



Distributed Tivoli Identity Manager

- A Topology Enabler for Large Scale TIM deployment

Karthik Satishkumar (karsati@au1.ibm.com), Tivoli Security Principal, IBM SWS

PulseANZ2010

Meet the people who can help
advance your infrastructure





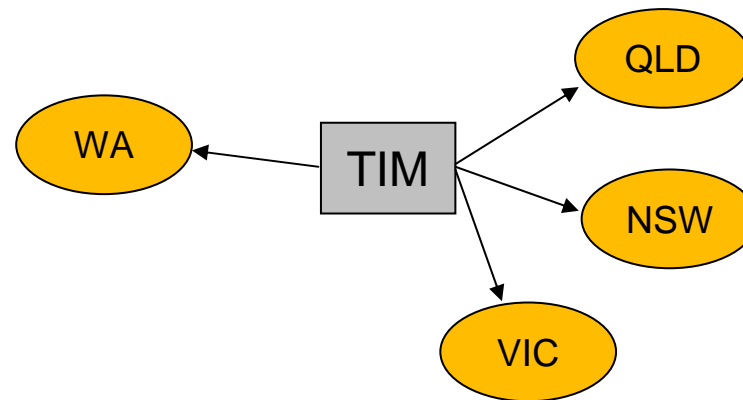
Agenda

- Large Scale TIM Deployment and Challenges
- What is DTIM?
- DTIM - Benefits
- DTIM architecture
- DTIM Reference UI
- DTIM API
- ITIM Web Services
- Q&A



A Large Scale TIM Deployment...

- Can be an TIM Deployment with Large Userbase
 - Hundreds and thousands of users; sometimes million+ user base
 - Typically observed in HealthCare solution providers, Telecoms, etc
 - Mergers and Acquisitions leading to complex consolidation exercises
- Can be an TIM deployment with Large number of services defined
- Can be an TIM deployment spread across a Large Enterprise spanning geographical boundaries





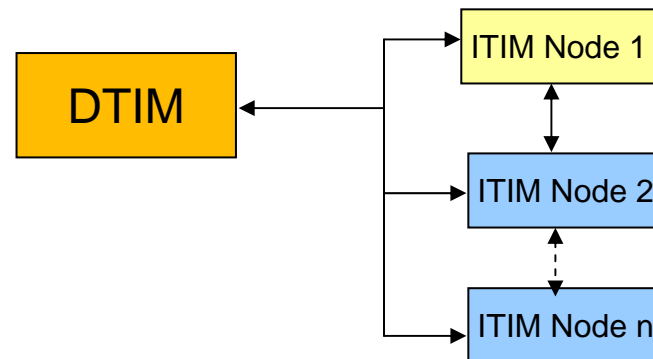
Key Challenges in Large Scale TIM deployments

- Performance Implications due to Large Userbase and Large number of policies and services
- Operational Issues with Centralised Administration
 - Especially in Large Enterprises where individual organization units operate as independent entities (e.g: Govt with multiple departments)
- Roll Outs/Downtime affects the entire organisation



What is DTIM?

- A distributed approach for deploying ITIM
- Distributes service workload on different ITIMs (called ITIM nodes).
 - Individual ITIMs host a subset of services.
- A central DTIM node combines information from different ITIMs and presents to end user
 - User requests are routed to apt target ITIM.
- Decentralizes ITIM administration and configuration.





DTIM - Benefits

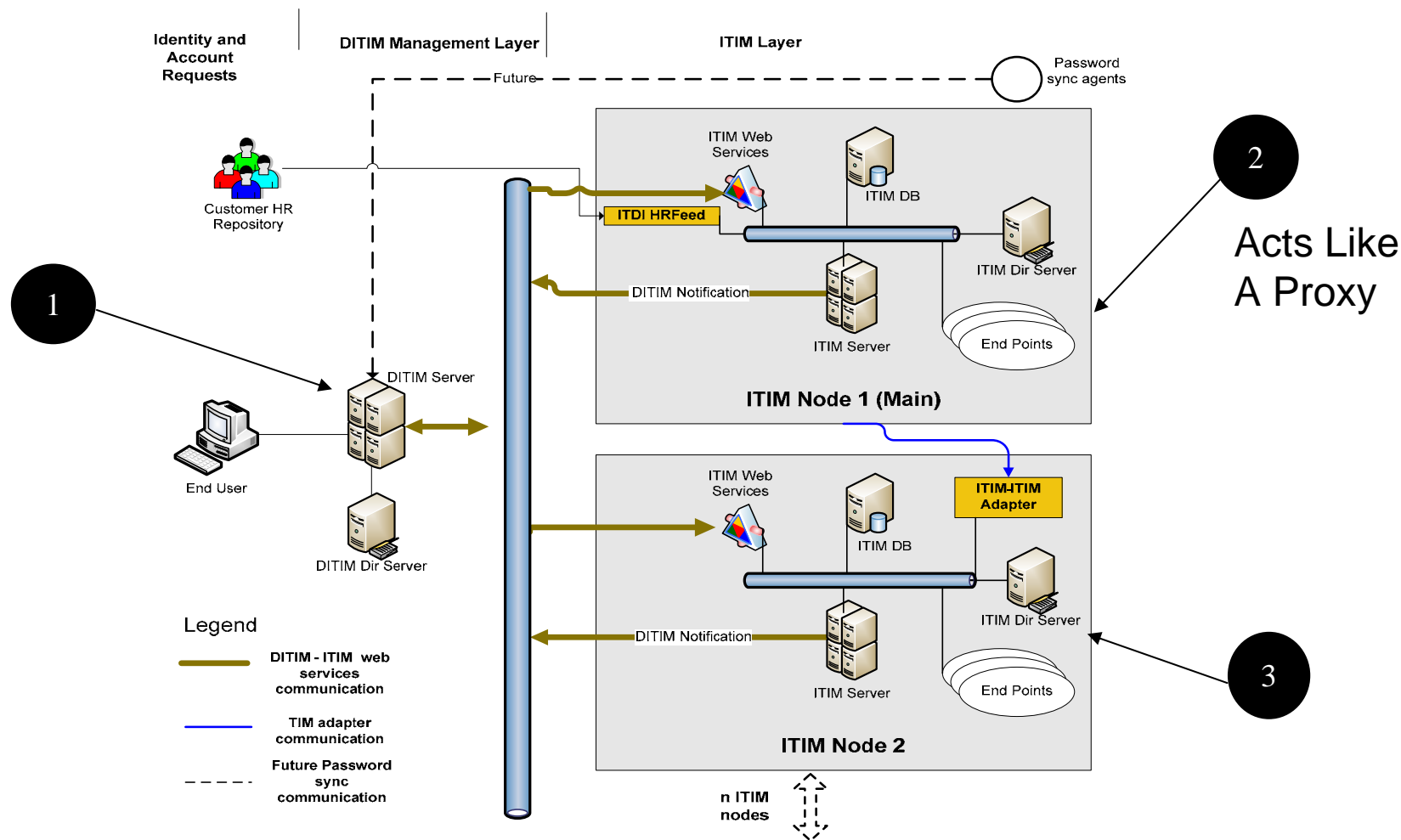
- Scalability
 - Add ITIM nodes as more services are rolled out.
- Avoid performance bottlenecks
 - Individual ITIMs process their own service requests *and recons.*
- ITIM nodes can be heterogeneous across platforms and ITIM versions.
 - Currently supports ITIM v4.6 and ITIM v5.x
- Allows “rolling” upgrade/maintenance of individual ITIMs.
 - Entire ITIM infrastructure does not shut down.



DTIM - Non Goals & Constraints

- Does not provide administrative and non end user tasks.
- Post Office consolidation will not take place at the DTIM level, only at the ITIM level.
- Constraints
 - Policies can only target multiple services on the same node.
 - Service pre requisites must be on the same node.
 - Custom workflow cannot use operations on entities not on the same node.

DTIM Architecture





Architecture

- Architecture is currently based on Master – Child topology.
- Each child ITIM can have its own subset of people as well as services.
- Leverages the custom **ITIM-ITIM adapter** for ITIM to ITIM communication.
- Long term goal is to provide Master – Child as well as Peer to Peer topologies.



Architecture – DTIM server

- Consists of J2EE application and local directory server (LDAP based).
 - Directory server contains stubs of selected objects on ITIM nodes (person, account, service).
 - Stub object points to complete object in target ITIM.
 - LDAP server also stores DTIM configuration.
 - J2EE application provides DTIM services and API implementation.



Architecture – DTIM node (contd.)

- Provides API to combine user information from ITIM nodes.
 - Communicates with ITIM nodes using a web services interface
 - Discovers services in ITIM nodes and maintains service to ITIM node mapping.
 - API provides functionality similar to ITIM self services capability.
 - Utilizes local LDAP server to derive node, person and account relationships.
- Routes user requests to appropriate ITIM over a web services interface.



Architecture – DTIM node (contd.)

- Retrieves person information from the Main ITIM (following the LDAP stub reference).
 - Changes are written back to Main ITIM which sprays to participating ITIMs via ITIM-ITIM adapter.
- Retrieves and updates account objects by following the account stub reference.
- All other objects are retrieved from participating ITIMs in parallel.
 - Time to retrieve objects is as long as the longest time to retrieve from any single ITIM.



Architecture – ITIM nodes

- One node is designated as Main and is used to host identity and optionally services.
- Other nodes host subsets of services.
- ITIM Web Services is installed on each node to enable web services communications.
 - ITIM Web Services is also available separately from DTIM.
 - Enables web services interface to ITIM for end user API.
 - Available as a free download from OPAL.



Architecture – ITIM nodes (contd.)

- Each ITIM node gets an identity feed from the Main ITIM via the ITIM - ITIM adapter.
 - Each child ITIM appears as a managed platform in the Main ITIM.
 - ITIM policies and automatic entitlements can be configured to distribute person objects to the child ITIMs based on person criteria.
 - ITIM-ITIM adapter uses standard adapter framework.

- Each ITIM node notifies DTIM of account and person changes via a Notifier module using a web services interface.
 - Adds and deletes are notified.
 - Attribute changes other than suspend/restore are not notified.



DTIM Reference UI

- DTIM UI is a reference UI that implements the DTIM API.
- Intention is to show DTIM functionality, not satisfy user serviceability requirements.
- Uses Java Server Faces (JSF) for view processing. Source code is included with DTIM.
- Provides self service user functions.
 - In the DTIM architecture, admin tasks are decentralized on local ITIMs.



DTIM Reference UI - Login

- Supports simple login or SSO.
- Authenticates against Main ITIM.

Tivoli Distributed Topology Enabler for ITIM (D-ITIM) **IBM.**

Help

Login To Distributed Topology Enabler For ITIM

Userid	<input type="text" value="gverma@us.ibm.com"/>
Password	<input type="password" value="....."/>

[Forgot your password?](#)



DTIM Reference UI – Home Page

- Lists footprint of logged in user.
 - User may have presence on only some of the ITIMs.
- Configurable to show accounts/pending items.

Tivoli Distributed Topology Enabler for ITIM (D-ITIM) **IBM.**

Hello, Girish Verma Help

Home
Logged in successfully

DITIM is managing your accounts distributed on 2 active ITIMs

ITIM Node List	
ITIM Node Name	ITIM Node Description
green	American Express ITIM
blue	A Global ITIM



DTIM Reference UI – DTIM Admin

- Allows configuration of list of nodes.
 - Nodes may be inactivated for maintenance.

Hello, Girish Verma

Home

DITIM Administration

My Personal Info

My Accounts

My Accesses

Manage my passwords

My Requests

My To Do Items

DITIM Administration

Perform DITIM administration activities

Import Topology From Global ITIM

ITIM Nodes [View Node Services](#) [Add ITIM Node](#)

[Interrogate ITIM Node](#) [Delete Node](#)

<input checked="" type="checkbox"/>	ITIM Node Id	Main Node	ITIM Node Description	ITIM Version	ITIM Fixpack Level	ITIM Node URL	Inactive node / reason	Test Connection
<input checked="" type="checkbox"/>	blue	<input checked="" type="radio"/>	<input type="text" value="A Global ITIM"/>	5.0	-1	<input type="text" value="http://blueserver:9080"/>	<input type="checkbox"/>	<input type="button" value="Test"/>
<input type="checkbox"/>	green	<input type="radio"/>	<input type="text" value="American Express ITIM"/>	5.0	-1	<input type="text" value="http://greenserver:9080"/>	<input type="checkbox"/>	<input type="button" value="Test"/>
<input type="checkbox"/>	red	<input type="radio"/>	<input type="text" value="Red node"/>	Unknown	Unknown	<input type="text" value="http://redserver:9080"/>	<input checked="" type="checkbox"/> <small>Red node is down until its configuration is completed</small>	<input type="button" value="Test"/>



DTIM Reference UI – DTIM Admin

- Import DTIM configuration automatically from the Main ITIM.

Tivoli Distributed Topology Enabler for ITIM (D-ITIM) **IBM**

Hello, Girish Verma

Home
DITIM Administration
My Personal Info
My Accounts
My Accesses
Manage my passwords
My Requests
My To Do Items

DITIM Administration x

Import DITIM Topology From Global ITIM

Import Topology Info
DITIM communicates with the Global ITIM to automatically find child ITIM nodes and set up their connection configuration. Child ITIM nodes defined in DITIM but not found on the Global ITIM are flagged but not deleted. They can be deleted manually (after confirmation) from the DITIM administration panel.

Click Start to start the import and synchronization process. Depending on the number of child ITIM nodes, this process could take a few minutes.

Node

Test Connection

Test



DTIM Reference UI – DTIM Admin

- View Services on an ITIM node
 - Services are imported by interrogating an ITIM node

Hello, Girish Verma

Home

DTIM Administration

My Personal Info

My Accounts

My Accesses

Manage my passwords

My Requests

My To Do Items

DTIM Administration

Perform DTIM administration activities

Import Topology From Global ITIM

ITIM Nodes | **View Node Services** | **Add ITIM Node**

Select node to display services: blue ▼ Go

Service Name	Prerequisite Service
ITIM Service	
LDAP base service	
Windows Local	
LDAP Service 2	
green	



DTIM Reference UI – DTIM Admin.

- Add new ITIM node (manually)
 - Also needs installation of DTIM node artifacts.

Hello, Girish Verma

Home
DITIM Administration
My Personal Info
My Accounts
My Accesses
Manage my passwords
My Requests
My To Do Items

DITIM Administration

Perform DITIM administration activities

Import Topology From Global ITIM

ITIM Nodes | **View Node Services** | **Add ITIM Node**

Enter information for new node

Node Id	<input type="text"/>
Node Description	<input type="text"/>
Node URL	<input type="text"/>
Inactive Node	<input type="checkbox"/>



DTIM Reference UI – My Personal Info

- Retrieved from Main ITIM
 - Rendered using the ITIM form definition.
 - ITIM form changes are reflected in real time.

Hello, Girish Verma

Home
DITIM Administration
My Personal Info
My Accounts
My Accesses
Manage my passwords
My Requests
My To Do Items

Manage Personal Information

IAMEssential Communication Other

Label	Value
Preferred user ID	9B0123896
Full name	Girish Verma
Last name	Verma
First name	Girish
Initials	
Organizational roles	greenrole EXECUTIVE Search Delete
Aliases	



DTIM Reference UI – My Accounts

- Accounts can be selected from one or all participating ITIM nodes

Manage Accounts

Select accounts to display

Select a node from which you want to list accounts, or select All ITIM nodes:

Select type of accounts to display:

Your account(s) on the selected ITIM nodes

<input checked="" type="checkbox"/>	ITIM Node Name (Node Id)	User id	Service Name	ITIM Version	Account status
<input type="checkbox"/>	A Global ITIM (blue)	gverma@us.ibm.com	ITIM Service	5.0	Active
<input type="checkbox"/>	American Express ITIM (green)	gverma@us.ibm.com	ITIM Service	5.0	Active
<input checked="" type="checkbox"/>	American Express ITIM (green)	user1	LDAP base service	5.0	Active
<input type="checkbox"/>	American Express ITIM (green)	gverma	Windows Local	5.0	Active
<input type="checkbox"/>	American Express ITIM (green)	user2	LDAP base service	5.0	Active
<input type="checkbox"/>	American Express ITIM (green)	9b0123896	LDAP base service	5.0	Active



DTIM Reference UI – My Accesses

- Retrieved only from ITIM 5.x nodes
 - Supports provisioning of new accesses.

Manage Accesses

Select access(es) to display

Select an ITIM node (or all ITIM nodes):

<input checked="" type="checkbox"/>	ITIM Node	User id	Access Name	Access Type	Service Name	Status
<input checked="" type="checkbox"/>	A Global ITIM (blue)		greenrole	AccessRole		Active
<input type="checkbox"/>	American Express ITIM (green)	user1	Finance App grp1	Application	LDAP base service	Active
<input type="checkbox"/>	American Express ITIM (green)	user2	HR App grp3	Application	LDAP base service	Inactive
<input type="checkbox"/>	American Express ITIM (green)	user2	Marketing app grp4	Application	LDAP base service	Inactive
<input type="checkbox"/>	American Express ITIM (green)	user1	Payroll App grp2	Application	LDAP base service	Active



DTIM Reference UI – Manage Passwords

- Submits password changes across ITIM nodes.
- Merges password rules across ITIM nodes.

Manage Passwords Help

Select accounts to display, then choose a new password

Select accounts that will be affected by this password change

Select an ITIM node (or all ITIM nodes)

<input type="checkbox"/>	ITIM Node Name	User id	Service Name	ITIM Version	Account status
<input checked="" type="checkbox"/>	A Global ITIM (blue)	gverma@us.ibm.com	ITIM Service	5.0	Active
<input checked="" type="checkbox"/>	American Express ITIM (green)	gverma@us.ibm.com	ITIM Service	5.0	Active
<input checked="" type="checkbox"/>	American Express ITIM (green)	user1	LDAP base service	5.0	Active
<input checked="" type="checkbox"/>	American Express ITIM (green)	gverma	Windows Local	5.0	Active
<input checked="" type="checkbox"/>	American Express ITIM (green)	user2	LDAP base service	5.0	Active
<input checked="" type="checkbox"/>	American Express ITIM (green)	9b0123896	LDAP base service	5.0	Active

Enter the password to be applied to selected accounts

For security purposes, first enter your current ITIM password

New password

Confirm new password



DTIM Reference UI – My Requests

- Retrieves Completed or Pending Requests.
- Pending requests can be aborted across ITIM nodes.

Manage Requests

Select requests to display

Select an ITIM node (or All ITIM Nodes)

Select requests

ITIM Node	Request Type	Date Submitted	Status	Account/Access
blue	Add Provisioning Policy	02-13-2009 08:32:43	Succeeded	Default Provisioning Policy for service dummy on
green	Change User Data	02-23-2009 13:56:09	Succeeded	Joe Biden
green	Change User Data	02-23-2009 13:56:06	Succeeded	Joe Biden
green	Change User Data	02-23-2009 13:48:51	Succeeded	Girish Verma
green	Change Account	02-18-2009 18:43:09	Succeeded	gverma@us.ibm.com on ITIM Service
green	Change User Data	02-02-2009 22:12:25	Succeeded	Girish Verma
green	Change User Data	02-02-2009 22:02:09	Succeeded	Girish Verma
green	Change User Data	02-02-2009 21:54:23	Succeeded	Girish Verma
green	Change User Data	02-01-2009 17:06:27	Succeeded	Girish Verma
green	Change User Data	02-01-2009 14:56:42	Succeeded	Girish Verma
green	Change User Data	02-01-2009 14:56:31	Succeeded	Girish Verma



DTIM Reference UI – My To Do Items

- Provides individual as well as grouped items.
- Provides Bulk Approve / Reject across ITIM nodes.

Manage To Do Items

Select ITIM node(s) from which To Do items will be retrieved (default is All)
Select a node from which you want to list to do items, or select All ITIM nodes | All ITIM Nodes

Submit Query

Approval Requests (0) Request(s) For Information (1) Workorder Requests (0) Grouped Recertification Requests (2) Compliance Alerts (0)

Click an activity to review it and provide information

ITIM Node Name	Assignment Type	Activity	Time due	Requestee	Requester	Account/Access
blue	Provide Information	RFI	03-04-2009 19:19:20	Girish Verma	Girish Verma	abc123121 on LDAP base service



DTIM Reference UI – My To Do Items

- Example of Bulk Approve / Reject

Review Grouped Recertification Request Hel

The grouped recertification request has the following items

Click an activity to review it before approving it, or select activities and use the Bulk Approve or Bulk Reject Buttons

<input type="checkbox"/>	ITIM Node Name	Assignment type	Activity	Time due	Requested For	Requested By	Account/Access
<input checked="" type="checkbox"/>	green	Approval/Reject	Recertification Approval	03-07-2009 08:39:32	Joe Biden	requesterType.P	ab1021001 on LDAP base service
<input checked="" type="checkbox"/>	green	Approval/Reject	Recertification Approval	03-07-2009 08:39:32	Girish Verma	requesterType.P	user1 on LDAP base service
<input checked="" type="checkbox"/>	green	Approval/Reject	Recertification Approval	03-07-2009 08:39:31	Girish Verma	requesterType.P	9b0123896 on LDAP base service
<input checked="" type="checkbox"/>	green	Approval/Reject	Recertification Approval	03-07-2009 08:39:31	Girish Verma	requesterType.P	user2 on LDAP base service
<input checked="" type="checkbox"/>	green	Approval/Reject	Recertification Approval	03-07-2009 08:39:31	System Administrator	requesterType.P	itimadmin on LDAP base service



DTIM API

- API is Java based.
- Provides a topology transparent API.
 - Client does not need to be aware of the ITIM node distribution.
- Provides self service functions.
- Can be used by a custom UI or a Java client application to communicate with DTIM.
- The Reference UI is an example of an application using the DTIM API.



DTIM API - Categories

- DTIM API categories
 - AccountServiceProvider
 - AuthenticationProvider
 - FormProvider
 - OrgContainerServiceProvider
 - PersonServiceProvider
 - RequestServiceProvider
 - RoleServiceProvider
 - ServiceServiceProvider
 - SystemUserProvider
 - ToDoProvider



DTIM API

- Selected examples of using the DTIM API.
- The authentication API provides an AuthInfo object that is used in subsequent API calls.
 - Example – Log in using DTIM API.
 - Client does not need to be aware of DTIM topology or configuration.

```
ITIMCredential itimCred = new
    ITIMCredential("jdoe", "abc");
AuthInfo authInfo = new AuthInfo(itimCred);
try {
    authInfo.authenticate();
    // authInfo now contains a valid session unless
    // a login exception was thrown.
```



DTIM API (Continued)

- Example – Get a list of To Do items from all participating ITIM nodes

```
// authInfo contains authenticated AuthInfo object.
```

```
ToDoProvider toDoProvider = new ToDoProvider(authInfo);
```

```
String selectedNode = "*"; // Select all ITIM nodes
```

```
Collection assignments = toDoProvider.getToDoList(selectedNode);
```

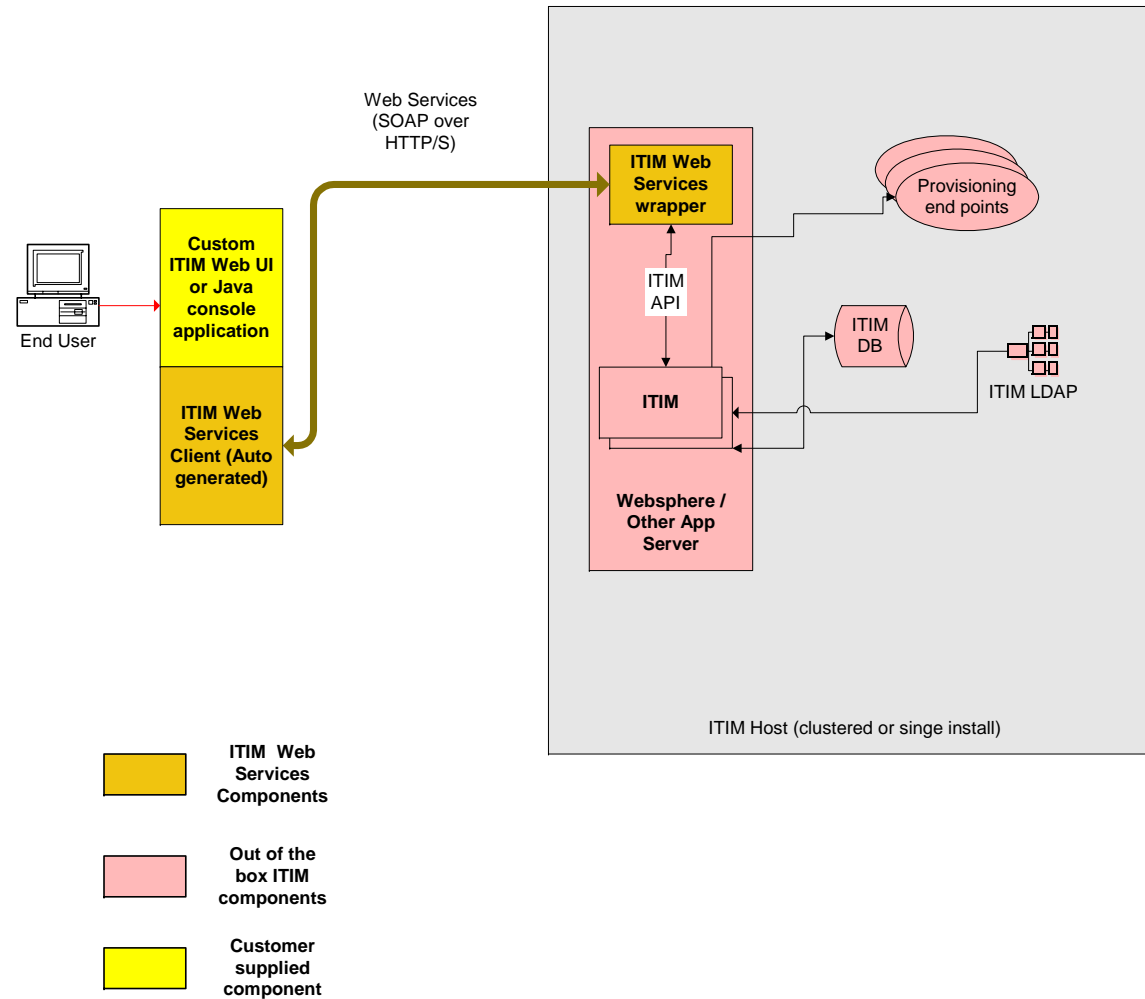



ITIM Web Services Overview

- Lightweight SOAP protocol over HTTP/S to talk to ITIM.
 - Eliminates the need for ITIM or Websphere jars on the client.
- Non Java clients can talk to ITIM.
 - .NET clients can talk to ITIM.
- ITIM API complexity is abstracted by the web services functional API.
- Runs as a web application co-located with ITIM.



ITIM Web Service Architecture



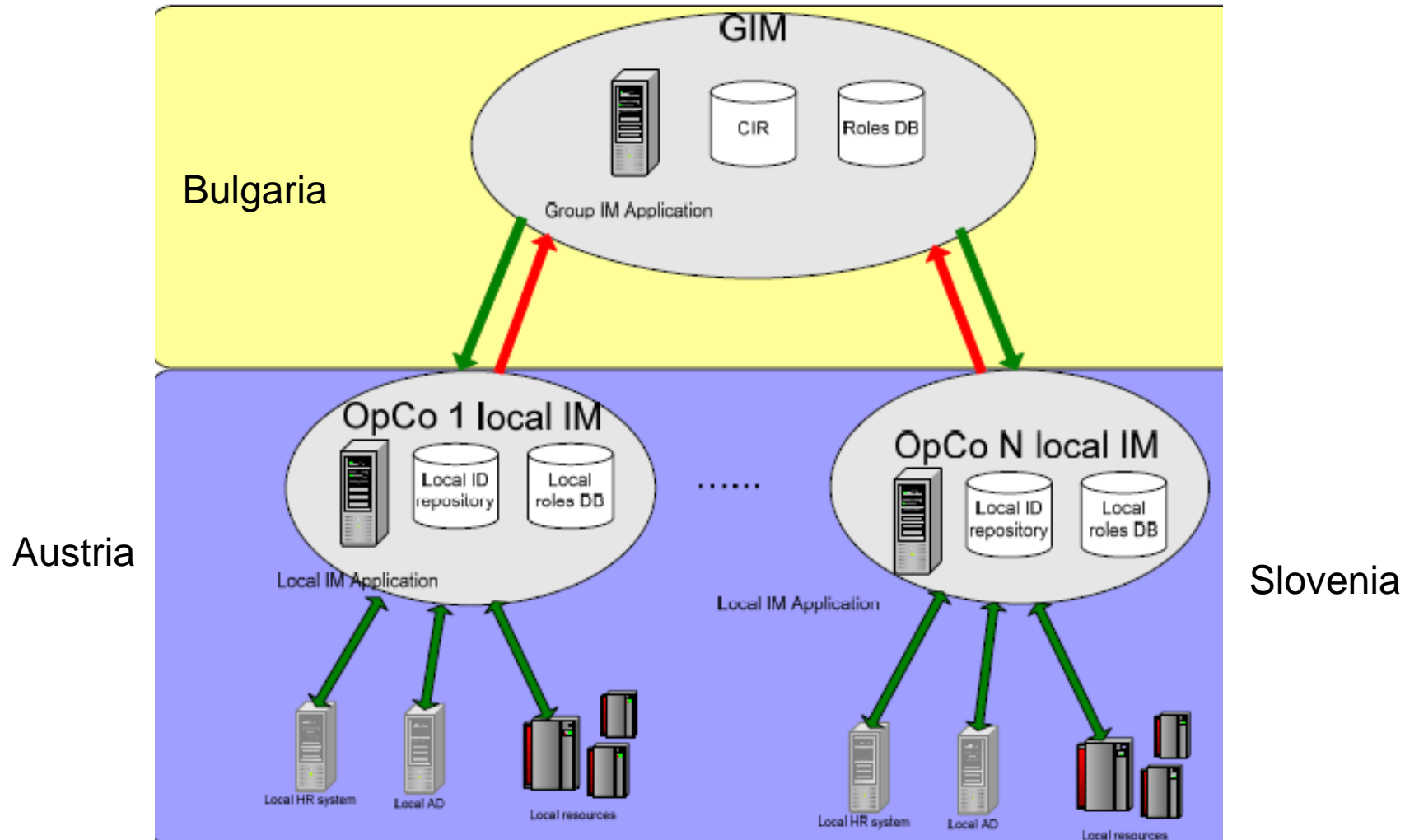


ITIM Web Services Suite

- The web services suite is made of functionally separate services
 - Session Service
 - Account Service
 - Form Service
 - Organizational Container Service
 - Password Service
 - Request Service
 - Role Service
 - Service Service
 - Search Data Service
 - System User Service
 - To Do Service
 - Access Service (ITIM 5.x Only)
- DTIM Solution Leverages WebServices Interfaces



Example Implementation – Telco based out of Bulgaria





**Questions?
Thank You**



Trademarks and disclaimers

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries./ Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. UNIX is a registered trademark of The Open Group in the United States and other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others. Information is provided "AS IS" without warranty of any kind.

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

© IBM Corporation 1994-2010. All rights reserved.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Trademarks of International Business Machines Corporation in the United States, other countries, or both can be found on the World Wide Web at <http://www.ibm.com/legal/copytrade.shtml>.



Why DTIM?

- Why is it needed?
 - To distribute workload in implementations with hundreds or thousands of services.
 - To provide progressive scaling using a distributed services model.
 - To provide enterprises with a rolling upgrade & maintenance window without bringing down ITIM completely.
 - To allow localized administration and centralized identity / account operations.
 - ITIM nodes can be geographically separate.
 - Can provide one off provisioning for a subset of population (say an isolated Dept or a lab).



ITIM Web Services example

- Example of using the web services to authenticate to ITIM and get user's person object.

```
ITIMWebServiceFactory factory = new ITIMWebServiceFactory("http://host/ITIMWebServices");  
WSSession session = factory.getWSSessionService().login(userid, password);  
WSPersonService personService = factory.getWSPersonService();  
WSPerson myPerson = personService.getPrincipalPerson(session);
```




ITIM Web Services Overview

- Runs as a web application co-located with ITIM.
- Simple client and data model
 - WSDL files can be used to generate a web services client and data model.
 - *WSDL can be used to generate non Java clients.*
 - A pre-generated Java client is included.
- Provides a threaded conversation by establishing a session id.



ITIM Web Service Factory

- The pre-generated web service client provides a web service factory (class).
 - The web service factory “publishes” each web service and eliminates the client’s need to determine the service address.
 - It can provide an instance of any of the ITIM Web Services. Obtaining a web service is functionally simple.
 - Example: `webServiceFactory.getWSPasswordService()`.

DTIM Architecture

