

Functional Security at NYS Department of Taxation and Finance

James Lieb, Director – Common Services
NYS Department of Taxation and Finance

1

SOA Concepts and Techniques

An Application Developers View

- Top-Down Design
- Focus on process and integration
- Leverage tools and products
- Use industry standards (e.g. XML) to increase capabilities of tools
- Develop standard design and integration patterns to facilitate future projects
- Should be focused on the business function not on how it is used

2

Security Objectives

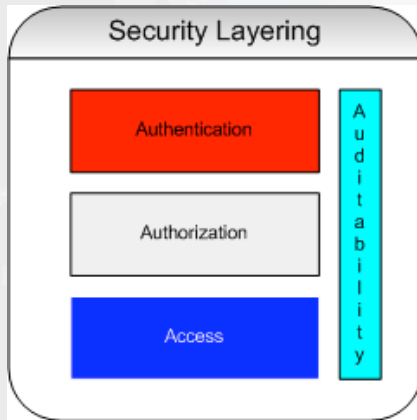
- Comply with DTF policies, IRS Guidelines, and other external auditing agencies, such as...
 - OSC (Office of the State Comptroller)
 - OCSCIC (Office of Cyber Security and Critical Infrastructure and Coordination)
- Enforce authorization externally from the e-MPIRE application code.
- Grant security access to enable staff to perform job-related functions.
- Simplify the administration of security access
- Support role based security definitions. A role defines the relationship between an e-MPIRE user and their authorized resources. For example, a Taxpayer Contact Center Supervisor is a role.

Security Approach

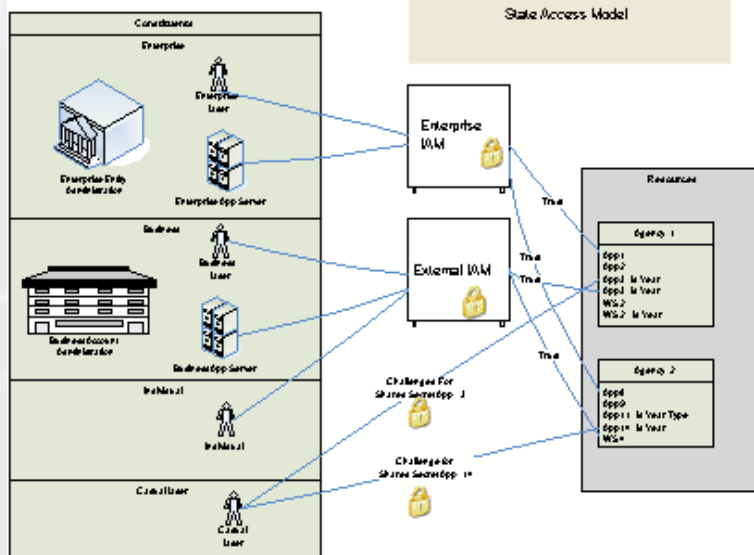
- The approach will be role based, not organizational.
- Leverage existing security infrastructure
- The approach will support the Department's business processes being implemented within e-MPIRE
- The approach will support either a "centralized" method of administration with administrative tasks handled by ESD Security Administration or a "decentralized" method of administration with administrative tasks handled by various individual business units.

Motto – "Security is no substitute for management"

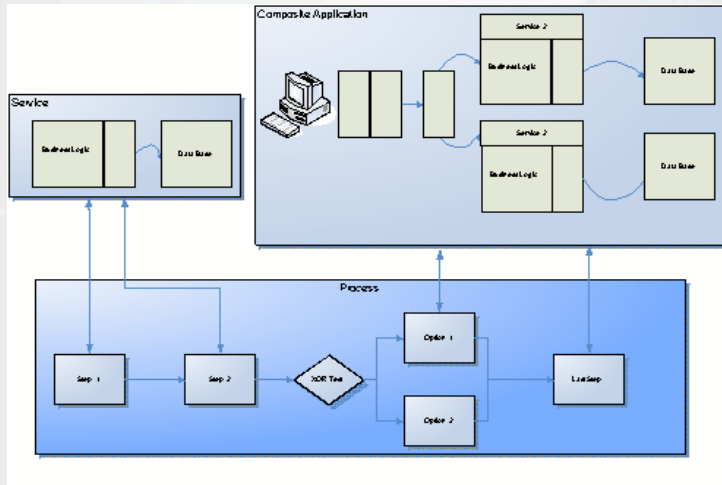
The 4 As of Security



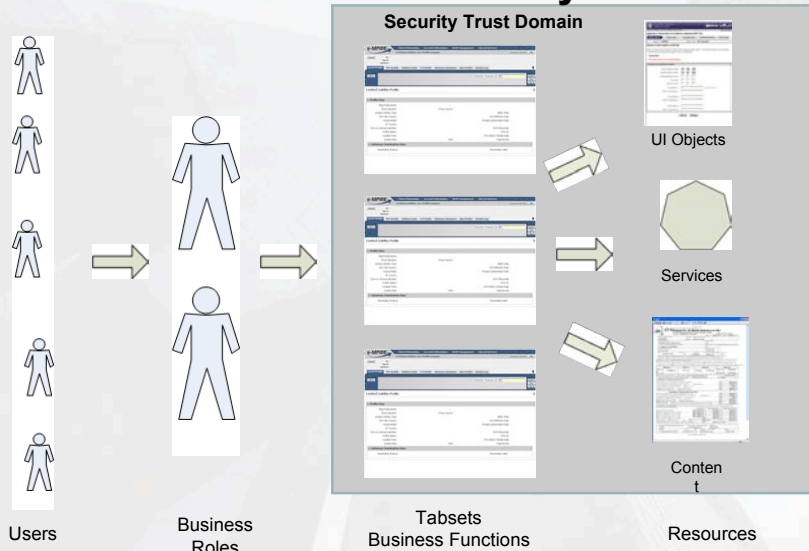
- Authentication (Who)
- Authorization (What)
- Access (What Specific)
- Auditability



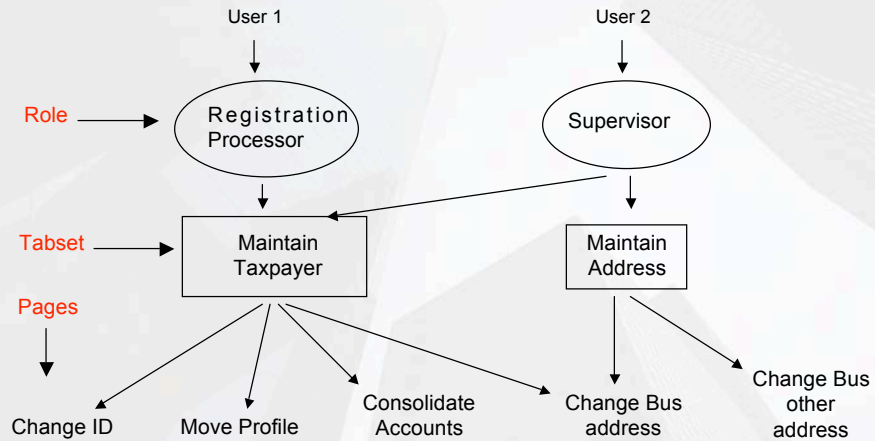
The New Paradigm Assembled Systems



E-MPIRE's SOA Security Overview



Roles Example



Business Roles & Navigation (BRAN) Team User based governance

- Establish roles in conjunction with Business Managers
- Design tab sets in conjunction with design teams and process owners
- Work with Process Owners to establish appropriate role to resource mapping
- Provide initial role to resource mappings to Security Administration
- Register menu options and pages to tab sets
- Develop the process and procedures for administration of roles and tab sets
- Provide LDAP initialization criteria to Security Architecture

e-MPIRE Tabset - Composite Application The Resource

Limited Liability Profile

Profile Data

DBA/Trade Name: _____ Phone Source: _____ BBNY Date: _____
 Phone Number: _____ DOS Effective Date: _____
 Limited Liability Type: _____ Foreign Authorization Date: _____
 Non-Filer Reason: _____ DOS Filing Date: _____
 County/State: _____ DOS ID: _____
 NY County: _____ DOS Name Change Date: _____
 Survivor Account Number: _____ Original DUN: _____
 Profile Status: _____
 Created From: _____
 Create Date: _____ DUN: _____

Voluntary Termination Data

Termination Reason: _____ Termination Date: _____

Tabset Creation

BABE Activity Setup

BABE ID: MYNEWBABE ID of the BABE: _____

Available Pages:

Page ID	Mod	Page Title	Tab Title
EMPFIND	TS	Non Tabset Page	Non Tabset Page
EMPTAB	TS	Tabset Page	Tabset Page Sample
ENTMP	EN	Enforcement Menu	Enforcement Menu 1
FWSPTSRH	TI	Reference Table Search	Table Search
FWWFTSRH	TI	Reference Table Search WLF	Table Search
HOME	ZZ	Administration	Administration
INDRATP	RP	RA - Taxpayer Profile	Independent Taxpayer Profile
PRTMP	PR	Processing Menu	Processing Menu 1
RAFS	RP	RA - Filing Summary	Filing Summary

Child Pages:

Page ID	Mod	Page Title	Tab Title	Update
ACHREQLIST	FW	Request List	Request List	<input checked="" type="checkbox"/>
FWDADUT	TI	Taxpayer - Address Add/Update	Address Add/Update	<input type="checkbox"/>
FWSPPRVW	TI	Reference Table Preview	Table Preview	<input checked="" type="checkbox"/>

Cancel << Prev Next >>

Field Element Registration Button Registration Action Handler Registration View Bean Registration Message Registration Page Comp. Setup Button Mapping Registration
 Field Element Search Button Search Action Handler Search View Bean Search Message Search Page Comp. Search Button Mapping Search

LDAP Directory - People

The screenshot shows the LDAP Browser Editor interface. The left pane displays a tree view of the directory structure, with 'ou=NYS Department of Taxation and Finance' expanded to show 'ou=People'. A callout labeled 'User Account' points to the 'ou=People' folder. The right pane shows the details for a selected user entry. A callout labeled 'User Attributes' points to the 'cn' attribute. Another callout labeled 'User's Role' points to the 'nyacctlevel1' attribute. A third callout labeled 'The attribute that defines a user's role' points to the 'nyacctlevel1idmethod' attribute.

Attribute	Value
cn	Tax Test
givenName	Tax
l	Albany
mail	robertzeglen@sun.com
nyacctgovernment	y
nyacctlevel0	y
nyacctlevel1	y
nyacctlevel1idmethod	rzeglen
nyacctlevel1idmethod	PPRSUPV
objectClass	nslicenseuser
objectClass	nslicenseuser
objectClass	nslicenseuser
objectClass	inetorgperson
objectClass	nyjperson
objectClass	nyjrole1
objectClass	nyjrole0
objectClass	organizationalPerson
objectClass	person
objectClass	top
ou	NYS Department of Taxation and Finance
sn	Test
st	New York
uid	150003
userPassword	BINARY (33b)

LDAP Directory - Resources

The screenshot shows the LDAP Browser Editor interface. The left pane displays a tree view of the directory structure, with 'ou=NYS Department of Taxation and Finance' expanded to show 'ou=ResourceToRoles'. A callout labeled 'Resource' points to the 'ou=ResourceToRoles' folder. The right pane shows the details for a selected resource entry. A callout labeled 'Allowed Roles' points to the 'nydtfallowedrole' attribute.

Attribute	Value
objectClass	top
objectClass	nydtfrole
nydtfallowedrole	AIFAUD
nydtfallowedrole	PPRSUPV
nydtfallowedrole	ASTECH
cn	EFDMTS01

LDAP Directory – Policies Authentication

- A Policy is what gets executed to test the access rights to a resource:

Requested Resource

- Target: http://hostname.nystax.gov/EMPIRE/EFDMTS01_gateway

- Policy: ((nyappdtfempire=PPRSUPV) (nyappdtfempire=AIFAUD) (nyappdtfempire=ASTECH))

Allowed Roles

Allowed Roles

Allowed Roles

Access Restrictions

Filtering work

- Implemented with parameters that filter within the application
- Can be implemented on role or role-resource level
- Way of implementing find grade security on Web
- Internal examples
 - Location
 - User
 - Skill
- Works with priority

Home **e-MPIRE Framework Registration Tools**
BABE Activity Setup - UI Controls For NEWBABE

Activity ID: Activity ID is required.
 Activity Title: Activity Title is required.
 Workflow Key: Workflow Key is required.
 Working ID: Select... Working ID is required. Use Select... Button to select Search Fields that will be used as the Working ID.
 Description: Workflow activity description.
 Work Items Accessed by: Activity Work List Get Next Work Item Select type of Work Item Access.
 Process Template Name: Process Template Name is required.

UI Controls

Type	Label	Completion Code	Criteria Required	Display Business Activity	Display in Activity Work List	Display in Personal Work List
Return Work Item to Activity Work List					<input type="checkbox"/>	<input type="checkbox"/>
Enable Comments				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
View Work Item Description				<input type="checkbox"/>		
Go to Work Management Screen				<input type="checkbox"/>		
Escalate					<input type="checkbox"/>	<input type="checkbox"/>
Complete			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Pend			<input type="checkbox"/>	<input type="checkbox"/>		
Route			<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>

| Home | All Tools |

Workflow Integration – Work Management

e-MPIRE Client Information Account Information Work Management Special Services

Worklist Management Favorites Help

Worklist Management

Worklist

Category

- CF Return Exception
- CT Default Data
- CT Duplicate Name
- CT-245
- Change of Address
- Comp-Dissolution
- Comp-Retired Requested
- Computational
- Conversion
- DOS Involuntary Dissolution Rejection
- Disapproved OP - Desk
- Disapproved OP - Field

Personal Worklist

Category	Taxpayer ID	Work ID	Name	Date Created	Date Assigned	Status
ID	220000758 (BUS)	CB09K5001107	AL DMECLA	01/18/2006	01/26/2006	IN PROGRESS
PAYMENT DISCREPANCY	321001067 (BUS)	CB09G5700812	MSADY1017M	01/18/2006	02/09/2006	IN PROGRESS
LIABILITY PERIOD	830000718 (BUS)	CB09L5402211	CSB 718	01/18/2006	02/09/2006	IN PROGRESS
MISC RECLASS	220001165 (BUS)	3304	JE-1165	01/18/2006	01/25/2006	IN PROGRESS
CT-245	220001235 (BUS)	CB09M5370811	JE-1235	01/18/2006	02/06/2006	IN PROGRESS

Local intranet

Workflow Integration - BABE Tabset

The screenshot displays the e-MPIRE web application interface. At the top, there are navigation tabs for Client Information, Account Information, Work Management, and Special Services. Below these, the user's ID (22-0001236(BUS)) and Name (JE-1236) are shown, along with the address: 100 BALLSTON AVE, BALLSTON SPA, NY 12020-1920. A search bar contains the DLN (DLN) and the document ID (CB09MS376812). A green message indicates "S01680 Retrieval Successful". Below this, there is a section for "EDMS Search for Documents" with a "Filter Documents" section containing various search criteria like Application Type, Form, Create Date From, Liability Period Begin, Tax Year, Processing Year, Document Type, Create Date To, and Liability Period End. A table shows the search results for the document CB09MS376812, which is a Case - CB05, Inbound, Corp, with a Create Date and Liability Period.

DLN	Form	Related Object Type	Document Type	Tax Type	Create Date	Liability Period
CB09MS376812	CT-245	Case - CB05	Inbound	Corp		

Summary

- Single signon for all systems
- Over 5,000 employees and only 150 roles
- Audit trail generated for all internal and web applications
- Audit trail also used in click stream analysis and problem resolution
- Help Desk support for security issues reduced by 80%

Serving External Customers Online Tax Center (OTC)

How do you give external customers (business partners and constituents) access to applications and resources?

Requirements for Authorization System

- Self Service
- Easy to use interface for account administration including delegation
- Low cost, easily maintained
- Single signon to multiple accounts
- Meets Statewide accessibility
- Auditable
- Resolves issues of previous models

IBM WebSphere Commerce

- Used by many companies (Home Depot, CVS, 40 of top 100 online shopping sites) for online shopping
- Highly scalable
- Highly configurable Accelerator feature allows quick updates (by non-programmers) and allows users to “own” their own catalogs and customization
- Gartner rated top Commerce software
- Supports Publish and Subscribe paradigm
- Supports multiple “sites”, “contracts”

WebSphere Commerce Advantages

Why buy instead of build?

- Whole CRM side of product which can promote resources and deliver information based on profile of account, users or resources
- Used by many companies, scalable
- Highly configurable (catalogs, products, etc.)
- Integrates with plug-in modules for payments, other web service products
- 300 off the shelf reports
- Allows for easy integration with Portal and new technologies (REST, Web 2.0)
- Secure chat (with known user) and other features built into product
- Supports multiple “sites”, “contracts”

Project Implementation

- Most of Customization went into customer venting
 - Individual
 - Business
 - Sales Tax Lite
 - Tax Practitioner
 - Manual
 - Others on way
 - Looking into Legislature, District Attorneys
- Interacts with NYSDS through web services
- Certain resources only available to certain customers

DTF Project Completion Information

- Started in May and first went to production Nov. 2006
- Last delivery of initial phase March 2007
- Over 265,000 registered users to date (no advertising)
(100% growth in last 9 months)
- Anticipated 500,000 new users next year
- Converted all existing applications to work with OTC
- All new applications work with OTC

DOL/DTF Project Plan

- Started in October with July 2009 delivery date
- DOL will be implemented as an independent storefront
- DOL and DTF will have the ability to share customers
- DOL will leverage many of the DTF customizations (create user, letters, administration, etc.)
- DTF can take advantage of DOL enhancements
- Customers could have a unified view

System Futures Marketplace of Services

- Web 2.0, Social Networks (User Communities – Legislature, Tax practitioners, District Attorneys)
- Servers – web service subscription. Essentially a repository of web services which can be subscribed to by only certain customers (catalog)
- Resources accessed only from known domains
- File Transfer automation
- User certificates and signatures

Where We Are Headed with SOA

- Leverage tools for faster delivery
- Expand composite applications using web 2.0 technologies
- Move to the “Real Time Enterprise” - Accept and process individual filings and payments at any time, from all sources - taxpayers, tax preparers, partners, over multiple channels – paper, electronic, web
- Make business rules and services available to tax preparers, taxpayers
- Improve call centers, VOIP, collaboration
- Increase in-line fraud detection (CISS, EAS)
- Enhance field operations productivity through new technologies such as mobile office tools; e.g., VOIP, IM
- Automate end-to-end systems management and control

Questions?