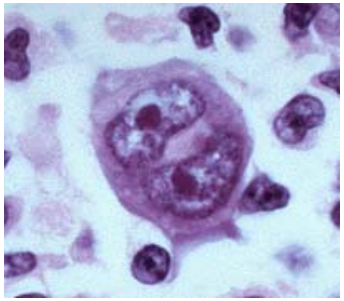
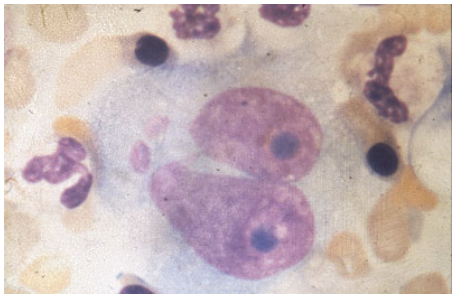
Marlin B. Pohlman

Chief Architect, Protected Enterprise
Technology Business Unit
Oracle Corporation





BC Public Sector

An Oncological

approach to Identity Management:

And Service Oriented Architectures in the public sector

In computer science, context is the circumstances under which a device (resource) is being used.

- Wikipedia

Why are we here?

Paix odre et bon gouvernment

(Peace, Order & G[illegible])

- We are here to define Identity in the [illegible] of "good government" in accord with the 1867 Constitution Act section 92(13)

*[illegible] Act is often referred to as *British North America Act* of 1867

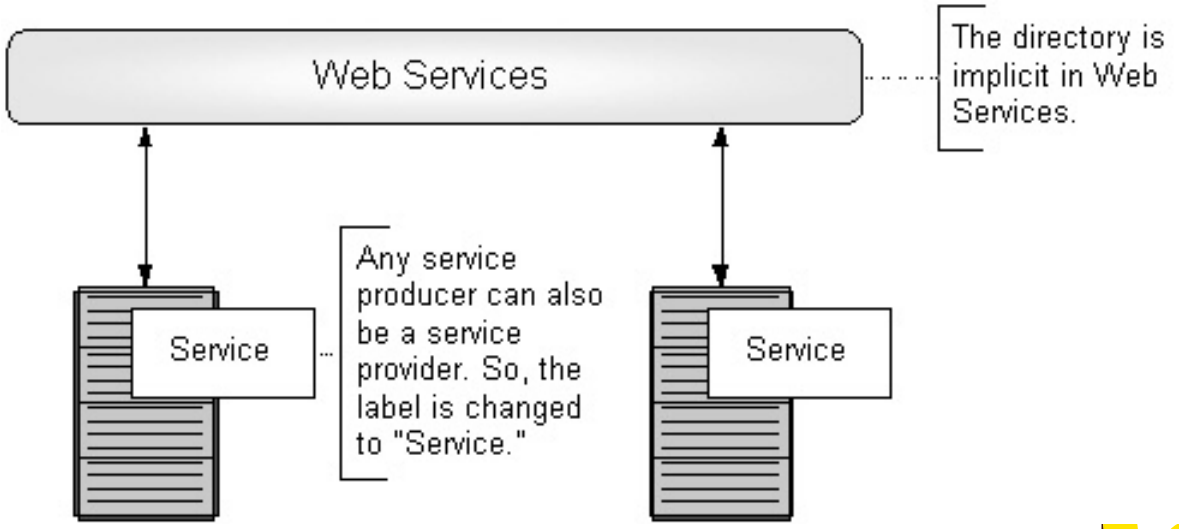
Appropriate Architecture

What "should" we do

How do we get there from here

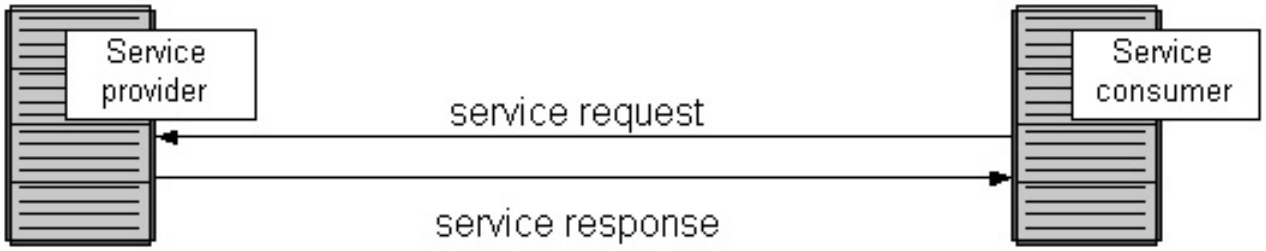
For BC Employees

For BC Citizens 92(13)



It all about Providi

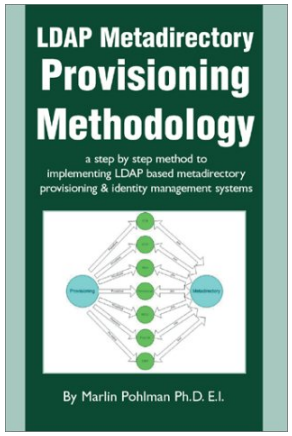
Behavior Patterns in Context

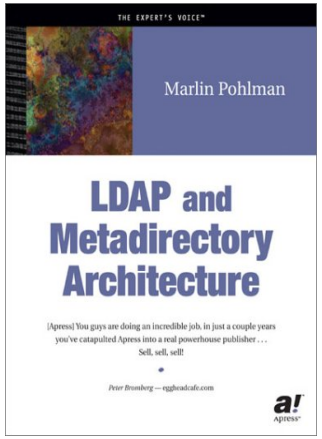


Ide provides that Context


Identity = Assertion + Certification
What I say about myself
What others say about me

An Example of a Self Assertion



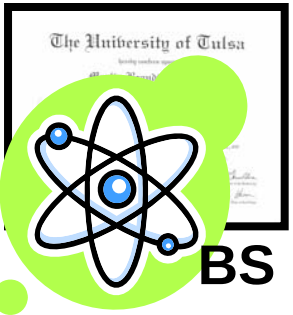


Marlin Pohlman

Ph.D., EI, SSP, CISA

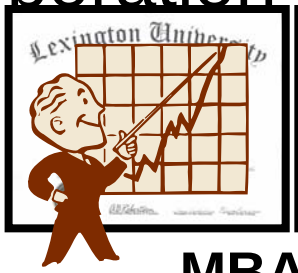
cal Director ogy Busine

Oracle Corporation

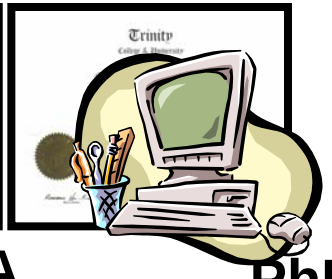


BS

EI



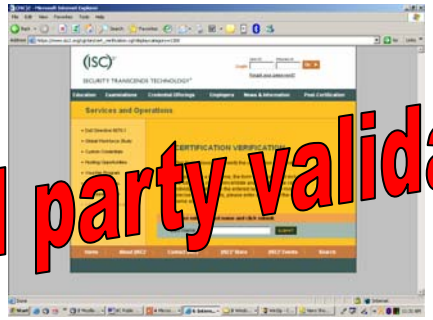
MBA

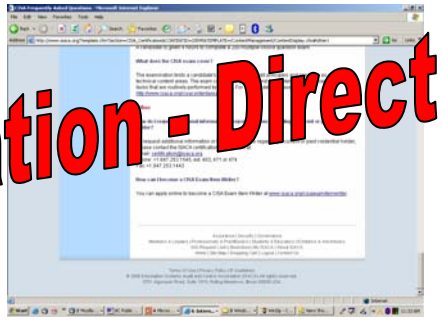


PhD

How do you Certify this to be true

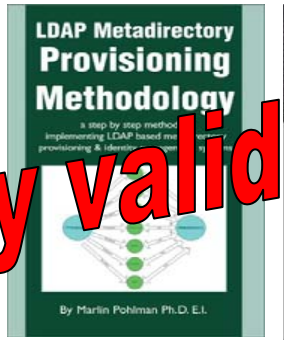
Surrender of Tokens in Owner's Possession - Indirect Certification

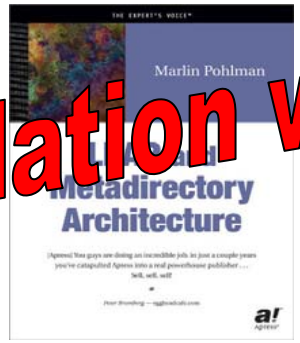




Tokenless 3rd party validation - Direct Certification

User Centric Reputation System





Tokened 3rd party validation with Context

But the best way is

Observe Behavior

Document History

Analyse Assertions

Knowledge via consistency

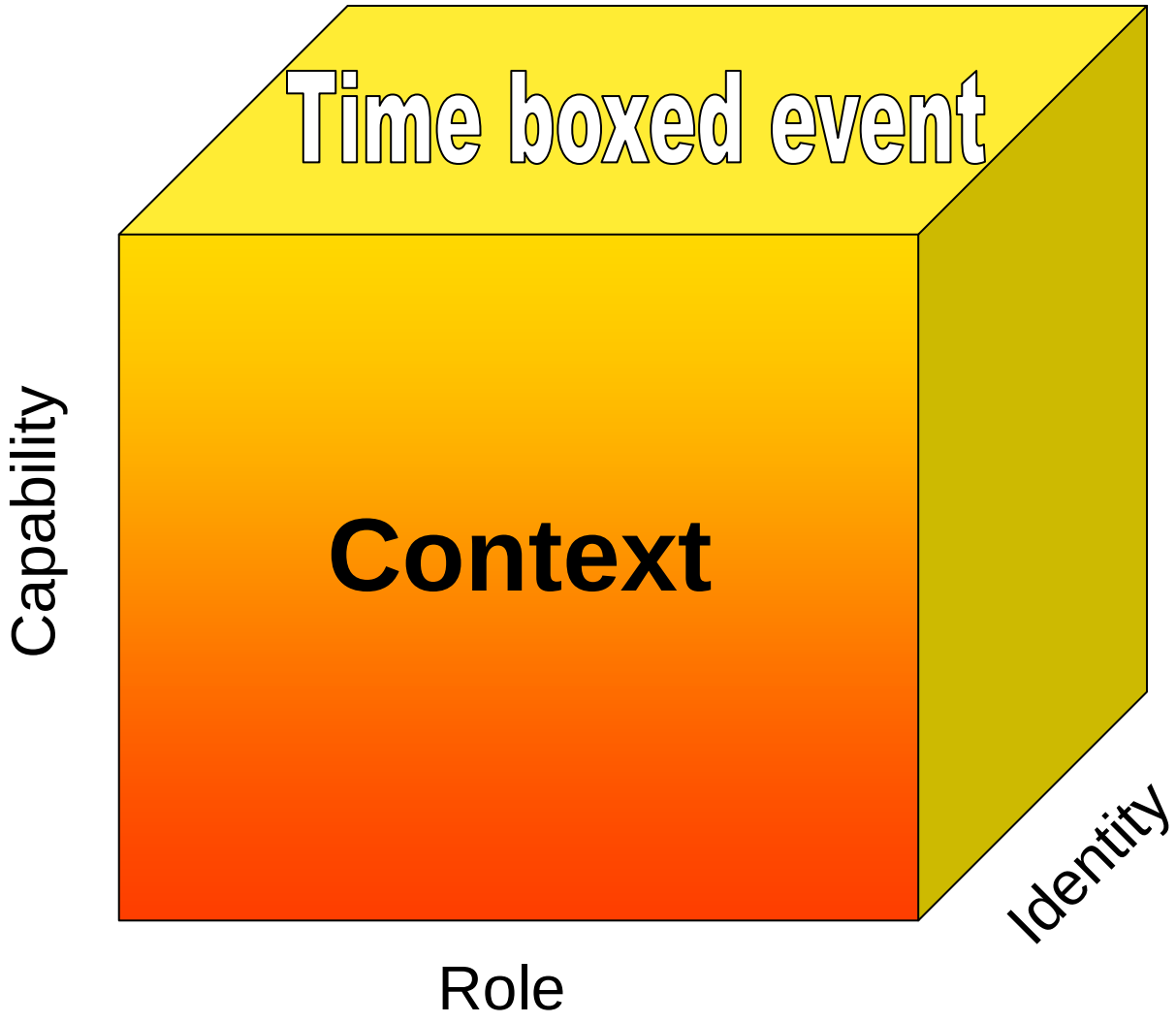
Action vs. Assertion

Profile and Anticipate Future Behavior

Knowledge of a person depends on context

What is Context?

Actions & Motivations


Time boxed event
Context
Capability
Role
Identity

Context in a Service Orientation or Society

- What [illegible] be gained
- How are those privileges to be [illegible]
- What is the [illegible] requirement to Certify that Assertion is true
- What is the [illegible] to the Service Provider community as a result of the validation process

Exchange of information for privilege

Validation of the information exchanged

Resource Cost for Identity Validation

Mitigation of risk as a result of escrow

So what’s left?

Establishing Acceptable Patterns of Use (Behavior) for providers (individuals) who have established Identity Escrow

- For four years I have made both an academic and a personal study of the Identity Management functions of the human body
- From my experience, I have discovered that it is not sufficient for [illegible] systems to [illegible] of [illegible] must be established are acceptable usage patterns (flight plans) that function as an operational checksum on identity in a service context

Epiphany while undergoing treatment of Stage 4 Hodgkin's Lymphoma

- Cells had established “Identity” through self assertion and token validation (B cells)
- In essence my disease was a failure of my own bodily services (CD4 - T cells) to effectively enforce established policies and procedures govering the proper operation of cellular function.
- My body was undergoing a crisis in Identity Management

Natural Immune Systems

- [illegible] depth")
- [illegible] several sub-systems:
  - innate immune system (sca[illegible]
  - [illegible] system (white blood cells which [illegible] to detect and eliminate pathogens / antigens)

Security at every functional level

Multilayered Security Services

Detection and elimination based on patterns

Acquired Immune System

(after a stemcell transplant)

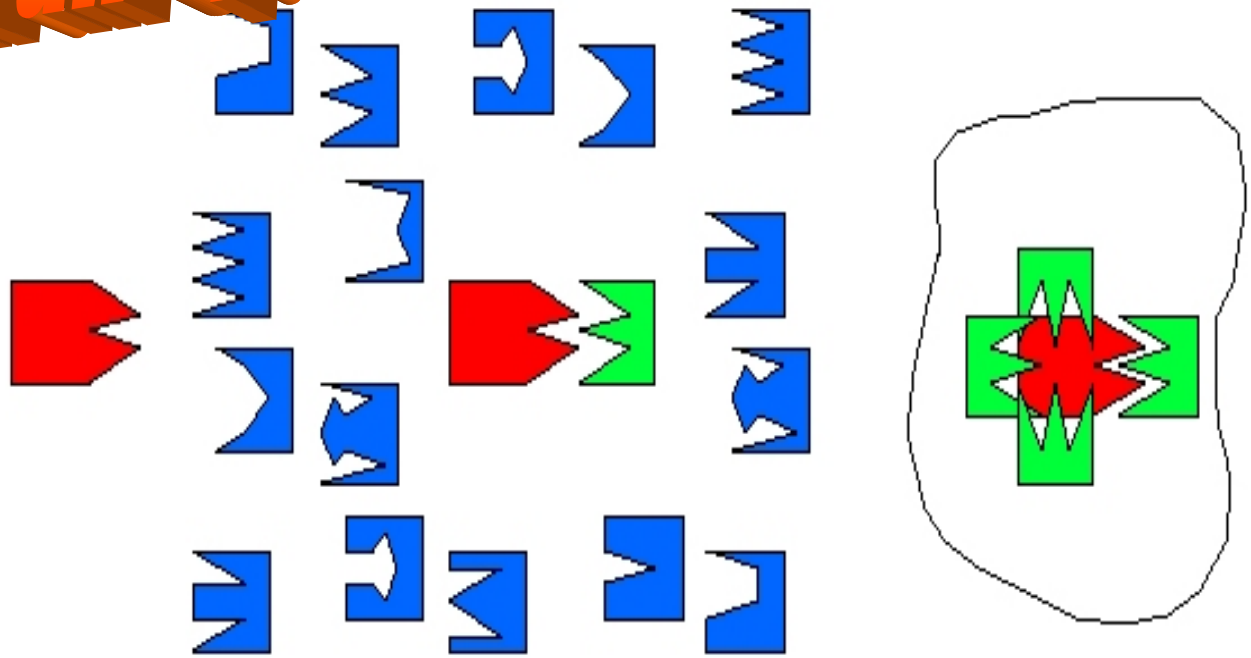
- [illegible] bone marrow (B-[illegible] lymph system but matured in thymus gland (T-cells).
- Self-bindi[illegible] destroyed by [illegible] selection) in thymus.
- B- & remaining T-detectors released to b[illegible] and destroy foreign (n[illegible]s)

Separation of duties

Enforcement based on operational context

Contextualy correct patterns implemented as Security Service

In an open service commons



Transparency enables enforcement

Digital Immune Systems

(aka Intrusion prevention systems)

- Train with known normal behaviour
- Generate behaviour signatures.
- Create (random) initial population of detectors and screen it against database(s)
- Monitor traffic with possibly unknown behaviour (may contain some "foreign" activity).

Apply Business Intelligence

Enforce operational context

Create Common Policy

Digital Immune Systems

(aka Intrusion prevention systems)

- An (approximate) m[illegible] a detector [illegible] indicates a possible [illegible].
- React to (w[illegible]f) t[illegible] h[illegible]y.
- R[illegible]tion of detectors to reflect [illegible]ssful and consistently unsuccessful detectors (cloning / killing).

Detect Anomaly

Act to correct

Reflect & Revise

Digital Immune Systems

(aka Intrusion prevention systems)

- Established approaches are host-based or network-based:
- Host-based systems [illegible] proc[illegible]
- [illegible] are of 2 types:
  - [illegible] traffic analysis using e.g. IP source & destination addresses and IP port / service.
    - Promiscuous mode ‘sniffing’ of IP packets for anomalous behaviour.

Insufficent in SOA context!

Digital Immune Systems

- Security must also be Service based :
- Enforcement via application of predicate logic and encryption at both the data and application
- Use of granular attributes for operational context
- Heuristic policy enforcement leveraging entity transaction pattern analysis
- Take the concept of federation to the next level incorporating aspects of monitoring to model the behavior within Social Networks

Security at every layer

Capabilibility based access control... in addition to RBAC

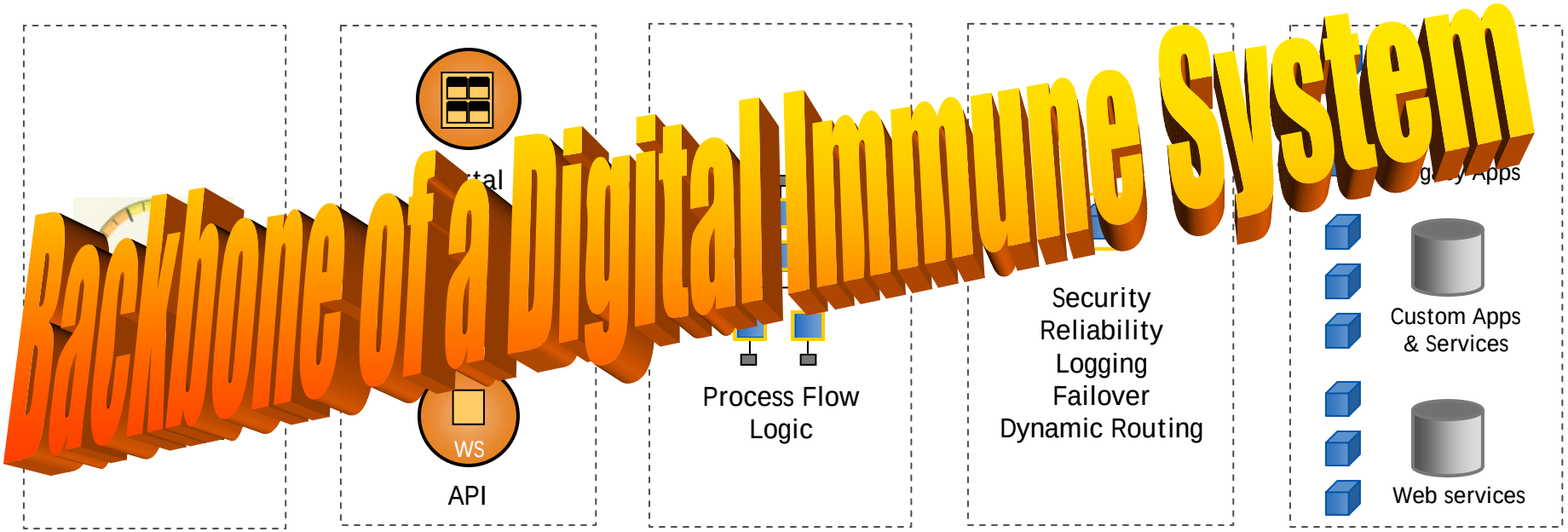
Apply Business Intelligence

Rethink Circle of Trust...adding Context

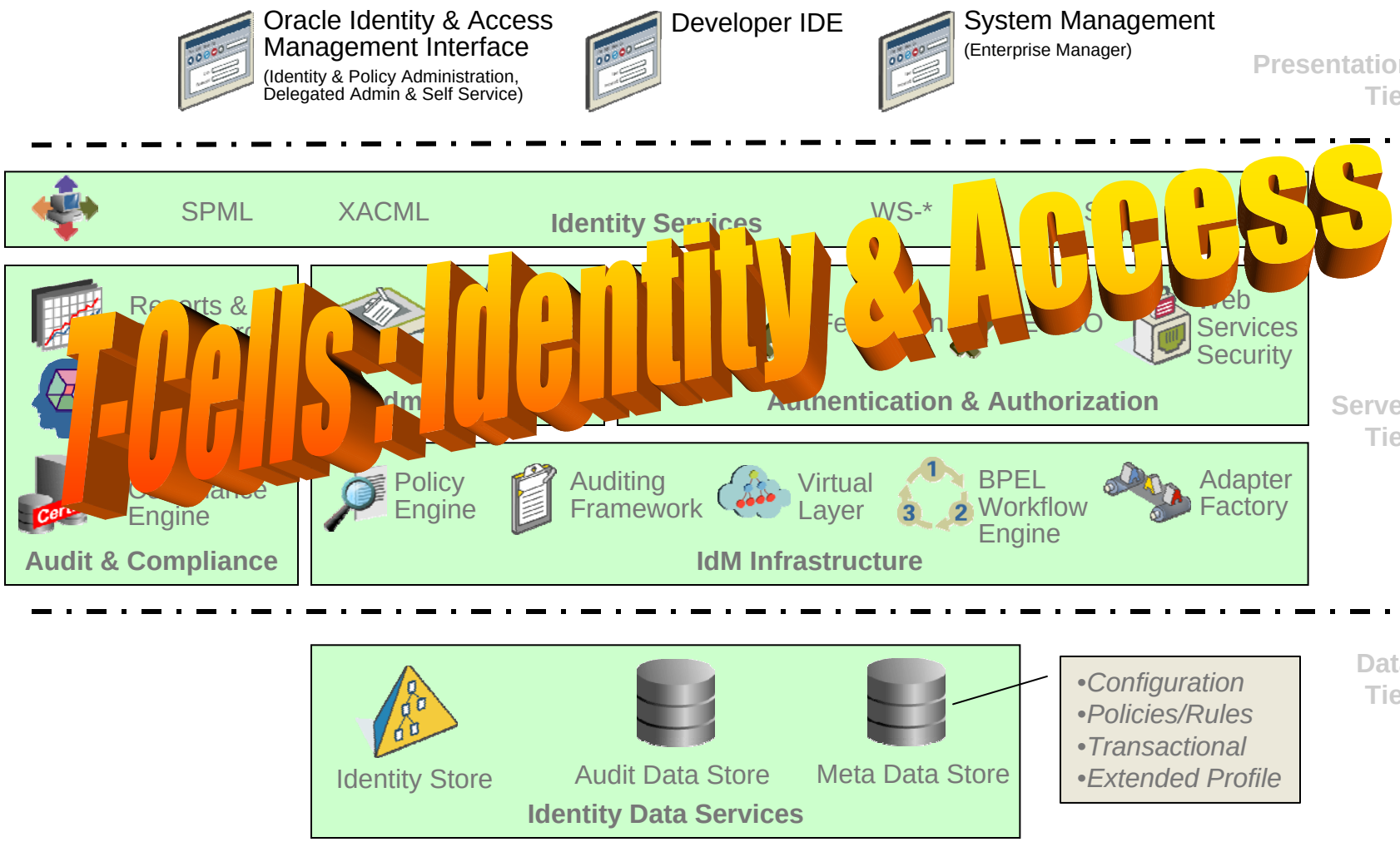
How do we do this

Service Oriented Architecture

Reduce friction, enhance visibility, thrive on change

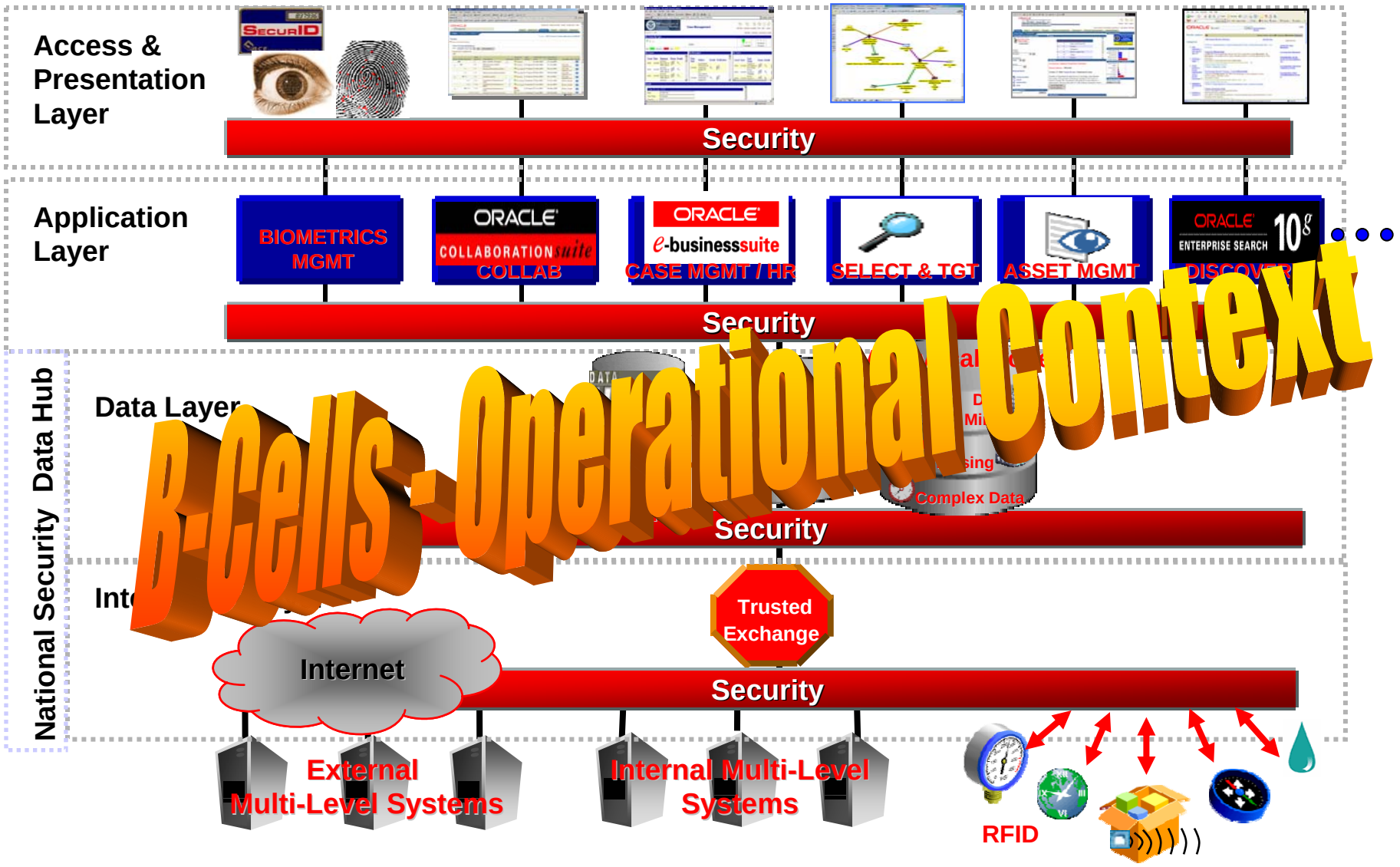


IdM Suite Component Architecture



T-Cells : Identity & Access

PROTECT for National Security Architecture



PROTECT Solutions

PROTECT Focus Areas

PROTECT for National Security	PROTECT for NCO & Warfighting	PROTECT for Justice & Public Safety	PROTECT for Identity	PROTECT for Healthcare

Trusted Information Sharing

PROTECT Business Solutions

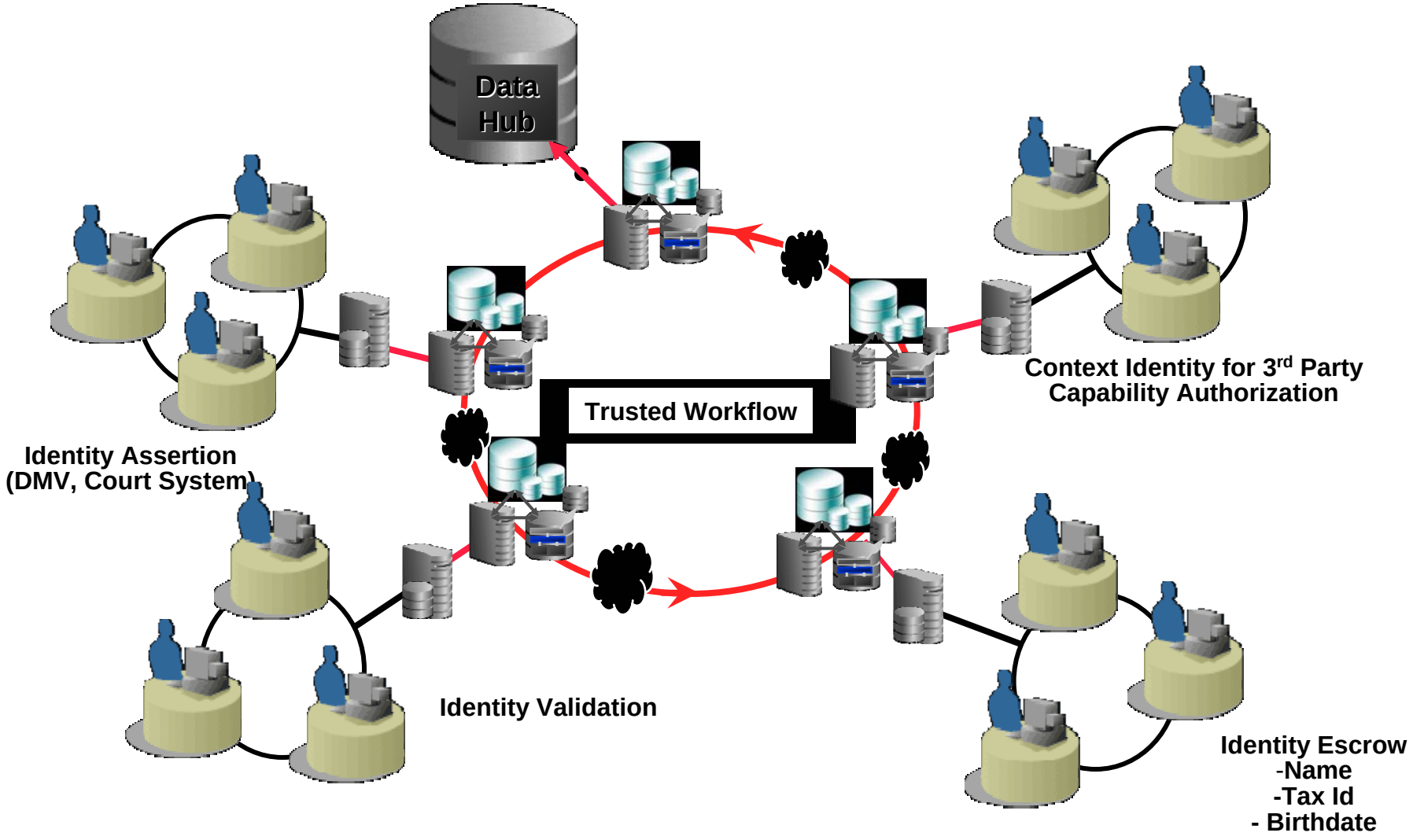
Cross-Domain Info Sharing	Cross-Domain Info Sharing	Regional Crime Fighting		Network (PHIN)
Enterprise Info Discovery				Oracle Health Alert Network (HAN)
Nat & P				
Ca			Oracle Virtual Directory	Oracle Electronic Health Records (EHR)
Co s	Geospatial Battlefield Awareness		Oracle COREid Federation –	
Se Location-Based Services	High Performance Tactical Grid		Oracle Access Manager	
Human Capital Mgmt	Secure Data Auditing		Oracle Internet Directory	
Biometrics Mgmt	Disconnected Operations		BPEL	
Selectivity & Targeting				
National Security Data Hub				

How they work togther


How do we get there from here
for anyone that is still following

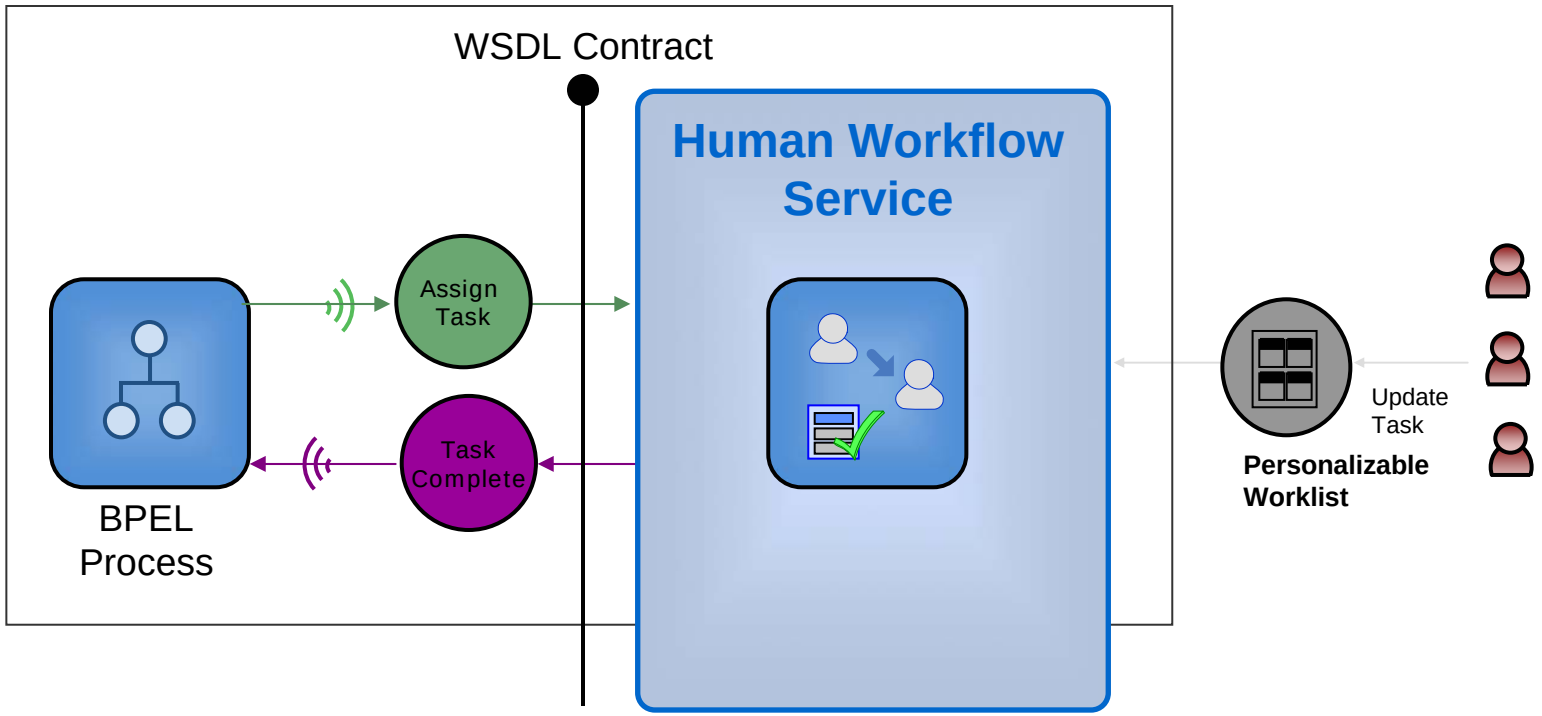
Automate Identity Data Exchange

Create a Trusted SOA Identity Flow



Use BPEL to automate Identity Assertion and Certification

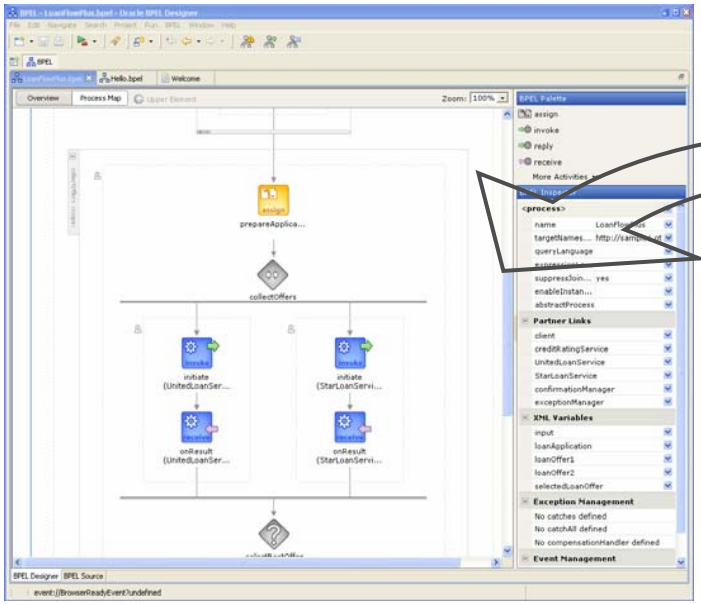
Leverage a Human Workflow Service which interacts with the BPEL engine and has pluggable services and encapsulates Notification, Assignment Service, TaskManager, WorklistManager, Identity Service



(1) assign tasks to a user/role
(2) wait for task completion as part of an end to end process flow

Implement continuous improvement by documenting identity related processes

Leverage BPEL to create a pattern of context for Identity



Patterns of Context

Drop-and-configure

Library of re-usable BPEL Fragments

Order Transform

Approval

fx

Validation Rule

Etc.

Recap

Questions to answer

- What is an appropriate architecture for identity management across the BC Public Sector?
- How does each organization manage its own
- How does each organization manage authentication for the other organizations who also need to access?
- How do we do this?

SOA with Context

Through established BPEL encoded processes : context

Leverage central security Service

Facilitate 3rd party Identity Assertion and Certification

Questions to Answer

- What is a roadmap associated with that
- What would be the steps or phases we would have to move through before we [illegible] point

SOA with Context - Capabilities and Roles

Define the Process & Policies involved

Questions to Answer

- What is the role that the BC Public Service should or could have within the effort to define digital identity given the public sector runs the majority of the processes that [illegible] identity information [illegible] most authoritative [illegible]. Drivers licenses, birth certificates, lawyers, doctors, engineers, architects, accountants, company incorporations, and so on)

Give the Public a mechanism for mitigation of Identity risk

explore an expanded [illegible]

[illegible]ent services

The automation of…

Identity = Assurance + Identification

“SO…

Do you haf any qvestions for my answers?”


Q&A
QUESTIONS
ANSWERS