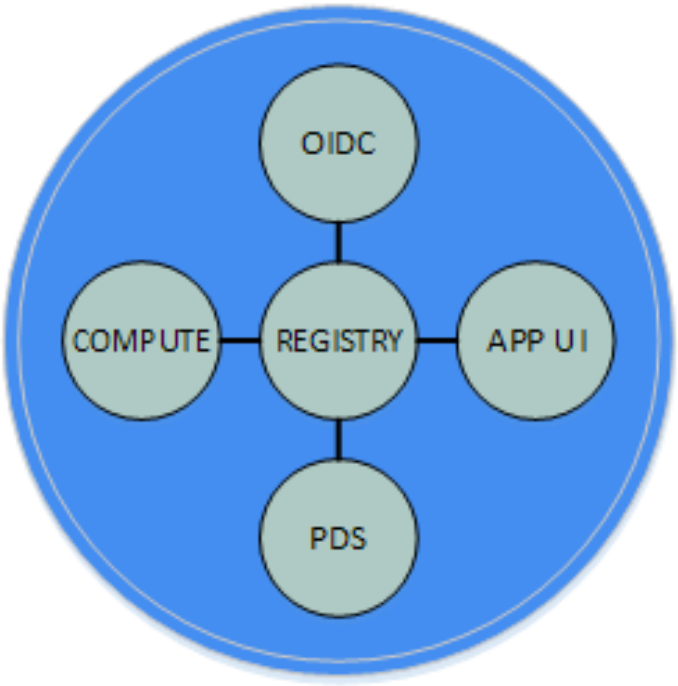
- Each user automatically setup by admin initiated, zero-knowledge deployment scripts.
- These create VM(s) and provision them with OMS core functionality and some admin selected set of apps
- User has complete transparency and control over data sharing policies and application agreements- opt in/opt out enforced by OMS
- Apps are essentially APIs to RESTful resources (OpenID Connect + General Purpose Access Control Engine)

Access Control

- First line of defense is that client must present a valid token
  - Tokens are granted to clients for which the user has successfully authenticated and granted, via attributes on a persona, certain access to particular scopes
  - The *client_id* and *Scopes* (sets of APIs) are predefined by the developer
- OMS middleware allows business/legal/technical policies to be codified
  - Integrated and executed after successful token validation via developer support for rule engine policy expression
  - Policies can chose from set of “Transfer functions” that are automatically applied to request- whether standard CRUD or developer defined action.

Trusted Compute Cell

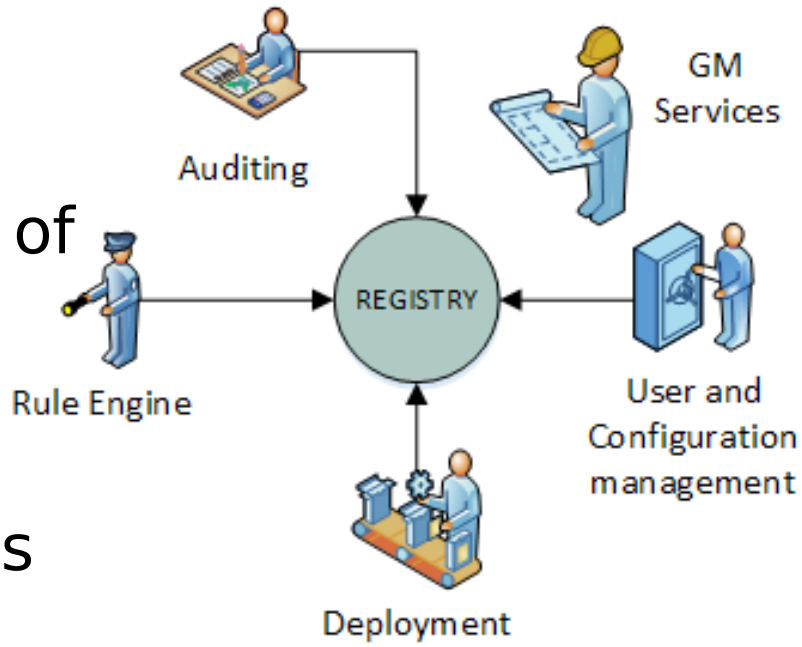
- Each TCC cell is composed of several virtual resource applications
  - OpenID Connect Server
  - (sub)Network of compute resources
  - Deployment of Web Application(s) and hosting environments
  - Personal Data Store



Network of Virtual Resources under control of Registry

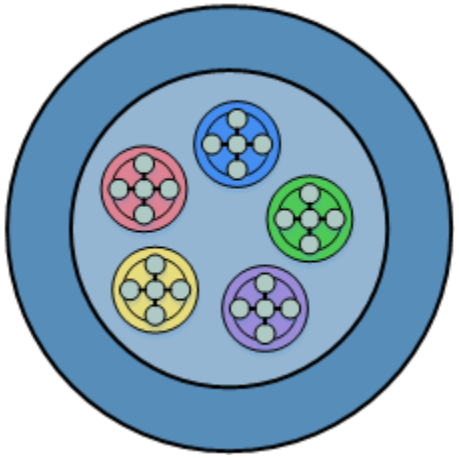
Registry as the hub

- Core functionality is provided by framework libraries
- Securely coupled network of services
- Governance Manifest ‘workers’ make sure that integrity of compute unit is maintained



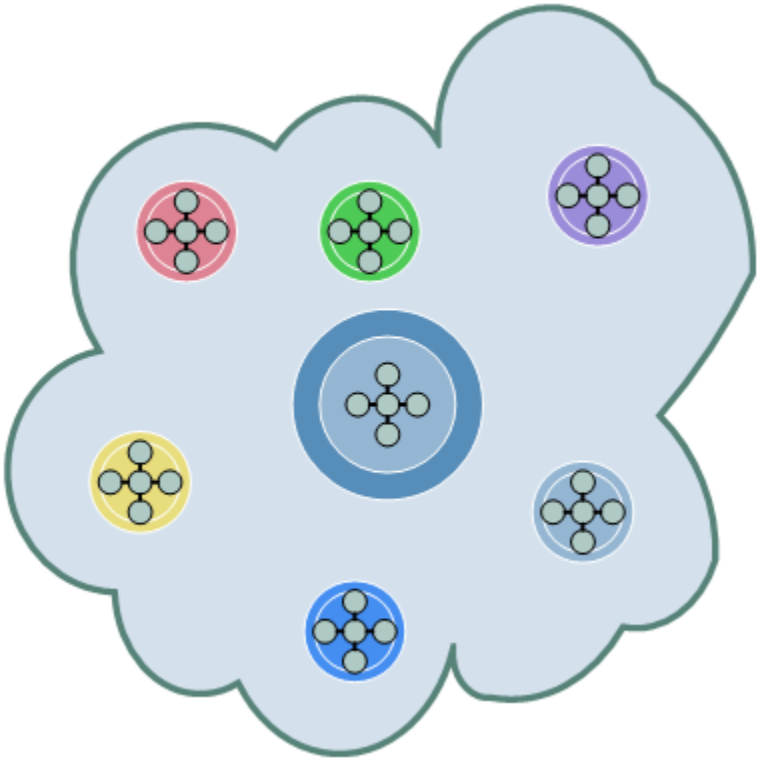
Trusted Compute Cell - Private

- Personalized hub for each user's visibility into:
  - the curation of their personas
  - the social scenes they belong to
  - the private registry for the data that they collect, produce, manage, and distribute
  - the applications they have deployed to further enable groups of people to securely communicate, share resources and generally interact



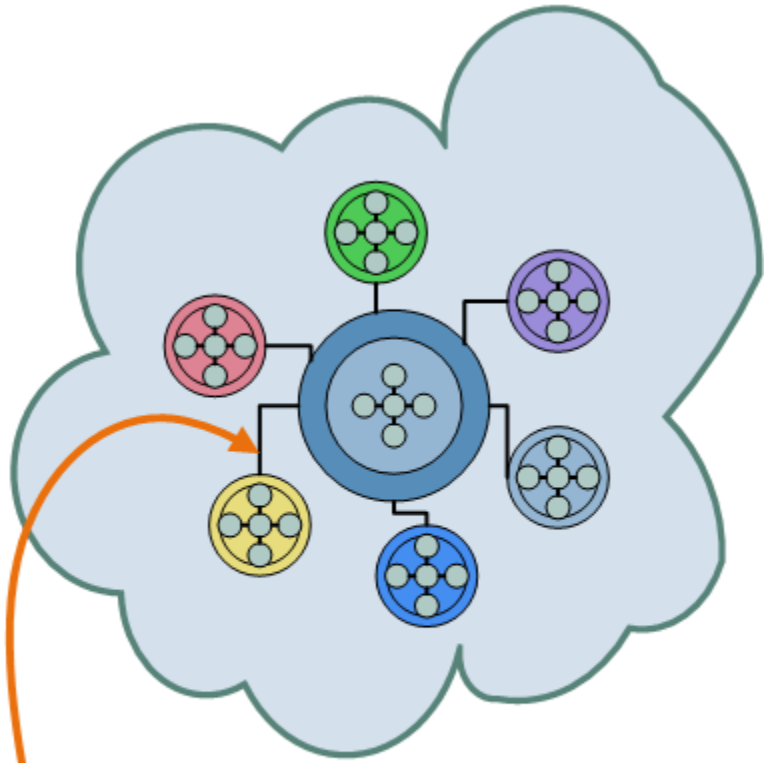
Trusted Compute Cell - Portal

- Users begin by registering one of their personas via
  - Native app or
  - Web portal
- If they don’t already have a Private TCC, one is created for them
  - Bootstrap virtual resource into OMS
  - deploy a ‘private TCC’ seed TAB
- Virtual Resource origins include
  - user owned
  - portal managed/provided



TCC – Portal Registration

- A ‘portal TCC’ seed TAB is automatically deployed after registration and affords members the privileges outlined in their opt-in agreement, minimally:
  - view other users
  - Install sanctioned TWMs/Apps
  - Invite other members to join groups

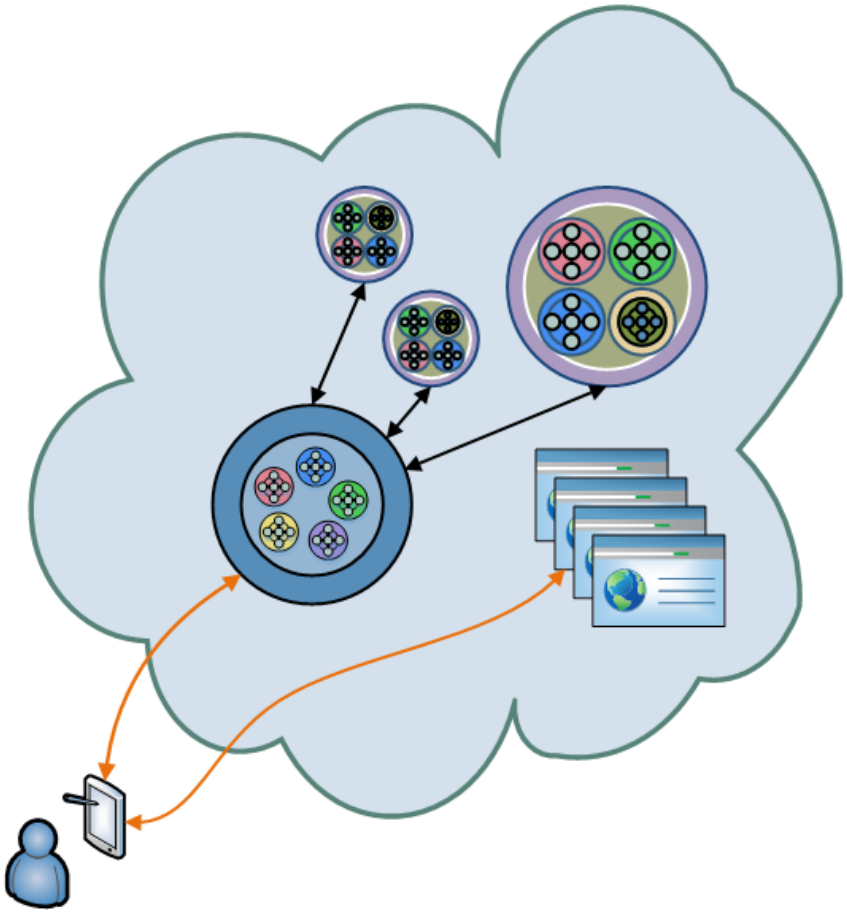


Expanding Engagement via Groups

- The “Branded” Portal TCC is a Trust Provider and acts as the central repository for:
  - Trusted Application Bundles for deploying social, secure, cloud based applications in the form of enforceable specifications into a user's Private TCC
  - Persona Directories providing scene members with services to locate and interact with other users that they can invite to circles, forming groups of users that are securely tied to particular instances of deployed TABs in the context of the Trust Provider

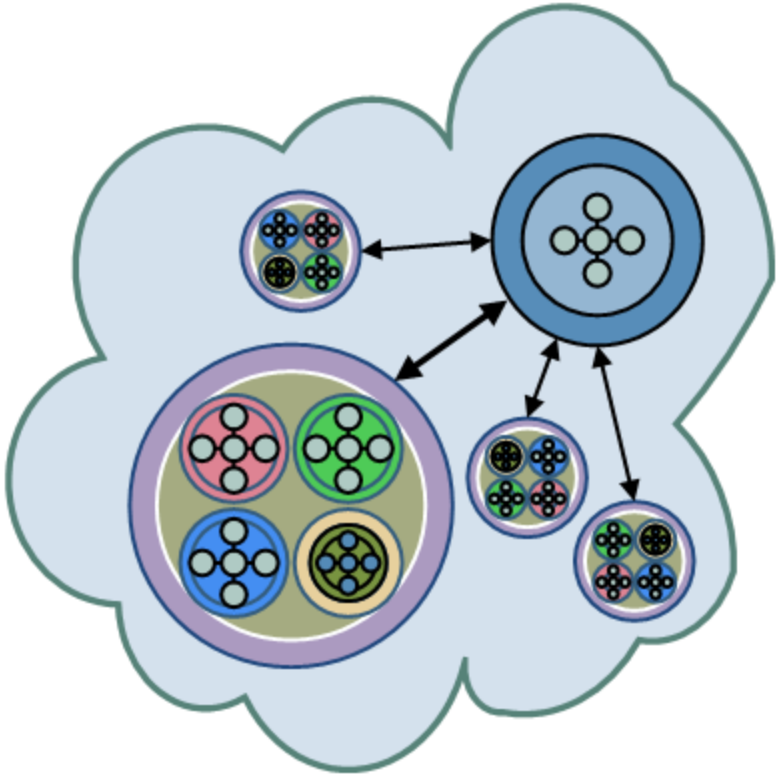
Users: Participate in groups

- User interacts with
  - Private Dashboard
  - Group features
  - Web Applications
- From a users perspective, they belong to many groups that benefit from the flow and sharing of their data



Organizations: Conduct Research Studies

- Analytics to discover different affinities, preferences, habits, etc.
- From perspective of developer/service provider the group cells provide
  - Sources of Data
  - Closure around high affinity social norms/profiles
  - New opportunities for direct and indirect collaboration (realizing low coordination costs) via exchanges, offers, markets, etc.



Communities: Form groups around contextual affinities

- Users can dynamically join groups
  - Attach to sensors in the real world
  - Interact with other users via TAB interoperability
  - Collectively manage shared resources
  - Coordinate via Governance Mechanisms