Redbooks
ibm.com/redbooks

Secure Hybrid Cloud Connectivity with IBM Bluemix and z Systems

Jeff Miller
Senior Software Engineer,
IBM Competitive Project Office

Cloud

z Systems

IBM

Redpaper

Cloud-mainframe connections can be secure and reliable

The cloud is a major force in computing today, with leading companies moving more and more of their information technology (IT) workloads away from their local data centers. It's easy to see why:

- Reduced entry cost (less labor, hardware, power, and so on)
- Simplified infrastructure management, particularly for multi-tiered applications
- Ability to grow and shrink capacity elastically, and with agility
- Support for self-service: New environments brought up and down quickly and easily

Of course, designing applications in multiple tiers is not a new trend. Systems have been split into front-end presentation tiers and a back-end business logic or data tiers for years. What's new is that, influenced by the rise of mobile computing, the tiers have become more formalized, and are now typically called the *System of Engagement* (SoE) and the *System of Record* (SoR).

Whatever you call them, SoEs and SoRs must react to rapid changes in demand. Spikes in workload can occur suddenly, with each new and often unpredictable change in user behavior.

This makes the cloud, with its elasticity, ideal for hosting SoEs, whose applications are typically a primary point-of-contact for thousands (or even millions) of web and mobile users. In contrast, SoR applications, such as databases and transaction managers, are updated less often. SoRs require the most stringent security, making them ideal for the mainframe.

Therefore, a rapidly emerging pattern is to host the SoE in the cloud, and keep the SoR with the other important business systems in the company data center, often on a mainframe. This hybrid cloud design offers elasticity and automation in the SoE, while maintaining the ability to tightly manage the security of the SoR.

Business data security in the SoR is paramount, and the current IBM® mainframes have been released with the highest-to-date Common Criteria Evaluation Assurance Level (EAL) ratings for overall security among commercial systems (5+ on a 1 - 7 scale). Yet some companies wonder if their cloud-based SoE can securely connect to an SoR on enterprise premises.

In this IBM Redpaper™ publication, we show that the IBM Bluemix™ cloud platform offers technologies that make it easy for cloud-based SoEs to securely connect to on-premises IBM mainframes, creating a fully secure, end-to-end, SoE-SoR environment.

Exposing mainframe assets

Even before addressing the connection to the cloud, you need to know that you can safely expose the information assets stored on your mainframe.

The mainframe is a strong back-end system, and an open one. Each mainframe server subsystem, such as IBM WebSphere® Application Server, IBM Customer Information Control System (IBM CICS®), IBM Information Management System (IBM IMS™), and so on, offers several individual connectivity options.

These connectivity options include products, such as IBM IMS Connect for z/OS® and IBM CICS Transaction Gateway, in addition to CICS SOAP and Representational State Transfer (REST) web services and RESTful requests to Java code running in the CICS Java virtual machine (JVM).

Fortunately, a newer technology, called IBM z/OS Connect, provides a single, uniform way to access these back-end resources. z/OS Connect simplifies mainframe application access by providing a single application programming interface (API) mechanism, regardless of which back-end system is involved.

z/OS Connect, which is a feature of the IBM WebSphere Liberty Profile, accepts JavaScript Object Notation (JSON)-based requests over Hypertext Transfer Protocol (HTTP) and forwards them (in the required data format) to the back-end systems using IBM WebSphere Optimized Local Adapters (WOLAs).

WOLAs provide high-speed, memory-to-memory data transfer. Responses returned from the back-end systems are converted back to JSON by z/OS Connect, and then sent back to the requester. z/OS Connect can also route requests to IMS using IMS Connect.

Figure 1 illustrates these interactions (the arrows show the bidirectional request/response flows).

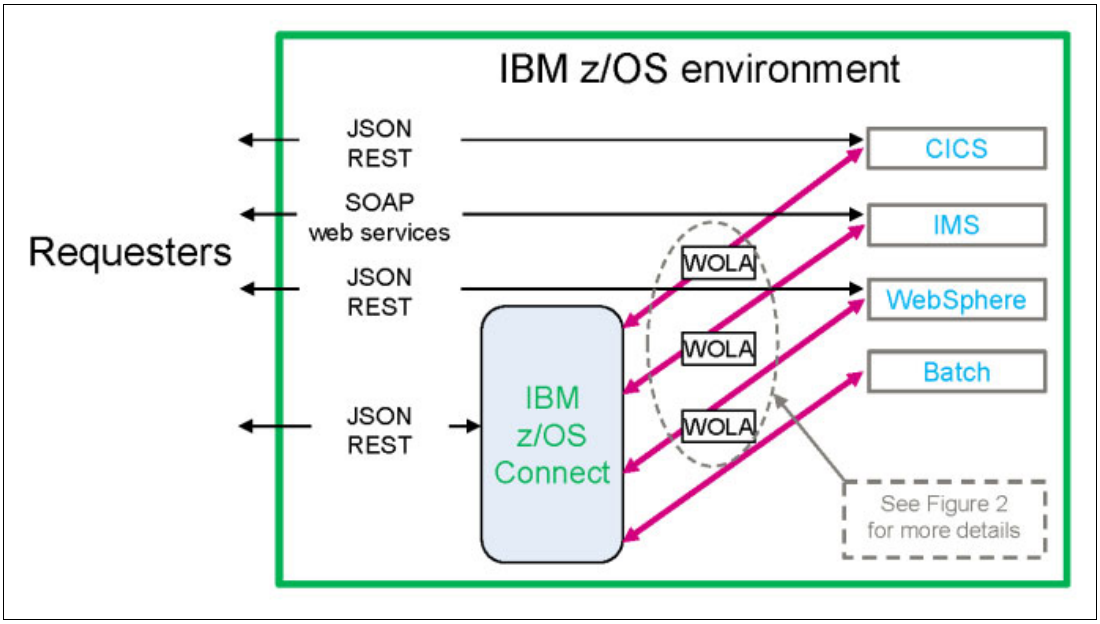

Figure 1 z/OS Connect provides unified connectivity options, even for batch processing

In addition, z/OS Connect provides added value in the form of *interceptors*, which, among other capabilities, can provide additional security in the form of auditing, credential validation and conversion, and more. Interceptors can be called in both directions, as shown in Figure 2 (the bidirectional arrow on the left side of the figure represents flows from, and back to, calling applications).

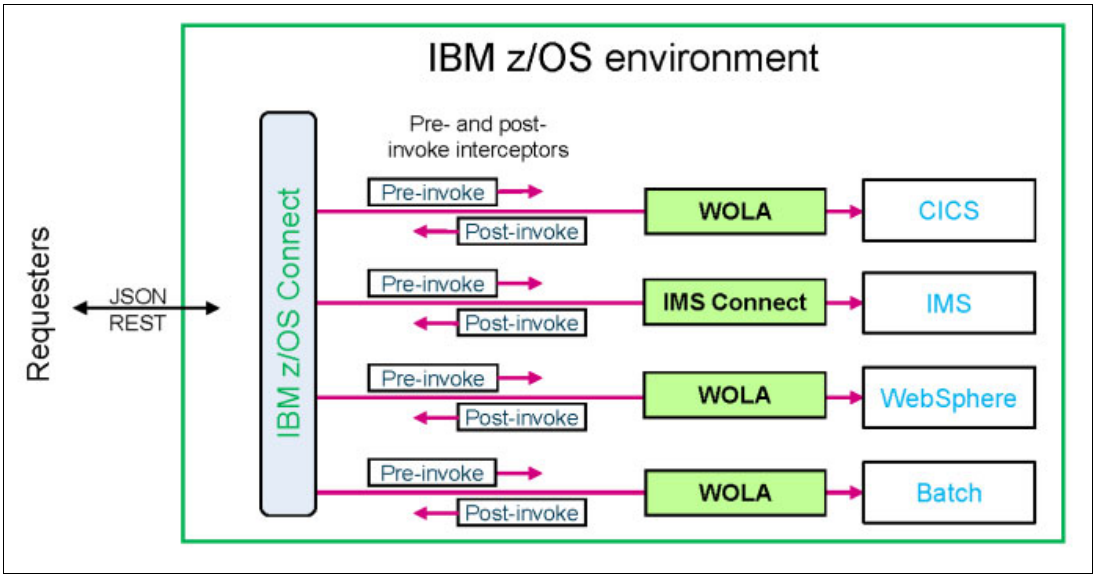

Figure 2 z/OS Connect supports pre-invoke and post-invoke interceptors for added security, auditing, and more

In this way, IBM adds additional security options to protect the mainframe every time an SoE communicates with it through z/OS Connect. With an infrastructure like this in place, the mainframe is secure. Cloud-based applications can then securely send requests to z/OS systems *if the connection between the cloud and the mainframe can be secured*. That's where IBM Bluemix enters the picture.

Securing the connection to the cloud

With the security of the mainframe well-established, the next link in an end-to-end security architecture is to lock down the communications between the cloud-based SoE and the mainframe-based SoR.

Bluemix is the IBM Platform as a Service (PaaS) that runs in the cloud and is hosted by IBM SoftLayer®, the IBM Infrastructure as a Service (IaaS) offering. Bluemix was initially based on the open source Cloud Foundry project, and enables developers to easily build and deploy applications by reusing existing components and services. This reuse reduces the need for custom code.

Bluemix offers multiple options for securely connecting to resources outside of Bluemix, such as to mainframe-based SoRs:

- IBM DataPower® Gateway
- Secure connectors
- IBM Secure Gateway for Bluemix

IBM DataPower Gateway

DataPower Gateway is a highly versatile gateway appliance that is typically found in the DMZ[1] in dual-firewall environments. Bluemix applications can connect directly to DataPower Gateway (whether in the DMZ or within the enterprise's firewall), after which requests are forwarded to the back-end systems.

DataPower Gateway comes in physical and virtual forms, with features that provide high availability, failover, load balancing, message security, data conversion, and more. It excels at Extensible Markup Language (XML) and RESTful web services processing. Version 7.2 of the product enhances cloud and on-premises security with support for Elliptic Curve Cryptography, Server Name Indication, and Perfect Forward Secrecy to protect against malicious protocol attacks.

IBM API Management is an optional feature available with DataPower Gateway. APIs are useful because they can be configured by developers of on-premises resources and used by developers of cloud applications. DataPower Gateway implements these API mappings, and API Management makes mainframe APIs more consumable.

Later in this paper, Figure 5 on page 6 shows a Bluemix application calling APIs that have been configured by mainframe developers to access mainframe services through z/OS Connect. Other access techniques and APIs can also be used.

Secure connectors

Secure connectors establish protected communication between cloud-hosted Bluemix applications and on-premises systems. Connectors are typically made available as *services*, which means that they can be called by SoE-based applications whenever needed.

In Bluemix, secure connections can be created with the Standard (IBM Cast Iron®) Connector, or by using DataPower Gateway as a connector.

Standard (Cast Iron) Connector

This simple, software-based connector acts as an intermediary between a Bluemix application running in the cloud and the back-end mainframe. A secure connection is established from the Bluemix application to a Cast Iron orchestration, which then connects securely to the on-premises system. In request-response environments, these orchestrations can provide extra capabilities by calling intermediaries to perform data conversion and other chores.

DataPower Gateway as a secure connector

DataPower Gateway can also be used as a secure connector, where it functions within a larger software construct, rather than as a stand-alone appliance as described earlier. Bluemix developers simply configure a service in which DataPower Gateway acts as the connector endpoint, and then call the service when needed to send requests to and from on-premises systems.

[1] DMZ is an acronym for *demilitarized zone*, which was originally a military term but is now also used in computing to represent a common secure construct in which two firewalls are installed. Often there is a reverse proxy server or a gateway server between the firewalls. Requests from the outside pass through the first firewall, and are processed in some way before being passed across the second firewall into the enterprise intranet. Figure 5 on page 6 shows DataPower Gateway inside the DMZ.

Figure 3 shows DataPower Gateway being used as the endpoint of a secure connector. DataPower Gateway can be installed either in the DMZ or in the enterprise's trusted zone (or intranet).

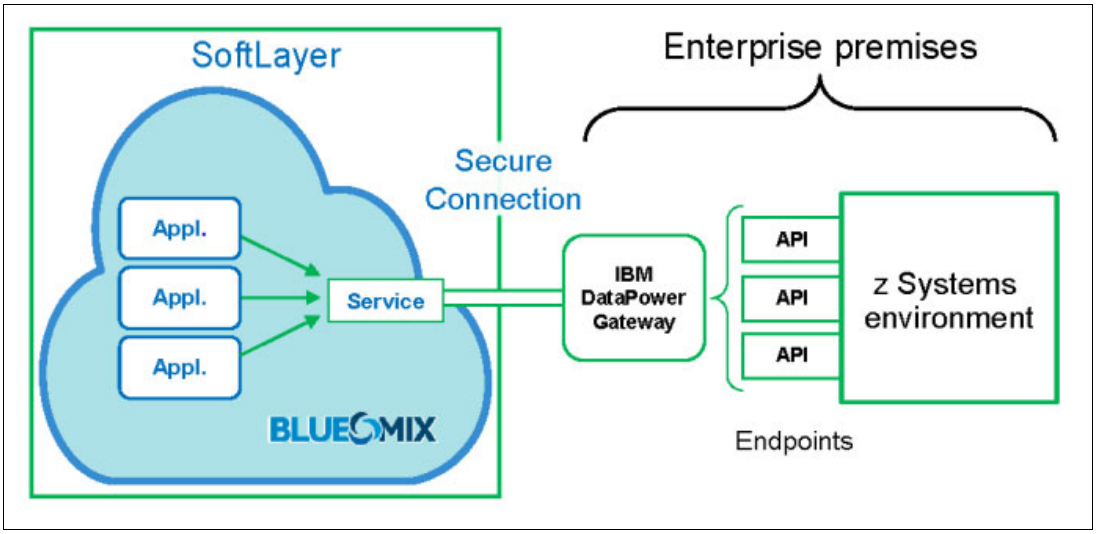

Figure 3 Using DataPower Gateway as a secure connector

IBM Secure Gateway for Bluemix

IBM Secure Gateway for Bluemix is a Bluemix service that enables the hybrid cloud with secure connectivity, traffic monitoring, and local endpoint mapping to on-premises applications and data sources. It creates a secure tunnel between Bluemix applications in the cloud and back-end resources. It is based on *web sockets*, which are bidirectional, persistent connections used for sending text and binary data.

The Secure Gateway features a dashboard that enables developers and administrators to view usage and performance analytics, manage and monitor gateway topology and configuration, and gain visibility into network traffic and endpoints.

The Secure Gateway client is remote software[2] provided by IBM as a Docker image that can be run on Linux systems on premises. Docker is an open source, lightweight, portable runtime container for executable code, analogous to a virtual machine but much smaller, because it comes without all of the operating system layers.

It's easy to create a new Secure Gateway with just a few clicks. The predefined Docker-based client software can be downloaded and configured to create an on-premises Secure Gateway client, and a Secure Gateway service that can be called when needed. In Figure 4 on page 6, the left side of the figure shows a Secure Gateway service in Bluemix, available to Bluemix applications. On the right side of the figure is an on-premises Secure Gateway client instance. The secure tunnel is established between the client and the service.

[2] The term *client* here is counterintuitive. In conventional terms, a remote client calls a back-end server or resource. With Secure Gateway, the client is local and is named for how the gateway is instantiated. The Bluemix developer (with Docker already installed on an on-premises machine) simply creates a new Secure Gateway. Bluemix generates a unique ID and provides downloadable client code, which the developer installs in Docker. This establishes the Secure Gateway connection *back* to Bluemix from the on-premises Secure Gateway client.

Figure 4 shows IBM Secure Gateway for Bluemix providing access to mainframe resources.

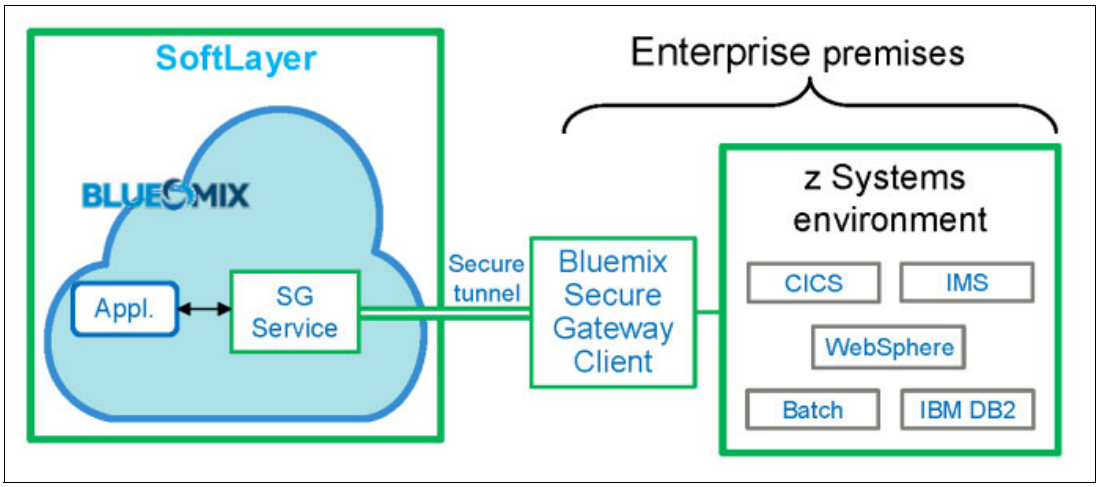

Figure 4 Accessing mainframe resources through an IBM Secure Gateway for Bluemix tunnel

Using Secure Gateway for Bluemix with DataPower Gateway

To avoid the need for a separate on-premises server in which to install the Secure Gateway client, Secure Gateway for Bluemix can now be plugged in as a module of DataPower Gateway version 7.2, combining their respective capabilities. With this design shown in Figure 5, the Secure Gateway runs from within the DataPower Gateway, either in the DMZ or in the enterprise intranet.

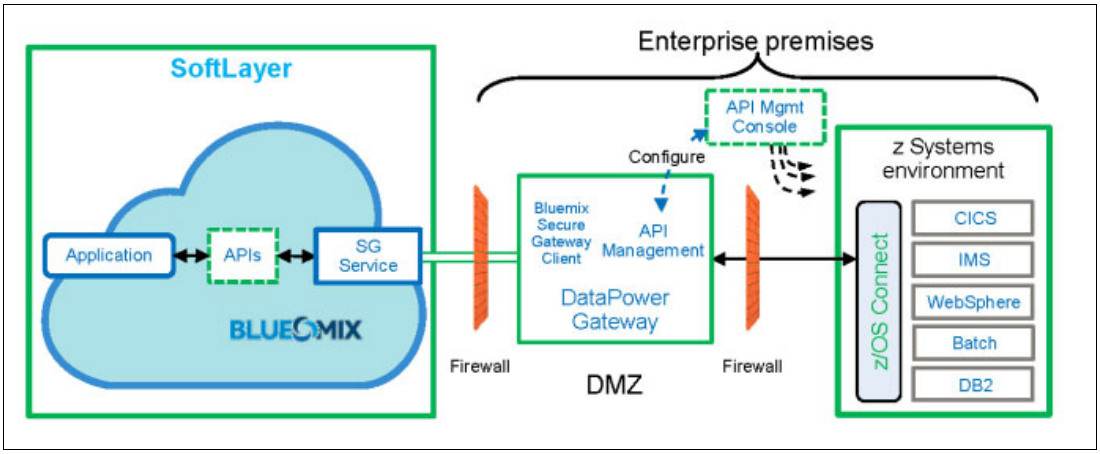

Figure 5 The Secure Gateway client and API Management modules running with DataPower Gateway

Completing the stack with application-level security in Bluemix

Often, for the most critical data, establishing secure connectivity through a secure tunnel is not enough, especially for SoEs designed primarily for use with mobile devices and applications. Designed with this in mind, Bluemix provides more security services at the application level.

IBM Mobile Application Security for Bluemix helps to protect applications and data, preventing unauthorized users and devices (or stolen or compromised devices) from accessing protected assets. IBM Advanced Mobile Access for Bluemix does even more.

IBM Advanced Mobile Access for Bluemix supports OAuth 2.0, a protocol that enables users to log in using identity providers such as Facebook, Google, and others. Advanced Mobile Access OAuth tokens serve as access tokens that are provisioned at deployment time, and not embedded in application code. OAuth provides assertions to services about the user, the client mobile app that is being run, and the device being used.

Single sign-on (SSO) is another security capability provided by Bluemix. IBM offers a policy-based authentication service that can be used by `Node.js` and WebSphere Liberty applications to support these single sign-on identity sources:

- SAML Enterprise: A user registry with which an exchange of Security Assertion Markup Language (SAML) tokens completes the authentication.
- Cloud Directory: A different user registry that is hosted in the IBM Cloud.
- Social identity sources using OAuth 2.0: Examples of these registries are the ones maintained by Google, Facebook, LinkedIn, and so on.

The primary roles and components in the OAuth 2.0 authorization flow are the Resource Owner, the OAuth Client, the Authorization Server, and the Resource Server. Figure 6 shows the typical OAuth 2.0 flow, and includes the User-Agent (the application (app) or browser used by the user). The example illustrates a browser-based service that enables a user to send facsimiles (faxes) of stored documents *without* revealing the user's authentication credentials to the fax service.

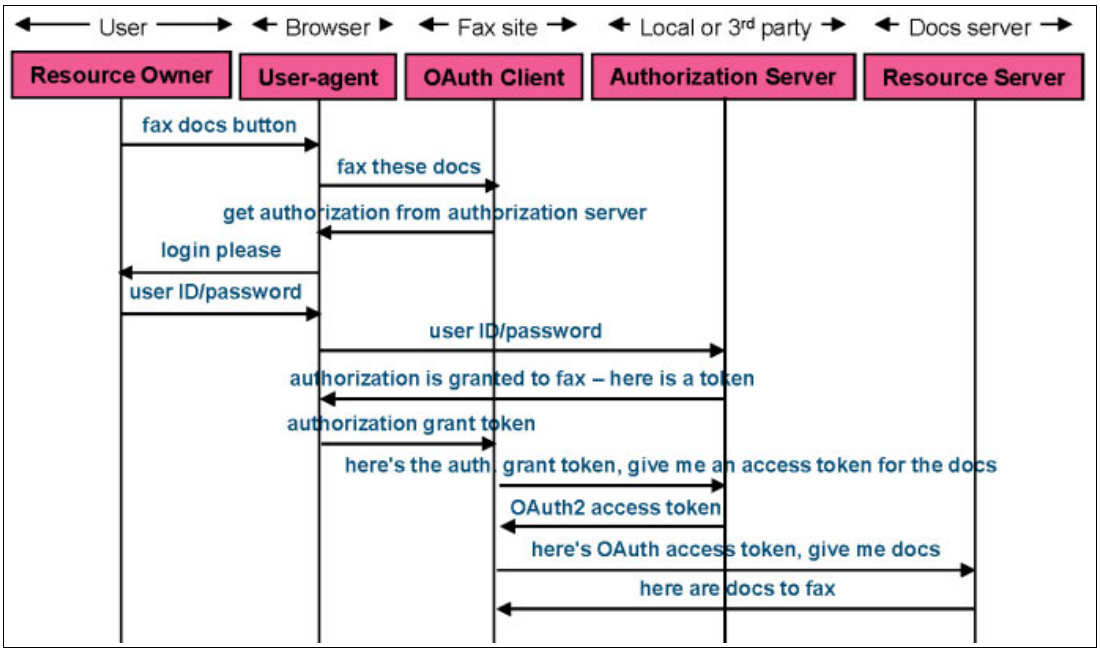

Figure 6 Typical OAuth 2.0 authorization flow

OAuth 2.0 can also be used in more specific scenarios, such as authorizing a mobile SoE application based on Bluemix to access CICS transactions on behalf of a mobile banking user. This more specific flow is shown in Figure 7 on page 8, and explained in the paragraphs that follow.

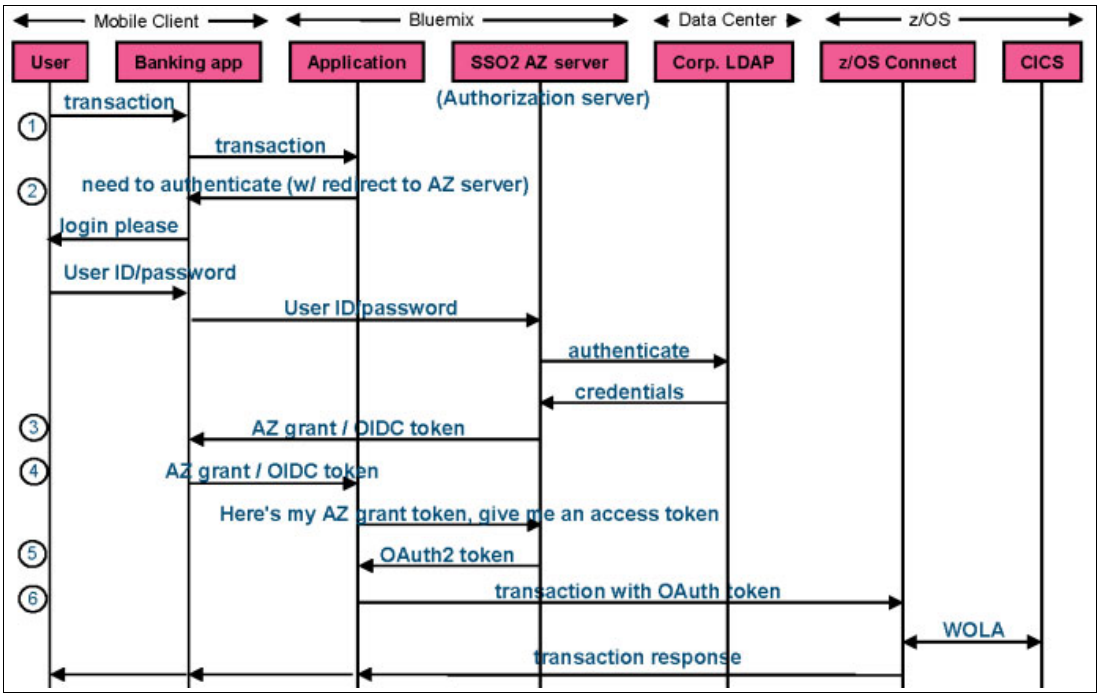

Figure 7 OAuth 2.0 flow from mobile user to CICS application (with single sign-on authorization)

In Figure 7, these OAuth roles are in action:

- Resource Owner: User
- User-Agent: Banking app (mobile or web)
- OAuth Client: Bluemix application (in the cloud)
- Authorization (AZ) Server: IBM Single Sign-On server
- Resource Server: CICS Transaction Server (on a mainframe)

The numbers on the left side of Figure 7 detail the OAuth flow from mobile user to CICS app:

1. When the user submits a transaction, the mobile banking app (the User-agent) connects to the Bluemix SoE application (the OAuth Client), which instructs the app to have the user log in if the user has not done so already.
2. The Bluemix application redirects the banking app to the authorization server to provide the user's identifying information (a client ID), the request (including its scope, which determines the permissions that are required), and a URL pointing back to the client. In product documentation, this redirect URL is referred to as a URI.
3. The SSO authorization server authorizes the user. It can also perform authentication, such as username/password verification, and confirmation of the requested action. Then it creates an authorization grant token to send back to the banking app.
4. If successful, the authorization server redirects the banking app back to the Bluemix application using the provided redirect URL, with the authorization grant token added to it. The redirect URL typically points to a server-side script that requests the access token through a **POST** to the authorization server.
5. The authorization server authenticates the **POST** by validating the client credentials, and provides an authorization code in the form of an OAuth2 token that proves that the banking app user is the individual who requested the transaction.
6. The application sends the transaction request and the OAuth2 token through z/OS Connect to CICS, with z/OS Connect validating the token along the way. CICS then sends back the result of the transaction that was invoked.

Conclusion

With the IBM Bluemix platform, you can design and implement a secure hybrid cloud environment on which Systems of Engagement run securely in the cloud, there is secure connectivity to the associated Systems of Record, and the mainframe assets that comprise those records are exposed in the most controlled manner possible. This functionality is enhanced when using IBM mainframes, such as the IBM z13™.

Using Bluemix, it's easy to create applications by reusing predefined components and services. IBM offers deeply detailed documentation and optional consulting services to help you make it happen.

In addition to the popular Bluemix platform described throughout this IBM Redpaper publication, IBM has more offerings that can help you secure your cloud-to-mainframe connections:

- **Single-tenant Bluemix**

  The Bluemix Dedicated platform is a single-tenant version of the product that is hosted on SoftLayer, but with access limited to just a single company. The platform brings even more control, security, and flexibility. Developers can build cloud-based SoEs that manage critical data that is visible only to the sponsoring enterprise. This is because Bluemix Dedicated includes the Bluemix virtual private network (VPN), which provides secure access to resources in the enterprise data center.

  Bluemix Dedicated generates interesting possibilities for SoEs that can't take full advantage of the Bluemix secure connectivity options discussed earlier. This can be helpful to mobile-oriented SoEs built with the IBM MobileFirst™ Platform Foundation (formerly known as IBM Worklight®). A recent IBM Statement of Direction announced that the MobileFirst Server will soon be able to run within Docker containers (which are supported by IBM Containers, which themselves are hosted in Bluemix).

  IBM Containers in the Bluemix run time extend Docker containers to handle lifecycle management, provide auto-scaling and auto-recovery, perform monitoring and logging, and make the Docker-based apps available with public Internet Protocol (IP) addresses. IBM Containers in Bluemix are secure, because they are isolated for each tenant and each organization. They make the Docker containers enterprise-ready.

- **Bluemix Developer Community**

  IBM hosts a community for Bluemix developers on IBM developerWorks®. The community has tutorials, blogs, and videos, and is a great place to ask questions about development on Bluemix.

- **IBM Bluemix Garages**

  Bluemix Garages are locations that customers can visit to get help from IBM to speed their adoption of Bluemix and move their Systems of Engagement to the cloud. In this collaborative environment, customers can more rapidly identify, design, build, and deploy the correct applications to their SoEs.

- **Hybrid Cloud Connect Test Drive**

  IBM offers a trial instance of Bluemix and a VPN for customers who want to test Bluemix connectivity to their mainframe. The Hybrid Cloud Connect Test Drive is available without charge. This includes a no-cost, three-month trial of SoftLayer, including a Gateway as a Service feature that serves as an access point for a VPN, plus one SoftLayer virtual server from which customers can test connectivity to their mainframe systems.

Resources

For more information about the concepts highlighted in this Redpaper publication, see these additional resources:

- Bluemix documentation and related resources:
  - IBM Bluemix:

    http://www.ibm.com/cloud-computing/bluemix/
  - IBM Bluemix for developers:

    https://console.ng.bluemix.net/
  - IBM Bluemix Dedicated Platform:

    https://console.ng.bluemix.net/solutions/dedicated
  - Using the IBM Bluemix Secure Gateway with IBM API Management:

    https://developer.ibm.com/bluemix/2015/05/27/bluemix-hybrid-integration/
  - IBM Bluemix Garages:

    https://www.ibm.com/cloud-computing/bluemix/garage/
  - IBM Bluemix Hybrid Cloud Connect Test Drive:

    http://www.eweek.com/cloud/ibm-takes-the-power-of-the-mainframe-to-the-cloud.html
  - IBM SoftLayer VPN access:

    https://www.youtube.com/watch?v=EdxkTZV5xCo
  - IBM Bluemix single sign-on:

    https://www.ng.bluemix.net/docs/#services/SingleSignOn/index.html#sso_gettingstarted
  - IBM Bluemix Mobile Application Security service

    http://www.ibm.com/developerworks/topics/mobile__application__security__service/index.html
  - IBM Bluemix Advanced Mobile Access:

    https://www.ng.bluemix.net/docs/#services/mobileaccess/index.html
- IBM Redbooks® publications:
  - *Getting Started with IBM Bluemix: Web Application Hosting Scenario on Java Liberty*, TIPS-1280

    http://www.redbooks.ibm.com/abstracts/tips1280.html?Open
  - *IBM Bluemix Architecture Series: Web Application Hosting on Java Liberty*, REDP-5184

    http://www.redbooks.ibm.com/abstracts/redp5184.html?Open
  - *IBM Bluemix Architecture Series: Web Application Hosting on IBM Containers*, REDP-5181

    http://www.redbooks.ibm.com/abstracts/redp5181.html?Open
  - *Extending IBM Business Process Manager to the Mobile Enterprise with IBM Worklight*, SG24-8240

    http://www.redbooks.ibm.com/abstracts/sg248240.html?Open

- Testing and compliance
  - Common Criteria Evaluation Assurance Level:

    https://www.commoncriteriaportal.org/
  - IBM Announces zEC12 Mainframe Server with EAL5+ Common Criteria Classification

    http://www.storagereview.com/ibm_announces_zec12_mainframe_server_with_eal5_common_criteria_classification
- Related products and information:
  - Cloud Foundry:

    http://www.cloudfoundry.org/index.html
  - Docker containers:

    https://www.docker.com/whatisdocker

Author

Jeff Miller is a Senior Software Engineer and subject matter expert (SME) in the areas of software development and architecture, mobile, security, web, Java Platform, Enterprise Edition (Java EE), IBM WebSphere, IBM Rational® tools, and mainframe computing. Before joining the IBM Competitive Project Office, Jeff was a technical consultant and adviser with IBM Independent Software Vendor (ISV) and Developer Relations. He has several industry and product certifications, and is a Security+ Certified Professional. Jeff has three undergraduate degrees, and a Master's degree in Computer Science from Rensselaer Polytechnic Institute.

This paper was produced by the International Technical Support Organization (ITSO), Raleigh Center. The work there was led by Shawn Tooley, Technical Writer.

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks
- Follow us on Twitter:

  http://twitter.com/ibmredbooks
- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806
- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm
- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information about the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document REDP-5243-00 was created or updated on August 21, 2015.

Send us your comments in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:
  ibm.com/redbooks

- Send your comments in an email to:
  redbooks@us.ibm.com

- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

Trademarks

REDP-5243-00

ISBN 0738454354

Printed in U.S.A.