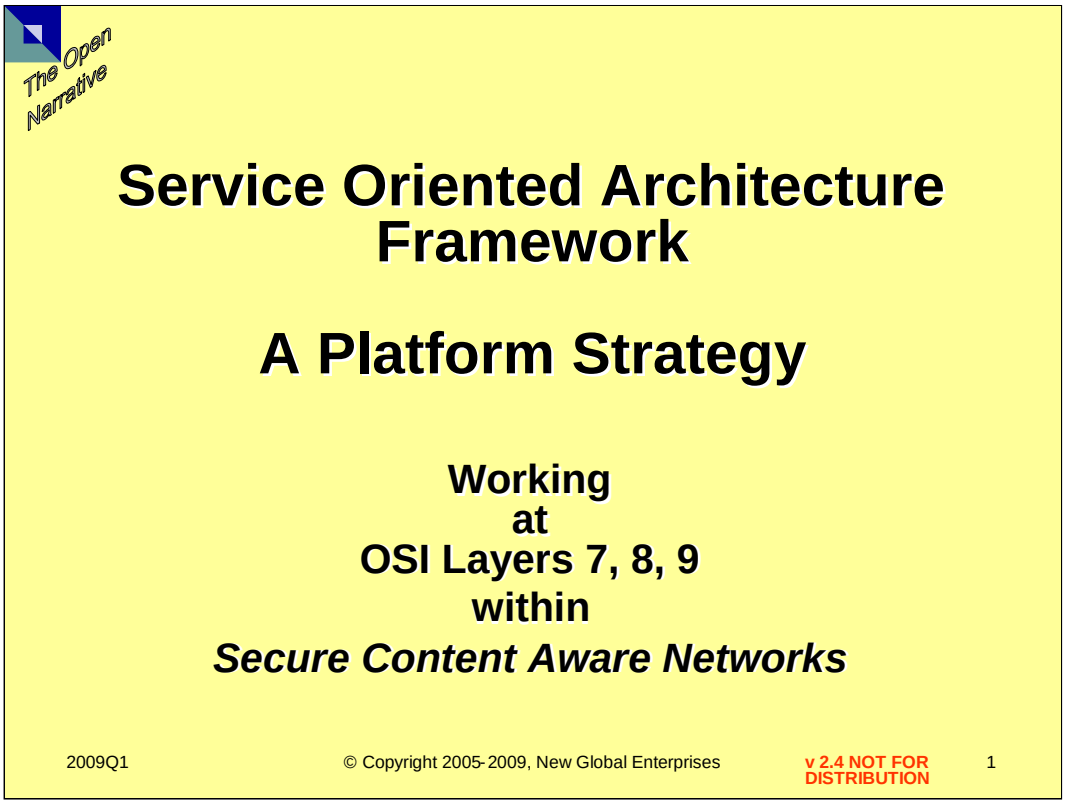


Is it enough to stay at Layer 5 and below where differentiation is based on product superior Commodity.

For one more year perhaps? What after that?

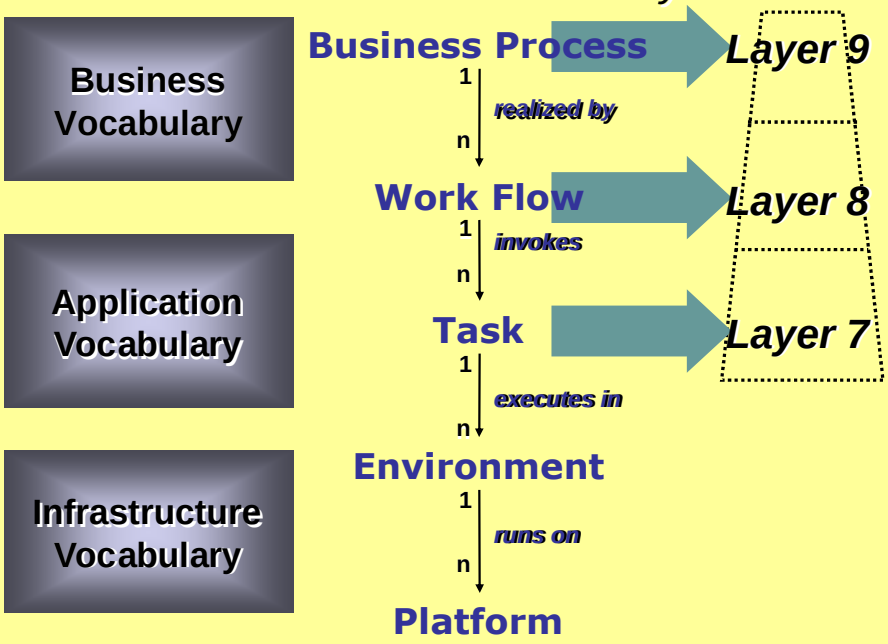
Layer 7: Application

Layer 8: Work Flow

Layer 9: Business Process

What are these “new” OSI Layers?

Answer: Refraction of OSI Layer 7



And Authority Happens.

The Open Narrative

Security Message Categories

Factored Functionality

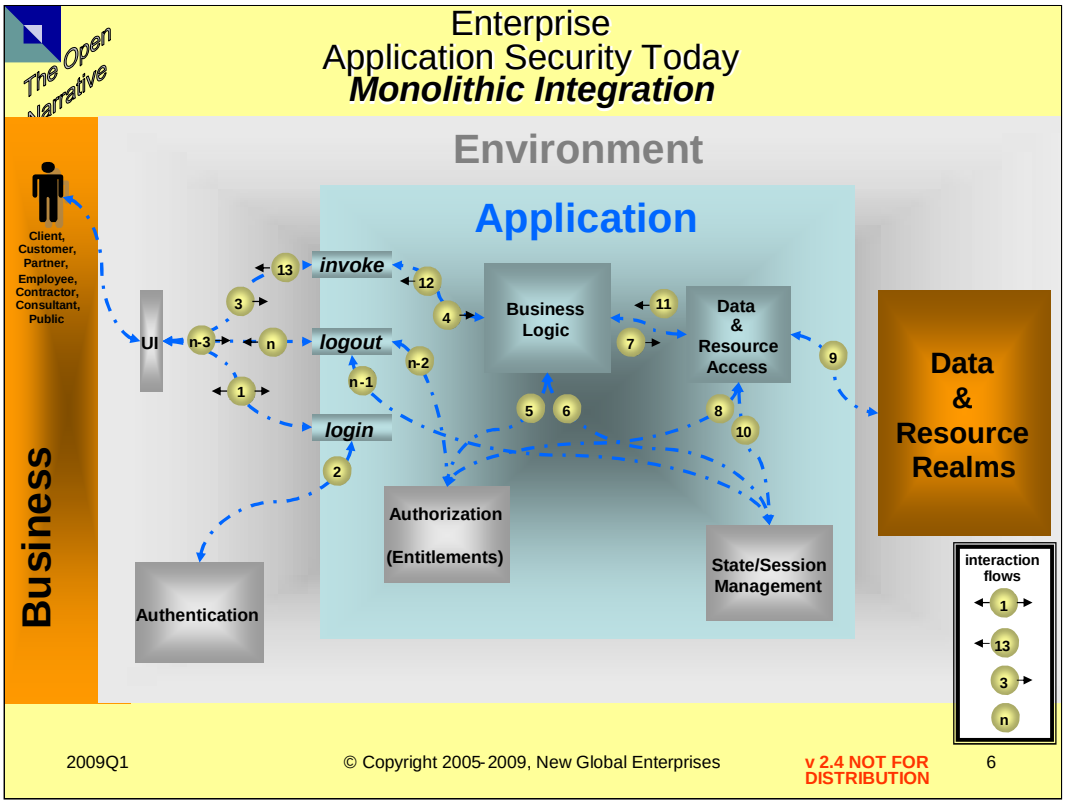
Security Protocols	**Service Invocation (SI)**	**Event Dispatch (ED)**	**Data Distribution (DD)**
Business	***login***	***login***	***login***
Application	***login***	***login***	***login***
	login	***login***	***login***
Infrastructure			

S C A N

e.g., ***login*** plays in every Category

Application Security Example

Factoring today's applications



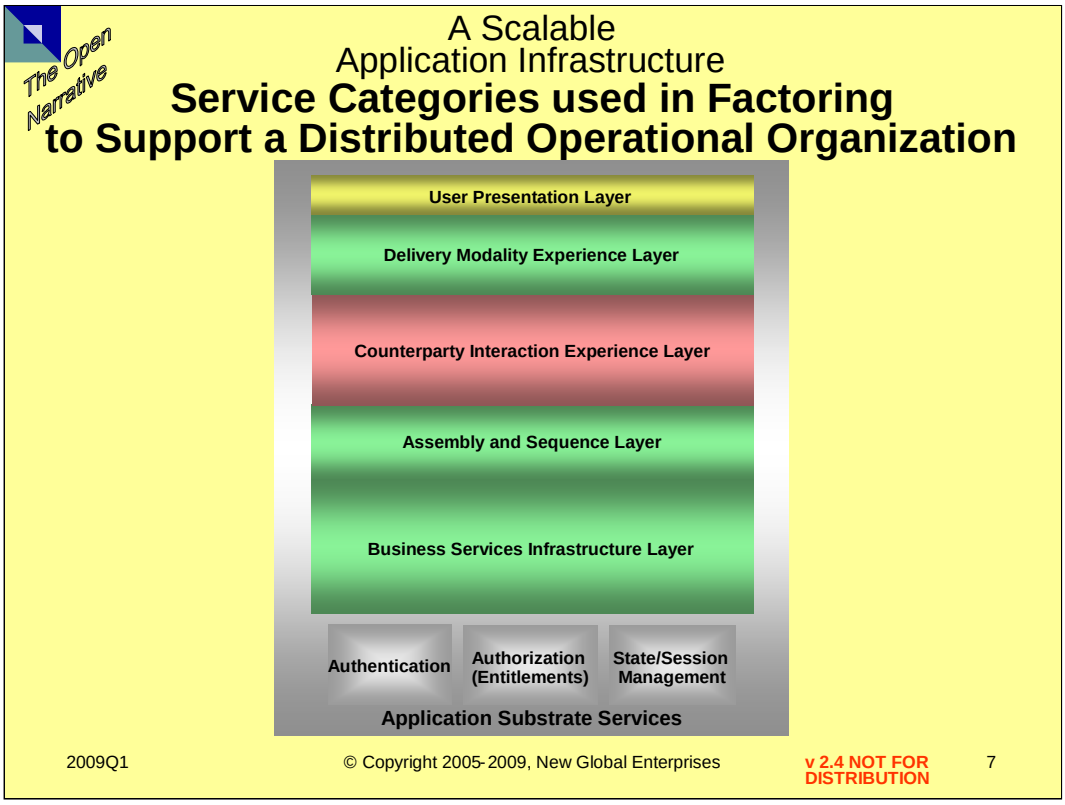
Example sequence and flow

1. Credential presentation protocol (https put ***login*** form + password factor and role resolution sequence: rich client?), ends with a Navigation Window
2. Verification Protocol, produces a Certificate which expires if not used within a variable but fixed period of time and always in a variable but fixed period of time
3. Selection protocol in navigation Window (https put ***invoke*** form)
4. Method invocation in app server of a Java Process: Application Function object
5. Verify credential for use in function (method invocation to Authorization Enterprise Java Bean)
6. Update State and Session Context (method invocation to State/Session Enterprise Java Bean)
7. Request object profile from Data Manager (method invocation to Data Realm Enterprise Java Bean)
8. Verify credential for access to data (method invocation to Authorization Enterprise Java Bean)
9. Send SQL statement to Data Base (e.g., Oracle PS SQL)
10. Update State and Session Context (method invocation to State/Session Enterprise Java Bean)
11. Return Protocol for Result Set
12. Formatting protocol for User View (JSP dhtml)
13. Presentation protocol for User (Browser)
14. Yada yada yada

-
-
-

n-3. Logout protocol
n-2. Destruction Protocol for Certificate
n-1. Destruction Protocol for State/Session
n. User Notification of exit from Application

Etc., etc., etc.



Business Investment Focus:

Creating Capabilities (Processes that produce significant results) known as Service Point Suites in the SOA World.

•Products
Targets basic Business Services Infrastructure like Customer, Product, Partner, Employee, etc, and the capabilities to orchestrate and integrate because this is the Product customization feature

•Channels
Targets Delivery Modality and User Presentation Experiences which are the modalities that the Customer/Clients Segments deal with the Services/Products of the Firm

•Segments
Targets the Counterparty Interaction Experience with Firm Business Processes

•All three Firm Business Units invest in the Application Substrate Services as these are common infrastructure for Applications

Service Layers

•User Presentation Experience—the look and feel of the Client and Provider interaction.

•Delivery Modality Experience—which is how a device/delivery mechanism mediates the Client Experience: a cell phone is different from a Blackberry is different from a mouse, keyboard and monitor which differ through direct-connect served by an agent as opposed to through the Web.

•Counterparty Interaction Experience—which is how the Client and Provider discover and deliver the Value in those services: this is, after all, the Business point of it all.

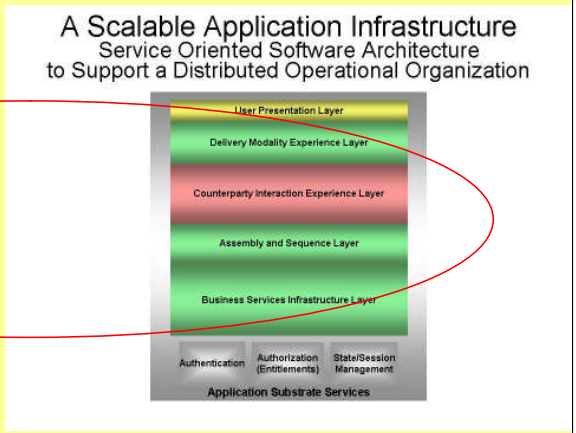
•Assembly and Sequence—which composes those basic and other composite services: the subject of current W3C working group debate.

•Business Services Infrastructure—which form the basic component substrate: IBM (PwC) has done a version of this for European Banking.

•Application Substrate Services—which handle the management of (1) security (Identity, Authorization and Role), (2) messaging protocols among components (both within and outside the enterprise, e.g., Web Services, E-Mail, IM, VoIP), (3) session/work flow, (4) personalization, and, (5) the collection, integration, storage and delivery of data to components of the Stack: all these functionalities "just happen" which allows the creator of functionality of the components to focus on business requirements

Layer 9
Business Process Engineering

- Business Processes, in economic terms, produce Significant Capabilities
  - Layer 9 is engineering for Significant Business Capabilities
    - This is Business Design and Optimization
      - Interaction Contracts with Counterparties

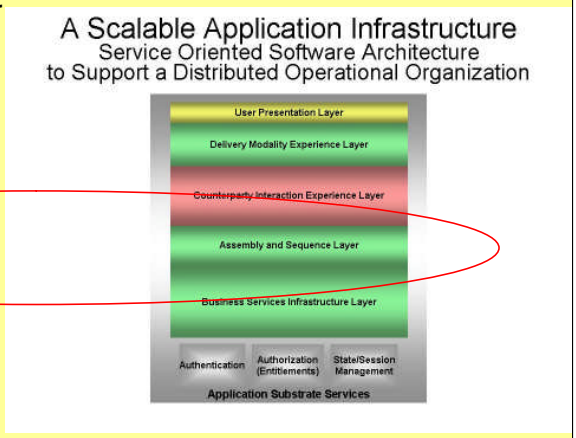


Level and Scope

Up the Stack and Aacross the Applications

Layer 8
People AND Workflow using Applications

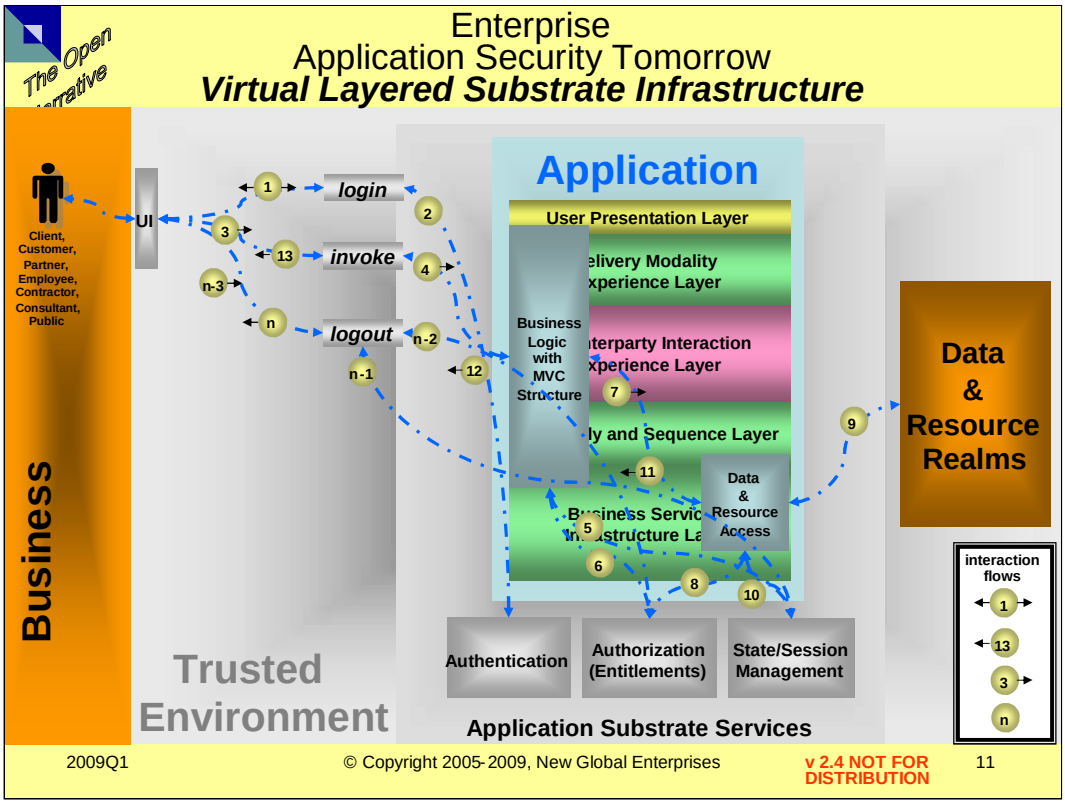
- Layer 8 is about what the **People** assemble & sequence executing **Business Processes** within Application Layer 7
  - **Workflow**
    - and all the ancillary protocols among peer components in this Layer



Process Implementation Focus

Applying Factor Categories

Implementing
Service Oriented Architecture



Example message sequence and flow
(Security Services are transparent to the Application)

1. Credential presentation protocol (https put ***login*** form + password factor and role resolution sequence: rich client?), ends with a Navigation Window
2. Verification Protocol, produces a Certificate which expires if not used within a variable but fixed period of time and always in a variable but fixed period of time
3. Selection protocol in navigation Window (https put ***invoke*** form)
4. Method invocation in app server of a Java Process: Application Function object
5. Verify credential for use in function (method invocation to Authorization Enterprise Java Bean)
6. Update State and Session Context (method invocation to State/Session Enterprise Java Bean)
7. Request object profile from Data Manager (method invocation to Data Realm Enterprise Java Bean)
8. Verify credential for access to data (method invocation to Authorization Enterprise Java Bean)
9. Send SQL statement to Data Base (e.g., Oracle PS SQL)
10. Update State and Session Context (method invocation to State/Session Enterprise Java Bean)
11. Return Protocol for Result Set
12. Formatting protocol for User View (JSP dhtml)
13. Presentation protocol for User (Browser)
14. Yada yada yada

-
-
-

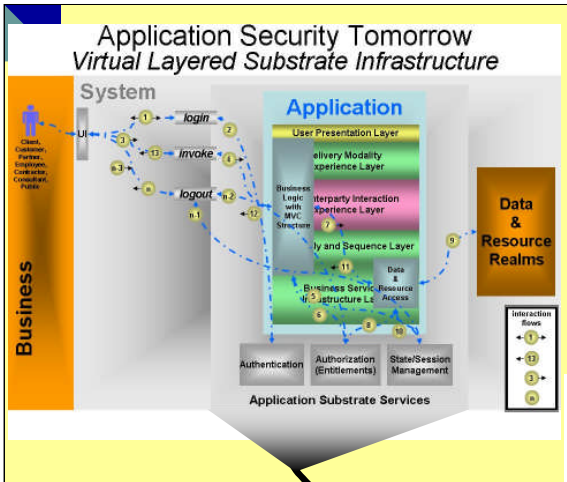
n-3. Logout protocol
n-2. Destruction Protocol for Certificate
n-1. Destruction Protocol for State/Session
n. User Notification of exit from Application

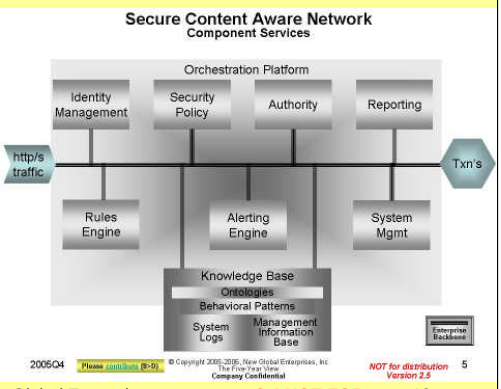
Etc., etc., etc.

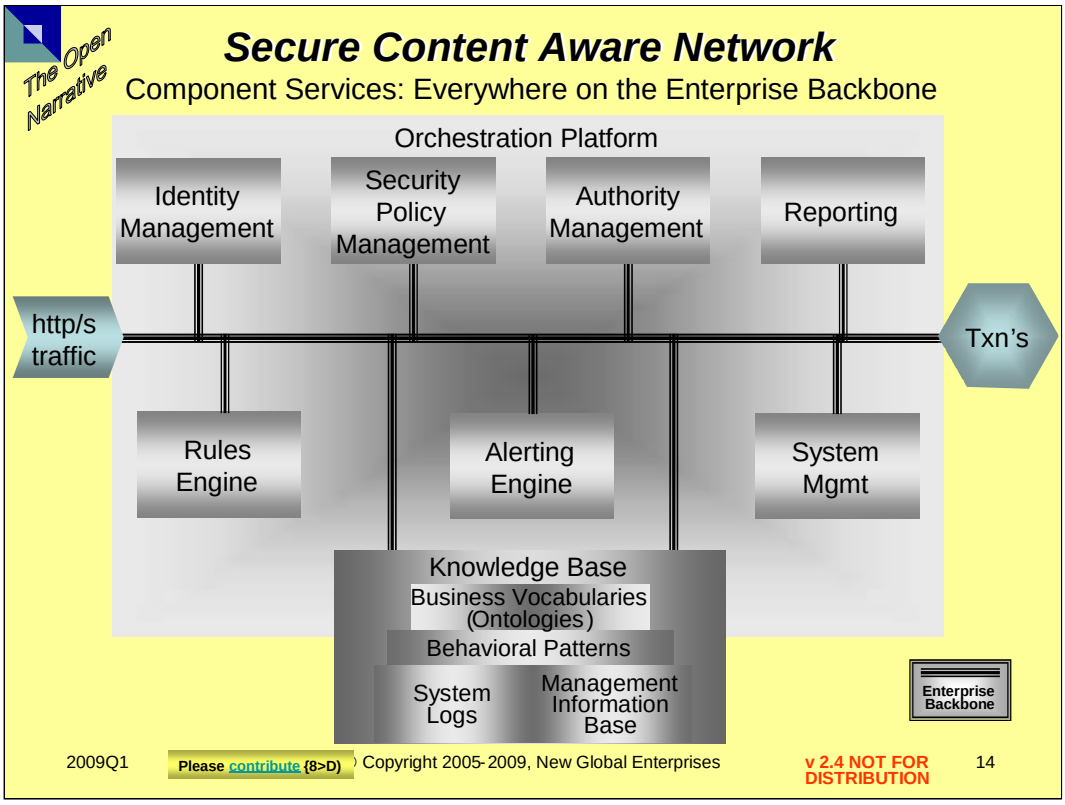
Full Set
of
Functional Categories
for
Secure Content Aware Networks

Well-Architected
Component
Service Point Suites
in the Application Layer 7.0

Drilling down into *SCAN*







Technology Portfolio Sectors of the Services that Implement the Instruction and Control Points: possible third party suppliers, including Open Source

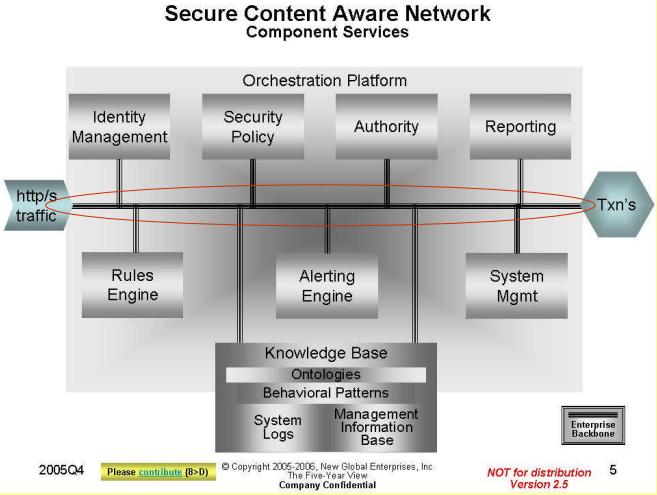
SCAN tracks the messages and sessions that result in create, read, update and delete of Enterprise Resources, CRUD being a transaction. Enterprise Resources include money, digital information, client data and goods.

The Open Narrative

Services that Implement the Instruction and Control Points for a *Secure Content Aware Network (SCAN)*

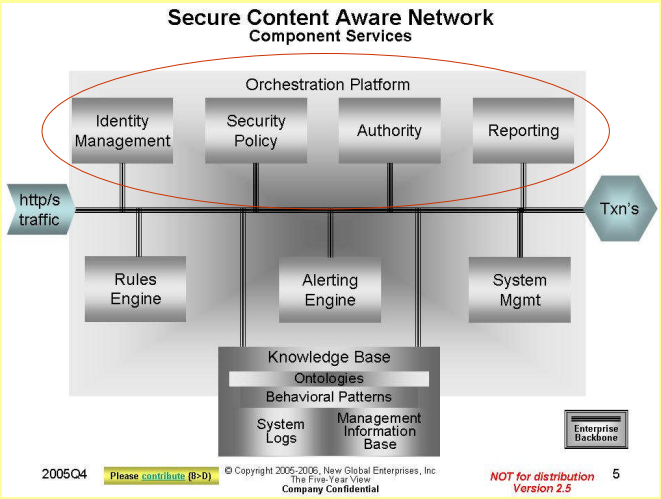
SCAN tracks the messages and sessions that result in create, read, update and delete of Enterprise Resources, CRUDE being the transaction.

- Enterprise Resources include money, digital information, client data and goods.



Functionality Descriptions
Possible third party suppliers, including open source

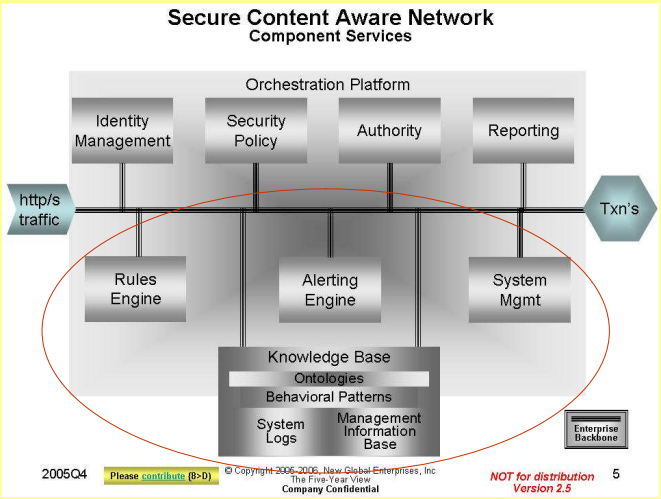
- Orchestration Platform
  - Functions to integrate data and processes amongst the component services in tracking of the traffic and interaction sessions.
    - PI Calculus based (assertions on parallel processes)
- Identity Management
  - Authentication services and key and certificate management services ,e.g., Improv
- Security Policy
  - Server that contains the set of rules, notification event dispatch, and possibly autonomic actions to intercede, prevent and/or correct.
    - Rohati, Securent
- Authority Server
  - Manager of role based permissions
    - Rohati, SOA Software
- Reporting
  - Structured Reports: Business Sessions Alert Reports; Active real-time dashboards; Visualizations
    - Quantum 4D



Functionality Descriptions

Possible third party suppliers, including open source

- Rules Engine
  - Inference management capability based on ontologies like OWL-based
    - Protégé, JESS, ActiveBPEL
- Alerting Engine
  - Server that oversees patterns of interest and raises events to be handled by appropriate process
    - Fast XML
- System Management
  - Services to collect and store instrumentation data and provide visibility on system processes
    - SOA Software
- Knowledge Base
  - Persistent store of semantic information (ontologies), behavioral patterns of interactions, log of system access and use and base of instrumentation data
    - XML, RDF, OWL, XDI, PostgreSQL, Protégé, Jess, sceptreTalk™



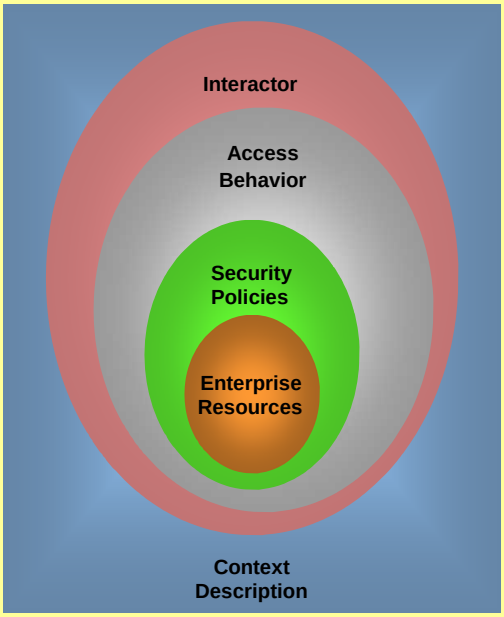
Appendix

The Abstractions
for
Security
and
Enterprise Resource Protection

Component Objects of Resource Protection

Hierarchy of Definition

- **Interactor**
  - Identity/Role of person or system engaging in the Behaviors against Resources controlled by Security Policies
- **Access Behavior**
  - Streams of http/s traffic, logs of actual and attempted entry into Zones of Privacy & Trust and actual and attempted access and usage of the Enterprise Resources
- **Security Policies**
  - Business rules on when who can do what to what
- **Enterprise Resources**
  - The things to protect: Money, Digital Property, Client Information, Shipment of Merchandise



Enterprise resources

The things to protect: Money, Digital Property, Client Information, Shipment of Merchandise

Security Policies

Business rules on who can do what with what by when

Access Behavior

Streams of http/s traffic, logs of actual and attempted entry into Enterprise Zones of Trust and actual and attempted access and usage of the Enterprise Resources

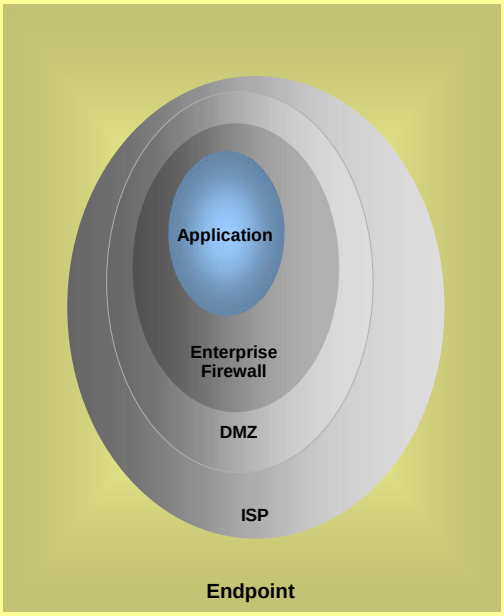
Interactor

Identity and Role of person or system engaging in the Behaviors

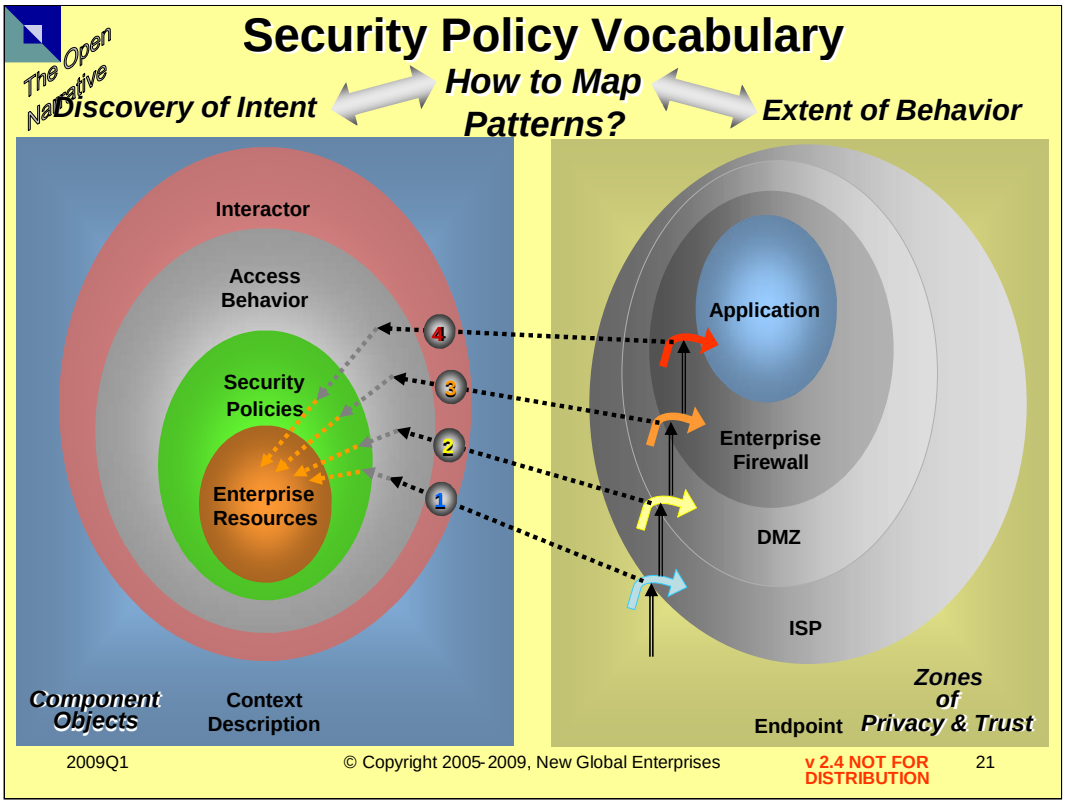
Concentric Zones of Privacy &Trust

Locales of Policy Enforcement Points

- **Endpoint**
  - Minimum visibility: 0th Zone of Privacy and Trust
- **ISP**
  - Perimeter of 1st Zone of Privacy & Trust
- **DMZ**
  - Perimeter of 2nd Zone of Privacy & Trust
- **Enterprise Firewall**
  - Perimeter of the 3rd Zone of Privacy & Trust
- **Application**
  - Core of enforcement: access and change



Thanks to John Macauley (jmacauley@insignisconsulting.com) for this observation



Do retinal scans: What you see is what you get.

Enterprise Resources (Thanks to Bob Ciccone (me@BobCiccone.com) for these categories

Control: Money, Digital Property, Customer Information, Shipments of Merchandise

Surveillance: Security, Risk and Regulation

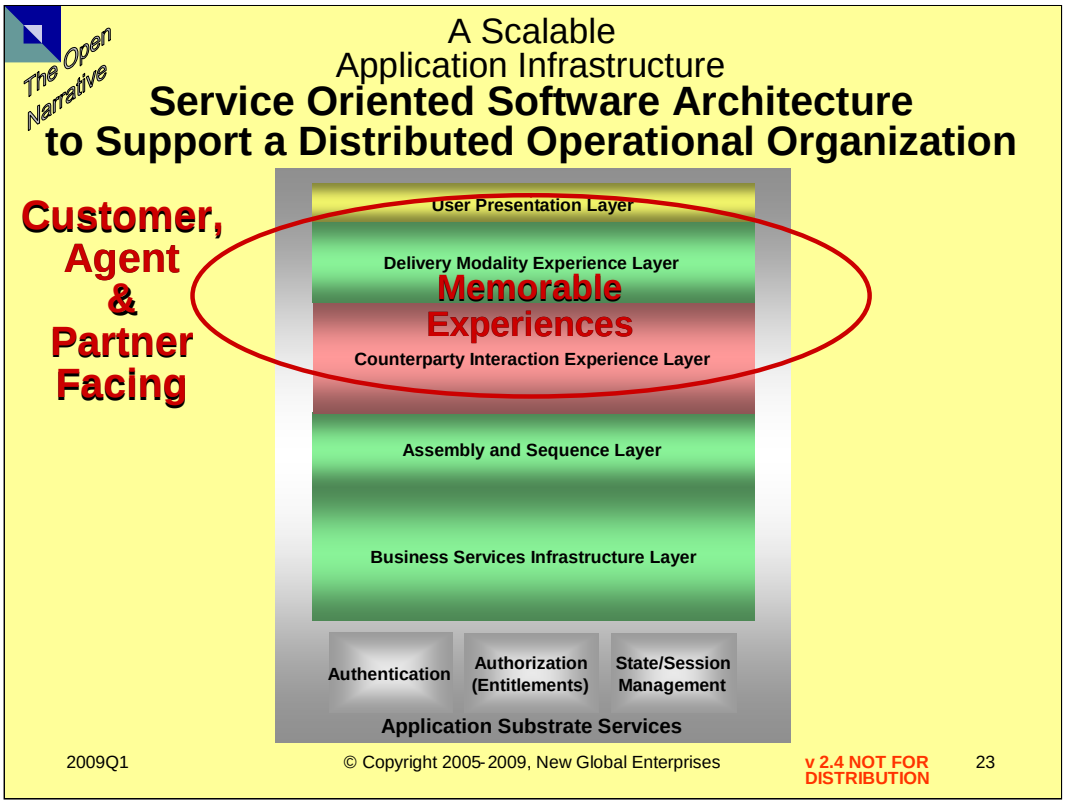
Transactions

Instruction (Order, Delivery, Payment, Information Request)

There is a business even more in this network architecture. IPV6 is still a dream.

User Value Creation

The Outside-In View
for
Customers, Agents and Partners



Business Investment Focus:

Creating Capabilities (Processes that produce significant outputs) known as Service Point Suites in the SOA World.

•Products
Targets basic Business Entity services like Customer, Product, Partner, Employee, etc, and the capabilities to orchestrate and integrate because this is the Product customization feature

•Delivery Modality
Targets Channel and User Presentation Experiences which are the modalities that the Customer/Clients Segments deal with the Services/Products of the Firm

•Segments
Targets the Client Services Experience with Firm Business Processes

•All three Firm Business Units invest in the Application Substrate Services as these are common infrastructure for Applications

Service Layers

•User Presentation Experience—the look and feel of the Client and Provider interaction.

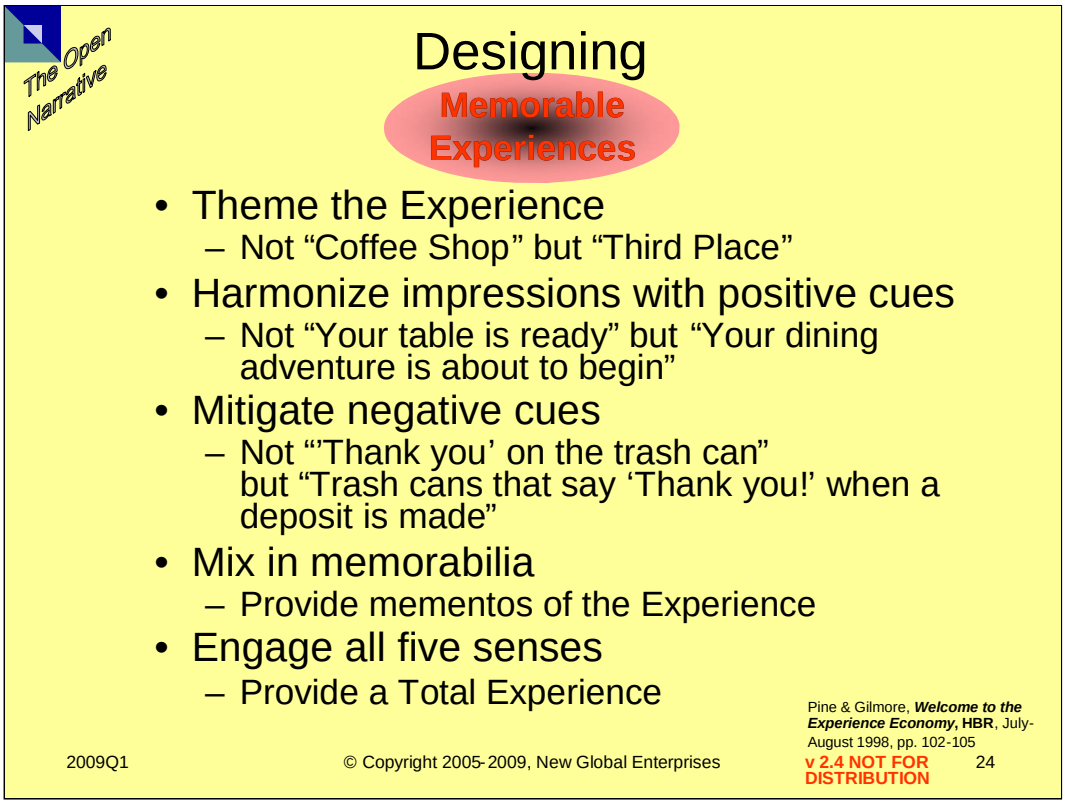
•Delivery Modality Experience—which is how a device/delivery mechanism mediates the Client Experience: a cell phone is different from a Blackberry is different from a mouse, keyboard and monitor which differ through direct-connect served by an agent as opposed to through the Web.

•Counterparty Interaction Experience—which is how the Client and Provider discover and deliver the Value in those services: this is, after all, the Business point of it all.

•Assembly and Sequence—which composes those basic and other composite services: the subject of current W3C working group debate.

•Business Services Infrastructure—which form the basic component substrate: IBM (PwC) has done a version of this for European Banking.

•Application Substrate Services—which handle the management of (1) security (Identity, Authorization and Role), (2) messaging protocols among components (both within and outside the enterprise, e.g., Web Services, E-Mail, IM, VoIP), (3) session/work flow, (4) personalization, and, (5) the collection, integration, storage and delivery of data to components of the Stack: all these functionalities "just happen" which allows the creator of functionality of the components to focus on business requirements



Theme

The Balcony

Increase (+Cue)

What happened today will be good to deal with.

Reduce (-Cue)

Something free as “A Small Thank You” for keeping your money with us.

Provide Memento

Rosebud

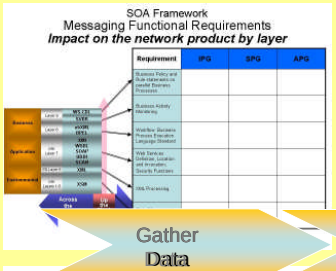
Engage Holistic Sensing

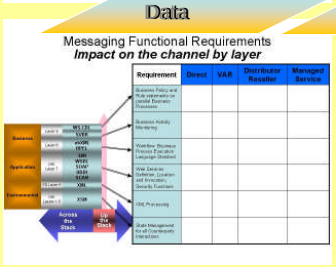
Total Immersion

Creating
a
SCAN
Service Oriented Architecture
Strategy

Analyzing Channels and Products
and
Creating a SOA Framework
Vendor Roadmap

SOA Strategy Planning Process





Gather Data

Layer 9

Layer 8

Analyze Data

OSI Layer 6

OSI Layers 1-5

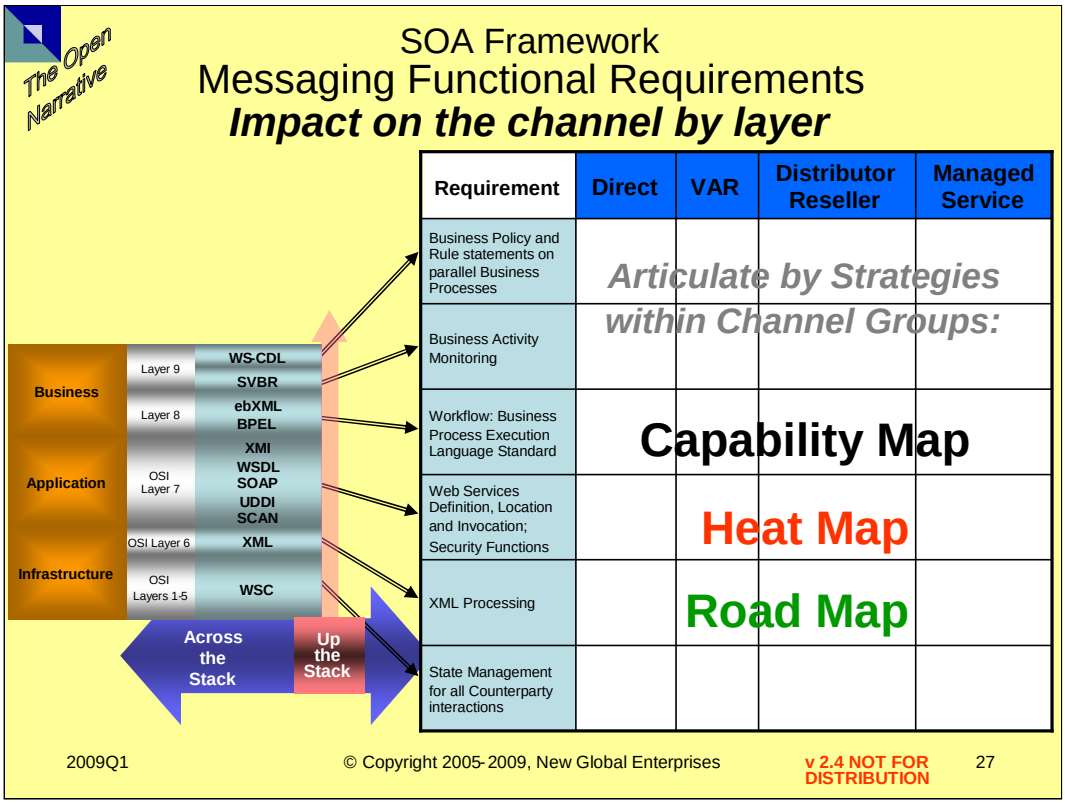
Synthesize Strategies

Articulate by Strategies

Capability Map

Heat Map

SOA Road Map



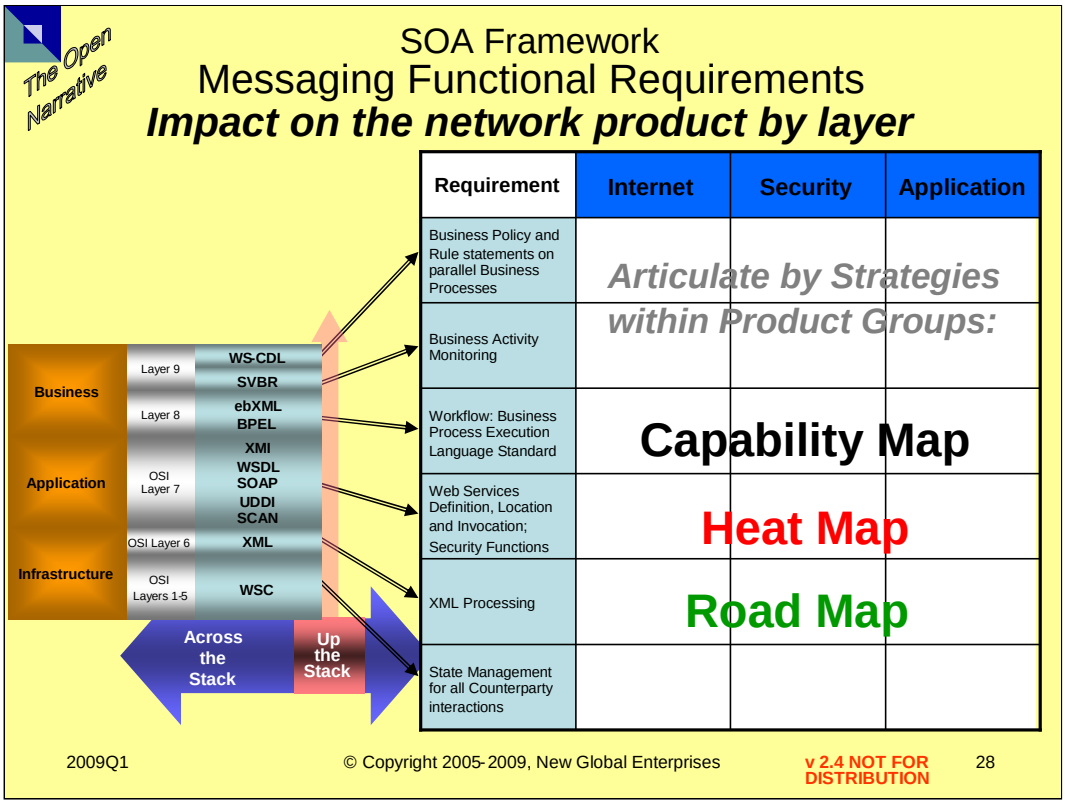
1. Capability Map
   What knowledge, skills and processes are required to deliver the functionality?
2. Heat Map
   What is state of Capability to Provide?
3. Road Map
   How do we get there in 3-5 years?

Equally applicable to Channel Services:

1. Direct
2. VAR
3. Distributor/Reseller
4. Managed Service

- Service

- Experience

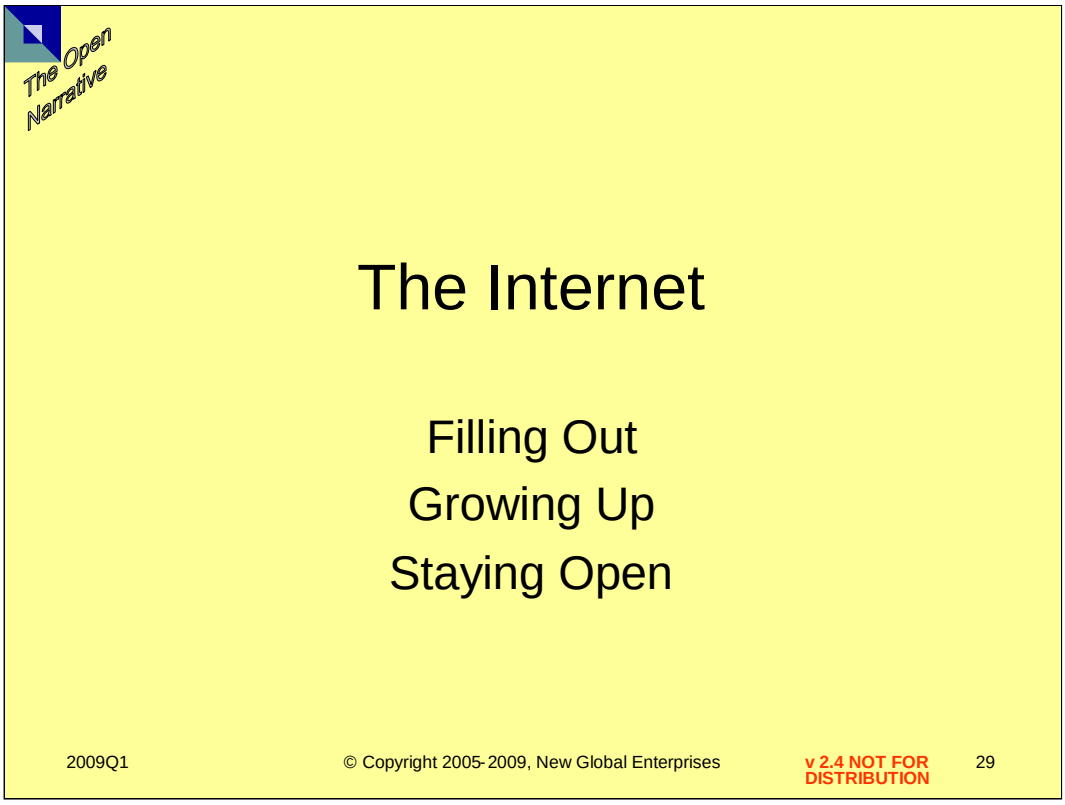


1. Capability Map
   What knowledge, skills and processes are required to deliver the functionality?
2. Heat Map
   What is state of Capability to Provide?
3. Road Map
   How do we get there in 3-5 years?

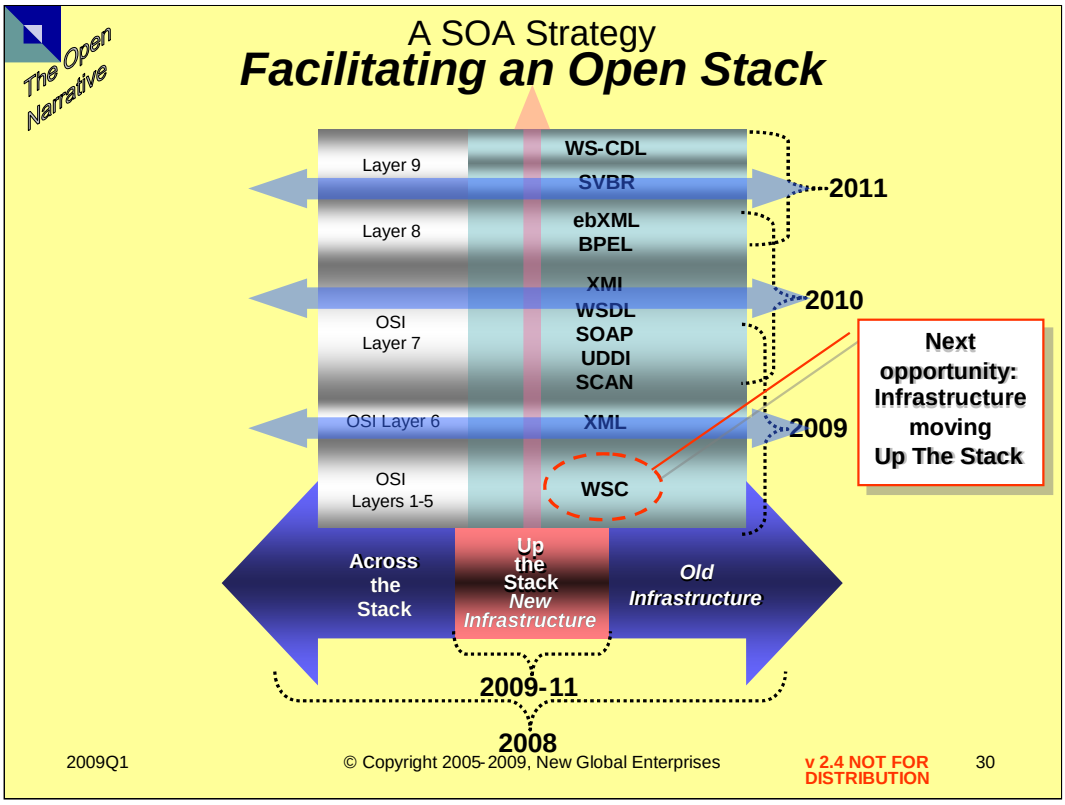
WS-CDL:

Equally applicable to Channel Services:

1. Direct
2. VAR
3. Distributor/Reseller
4. Managed



IPSphere is a great starting point



XSM

A state machine standard spec, REST works fine as the framework

Notice the caliper icon

Secure Content Aware Network