IBM 2007 IMPACT

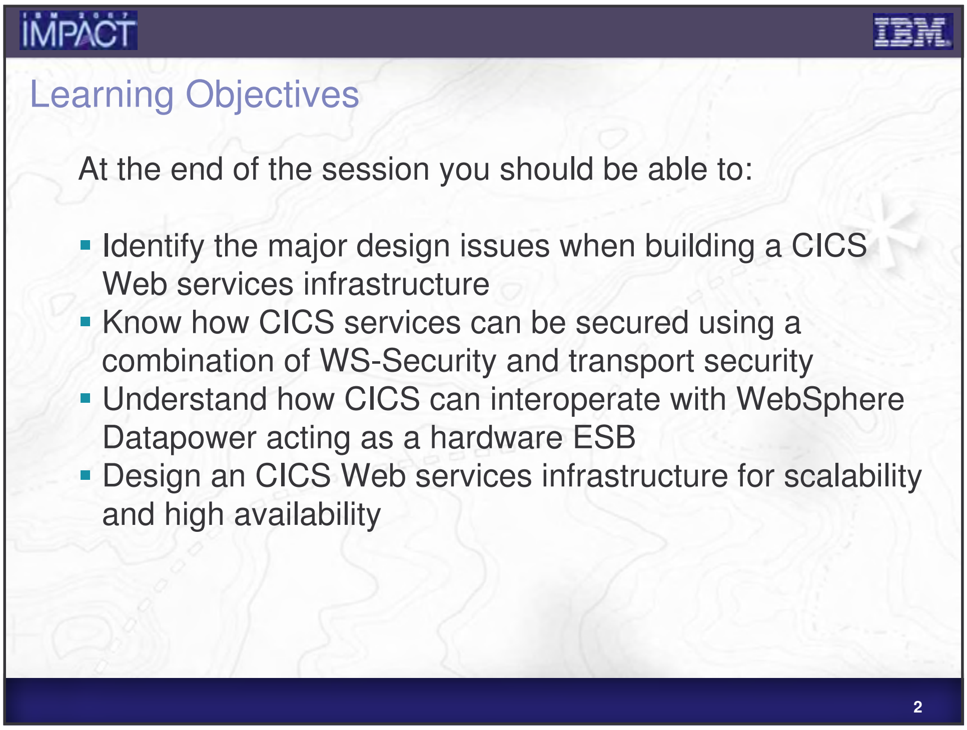
IBM

Implementing CICS Web Services: a customer example

Nigel Williams (IBM Design Center)
(nigel_williams@uk.ibm.com)

Session Number: 4137A

impact·venture*



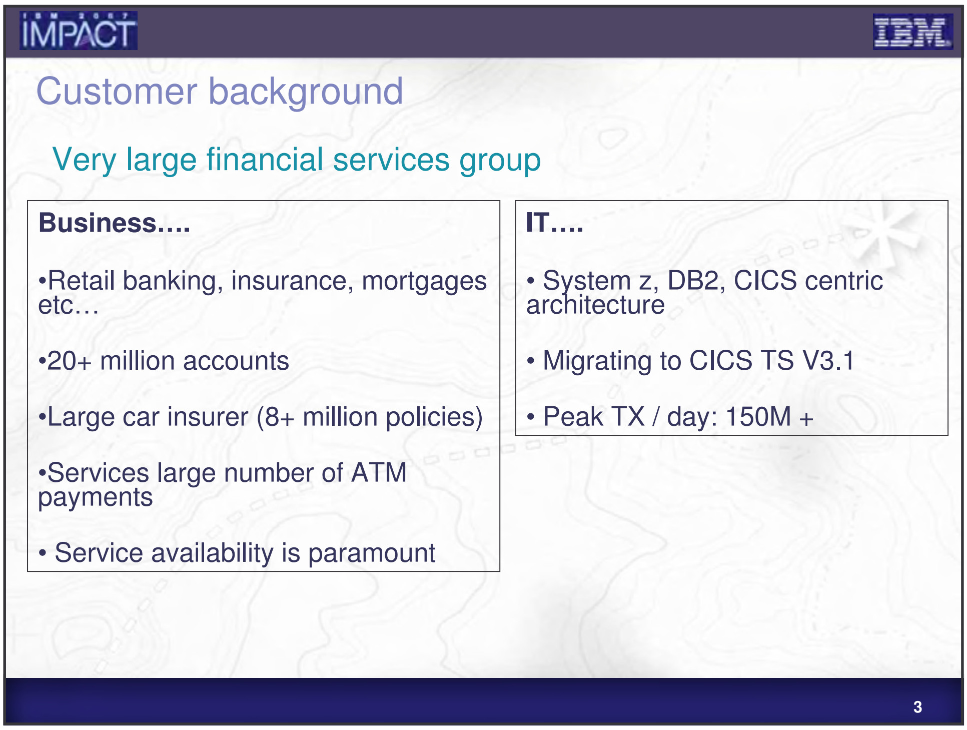
IBM 2007 IMPACT

IBM

Learning Objectives

At the end of the session you should be able to:

- Identify the major design issues when building a CICS Web services infrastructure
- Know how CICS services can be secured using a combination of WS-Security and transport security
- Understand how CICS can interoperate with WebSphere Datapower acting as a hardware ESB
- Design an CICS Web services infrastructure for scalability and high availability



Customer background

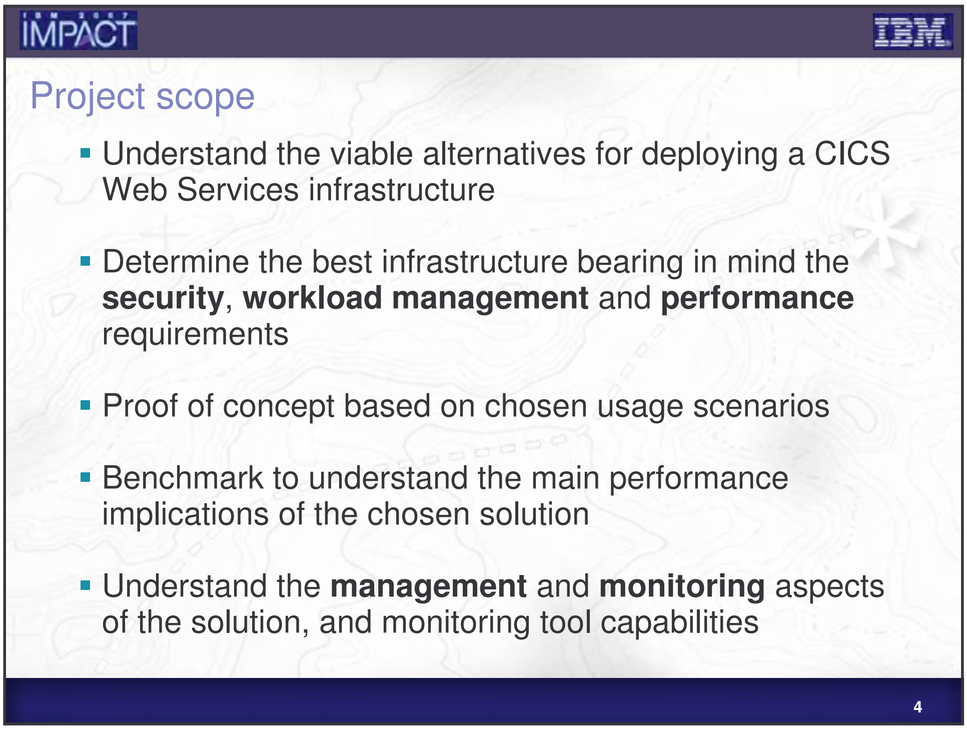
Very large financial services group

Business….

- Retail banking, insurance, mortgages etc…
- 20+ million accounts
- Large car insurer (8+ million policies)
- Services large number of ATM payments
- Service availability is paramount

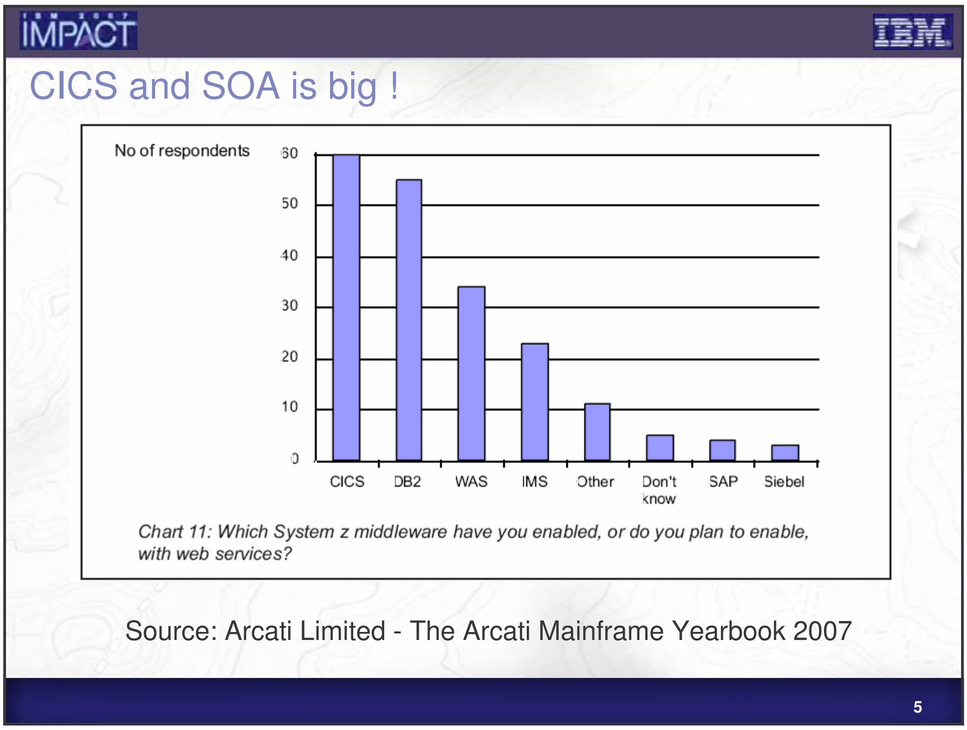
IT….

- System z, DB2, CICS centric architecture
- Migrating to CICS TS V3.1
- Peak TX / day: 150M +



Project scope

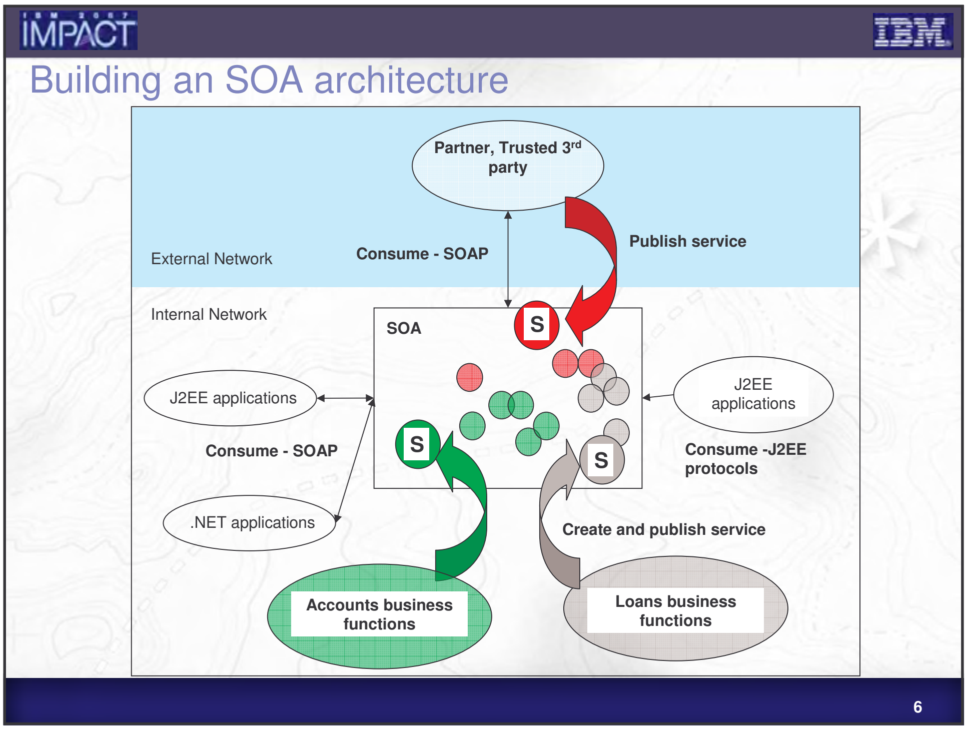
- Understand the viable alternatives for deploying a CICS Web Services infrastructure
- Determine the best infrastructure bearing in mind the **security**, **workload management** and **performance** requirements
- Proof of concept based on chosen usage scenarios
- Benchmark to understand the main performance implications of the chosen solution
- Understand the **management** and **monitoring** aspects of the solution, and monitoring tool capabilities



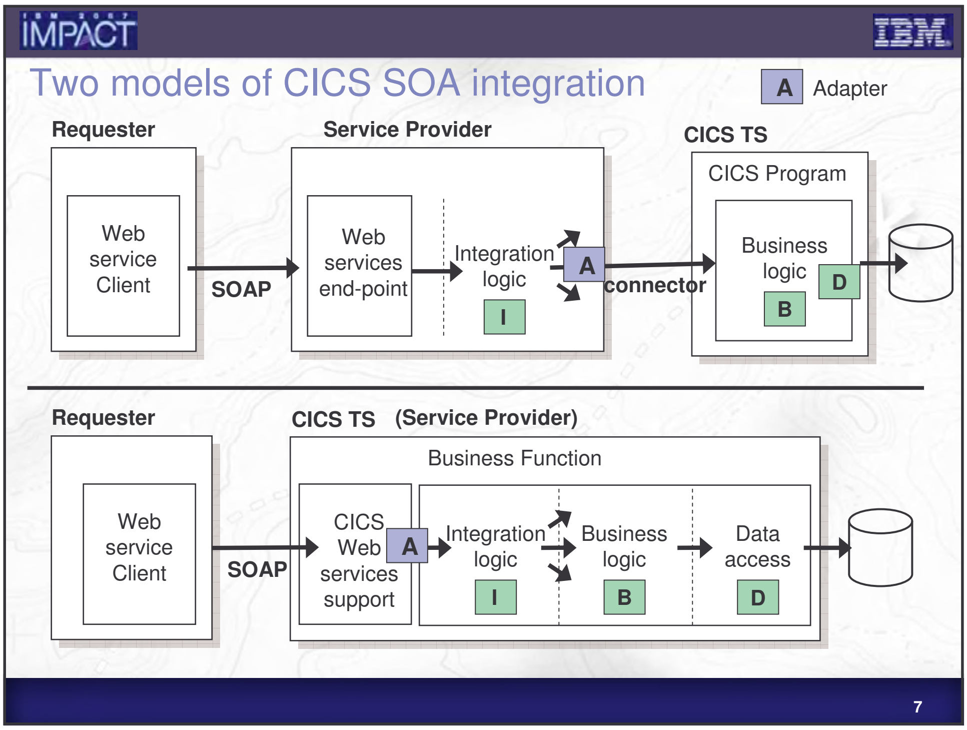
CICS and SOA is big !

Chart 11: Which System z middleware have you enabled, or do you plan to enable, with web services?

Source: Arcati Limited - The Arcati Mainframe Yearbook 2007



Building an SOA architecture



Two models of CICS SOA integration

A Adapter

Requester

Web service Client

SOAP

Service Provider

Web services end-point

Integration logic

I

A

connector

CICS TS

CICS Program

Business logic

B

D

Requester

Web service Client

SOAP

CICS TS (Service Provider)

Business Function

CICS Web services support

A

Integration logic

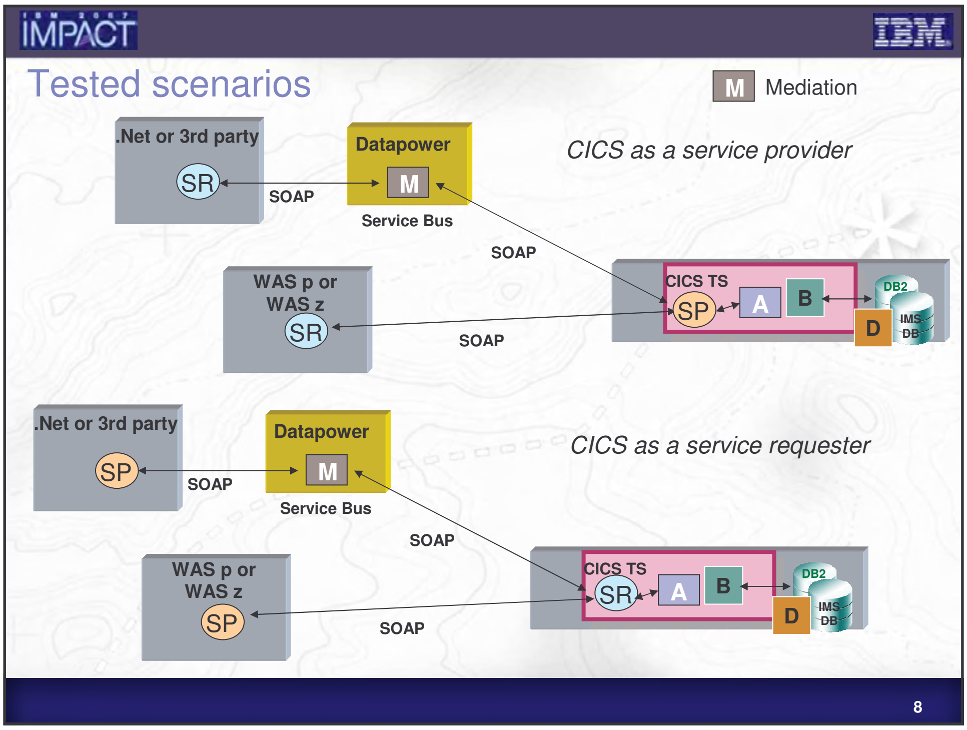
I

Business logic

B

Data access

D



Tested scenarios

M Mediation

CICS as a service provider

.Net or 3rd party

SR

SOAP

Datapower

M

Service Bus

SOAP

WAS p or WAS z

SR

SOAP

CICS TS

SP

A

B

D

DB2

IMS DB

CICS as a service requester

.Net or 3rd party

SP

SOAP

Datapower

M

Service Bus

SOAP

WAS p or WAS z

SP

SOAP

CICS TS

SR

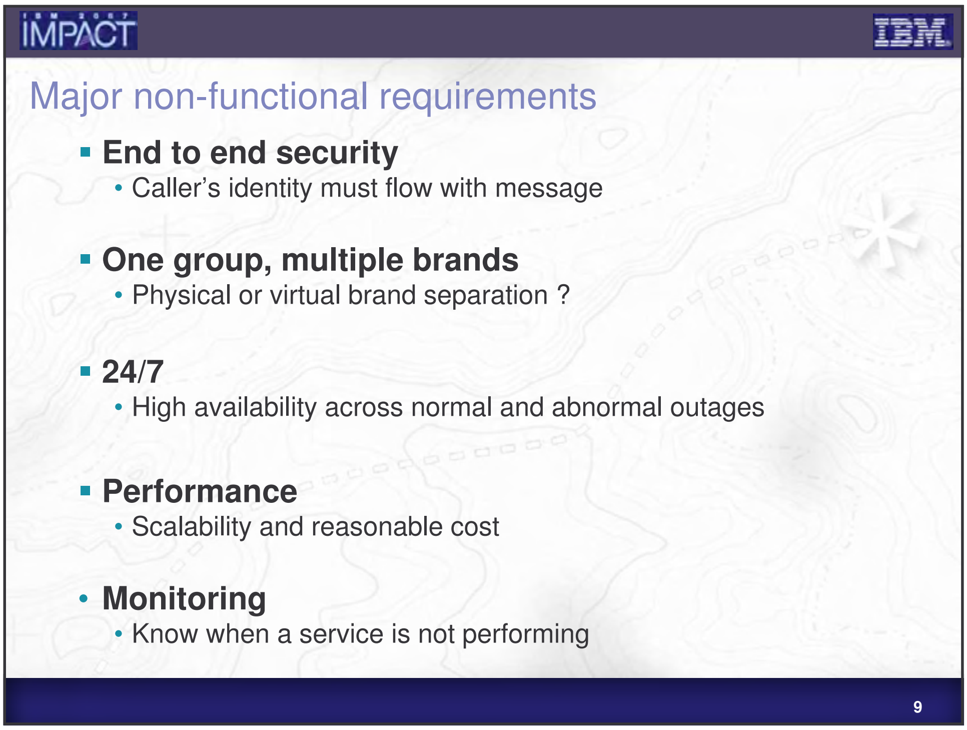
A

B

D

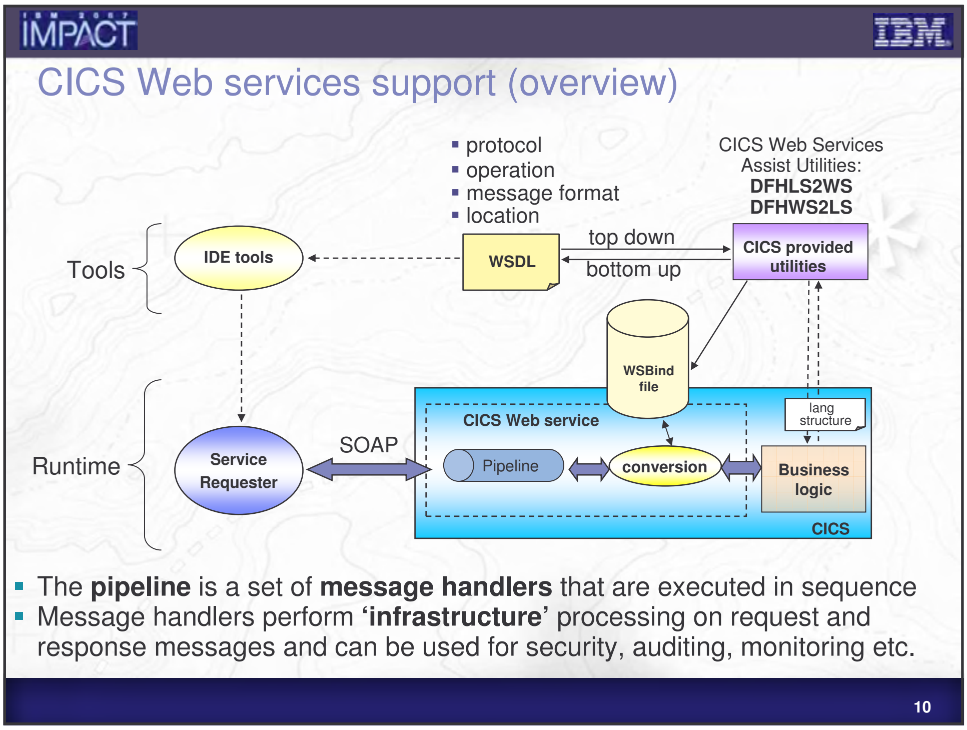
DB2

IMS DB



Major non-functional requirements

- **End to end security**
  - Caller’s identity must flow with message
- **One group, multiple brands**
  - Physical or virtual brand separation ?
- **24/7**
  - High availability across normal and abnormal outages
- **Performance**
  - Scalability and reasonable cost
- **Monitoring**
  - Know when a service is not performing



CICS Web services support (overview)

- protocol
- operation
- message format
- location

CICS Web Services Assist Utilities:
DFHLS2WS
DFHWS2LS

Tools

IDE tools

WSDL

top down

bottom up

CICS provided utilities

WSBind file

lang structure

Runtime

Service Requester

SOAP

CICS Web service

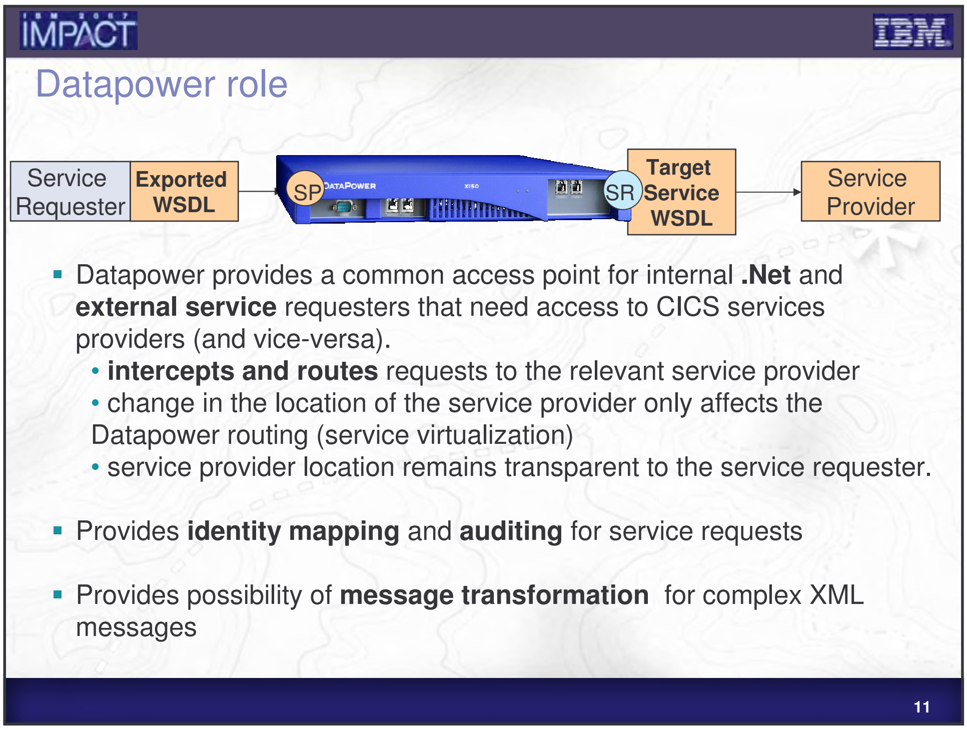
Pipeline

conversion

Business logic

CICS

- The **pipeline** is a set of **message handlers** that are executed in sequence
- Message handlers perform ‘**infrastructure**’ processing on request and response messages and can be used for security, auditing, monitoring etc.

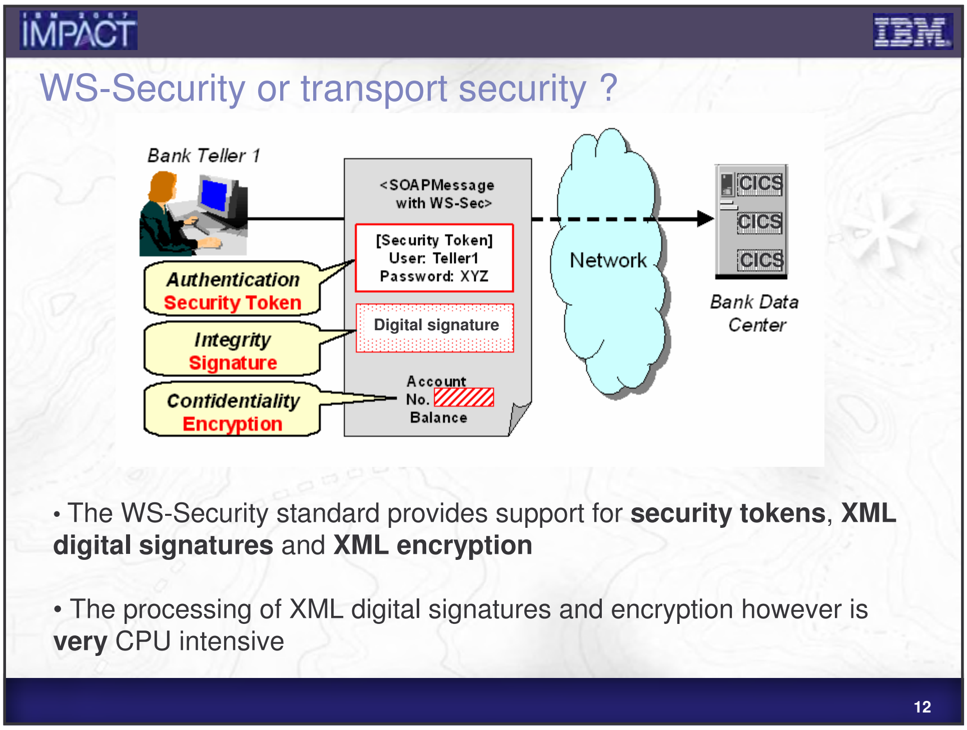


IMPACT IBM

Datapower role

Service Requester
Exported WSDL
SP
SR
Target Service WSDL
Service Provider

- Datapower provides a common access point for internal **.Net** and **external service** requesters that need access to CICS services providers (and vice-versa).
  - **intercepts and routes** requests to the relevant service provider
  - change in the location of the service provider only affects the Datapower routing (service virtualization)
  - service provider location remains transparent to the service requester.
- Provides **identity mapping** and **auditing** for service requests
- Provides possibility of **message transformation** for complex XML messages

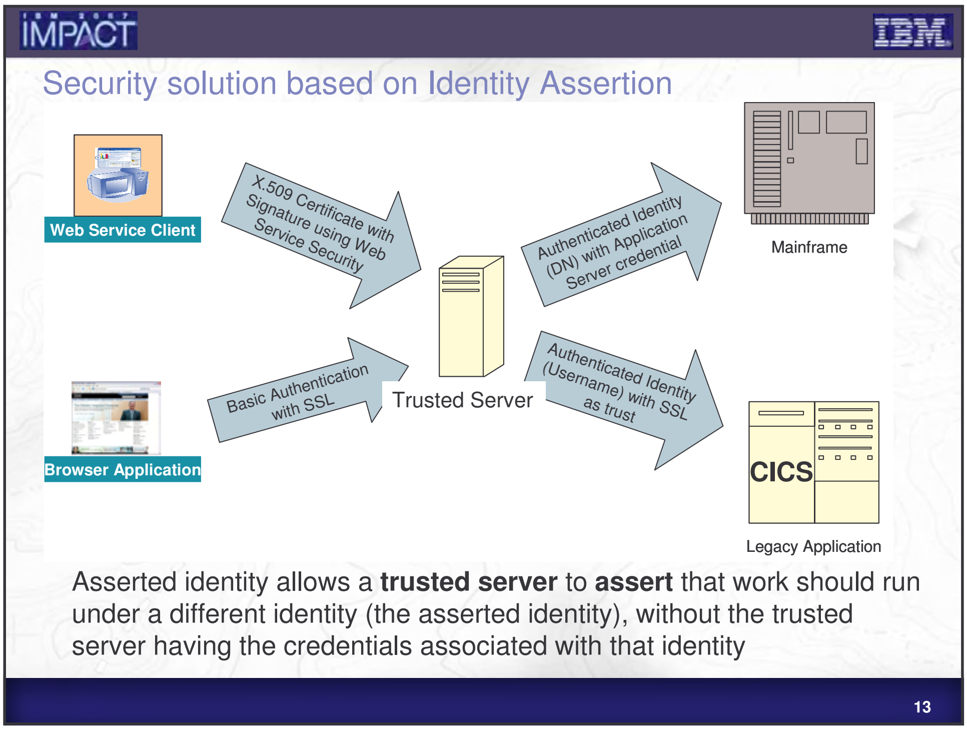


IMPACT IBM

WS-Security or transport security ?

Bank Teller 1
Authentication
Security Token
Integrity
Signature
Confidentiality
Encryption
<SOAPMessage with WS-Sec>
[Security Token]
User: Teller1
Password: XYZ
Digital signature
Account No.
Balance
Network
CICS
CICS
CICS
Bank Data Center

- The WS-Security standard provides support for **security tokens**, **XML digital signatures** and **XML encryption**
- The processing of XML digital signatures and encryption however is **very** CPU intensive



Security solution based on Identity Assertion

Web Service Client

X.509 Certificate with Signature using Web Service Security

Browser Application

Basic Authentication with SSL

Trusted Server

Authenticated Identity (DN) with Application Server credential

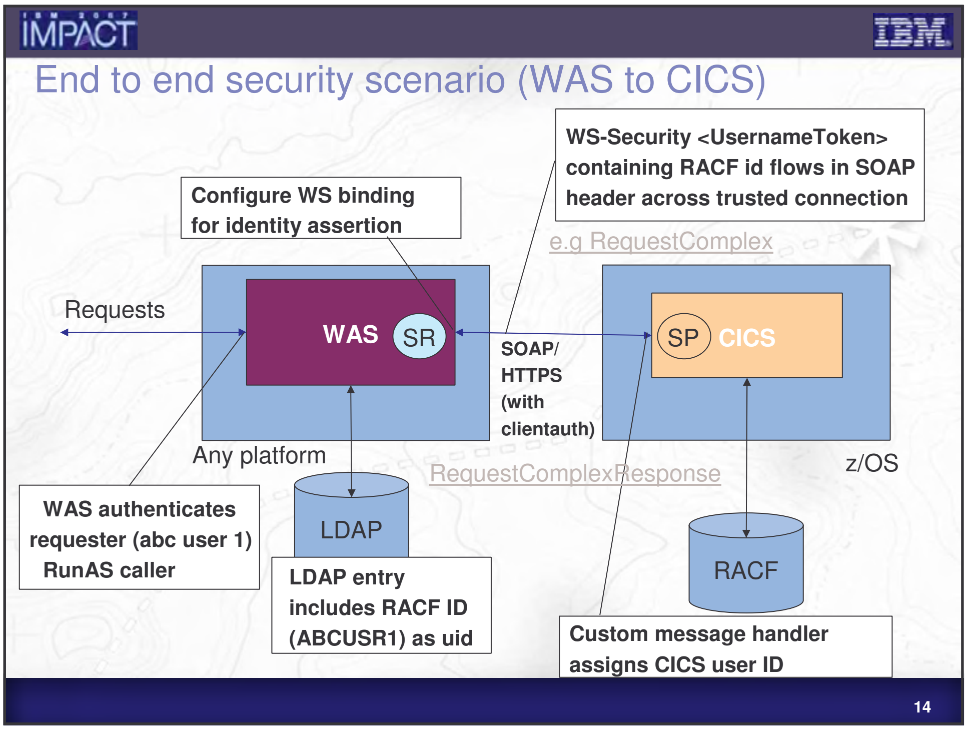
Mainframe

Authenticated Identity (Username) with SSL as trust

CICS

Legacy Application

Asserted identity allows a **trusted server** to **assert** that work should run under a different identity (the asserted identity), without the trusted server having the credentials associated with that identity



End to end security scenario (WAS to CICS)

WS-Security <UsernameToken> containing RACF id flows in SOAP header across trusted connection

Configure WS binding for identity assertion

e.g RequestComplex

Requests

WAS

SR

SOAP/ HTTPS (with clientauth)

SP

CICS

Any platform

RequestComplexResponse

z/OS

WAS authenticates requester (abc user 1) RunAS caller

LDAP

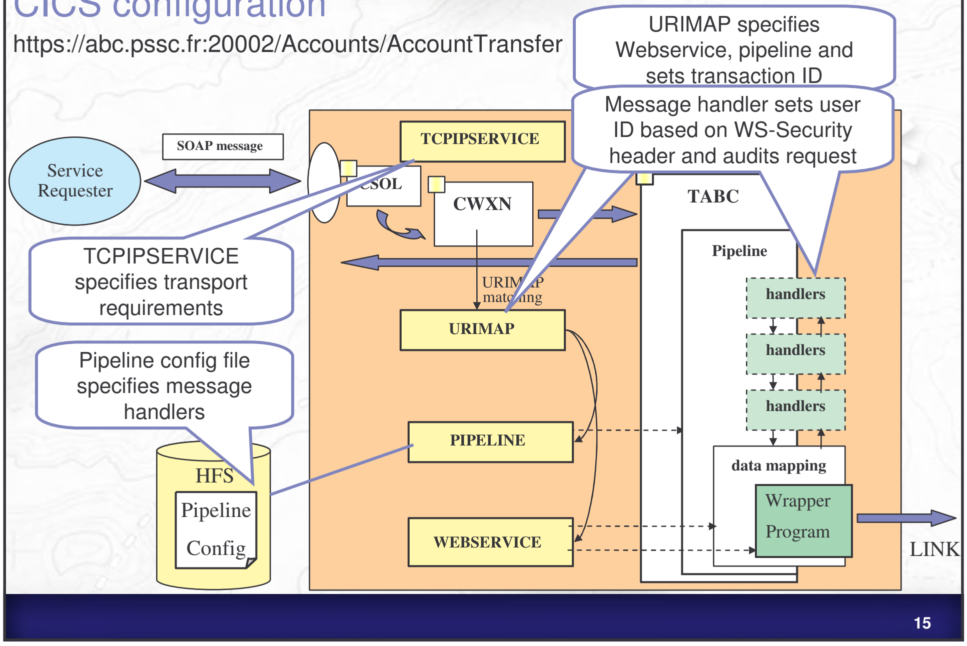
LDAP entry includes RACF ID (ABCUSR1) as uid

RACF

Custom message handler assigns CICS user ID

CICS configuration

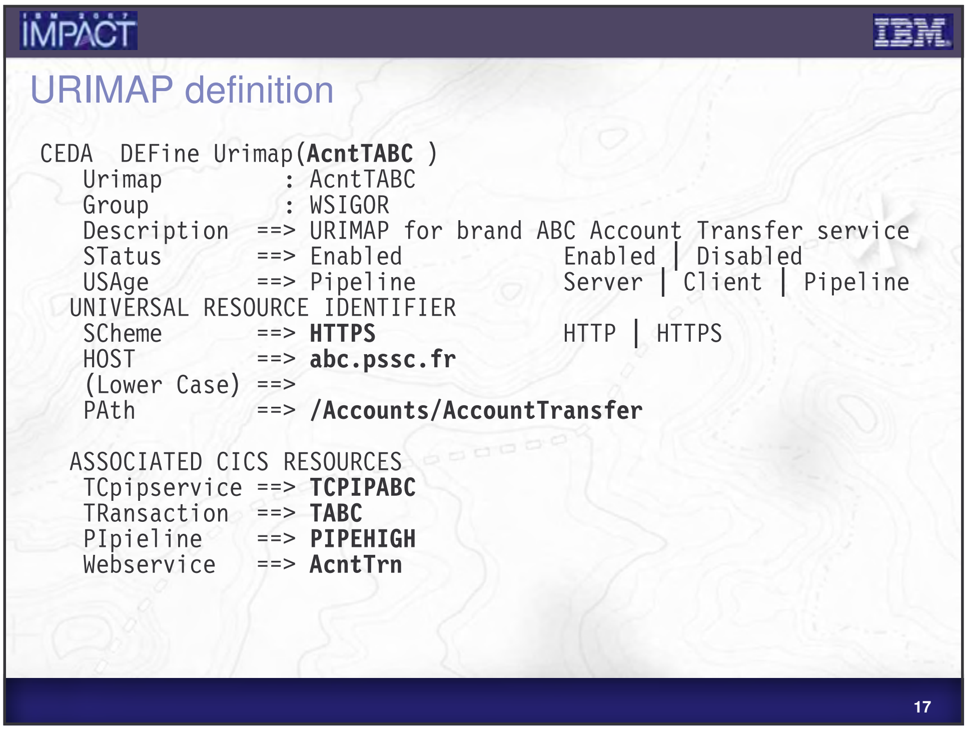
https://abc.pssc.fr:20002/Accounts/AccountTransfer



URIMAP specifies Webservice, pipeline and sets transaction ID
Message handler sets user ID based on WS-Security header and audits request
SOAP message
Service Requester
TCPIPSERVICE
CSOL
CWXN
TABC
Pipeline
TCPIPSERVICE specifies transport requirements
URIMAP matching
URIMAP
handlers
handlers
handlers
Pipeline config file specifies message handlers
PIPELINE
data mapping
HFS
Pipeline Config
Wrapper Program
WEBSERVICE
LINK

TCPIPSERVICE definition

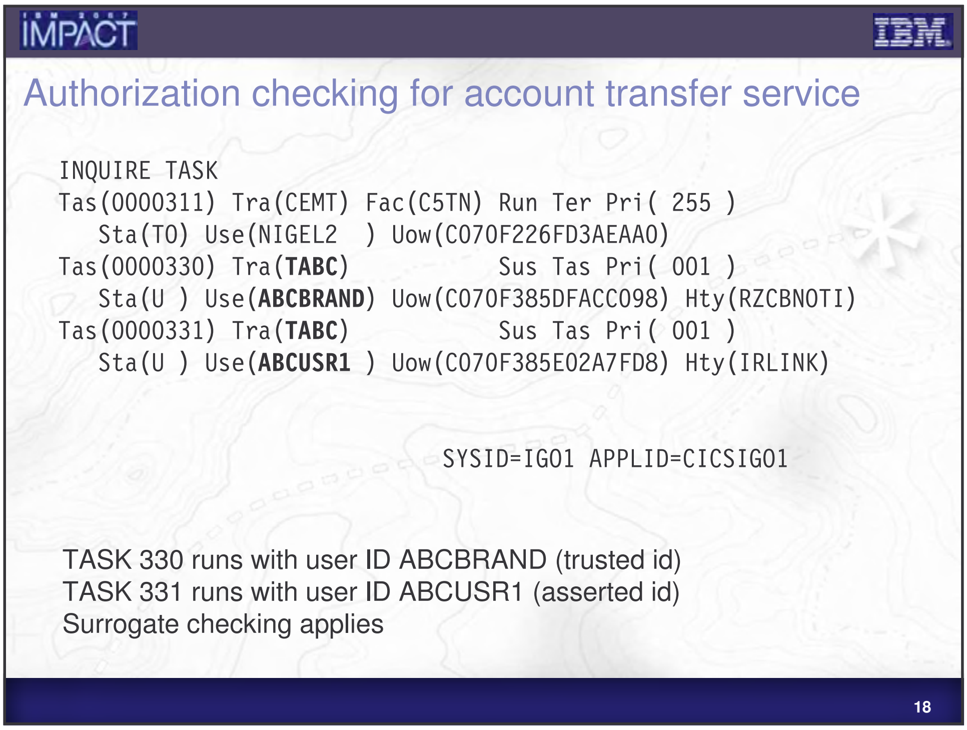
```
CEDA  DEFine TCpipservice( TCPIPABC )
   TCpipservice    : TCPIPABC
   GROup           : WSIGOR
   DEscription  ==> TCPIPSERVICE FOR BRAND ABC
   Urm          ==> DFHWBADX
   POrtnumber   ==> 20002              1-65535
   STatus       ==> Open               Open ! Closed
   PROtocol     ==> Http               Iiop ! Http ! Eci ! User
   TRansaction  ==> CWXN
   Backlog      ==> 00005              0-32767
   TSqprefix    ==>
   Ipaddress    ==>
   SOcketclose  ==> 000030             No ! 0-240000 (HHMMSS)
   Maxdatalen   ==> 000032             3-524288
 SECURITY
   SSl          ==> Clientauth         Yes ! No ! Clientauth
```



URIMAP definition

```
CEDA  DEFine Urimap(AcntTABC )
   Urimap         : AcntTABC
   Group          : WSIGOR
   Description  ==> URIMAP for brand ABC Account Transfer service
   STatus       ==> Enabled            Enabled | Disabled
   USAge        ==> Pipeline           Server | Client | Pipeline
  UNIVERSAL RESOURCE IDENTIFIER
   SCheme       ==> HTTPS              HTTP | HTTPS
   HOST         ==> abc.pssc.fr
   (Lower Case) ==>
   PAth         ==> /Accounts/AccountTransfer

  ASSOCIATED CICS RESOURCES
   TCpipservice ==> TCPIPABC
   TRansaction  ==> TABC
   PIpieline    ==> PIPEHIGH
   Webservice   ==> AcntTrn
```



Authorization checking for account transfer service

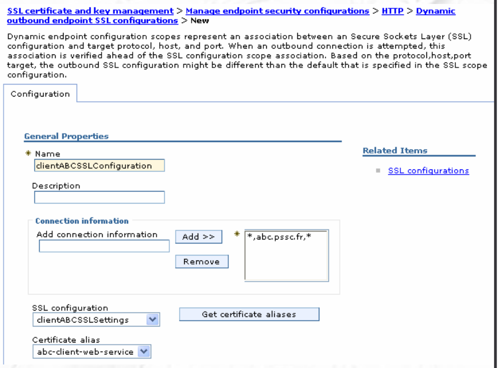
```
INQUIRE TASK
Tas(0000311) Tra(CEMT) Fac(C5TN) Run Ter Pri( 255 )
   Sta(TO) Use(NIGEL2  ) Uow(C070F226FD3AEAA0)
Tas(0000330) Tra(TABC)           Sus Tas Pri( 001 )
   Sta(U ) Use(ABCBRAND) Uow(C070F385DFACC098) Hty(RZCBNOTI)
Tas(0000331) Tra(TABC)           Sus Tas Pri( 001 )
   Sta(U ) Use(ABCUSR1 ) Uow(C070F385E02A7FD8) Hty(IRLINK)


                           SYSID=IG01 APPLID=CICSIG01
```

TASK 330 runs with user ID ABCBRAND (trusted id)
TASK 331 runs with user ID ABCUSR1 (asserted id)
Surrogate checking applies

WebSphere configuration

- **WS-Security identity assertion**
  - Configure the request generator
    - Include **UsernameToken** in SOAP message request based on **RunAs** identity
- **SSL**
  - Configure JSSE truststore and keystore
  - Configure WebSphere to use **dynamic outbound endpoint SSL** configurations (new in V6.1)



SSL certificate and key management > Manage endpoint security configurations > HTTP > Dynamic outbound endpoint SSL configurations > New

Dynamic endpoint configuration scopes represent an association between an Secure Sockets Layer (SSL) configuration and target protocol, host, and port. When an outbound connection is attempted, this association is verified ahead of the SSL configuration scope association. Based on the protocol,host,port target, the outbound SSL configuration might be different than the default that is specified in the SSL scope configuration.

Configuration

General Properties

* Name: clientABCSSLConfiguration

Description:

Connection information

Add connection information:

* *,abc.pssc.fr,*

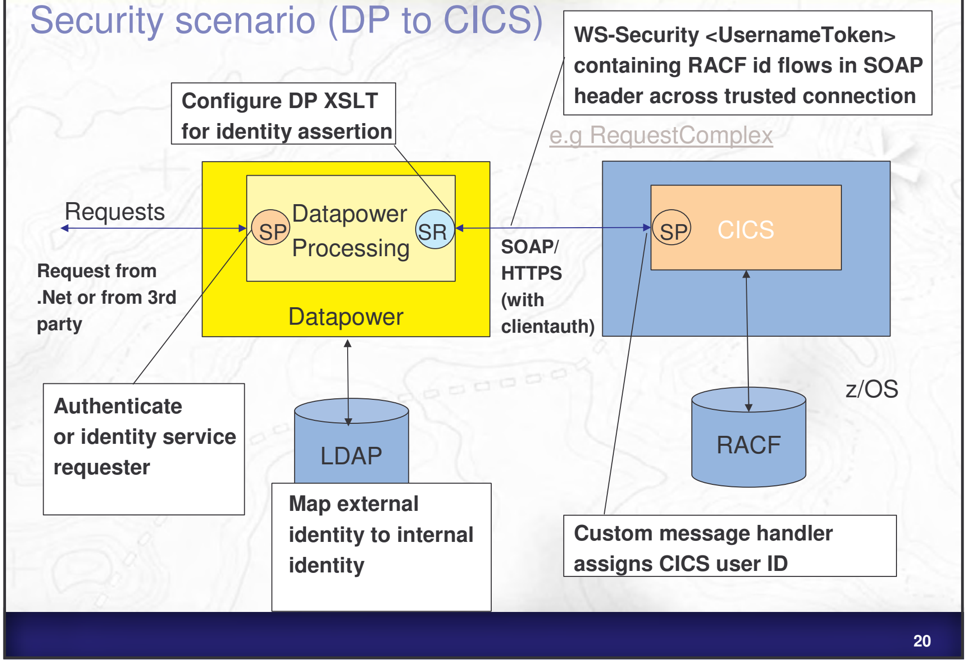
SSL configuration: clientABCSSLSettings

Certificate alias: abc-client-web-service

Related Items

- SSL configurations

Security scenario (DP to CICS)



WS-Security <UsernameToken> containing RACF id flows in SOAP header across trusted connection

e.g RequestComplex

Configure DP XSLT for identity assertion

Requests

Request from .Net or from 3rd party

SOAP/ HTTPS (with clientauth)

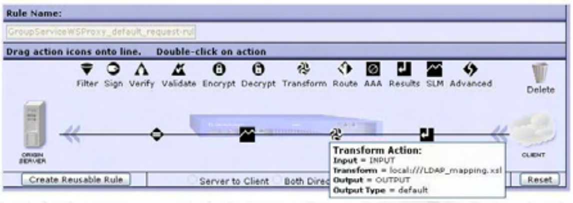
Authenticate or identity service requester

Map external identity to internal identity

Custom message handler assigns CICS user ID

Datapower configuration

- **Web Service Proxy WSDLs**
  - For local endpoint (DP) and for target endpoint (CICS)
- **SSL**
  - Add certificates and create SSL Proxy Profile
  - Configure Crypto key for each brand
- **WS-Security**
  - Create **Transform** rule to add UsernameToken to SOAP message
- **Routing**
  - Create **Route** rule to route to brand CICS TCP/IP port and to dynamically choose client certificate based on brand

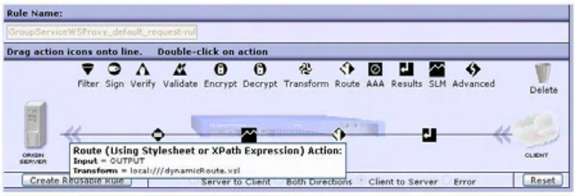


Rule Name:

GroupServiceWSProxy_default_request-rul

Drag action icons onto line. Double-click on action

Transform Action:
Input = INPUT
Transform = local:///LDAP_mapping.xsl
Output = OUTPUT
Output Type = default



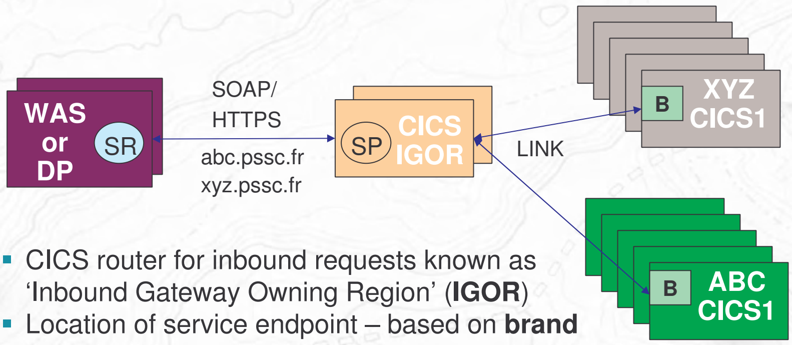
Rule Name:

GroupServiceWSProxy_default_request-rul

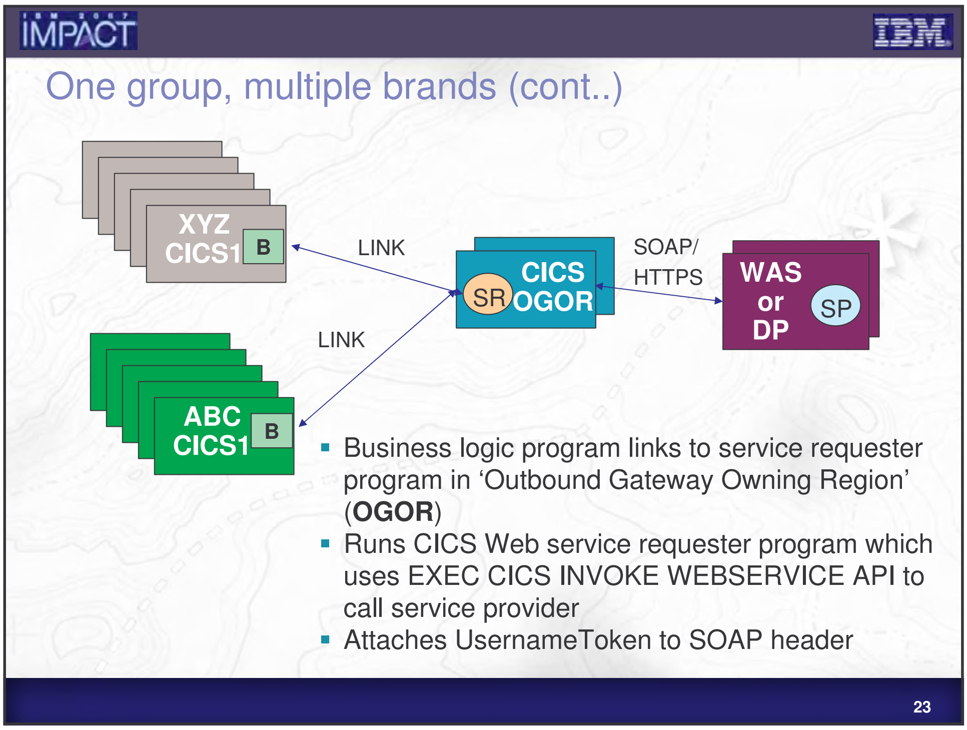
Drag action icons onto line. Double-click on action

Route (Using Stylesheet or XPath Expression) Action:
Input = OUTPUT
Transform = local:///dynamicRoute.xsl

One group, multiple brands

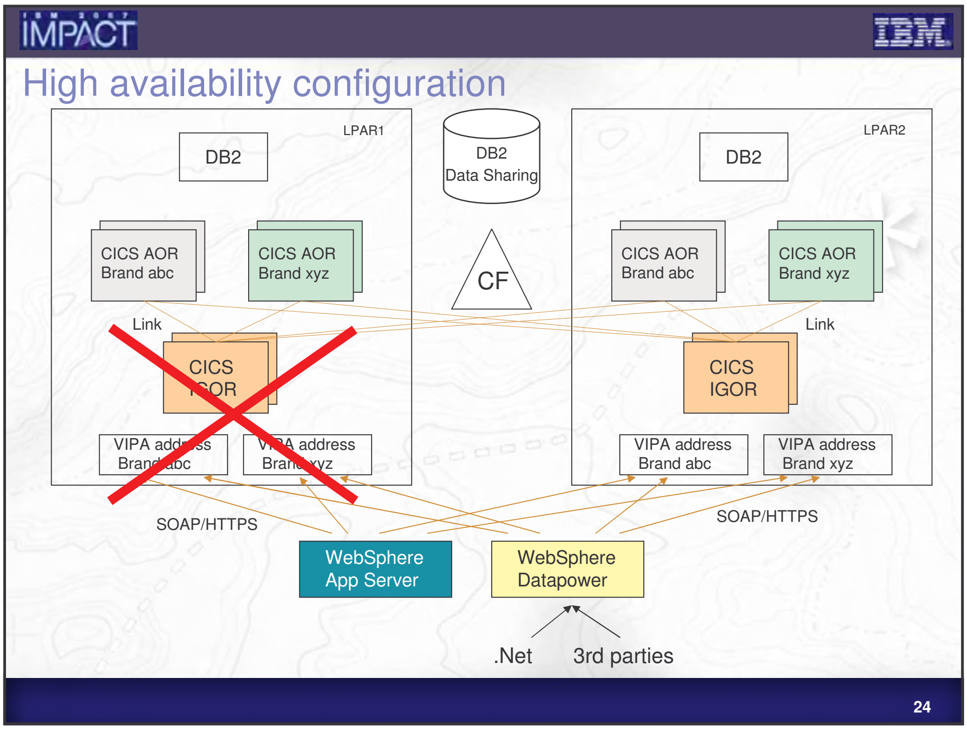


- CICS router for inbound requests known as 'Inbound Gateway Owning Region' (**IGOR**)
- Location of service endpoint – based on **brand** host names
- IGOR runs CICS **wrapper** program ('meet in the middle' approach)
- Establishes transaction context (brand specific transaction id and user id from **UsernameToken**)



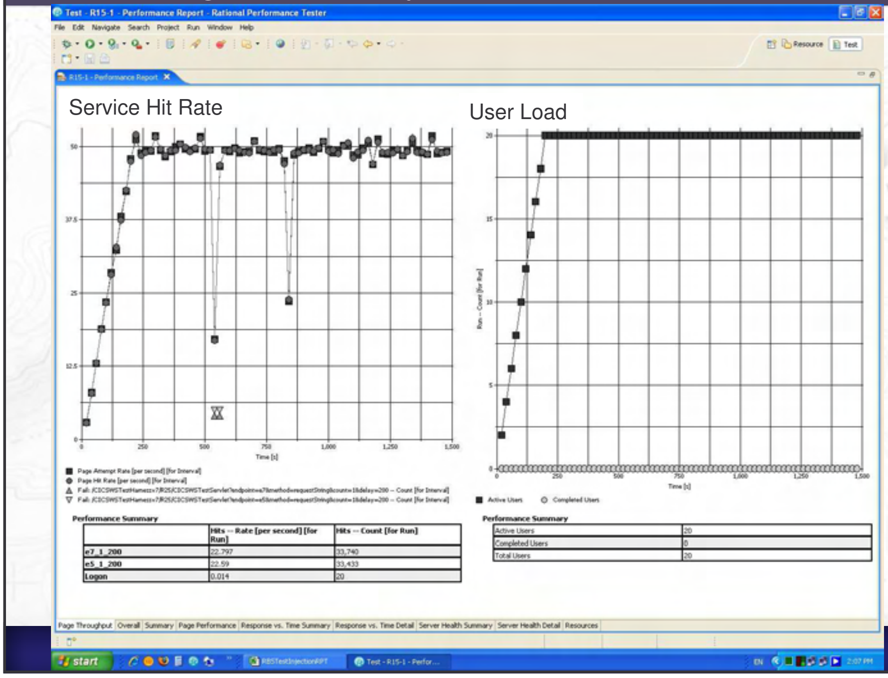
One group, multiple brands (cont..)

- Business logic program links to service requester program in ‘Outbound Gateway Owning Region’ (**OGOR**)
- Runs CICS Web service requester program which uses EXEC CICS INVOKE WEBSERVICE API to call service provider
- Attaches UsernameToken to SOAP header



High availability configuration

High availability tested scenario



■ Page Attempt Rate [per second] [for Interval]
● Page Hit Rate [per second] [for Interval]
△ Fail: /CICSWSTestHarness/v7/R25/CICSWSTestServlet?endpoint=e7&method=requestString&count=1&delay=200 -- Count [for Interval]
▽ Fail: /CICSWSTestHarness/v7/R25/CICSWSTestServlet?endpoint=e5&method=requestString&count=1&delay=200 -- Count [for Interval]

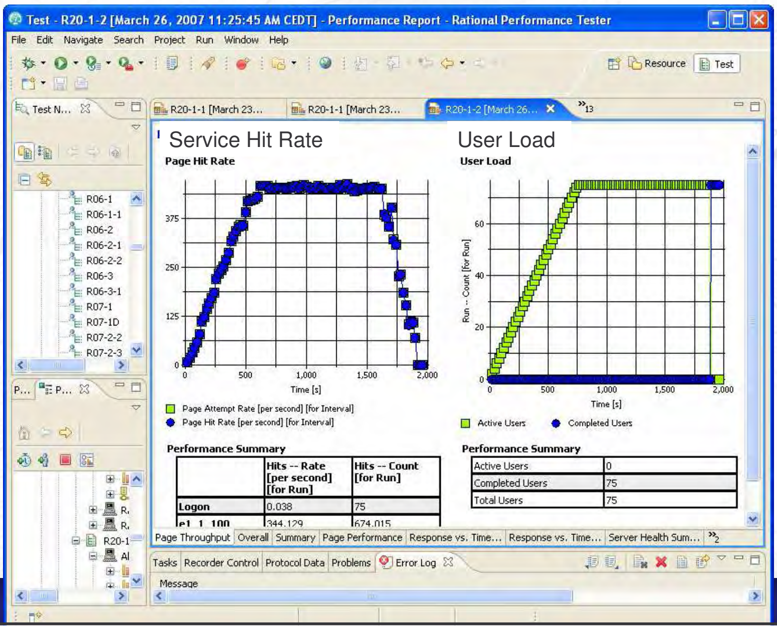
Performance Summary

	Hits -- Rate [per second] [for Run]	Hits -- Count [for Run]
e7_1_200	22.797	33,740
e5_1_200	22.59	33,433
Logon	0.014	20

Performance Summary

Active Users	20
Completed Users	0
Total Users	20

Performance tests



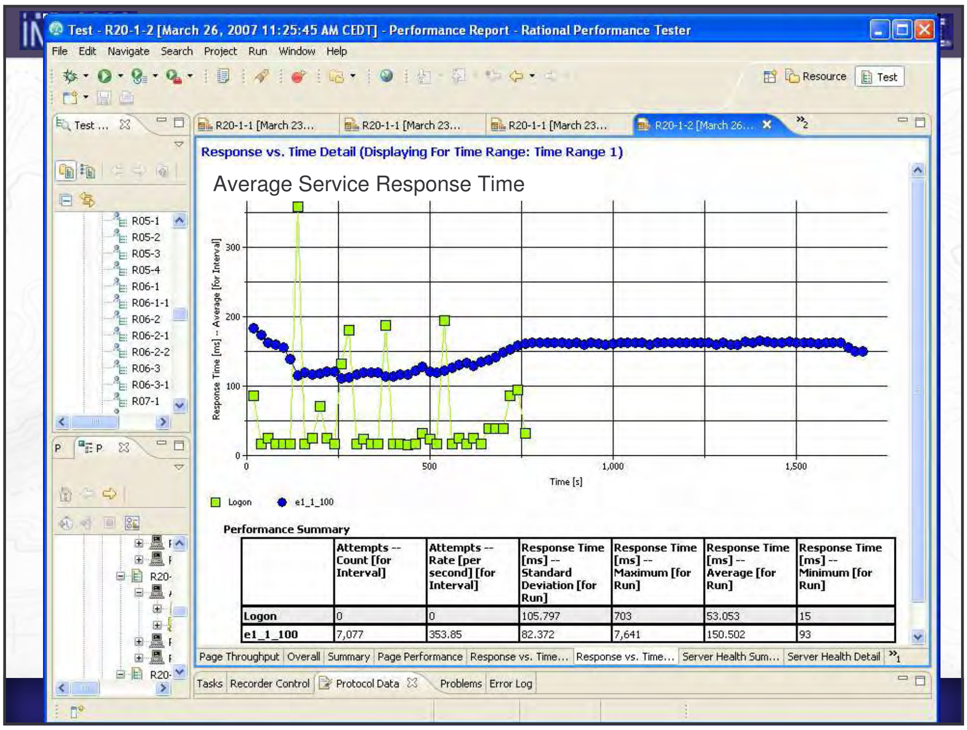
🟩 Page Attempt Rate [per second] [for Interval]
● Page Hit Rate [per second] [for Interval]

Performance Summary

	Hits -- Rate [per second] [for Run]	Hits -- Count [for Run]
Logon	0.038	75
e1_1_100	344.129	674.015

Performance Summary

Active Users	0
Completed Users	75
Total Users	75



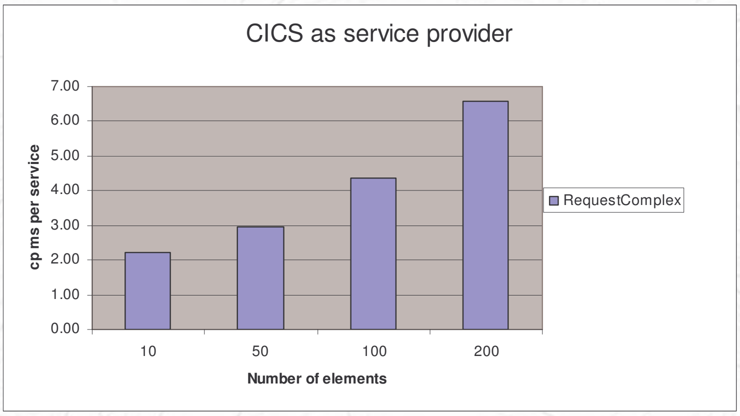
Test - R20-1-2 [March 26, 2007 11:25:45 AM CEDT] - Performance Report - Rational Performance Tester

Response vs. Time Detail (Displaying For Time Range: Time Range 1)

Performance Summary

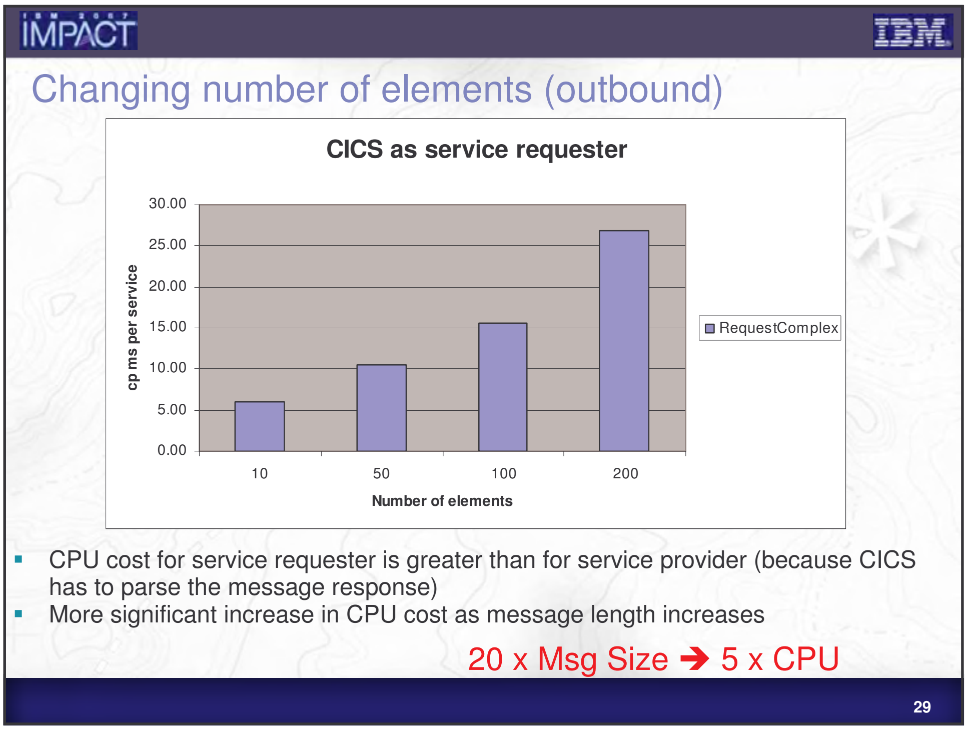
	Attempts -- Count [for Interval]	Attempts -- Rate [per second] [for Interval]	Response Time [ms] -- Standard Deviation [for Run]	Response Time [ms] -- Maximum [for Run]	Response Time [ms] -- Average [for Run]	Response Time [ms] -- Minimum [for Run]
Logon	0	0	105.797	703	53.053	15
e1_1_100	7,077	353.85	82.372	7,641	150.502	93

Changing the number of elements (inbound)



- Web service performance depends on the length and complexity of the message
- **Note:** each element in this test contains 10 sub-elements; the length of the 10 element message is 3.3K

20 x Msg Size ➔ 3 x CPU

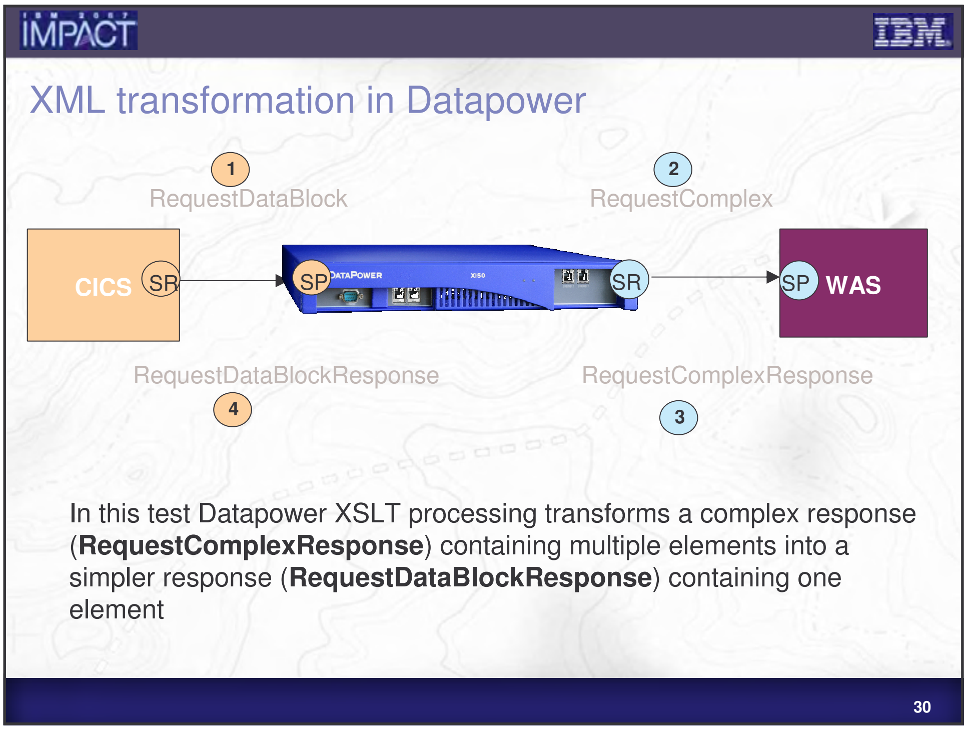


Changing number of elements (outbound)

- CPU cost for service requester is greater than for service provider (because CICS has to parse the message response)
- More significant increase in CPU cost as message length increases

20 x Msg Size ➔ 5 x CPU

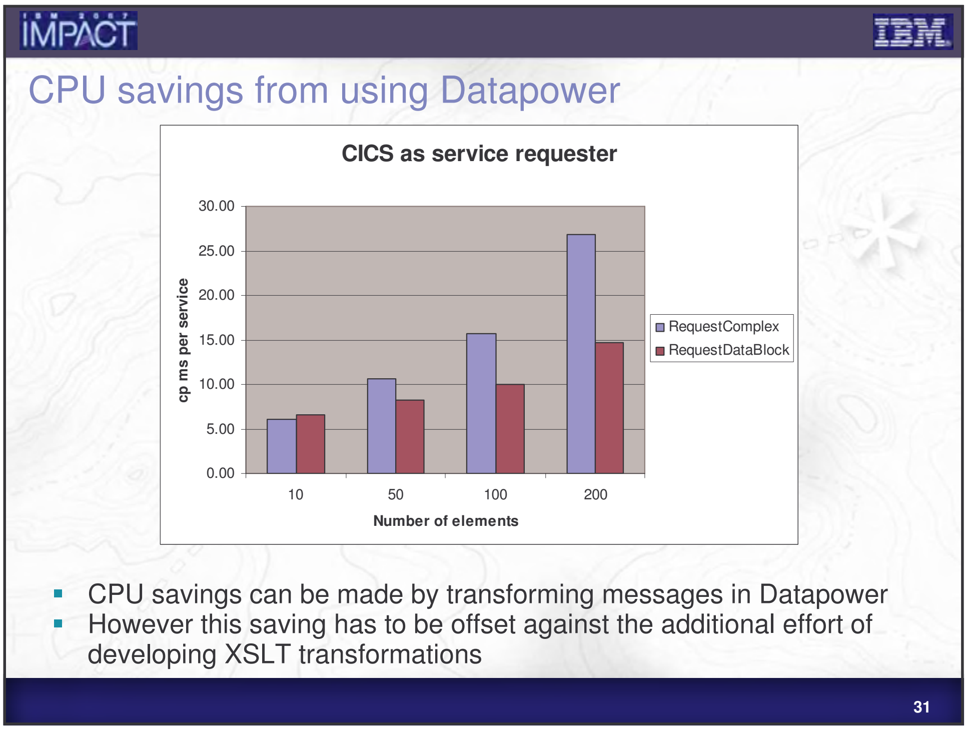
29



XML transformation in Datapower

In this test Datapower XSLT processing transforms a complex response (**RequestComplexResponse**) containing multiple elements into a simpler response (**RequestDataBlockResponse**) containing one element

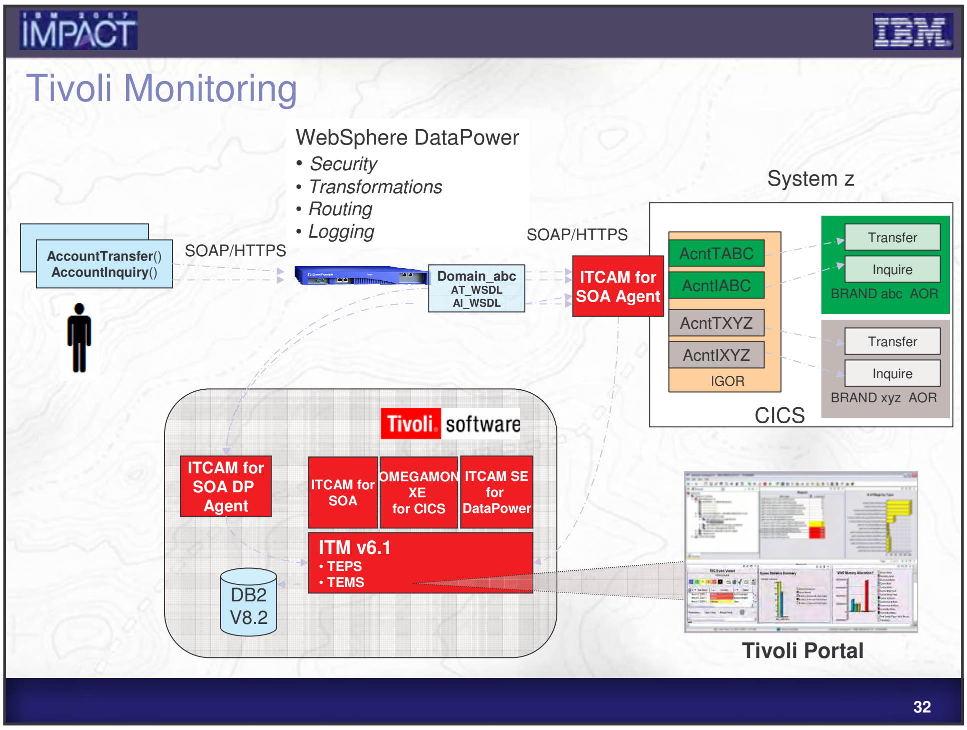
30



CPU savings from using Datapower

- CPU savings can be made by transforming messages in Datapower
- However this saving has to be offset against the additional effort of developing XSLT transformations

31

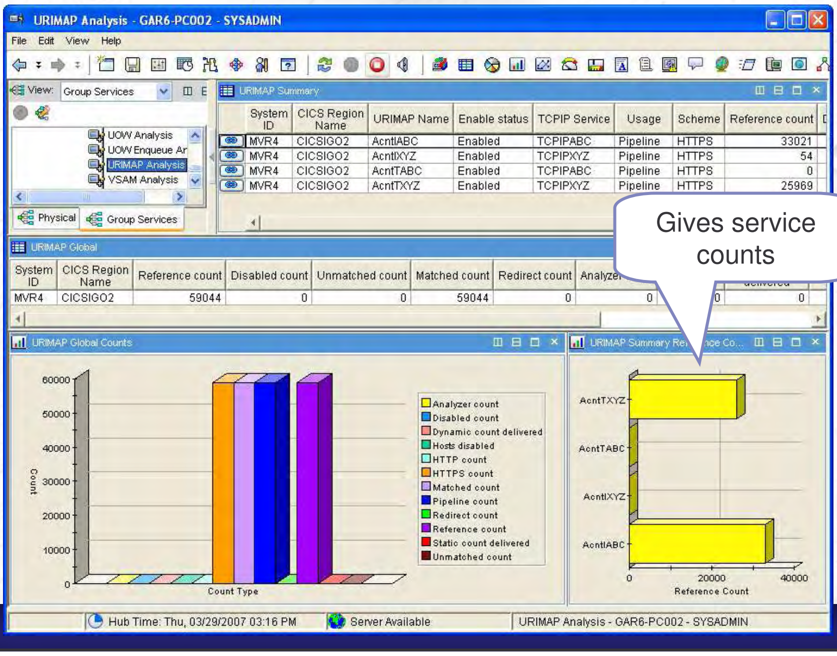


Tivoli Monitoring

WebSphere DataPower
- *Security*
- *Transformations*
- *Routing*
- *Logging*

32

IMPACT OMEGAMON XE for CICS



URIMAP Summary

System ID	CICS Region Name	URIMAP Name	Enable status	TCPIP Service	Usage	Scheme	Reference count
MVR4	CICSIGO2	AcntIABC	Enabled	TCPIPABC	Pipeline	HTTPS	33021
MVR4	CICSIGO2	AcntIXYZ	Enabled	TCPIPXYZ	Pipeline	HTTPS	54
MVR4	CICSIGO2	AcntTABC	Enabled	TCPIPABC	Pipeline	HTTPS	0
MVR4	CICSIGO2	AcntTXYZ	Enabled	TCPIPXYZ	Pipeline	HTTPS	25969

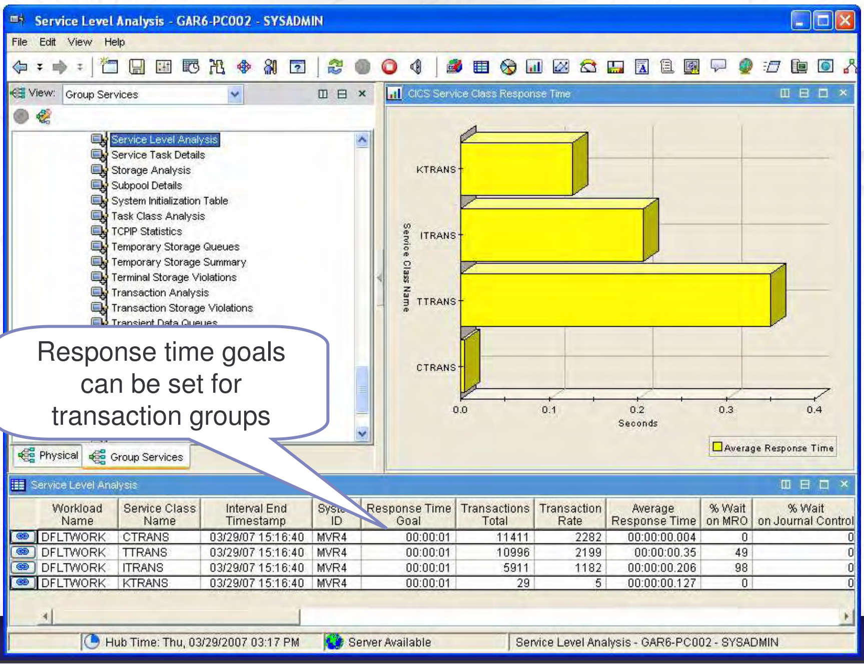
URIMAP Global

System ID	CICS Region Name	Reference count	Disabled count	Unmatched count	Matched count	Redirect count	Analyze		delivered
MVR4	CICSIGO2	59044	0	0	59044	0	0	0	0

Hub Time: Thu, 03/29/2007 03:16 PM | Server Available | URIMAP Analysis - GAR6-PC002 - SYSADMIN

Gives service counts

IMPACT OMEGAMON XE for CICS



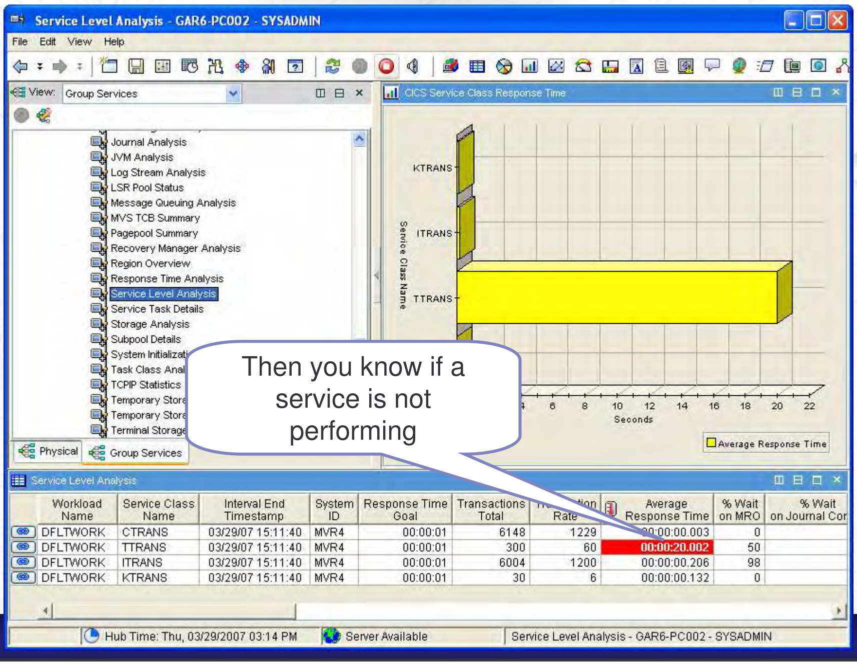
Service Level Analysis

Workload Name	Service Class Name	Interval End Timestamp	Syste ID	Response Time Goal	Transactions Total	Transaction Rate	Average Response Time	% Wait on MRO	% Wait on Journal Control
DFLTWORK	CTRANS	03/29/07 15:16:40	MVR4	00:00:01	11411	2282	00:00:00.004	0	0
DFLTWORK	TTRANS	03/29/07 15:16:40	MVR4	00:00:01	10996	2199	00:00:00.35	49	0
DFLTWORK	ITRANS	03/29/07 15:16:40	MVR4	00:00:01	5911	1182	00:00:00.206	98	0
DFLTWORK	KTRANS	03/29/07 15:16:40	MVR4	00:00:01	29	5	00:00:00.127	0	0

Hub Time: Thu, 03/29/2007 03:17 PM | Server Available | Service Level Analysis - GAR6-PC002 - SYSADMIN

Response time goals can be set for transaction groups

OMEGAMON XE for CICS

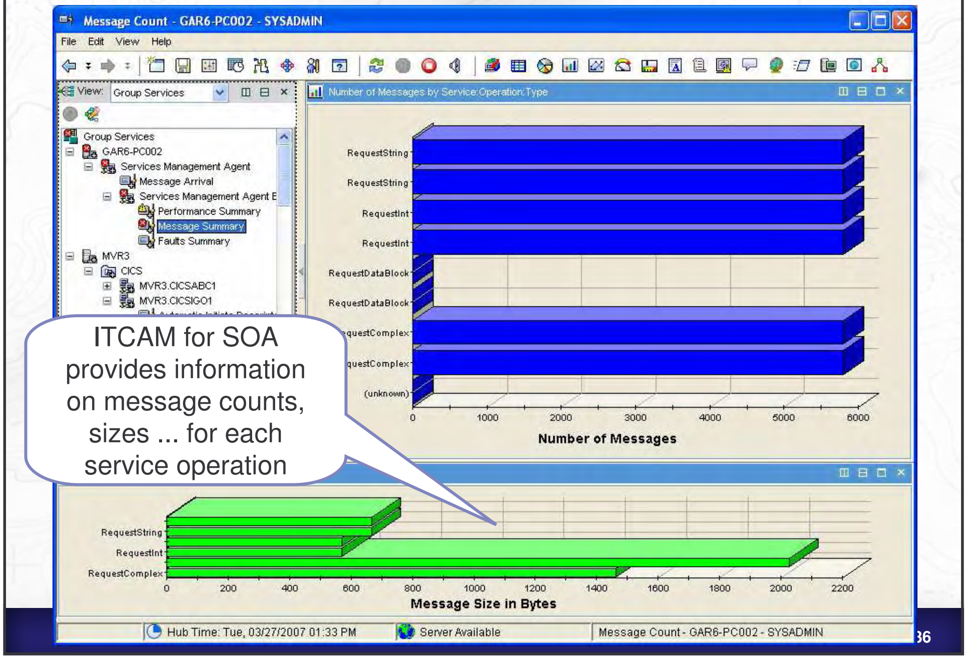


Then you know if a service is not performing

	Workload Name	Service Class Name	Interval End Timestamp	System ID	Response Time Goal	Transactions Total	Rate	Average Response Time	% Wait on MRO	% Wait on Journal Cor
	DFLTWORK	CTRANS	03/29/07 15:11:40	MVR4	00:00:01	6148	1229	00:00:00.003	0	
	DFLTWORK	TTRANS	03/29/07 15:11:40	MVR4	00:00:01	300	60	00:00:20.002	50	
	DFLTWORK	ITRANS	03/29/07 15:11:40	MVR4	00:00:01	6004	1200	00:00:00.206	98	
	DFLTWORK	KTRANS	03/29/07 15:11:40	MVR4	00:00:01	30	6	00:00:00.132	0	

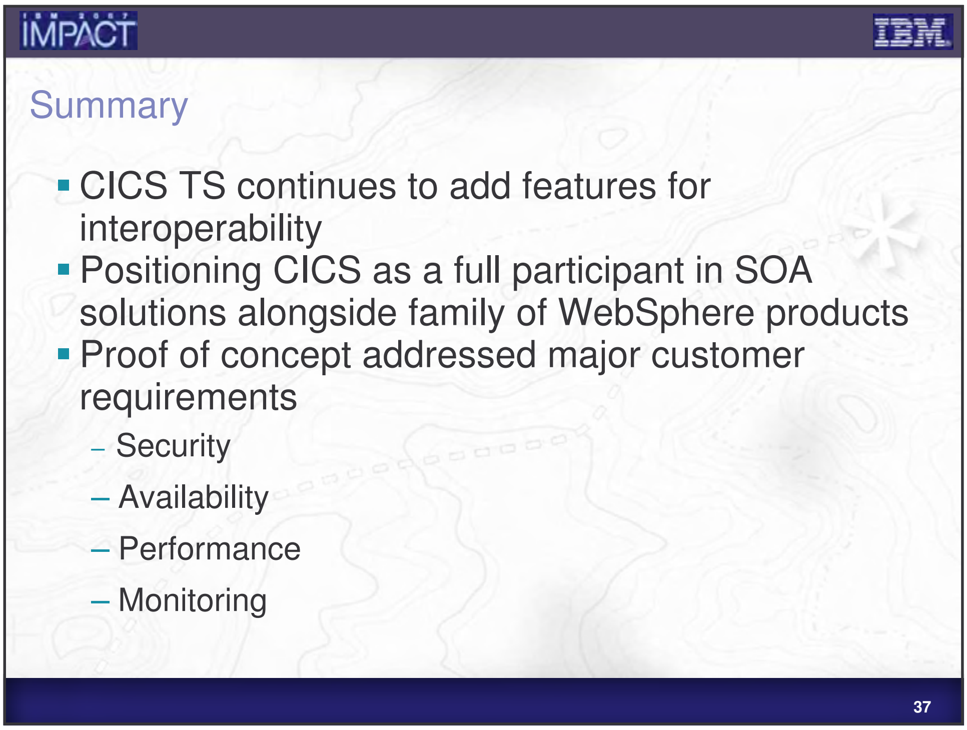
Hub Time: Thu, 03/29/2007 03:14 PM | Server Available | Service Level Analysis - GAR6-PC002 - SYSADMIN

ITCAM for SOA (Datapower Agent)



ITCAM for SOA provides information on message counts, sizes ... for each service operation

Hub Time: Tue, 03/27/2007 01:33 PM | Server Available | Message Count - GAR6-PC002 - SYSADMIN



Summary

- CICS TS continues to add features for interoperability
- Positioning CICS as a full participant in SOA solutions alongside family of WebSphere products
- Proof of concept addressed major customer requirements
  - Security
  - Availability
  - Performance
  - Monitoring

Thank You

شكراً
Arabic

Merci
French

감사합니다
Korean

धन्यवाद
Hindi

多謝
Traditional Chinese

תודה רבה
Hebrew

Obrigado
Brazilian Portuguese

Gracias
Spanish

go raibh maith agat
Gaelic

Спасибо
Russian

Grazie
Italian

Thank You
English

多谢
Simplified Chinese

நன்றி
Tamil

ありがとうございました
Japanese

ขอบคุณ
Thai

Danke
German

Questions
and
Answers

impact·venture*

The workshops, sessions and materials have been prepared by IBM or the session speakers and reflect their own views. They are provided for informational purposes only, and are neither intended to, nor shall have the effect of being, legal or other guidance or advice to any participant. While efforts were made to verify the completeness and accuracy of the information contained in this presentation, it is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this presentation or any other materials. Nothing contained in this presentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.
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 many factors, including 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 results similar to those stated here.

All 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.

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM trademarks, see www.ibm.com/legal/copytrade.shtml
AIX, CICS, CICSPlex, DB2, DB2 Universal Database, i5/OS, IBM, the IBM logo, IMS, iSeries, Lotus, OMEGAMON, OS/390, Parallel Sysplex, pureXML, Rational, RCAF, Redbooks, Sametime, System i, System i5, System z , Tivoli, WebSphere, and z/OS.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.