IBM Software Group

CICS Web Services Part 2: Deployment

Dave Key and James O'Grady
dave_key@uk.ibm.com, jamograd@uk.ibm.com
CICS Transaction Server
IBM Hursley Park

WebSphere® Support Technical Exchange

ON DEMAND BUSINESS

Agenda

- This session will explore aspects of deployment of Web Services in CICS® Transaction Server for z/OS® covering:
  - Major deployment considerations and best practice
    - Security
    - Workload Management and Availability
    - Cloud Applications and the CICS Explorer®
  - new security support for
    - Security Assertion Markup Language (SAML) Assertions
    - Kerberos Tickets.
- CICS version differences

Note: This WSTE Webcast is a follow-on from the Webcast of November 4, 2014 'CICS Web Services Part 1: Development'

Useful Resources

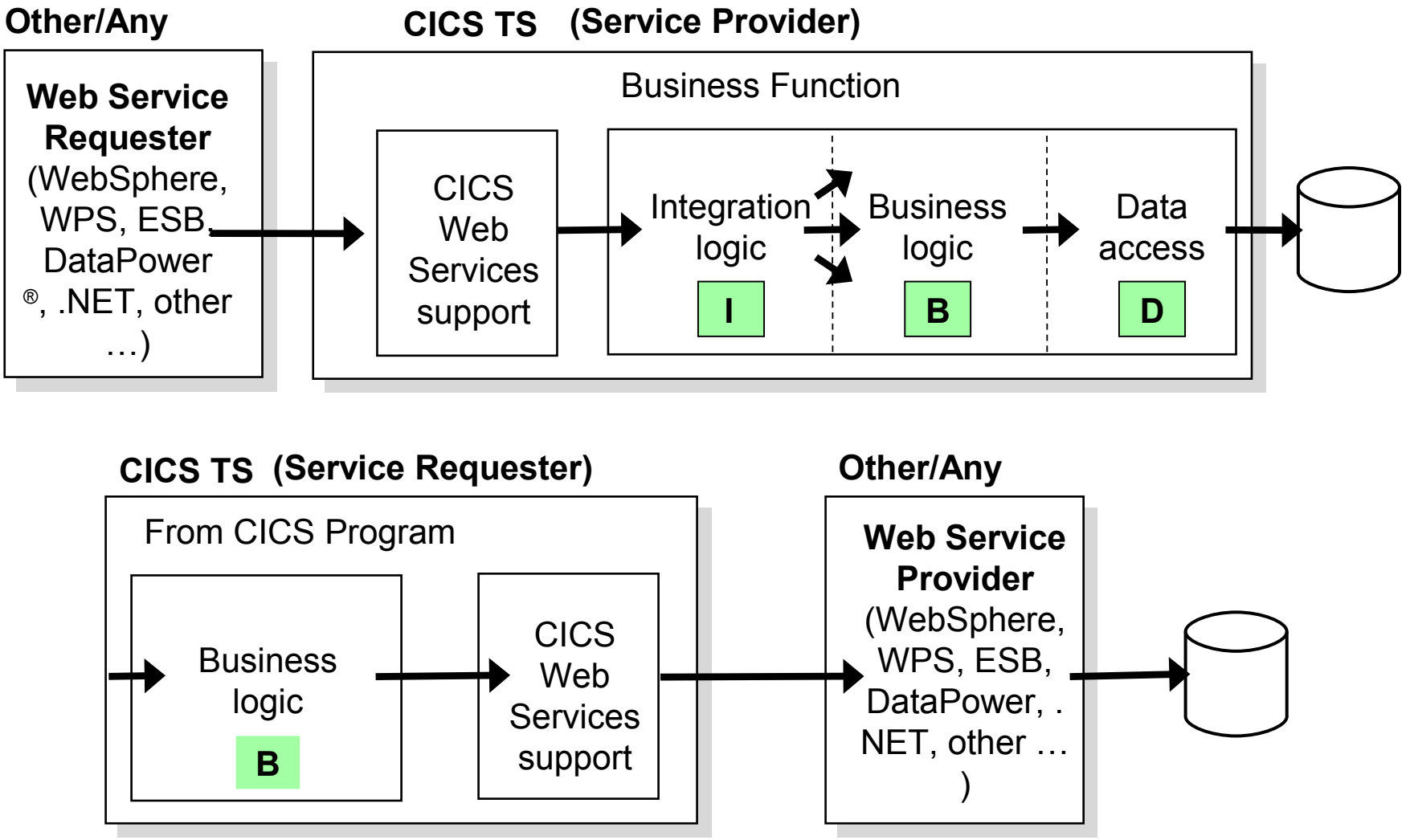
- IBM Web Services Redbooks

Architecture	http://www.redbooks.ibm.com/abstracts/sg245466.html
Implementation	http://www.redbooks.ibm.com/abstracts/sg247657.html
Performance	http://www.redbooks.ibm.com/abstracts/sg247687.html
Security	http://www.redbooks.ibm.com/abstracts/sg247658.html
WLM	http://www.redbooks.ibm.com/abstracts/sg247144.html
Development*	**http://www.redbooks.ibm.com/abstracts/sg247126.html**
JSON in CICS	**http://www.redbooks.ibm.com/abstracts/sg248161.html**
Cloud Enabling CICS	**http://www.redbooks.ibm.com/abstracts/sg248114.html**

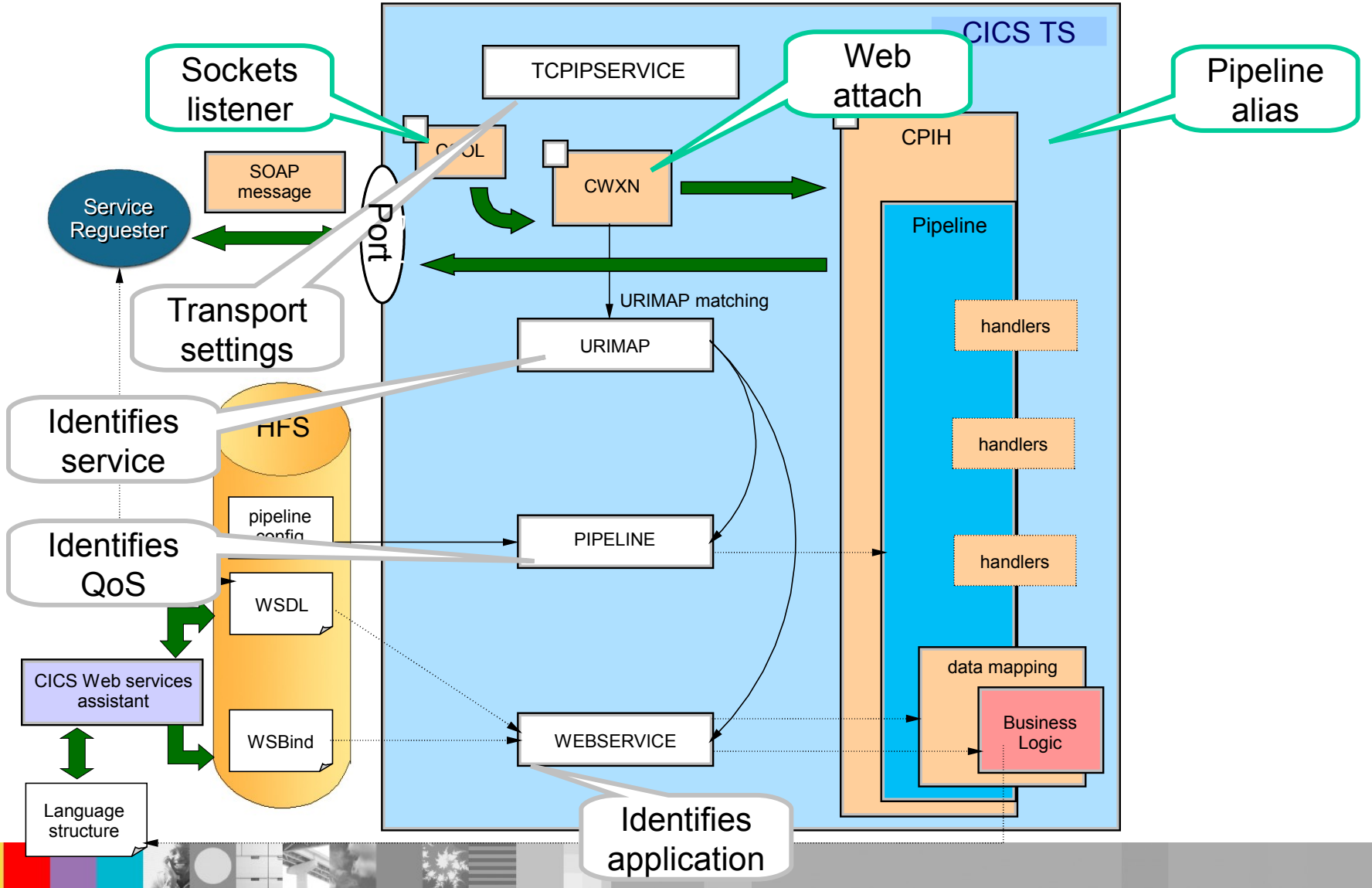
- Examples http://www.ibm.com/support/docview.wss?uid=swg24020774
- Knowledge Collection http://www.ibm.com/support/docview.wss?uid=swg27010507

* Updated edition out soon

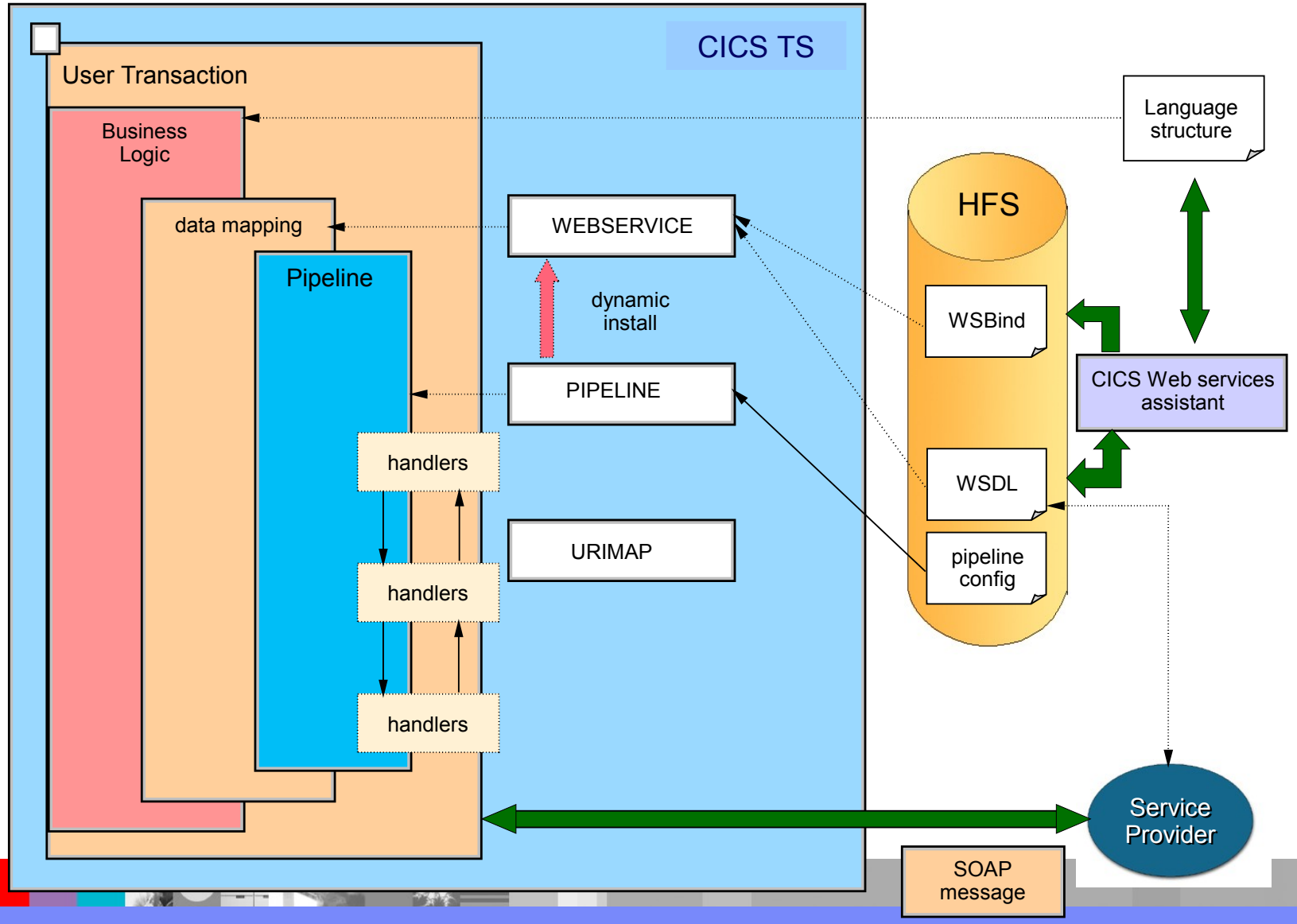
Typical CICS Web services scenarios



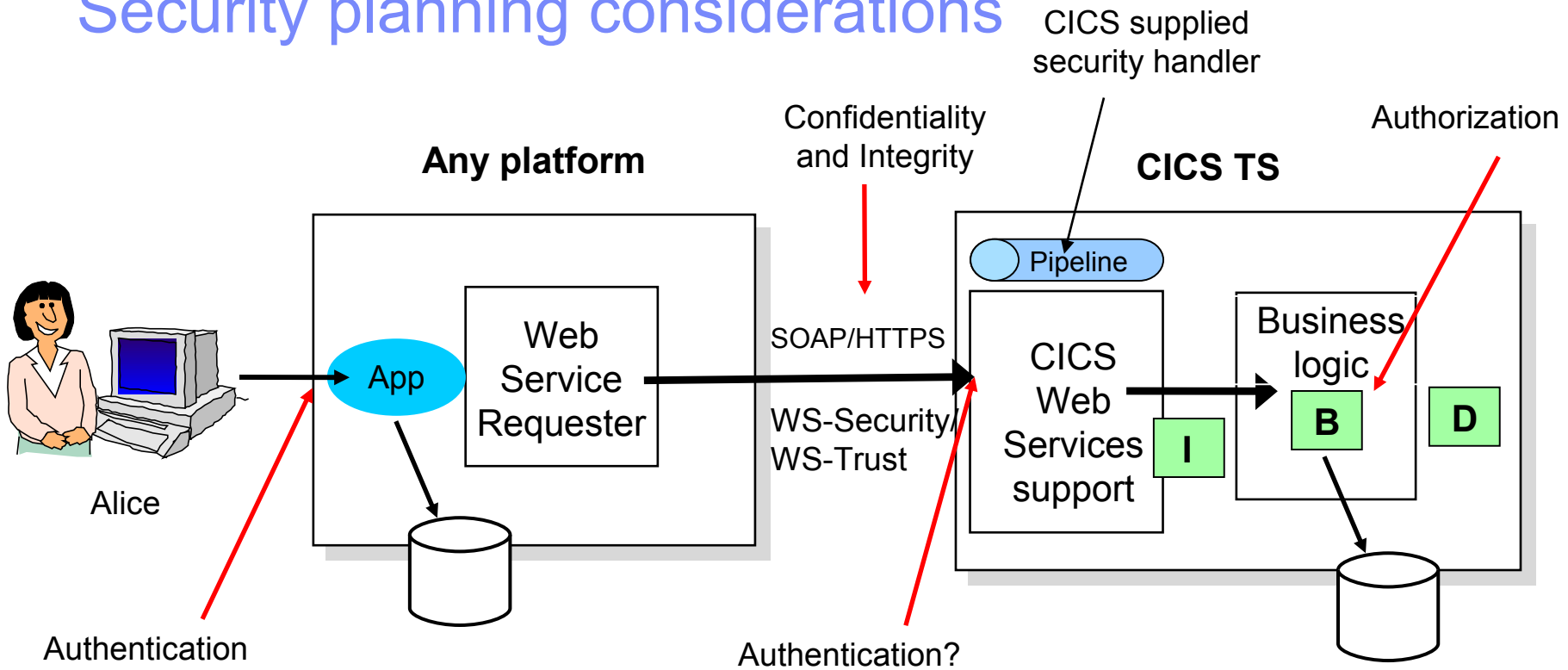
CICS service provider



CICS service requester

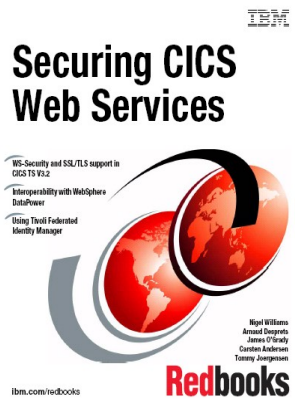


Security planning considerations



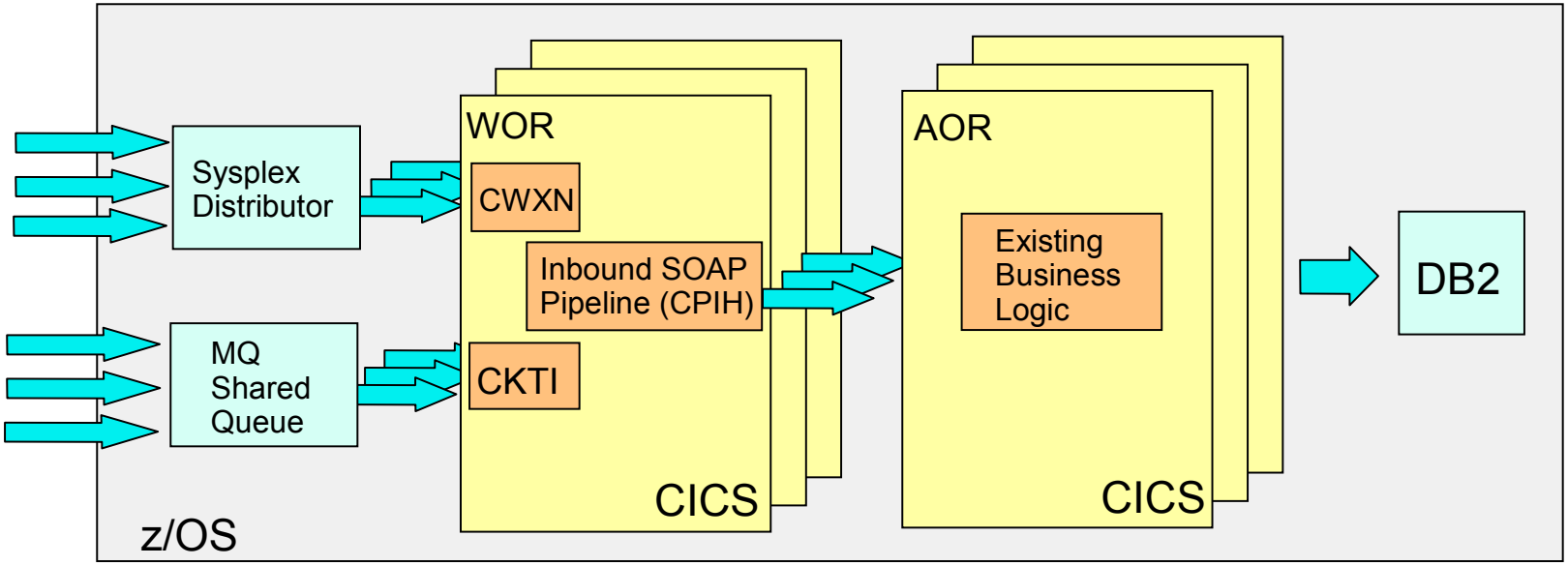
- How to authenticate
- Use CICS supplied security handler or custom-written
- Whether identity assertion is required and how to establish trust
- How to transport security credentials in the message
- How to ensure confidentiality and data integrity
- Whether to use WS-Security/WS-Trust, transport security or both

Security best practice



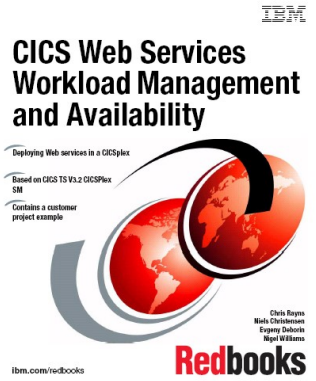
- Keep it simple if possible
  - Transport security alone (e.g SSL/TLS) may be sufficient in simple environments
- Use cryptographic hardware and ICSF (Integrated Cryptographic Hardware Facility) to maximize performance of SSL/TLS
  - Chose a cypher suite that can benefit from hardware assist
- WS-Security and WS-Trust can be used for more advanced requirements
  - WS-Security enables message-level authentication, data integrity and encryption
  - CICS supports WS-Security UsernameTokens and X.509 certificates natively
  - WS-Trust support enables CICS to indirectly support other token types (Kerberos, SAML …) by interoperating with a Security Token Service (STS)
- Consider using WebSphere DataPower for internet solutions (XML validation, protection against XML DNS attacks) and to offload expensive operations (e.g XML digital signature processing)

WLM and Availability considerations



- How to workload manage service requests
- How to set the pipeline transaction id
- How to process Web service requests across a CICSplex
- How to ensure service availability
- How to view service requests

WLM and availability best practice



- Build a highly available robust Web services infrastructure using a combination of different technologies, including
  - Sysplex Distributor, TCP/IP port sharing and MQ queue sharing to workload manage connections across different CICS regions
  - CICSPlex SM to dynamically route requests after the SOAP message has been processed
  - Monitoring tools like OMEGAMON XE for CICS for tracking against service response-time goals
- Set a private pipeline transaction id (default CPIH) for setting WLM goals, monitoring, statistics etc.
  - Set in URIMAP or modify contents of the container DFHWS-TRANID in a message handler program
- DPL routing is preferred to transaction routing
  - Cleaner separation between system and application code
  - DPL approach performs better
  - Additional resource definitions required in AOR if routing pipeline

Cloud Applications and the CICS Explorer

CICS Cloud - general.insurance.customer.applicationservices.to.dev.bundle/META-INF/cics.xml - IBM CICS Explorer - C:\CICSWorkspace

File Edit Navigate Search Project Window Help

Quick Access | CICS Cloud

Cloud Explorer

Server: ZLVC

CICSplex: GNAPPLEX

GeneralInsuranceDev ACTIVE ENABLED
- Applications
  - GENACUST (1.0.0)
  - GENACUST (1.0.1)
- Region Types
  - ApplicationServices (1/1)
  - DataAccess (1/1)
  - Presentation (1/1)

Project Explorer

- general.insurance.customer.application
- general.insurance.customer.applicationservices.to.dev.bundle
  - META-INF
  - GENAAPSV.library
- general.insurance.customer.data.bund
- general.insurance.customer.policy
- general.insurance.customer.presentation.bundle
- general.insurance.customer.services.bundle
- general.insurance.customer.to.dev.platform.binding
- general.insurance.dev.platform
- general.insurance.platform.policy

GeneralInsuranceCustomerApplicationServicesDev

Bundle Overview

General Information

This section describes general information about this bundle.

ID: GeneralInsuranceCustomerApplicationServicesDev

Version: 1.0.0

Actions

You can perform the following actions on this bundle:

1. Add or remove CICS resource definitions using this editor
2. Create an entry point to define an application operation
3. Apply a policy to an application operation
4. Export the bundle to a platform or specific location in zFS

Defined Resources

Specify the CICS resources that are installed and managed by this bundle.

GENAAPSV (LIBRARY)

New... Remove Move Up Move Down

Imported Resources

Specify CICS resources on which this bundle depends. The bundle will only become ENABLED when all required dependencies are met.

Add... Remove Properties...

Overview | Entry Points | Policy Scopes

Search

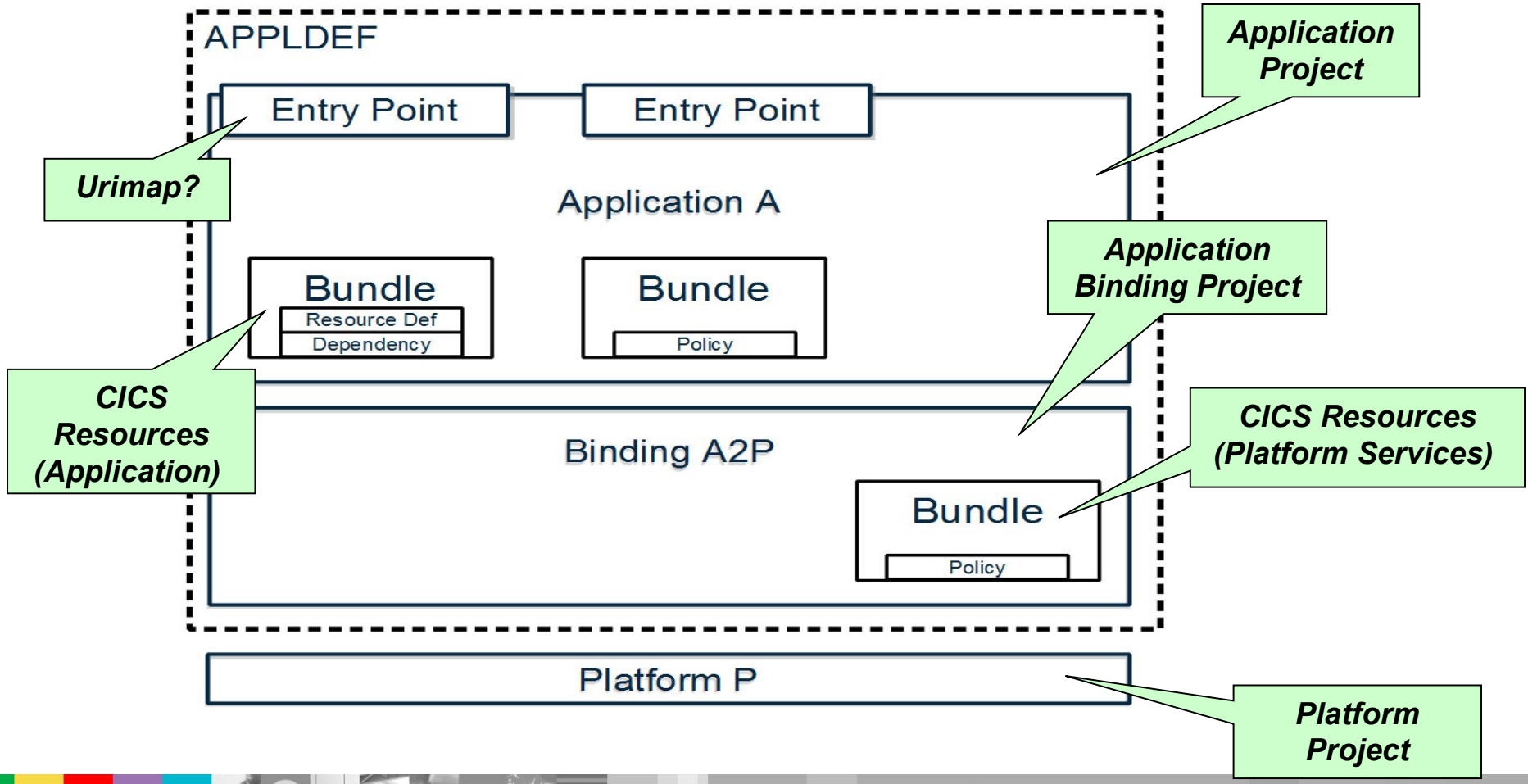
Resource | Path | Location | Type

Cloud Explorer

Project Explorer

CICS Cloud perspective

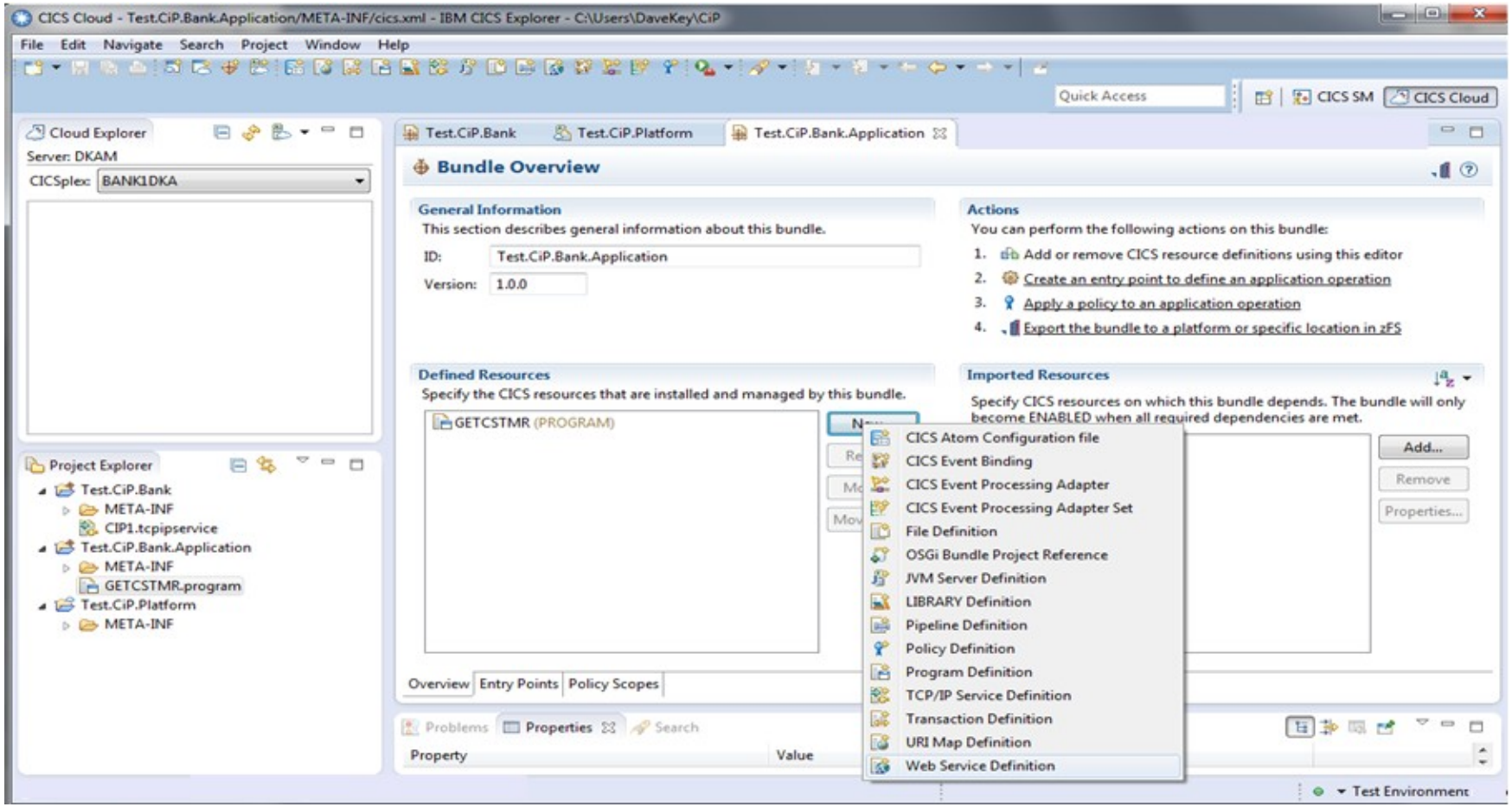
CICS TS Application Overview



Application

- The Application Project describes
  - The Application itself, including the name and version
  - The CICS Bundles (resources) that make up the application
    - Webservice resources can be defined to CICS Bundles
- The Application Binding describes
  - The mapping of the CICS Bundles to the region Types within the Platform
  - Environment specific resources e.g. differentiated between a Test and production Platform

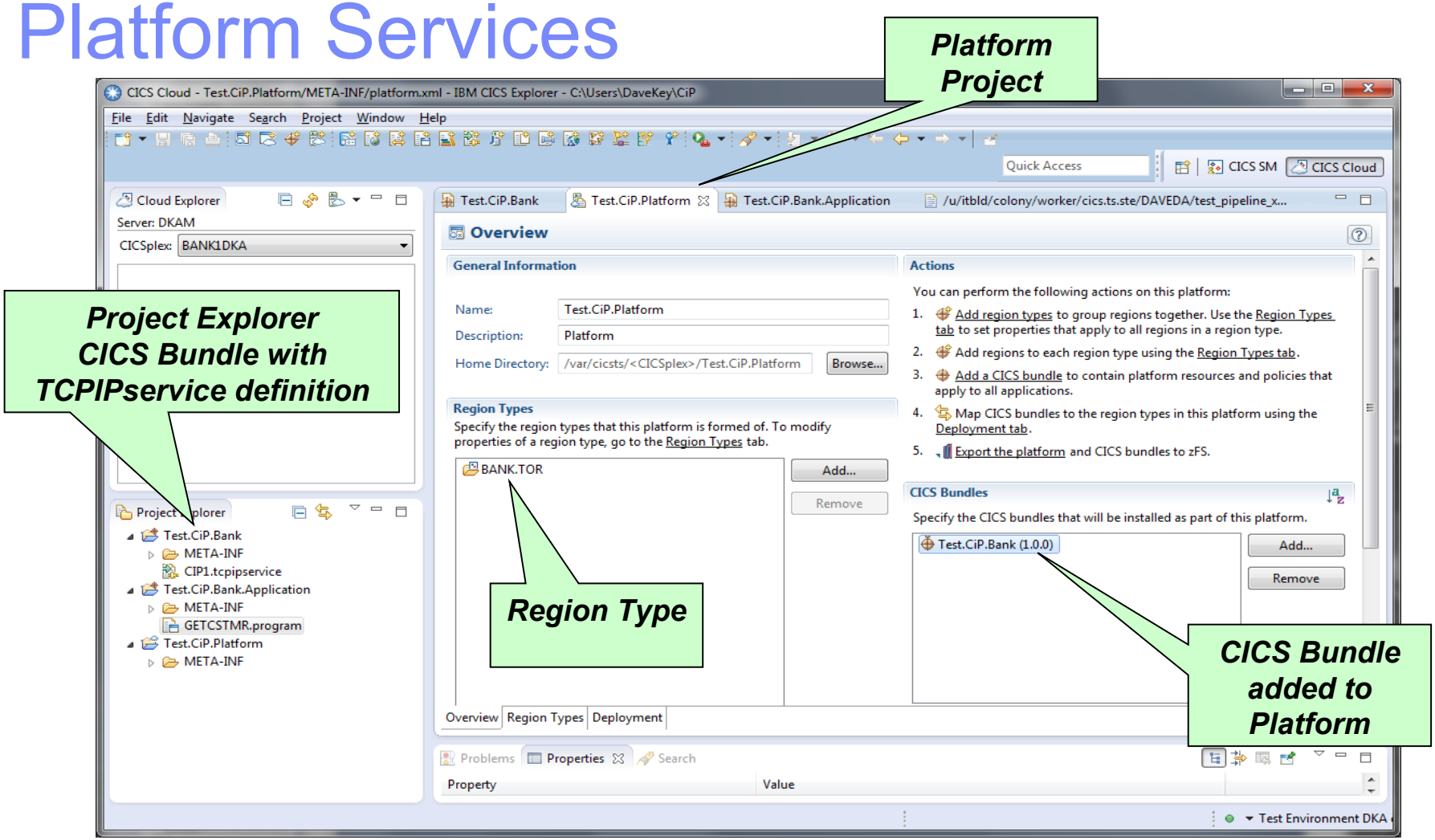
CICS Bundles & Resource Definitions



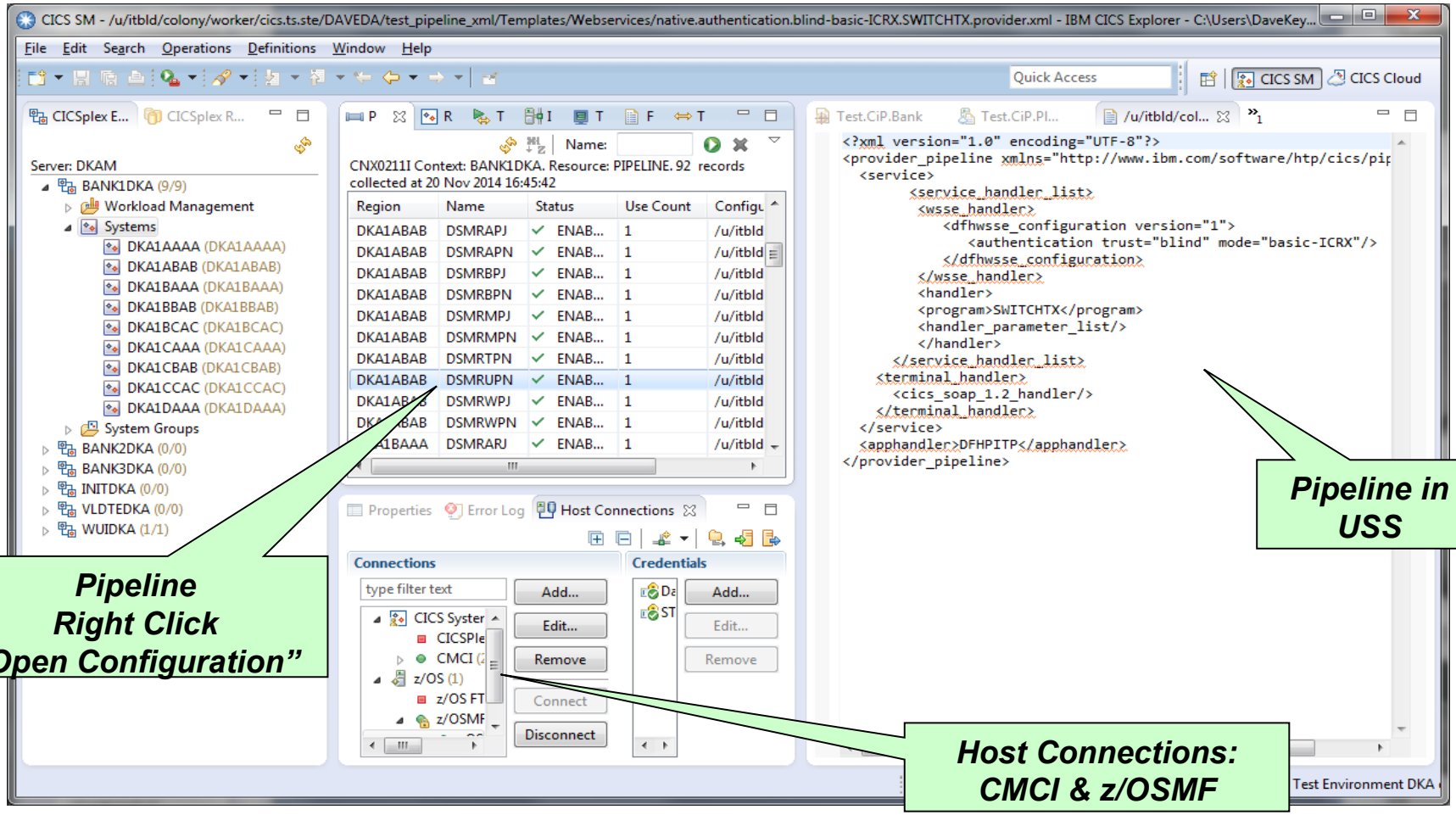
Platform Services

- A platform provides an environment into which ...
  - Applications are deployed
    - Regions are grouped together by capability and configuration
  - Services can be provided that applications may depend on to operate
    - For example, a platform may provide:
      - a TCP/IP® service that the application may consume using an URIMAP. All services installed in this manner can be managed across the platform in a single action.
      - A Pipeline with a level of authentication specific to the environment (test/production)

Platform Services



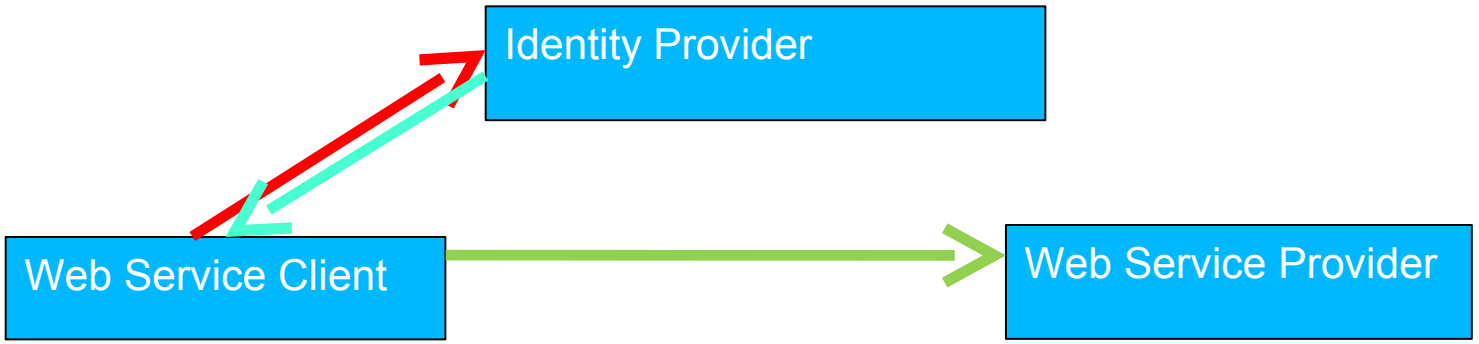
CICS Explorer – Pipeline & z/OSMF



SAML Assertion support in CICS TS

- First introduced with the CICS TS Feature Pack for Security Token Extensions V1.0 in CICS TS V4.2 and V5.1.
- Now an integral part of CICS TS V5.2.
- IBM supplies a CICS Security Token Service (STS) that is intended to run in a dedicated CICS region.

How do SAML assertions work?



- How do SAML assertions work?
  - A web service client makes a request to an “identity provider”.The identity provider supplies the web service client with an “assertion” that the client is who they say they are and that they are permitted to perform certain actions.
  - This SAML assertion is typically signed by the identity provider, and is then supplied to the web service provider.
  - The web service provider verifies the signature and can decide to trust the assertion.

SAML validation in a dedicated region

- *This is the recommended practice*
- It can be difficult to tune a CICS region for good performance for both traditional (COBOL, PL/I, et cetera) workloads and Java™ workloads at the same time
- If you need to validate signed SAML Assertions, there are restrictions on which certificates can be on the CICS region's key ring. A separate region can have a separate key ring.
- It avoids a single point of failure and allows workload management using DFHSAML program.

How to configure SAML for CICS

- The provider pipeline must be configured to use SAML.
  - The `<sts_authentication>` element must be specified with `action="validate"`.
  - You must specify which version of SAML you wish to support in the `<auth_token_type>` element. CICS supports SAML 1.1 and 2.0.
  - You must specify the `<sts_endpoint>`. To use the IBM supplied Security Token Service, specify this as `cics://PROGRAM/DFHSAML`
  - You may wish to make DFHSAML a dynamic program to workload balance SAML validation.

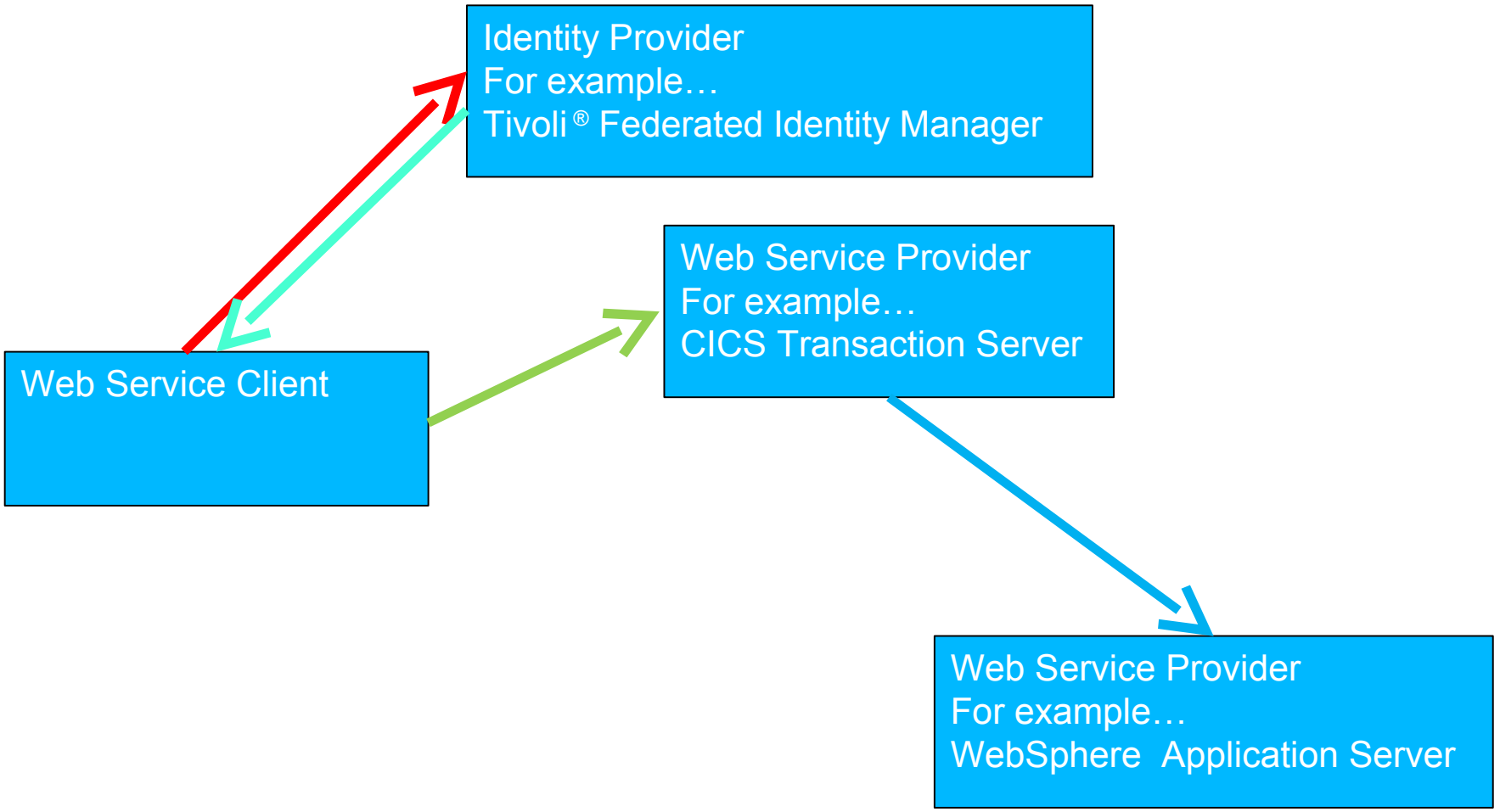
What does a SAML Assertion look like?

- A sample is provided in
  `samples/security/SAML`
- A SAML Assertion contains:
  - An Issuer
  - A Subject
  - A number of Conditions (for example NotBefore and NotOnOrAfter)
  - Optional authorisation and attribute statements
  - Optional signatures

DFHSAML Linkable Interface

- The IBM supplied Security Token Service will take a SAML Assertion and return a number of containers onto the pipeline channel.
  - These containers can be examined and used by a customer written pipeline handler to make decisions.
  - For example, you can extract a userid from an email address in the SAML Assertion.
  - DFHSAML also checks that the signature is valid, if this is required.

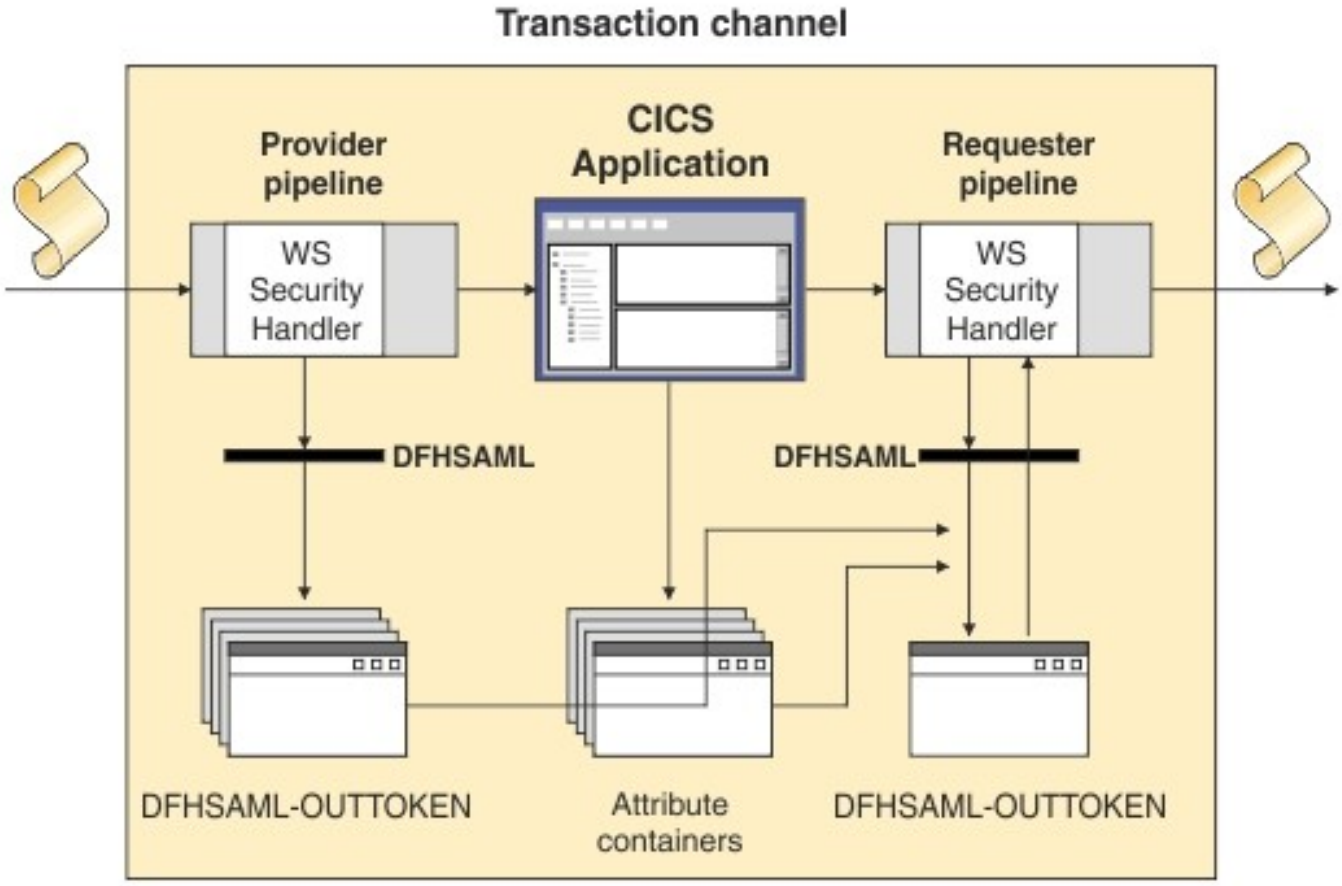
Enhancements at CICS TS V5.2



In CICS TS 5.2, we can reuse SAML

- Web service provider programs may need to invoke a web service outside of CICS using a SAML assertion.
- If a SAML assertion is supplied to the task, CICS can place all the containers on a new task based channel called DFHTRANSACTION.
- A configured requester pipeline can pass this on an outbound request using the DFHSAML-OUTTOKEN container.
- DFHSAML can reissue a SAML token after adding attributes, and can sign the token anew.

Transaction channel



SAML Assertion Issuer

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  ID="b07b804c-7c29-ea16-7300-4f3d6f7928ac"
  Version="2.0"
  IssueInstant="2004-12-05T09:22:05">
<saml:Issuer>https://idp.example.org/SAML2
</saml:Issuer>
```

SAML Subject

```
<saml:Subject>
    <saml:NameID
      Format="urn:oasis:names:tc:SAML:2.0:nameid-
   format:transient">
      3f7b3dcf-1674-4ecd-92c8-1544f346baf8
    </saml:NameID>
    <saml:SubjectConfirmation
      Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml:SubjectConfirmationData
        InResponseTo="aaf23196-1773-2113-474a-fe114412ab72"
        Recipient="https://sp.example.com/SAML2/SSO/POST"
        NotOnOrAfter="2020-12-05T09:27:05"/>
    </saml:SubjectConfirmation>
  </saml:Subject>
```

SAML Subject alternative (email)

```
<saml:Subject>
<saml:NameIdentifier
   Format="urn:oasis:names:tc:SAML:1.0:assertion#emailAddress">
STUAAAAA@example.com
</saml:NameIdentifier>
<saml:SubjectConfirmation>
<saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer
</saml:ConfirmationMethod>
</saml:SubjectConfirmation>
</saml:Subject>
```

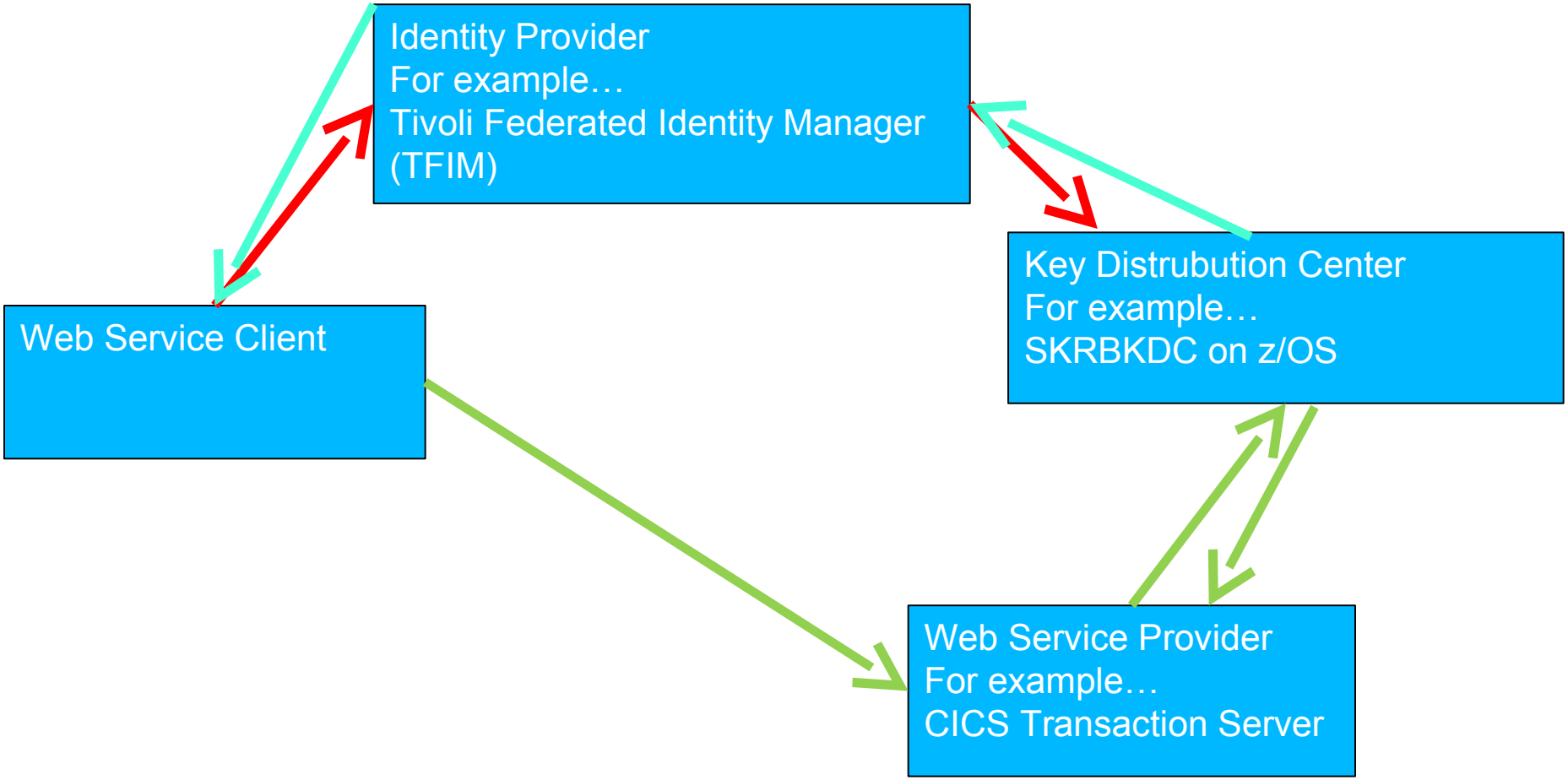
SAML Conditions… valid until 2020

```
<saml:Conditions
    NotBefore="2004-12-05T09:17:05"
    NotOnOrAfter="2020-12-05T09:27:05">
<saml:AudienceRestriction>
<saml:Audience>https://sp.example.com/SAML1</saml:Audience>
<saml:Audience>https://sp.example.com/SAML2</saml:Audience>
<saml:Audience>https://sp.example.com/SAML3</saml:Audience>
<saml:Audience>https://sp.example.com/SAML4</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
```

Kerberos Ticket support in CICS TS 5.2

- A form of WS-Security authentication added in CICS Transaction Server V5.2
- Clients request a “ticket” from a Key Distribution Center, for example SKRBKDC on z/OS.
- This ticket can then be used to create a session ticket which can then be sent to a third party.
- This third party can authenticate the ticket with the Key Distribution Center.
- Kerberos session tickets typically have a very short life span of around 5 minutes.

Kerberos at CICS TS V5.2



RACF User IDs and the KERB segment

- User ids can be set up to use Kerberos, and all information is stored in the KERB segment in RACF.
- In the previous scenario, a user would supply the KERBNAME and password to the Identity Provider, which then validates with the KDC
- Once inside CICS, the Kerberos Ticket can be verified and resolved to a standard user id.

How to configure Kerberos for CICS

- The CICS region userid must have a service principal name in its KERB segment.
- The provider pipeline must be configured to use Kerberos.
  - The `<wsse_handler>` element must be present.
  - The `<authentication>` element must specify

    `trust="basic"`

    and

    `mode="basic-kerberos".`

EXEC CICS VERIFY TOKEN

```
EXEC CICS Verify Token()
          TOKENLen()
          < TOKENType()  | Kerberos >
          < Isuserid() >
          < Datatype()  | BIt  | BAse64 >
          < ESMRESp() >
          < ESMREAson() >
```

- Default token type is Kerberos, and default data type is BIT. BASE64 is useful for Pipeline programs.

Cipher Suite selection in CICS TS 5

- In CICS TS 4.2 and earlier, selecting cipher suites was done by specifying a list of 2 hexadecimal character codes.
  - This was hard to read, did not allow for support for newer, 4 character cipher suites and limited the number of ciphers that could be supported.
- At CICS TS 5.1 and later, TCPIPSERVICEs, URIMAPs and IPCONNs allow the CIPHERS attribute to contain the name of a file stored in zFS

Summary of Enhancements in CICS TS

Release by Release summary of major enhancements from CICS TS V3.1 to CICS TS V5.2

Enhancements in CICS TS V3.2

- Faster for most workloads than TS V3.1
  - 64bit containers
  - Code page enhancements
  - More of CICS is Thread-safe
    - PIPELINE processing is done on an L8 TCB so thread-safety is relevant
- Support for more data mapping options
  - Easier to create applications top-down
  - Supports more WSDL documents
- Support for more specifications
  - MTOM/XOP
  - WSDL 2.0
  - WS-Trust (with IBM Tivoli Federated Identity Manager – TFIM)

Enhancements in CICS TS V4.1

- Faster for most workloads than TS V3.2
  - Mostly due to a rewrite of the SOAP node
  - A small part of which is zAAP off-loadable
- Support for more data mapping options
  - Truncated (variable length) data
  - Bottom-up support for channel based applications
- A new XML processing API
  - EXEC CICS TRANSFORM XMLTODATA ...
  - EXEC CICS TRANSFORM DATATOXML ...
  - Useful for scenarios such as:
    - Writing PIPELINE handler programs that work with XML
    - Handling dynamic content in XML
- Support for more specifications
  - WS-Addressing

New with CICS TS V4.2

- Support for JSON
  - Through the Mobile Feature Pack
- Support for JAX-WS
  - Using Java based SOAP pipelines
- Support for SAML
  - Through the Security Token Extensions Feature Pack

New with CICS TS V5.1

- API improvements for Containers
  - Read content in chunks
  - Append to existing containers
  - Useful for variably recurring data, top-down
- Improved support for JAX-WS
  - Using WebSphere Liberty Profile

New with CICS TS V5.2

- Mapping Level 4.0
  - UTF-16 text
  - OCCURS DEPENDING ON supported
- Security Enhancements
  - Kerberos,
  - Cipher Suites
- Cloud Style Deployment

Summary

- CICS provides a robust and scalable Web services infrastructure
- CICS is enabling Cloud based deployment of Web services through the CICS Explorer
- Web services enable secure interoperability with internal systems and external business partners
- Many of IBMs largest customers are using CICS Web services today
- Check out the CICS Information Center and the many ITSO Redbooks for more information on deploying CICS Web services

Connect with us!

1. **Get notified on upcoming webcasts**
   Send an e-mail to wsehelp@us.ibm.com with subject line “wste subscribe” to get a list of mailing lists and to subscribe
2. **Tell us what you want to learn**
   Send us suggestions for future topics or improvements about our webcasts to wsehelp@us.ibm.com

Questions and Answers

Additional WebSphere Product Resources

- Learn about upcoming WebSphere Support Technical Exchange webcasts, and access previously recorded presentations at:
  http://www.ibm.com/software/websphere/support/supp_tech.html
- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at:
  http://www.ibm.com/developerworks/websphere/community/
- Join the Global WebSphere Community:
  http://www.websphereusergroup.org
- Access key product show-me demos and tutorials by visiting IBM Education Assistant:
  http://www.ibm.com/software/info/education/assistant
- View a webcast replay with step-by-step instructions for using the Service Request (SR) tool for submitting problems electronically:
  http://www.ibm.com/software/websphere/support/d2w.html
- Sign up to receive weekly technical My Notifications emails:
  http://www.ibm.com/software/support/einfo.html