Enabling B2C Solutions with Identity and Access Management

Redguides
for Business Leaders

Rob Macgregor
Colin Miles

- Learn how Identity and Access Management solutions can help organizations deliver better services to more customers
- Understand approaches for optimizing the user experience and integrating with business and technical processes
- Gain insight into real-world Identity and Access Management solutions for B2C

Redbooks

Executive overview

Traditionally, Identity and Access Management (IAM) solutions have been targeted to meet business imperatives for establishing control, accountability, and transparency for access permissions across enterprise IT systems and applications.

This IBM® Redguide™ publication describes how IAM has reached a state of maturity that allows organizations to seek value beyond a previously narrow focus on security, cost savings, and administrative efficiency. New IAM solutions offer opportunities to achieve so much more by delivering new services to wider user communities in innovative ways that closely align to objectives for brand management and marketing.

This guide describes solutions from IBM and Pirean that enable organizations to realize the new and significant routes to value from IAM, with examples of real-world Business-to-Consumer (B2C) scenarios, where these solutions are deployed to meet strategic business objectives beyond security and control alone.

Business challenges

Faced with an ever-changing set of external forces and market drivers, IT departments continually must adapt and update their approach to IT service delivery. As the demands of customers, business partners, and employees change and grow, there is a need to balance their needs against the business-outcome focused demands from a multitude of internal stakeholders.

In the IAM industry, recent developments added new layers of complexity to the challenges of identifying users, controlling the resources to which they get access, certifying access entitlements, and general management of the user journey. Here are some examples:

- The increasing adoption of cloud-based services and Software-as-a-Service (SaaS) delivery models introduces the need for new models for user authentication that often are based on federated protocols. New requirements for user provisioning go hand-in-hand with these challenges, including just-in-time methods that can have significant implications for a conventional compliance reporting approach.
- The rise and rise of social media services and related web-based utilities introduces new sources of user identity, which are increasingly finding uses in the commercial world, particularly in the gray area where marketing contacts and prospective clients mingle.
- The use of advanced mobile computing for application access (combined with *Bring Your Own Device* (BYOB) schemes within the enterprise) adds new factors to consider, from the use of a device as an auxiliary authentication factor to the emerging practice of Responsive Web Design.

In the face of this combination of complexity and emerging requirements, analysts and systems integrators are working to develop a set of common criteria against which future IAM solution delivery can be measured. An example set of emerging criteria is shown in Table 1.

Table 1 The new criteria for IAM solution delivery

Criteria	Requirement
Secured	Ensure the confidentiality, integrity, and availability of systems and data.
Controlled	Ensure that the right people get access to the right systems at the right time. Make sure that there is accountability for the correct assignment and use of access entitlements. Be able to demonstrate compliance with regulatory requirements and adapt processes as these requirements change.
Transparent	Provide a clear view on all matters relating to identity and access to help the business make the correct strategic decisions.
Agile	Support the competitive goals of the organization by providing an IAM platform that enables the rapid rollout of new services to large and diverse user communities.
Optimized	Avoid IT service delivery lock-in by promoting framework-based deployment models that allow for component swap-in/out based on the availability of best-of-breed technology. Ensure currency of the IT solution delivery against strategic business requirements always.
Consolidated	Support the migration and assimilation of identity information when driven by business change programs or acquisition activity. Help the business provide uniform and centralized platforms for controlling access.
Scalable	Ensure that solutions can be used in the future as the market demands grow over time. Deliver optimal system performance as system load increases.

Criteria	Requirement
Person-centric	Deliver solutions and interfaces that have usability and a user results focus as overriding design principles.
Simplified	Provide interfaces for identity and access that avoid needless complexity and aid the application of easy-to-use processes.

IAM services for B2C

To meet these new criteria, IAM vendors and systems integrators must reevaluate how their solutions are designed and deployed within any customer environment. The most successful approaches today focus on three core areas of expertise:

1. Business process integration

   Ensuring that identity and access are aligned to business processes and that it can adapt as business requirements change.

2. Technical integration

   Building the information flows between directories, databases, applications, and systems (both onsite and cloud-based) that ensure identity and access controls can be enforced across a heterogeneous estate.

3. User experience

   Ensuring that a first class user experience is delivered for all system touch points. Actively promoting the use of new identity and access services to drive new business value.

A typical B2C scenario supplies a distinct set of functional requirements that IAM solutions are well placed to help address. Typically, these requirements cover essential items relating to the identification of a customer and the management of that user's experience and interaction with the service that is being provided. Common solution themes here are to ensure a single, consistent view of the customer across all channels and services, the delivery of a personalized experience, and the evolution of an "intelligent" view of the person behind the identity to enable the presentation of relevant and engaging content.

The delivery of such services require consideration of the IAM building blocks that are needed to support the service. Here are some examples:

- The solution requires a scalable and responsive user registry, typically implemented as a Directory Service. Hand-in-hand with this registry is the need to get the correct user data into this registry. User migration strategies might be required to load or consolidate user data from other existing repositories. Care is needed to make sure that any back-end changes have a minimal impact upon the user experience, allowing previous credentials to persist and the migration of customers to new service platforms to be handled seamlessly.
- User registration services are required to be multi-tiered to reflect the developing nature of the relationship between a business and its customers. These services recognize that you must capture different levels of information from a customer who progresses from "first-time visitor" to "interested party" and "committed customer".

- Authentication services that are external to the enterprise applications that they support are required. Basic capabilities must include a range of authentication options, from support for multi-factor authentication (where it can be justified) and the ability to process Federated Identity protocols to enable authentication to be asserted from trusted third-party sources. These services also must be extended to provide user redirection and Single Sign-On (SSO) to the relying applications of the enterprise, whether through SAMLv2 IdP services or the usage of a secure reverse proxy.
- An IAM service should be able to act as more than just the source of login identity of a user. Credential enrichment services enable you to work alongside authentication services to assert what level of assurance you have that the user is who you think they are and also provides tracking information about the likes and dislikes of a returning user.
- For any online system with a large user base, it is imperative that strong user self-care options are made available. Not only does this feature minimize the organization's exposure to potentially expensive administrative impact from managing their user communities, it also provides an opportunity to enable the user to retain ownership of the personal data that they choose to share with the service provider and provide the most up-to-date view.

Meeting the challenges: Pirean Access: One and IBM Security Solutions

As an integrated solution platform, Pirean Access: One and IBM Security software provide a flexible, enterprise-grade solution to the challenges for providing IAM services in B2C environments.

For example, a typical solution deployment might include the following functions:

Web Access Management	A central integration point for security services that are associated with the web channel, orchestrating user authentication and providing SSO.
ID&V	An identification and verification solution with various flexible authentication methods and access workflows, and the capability to be customized for specific user experience requirements.
Web Federation	Handles federation protocols to enable both customers and colleagues to seamlessly access services that are provided by third parties, and to enable the organization to provide services to customers of third parties.
Authorization Service	Central services to allow coarse- and fine-grained access control to enable the organization to make decisions about the types of services and transactions that are available to customers and colleagues, and to be agile in changing those decisions as the business dictates.
Security Directory	A highly scalable, and highly resilient, standards-based central identity store for customer, partner, and colleague identity information.
Account Management	A centralized customer identity lifecycle management capability that manages customer information in LDAP and other identity repositories.

The IBM/Pirean solution framework that is built around these functions provides components that are robust, scalable, and secure, and that are proven in successful deployment across high demand B2C operations for enterprises across the world. Figure 1 shows an example component model for such a solution.

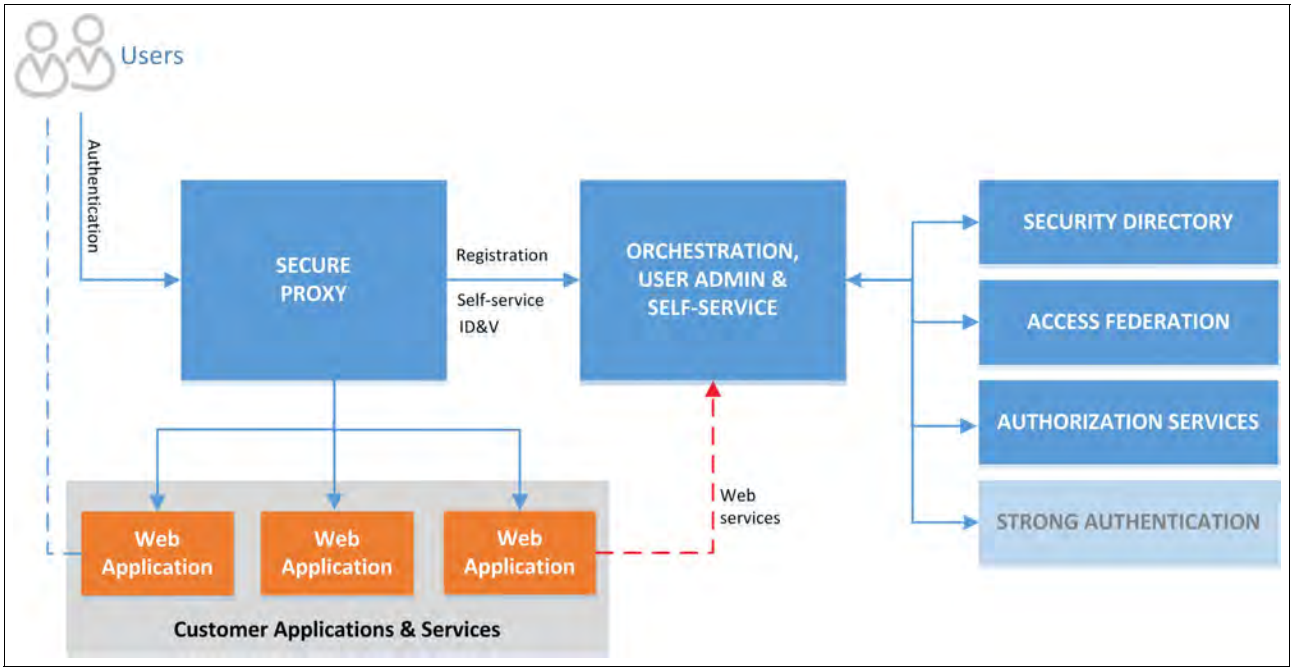

Figure 1 Sample component logical architecture for a B2C IAM solution

About Pirean Access: One

Pirean Access: One enables organizations to build the login and user management processes that are required for B2C flexibly and without the need for custom development or changes to existing applications or infrastructure. By using Access: One, organizations that deploy B2C services get the benefit of specialized authentication options and orchestration of the user journey, which allows the organization to focus on its own area of expertise: the delivery of the business applications and services to the customer.

The Access: One framework: Plug-ins and workflow

The Access: One framework provides great flexibility for the deployment of IAM services to meet a full range of internal enterprise, business-to-business (B2B), and B2C use cases. For example, a single Access: One service can provide the following items:

- Different types of user and application targets, with each combination subject to the appropriate authentication method
- Different page style and themes that are based on the request being made, to reflect a different brand or service type
- Support for multiple languages
- Access to multiple systems for user identification and credential enrichment
- Accumulation of audit data and built-in reporting

Access: One is implemented as a core framework that handles interactions with the user and management of the user session by using a series of plug-ins, each of which is responsible for interacting with a specific target service. Target services may be directories, Identity Management solutions, authentication mechanisms, secure gateways, federation service providers, or any service that can play a role in an IAM process. This high-level architecture is shown in Figure 2.

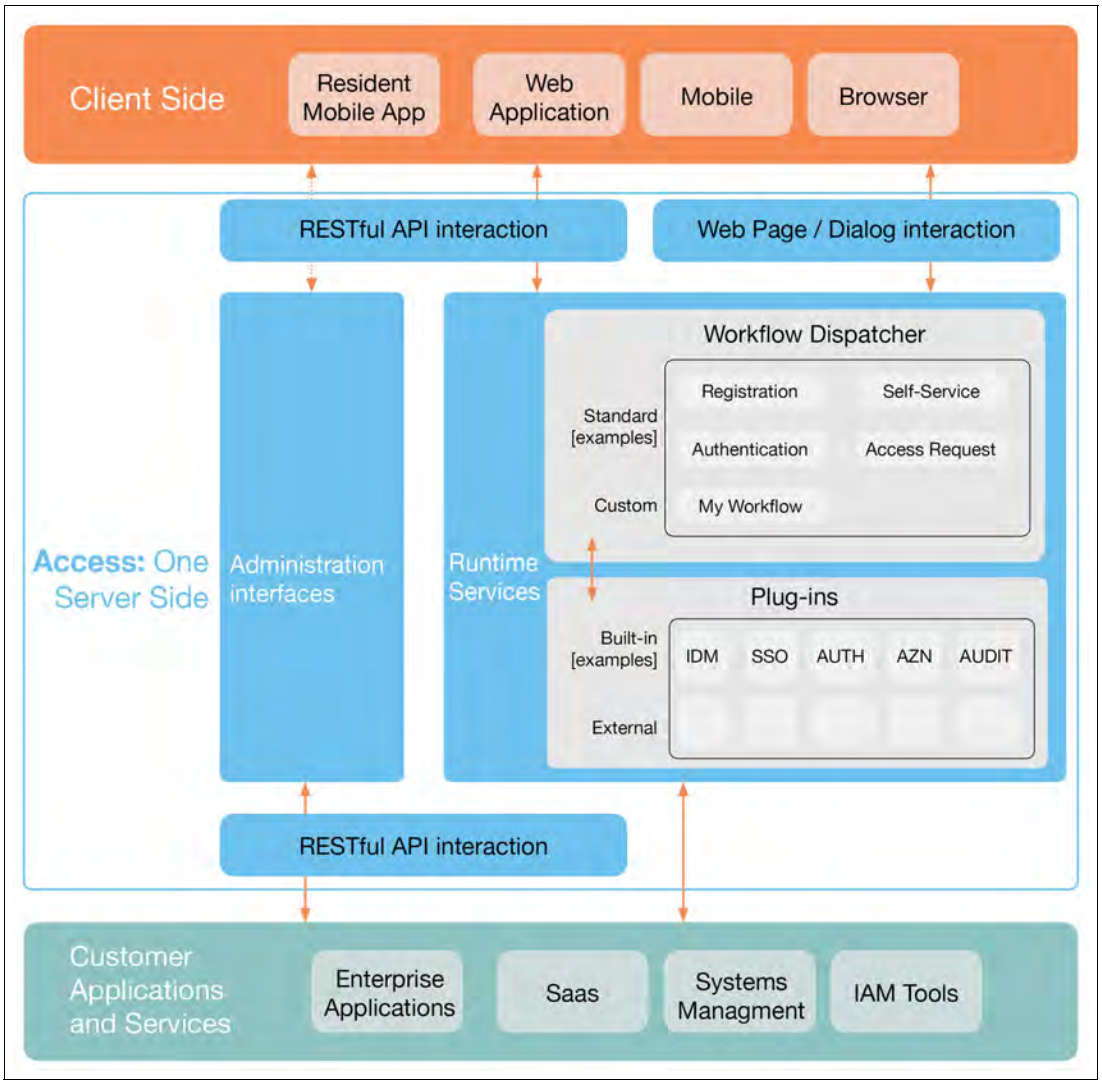

Figure 2 Pirean Access: One high-level architecture

Access: One plug-ins are started by the Access: One framework in the form of workflows. These are sequences of plug-ins that are configured to satisfy a particular user journey or business process. The framework ensures that the plug-ins are started in the correct sequence and that each plug-in stays active until it finishes its job. The framework also is responsible for presenting pages to the user that are correctly themed and in the chosen language, and for writing audit data.

Although workflows are normally run sequentially, from the first plug-in to the last one, they also include logical tests that allow the sequence to be varied, based on tests against user context data and information that previous plug-ins have acquired. These tests are called *next-step rules*. They apply simple pattern-matching rules that might result in control branching to a specific plug-in, or to a separate workflow.

When a request is received, the framework also must decide which workflow to run. This also involves some pattern-matching rules. The HTTP request is compared against a set of rules, each of which is associated with a given theme (which is reflected in a branded web page style) and workflow. When a match is found, the appropriate workflow is dispatched.

To understand how the framework, workflow configuration, and plug-ins interact, consider an example. Figure 3 shows a simple two-factor authentication workflow with Access: One acting as an external authentication provider for the IBM Security Access Manager Web Reverse Proxy Server (WebSEAL).

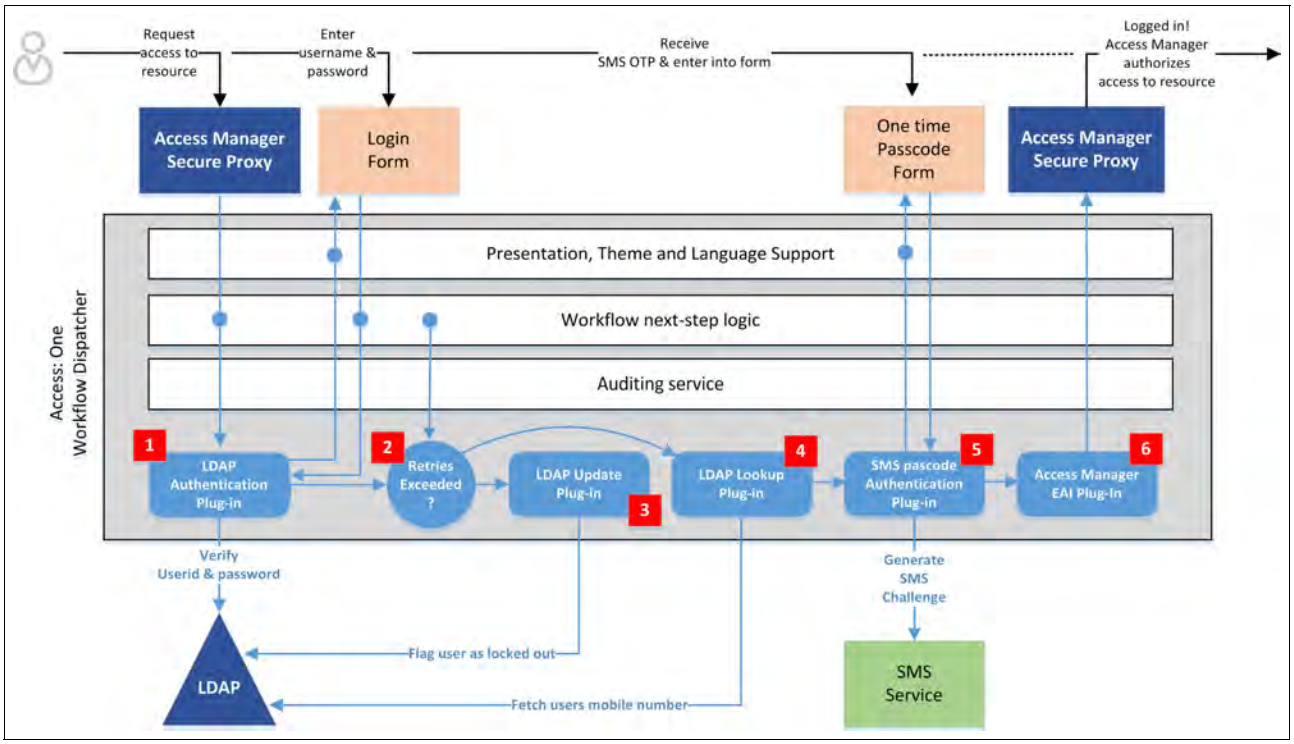

Figure 3 Dispatching a workflow

Access: One is first involved when the Access Manager Web Reverse Proxy detects that a request requires the user to be authenticated. A mapping rule in the framework routing service causes a given workflow to be started, which is allied to a specific visual theme. The workflow dispatcher then starts each plug-in in turn. So, for the example flow that is shown here, the plug-in sequence (as numbered in the diagram) is as follows:

1. The first plug-in attempts to authenticate the user to LDAP, using a user name and password. It presents the login form and then tests the credentials that are provided by the user. It remains as the current plug-in until either the user successfully enters a valid ID and password or the user exceeds the configured retry count.
2. A next-step rule then checks whether the user exceeded the allowed number of retries.
3. If the number of retires is exceeded, the sequence branches to an LDAP update plug-in that flags the user ID as locked out in LDAP and presents an error page.
4. Otherwise, the workflow continues to the next plug-in. This plug-in does not interact directly with the user, but sends an LDAP search request to retrieve user information that is added to the current user context. The information that is retrieved includes the user's mobile phone number.

5. Using the phone number that is retrieved in step 4 on page 7, the next plug-in generates a random 6-digit one-time passcode, which is sent to the user in an SMS text message. As was the case with the user name/password test, the plug-in stays active until either the user correctly enters the expected passcode or a retry counter is exceeded.
6. Finally, the user is identified to your satisfaction by using two separate login factors. The final plug-in assembles HTTP headers that inform the Reverse Proxy of the user identity and then pass control back to it.

Levels of Assurance

Access: One categorizes each logged-in user at a given Level of Assurance (LoA), based on the degree to which the identity may be trusted. The levels are based on NIST standards and are shown in Table 2.

Table 2 Levels of Assurance in Access: One

LoA	Description
0.5	User who is not verified securely, but known from a previous visit
1.0	User who is verified by replayable credentials (that is, user name and password)
2.0	User who is verified by non-replayable credentials (for example, OTP or soft token)
3.0	User who is verified by a combination of credentials (two-factor authentication)

The LoA is present in the credentials that Access: One retains for each user and may be passed to applications in SSO credentials, or queried through web service calls.

Access: One Application Launchpad

Access: One frequently is used in highly diverse environments, where many different web-based applications are linked by a set of IAM-based dialogs. In such an environment, one common issue that arises: How do you present the user with a view of the applications that are available to them? In a conventional corporate network, such a role often is played by a portal application, so Access: One can integrate seamlessly into such a system. However, in more dynamic and B2C environments, this integration might not be feasible or appropriate. In particular, many portal applications do not work well with the restricted screen space of mobile devices.

Access: One provides a standard plug-in that helps you handle this requirement. The Application Launchpad (Webtop) plug-in is a centrally configured application that allows an organization to present applications to the user as simple graphical links, which are divided into three categories:

- Applications that do not require authentication
- Applications to which the logged-in user has access
- Applications for which the user does not yet have, but might request, access

As an example, Figure 4 shows the publicly accessible applications that are accessible to a non-authenticated user.

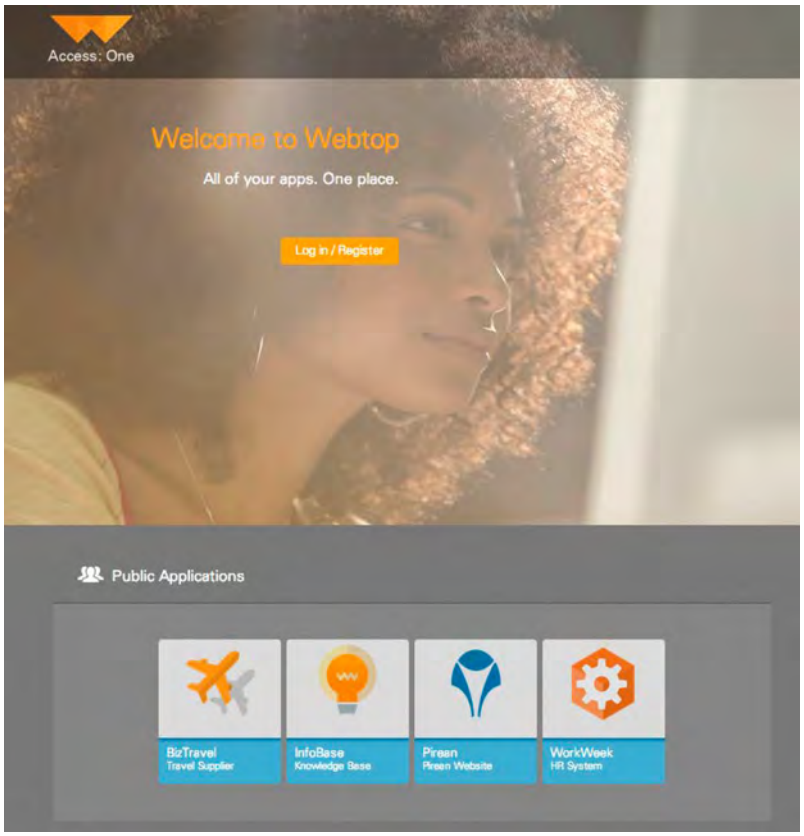

Figure 4 Webtop example for unauthenticated access

Figure 5 shows the view for an authenticated user. Now, a personalized display of each of the applications that the user is authorized to access is shown. The user can click each tile to be seamlessly signed-on (through SSO) to each relevant application. Also available are options to view a store of additional accesses for which access may be requested and self-care functions for managing the user's personal information (*My Identity*) and registered access devices (*My Devices*).

Figure 5 Webtop example for authenticated users

Integration with IBM Security Solutions

Access: One integrates with IBM Security Solutions to enable the full enterprise-grade delivery of IAM services for a B2C environment. Figure 6 shows the integration points that are available and highlights some of the use cases that these integrations support.

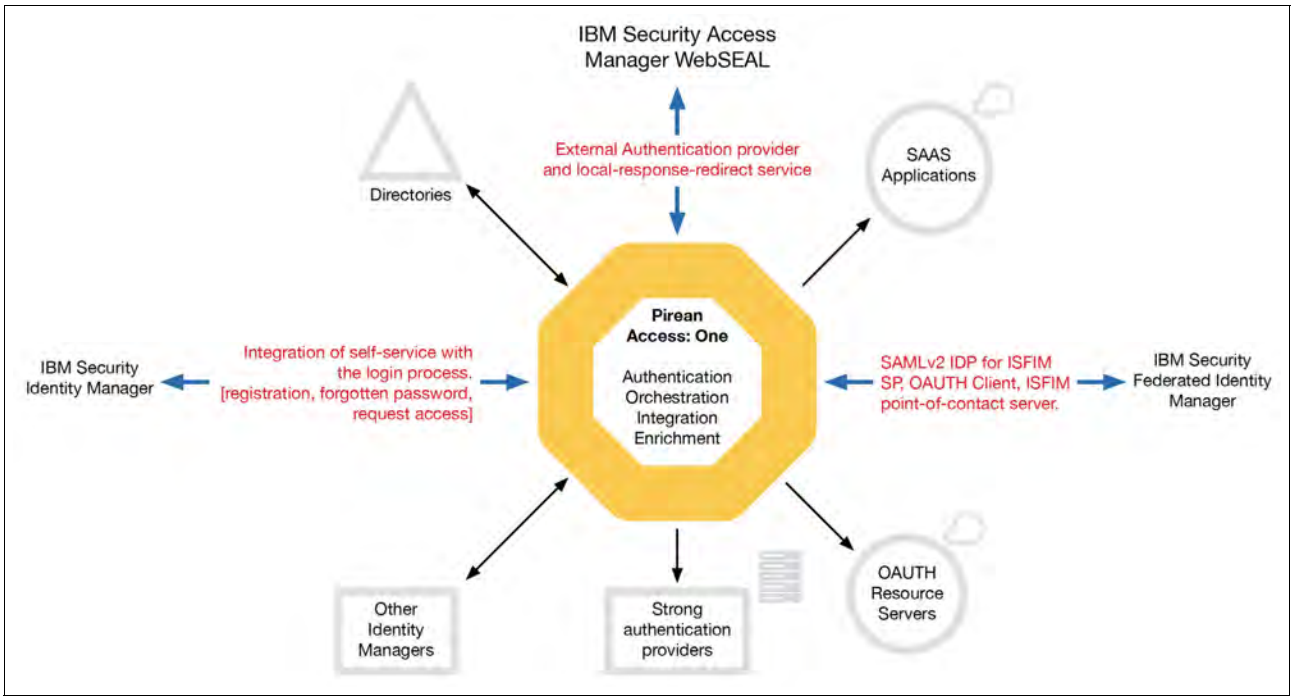

Figure 6 Access: One integration with IBM Security Solutions

Reporting and dashboards

In addition to its configuration role, Access: One uses an underlying audit database to provide a dashboard facility, providing a graphical view of system activity and a capability for identity and access reporting, as shown in Figure 7. In a B2C environment, such information can be invaluable as input to detailed analysis of user behavior that is used to define and refine future service offerings to consumers.

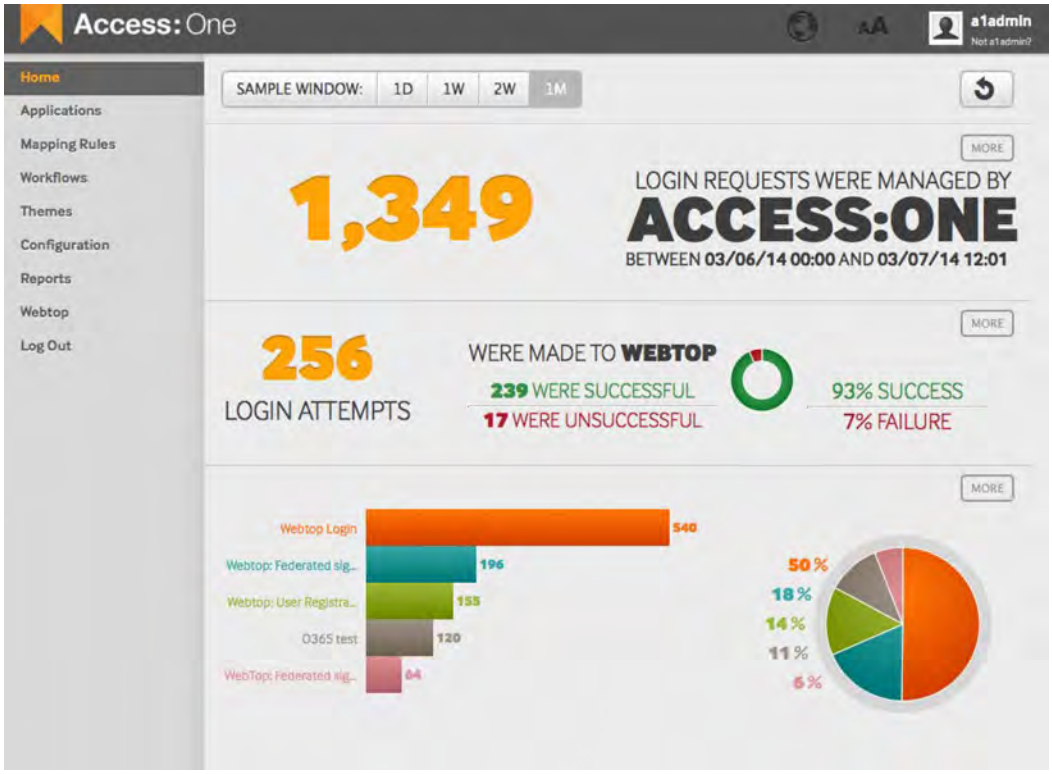

Figure 7 The Access: One dashboard

Access: Apps

Access: Apps provide a versatile method for delivery of a discrete set of IAM use cases that are targeted at meeting specific business requirements.

With Access: Apps, you use the same underlying framework of Pirean and IBM solution components overlaid with packaged, ready for use solutions that can realize quick value for the business with minimal configuration and customization. These applications are tailored to specific industry “pain points” and deliver preferred practice configurations and user journeys that are based on the experience of delivering IAM solutions for customers across a wide range of internal, B2C, and B2B scenarios.

Examples of ready-to-deploy Access: One applications include solutions for user self-service for the requesting, authorization, and provisioning of new systems access, the application launchpad (Webtop) for a personalized portal for employees and customers to access authorized web applications (with seamless SSO), and a Password Self-Care application for preferred practice management of some common user self-service journeys.

Case study: Enabling delivery of new online services with IAM

This section looks at a case study in the financial services sector.

The requirements

A large financial services organization was undertaking a major program to transform its digital presence and improve the quality of the online services that they offered to their customers. They required support from Pirean to design and implement an IAM solution that can support the critical business and operational goals of the program.

The requirements brief for the solution focused on a number of business outcomes, as shown in Table 3.

Table 3 Case study - business goals

Business requirement	Detail
Improve the customer experience.	Simplify the journey that a customer undertakes when interacting with digital services. Provide access to multiple services through a single consistent identity and interactive experience.
Enable revenue growth.	Support business goals to return more value from online services by enabling the delivery of personalized and targeted content.
Improve operational efficiency and enable consolidation.	Support the assimilation of previous disparate business units and service operations under single, centralized services. Reduce workloads for support and operational teams by providing improved and more secure administrative functions alongside customer self-care facilities.
Build for the future.	Provide a flexible foundation for the delivery of additional customer services and related IAM functions in the future. Ensure best-of-breed technology solutions can be deployed rapidly in future without the need for significant infrastructure upheaval and with minimal customer impact at all times. Provide a platform that is fully scalable for anticipated future demand of hundreds of thousands of users.

Through the process of detailed requirements gathering with the customer, a set of functional IAM use cases were agreed upon as deliverables for the project. Some of the key items from this review are shown in Table 4.

Table 4 Case study - key IAM use cases for the solution

Required function	Detail
User registration	Registration of new online customers through clear, efficient, and brief user journey orchestration.
User migration	Migration of existing customers from existing platforms to new services, while providing a seamless integration and customer experience at login time for the customer.
Authenticate user	Verify the identity of a user through mechanisms that are commensurate with the risk that is associated for the transaction being run.
SSO	Provide access to multiple services through a single authentication event.

Required function	Detail
User self-care	Provide services to allow users to reset their personal password. Provide security functionality to allow users to set and change a number of different security questions and answers. Allow forgotten user IDs to be retrieved through completion of the security Q&A process and a link to a previously registered email address. Allow authenticated users to update their personal account details. This includes the ability to update the linked email address and manually reset passwords.
User administration	Provide central identity administration interfaces supporting a single view of the customer. Provide account administration functions, that is, lock the account of a user who is unsuccessful in authenticating after a configurable number of attempts. Also, support the unlocking of account when the identity subsequently is verified by an alternative route.
User experience	Ensure that all customer facing interfaces reflect corporate branding that is appropriate for the owner of the account (allowing for differences in geography and customer history). Multiple corporate brands are applicable to the organization. Provide an interface that shows content that is appropriate for the user accessing the system. Support for multiple different national languages is required.
Support Business Intelligence	Integrate user identity/tracking services with existing enterprise services for BI and mobile device management (MDM). Provide identity and access insight that supports the business in making better decisions regarding the provision of future services.

The solution

The customer solution was implemented using integrated IBM and Pirean software solutions for IAM (Pirean Access: One, IBM Security Access Manager for Web, IBM Security Directory Server, IBM Federated Identity Manager, and IBM Security Directory Integrator). The physical architecture for the solution is shown in Figure 8 on page 15.

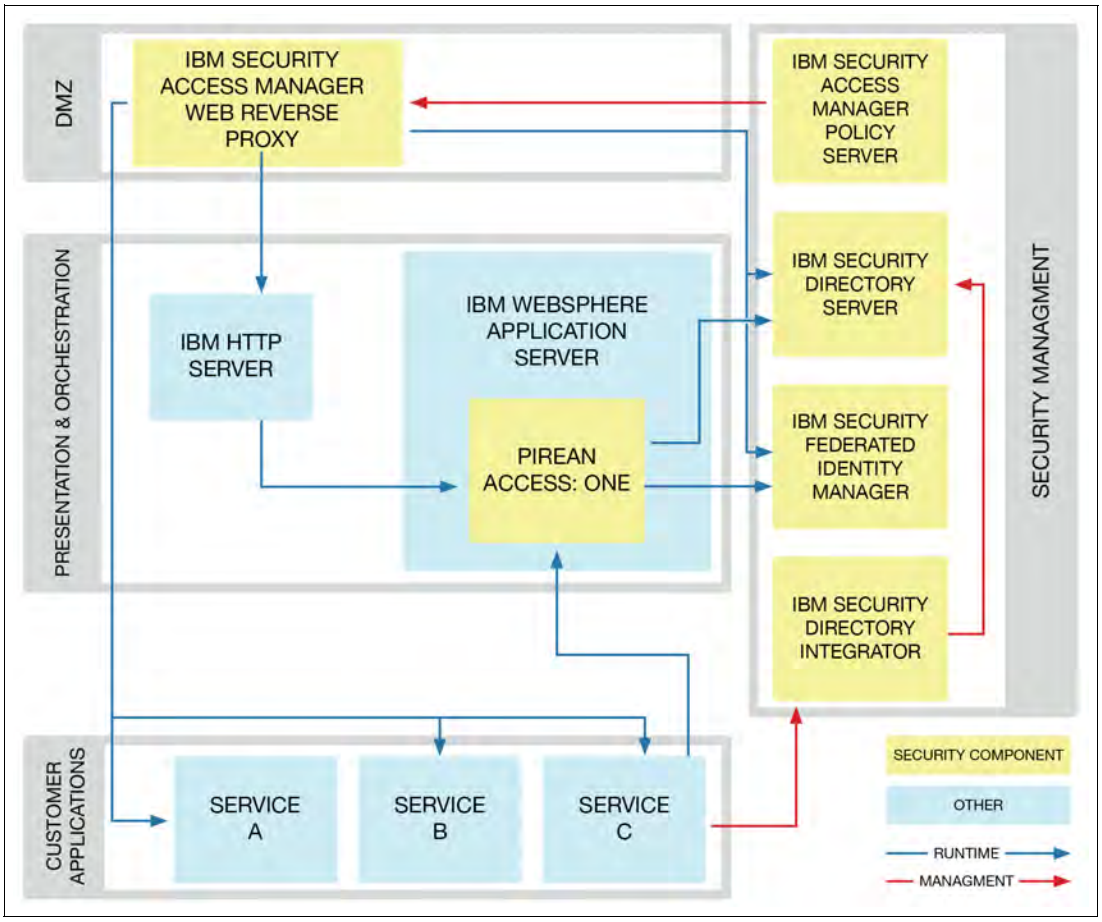

Figure 8 Case study - physical architecture for IAM solution

Upon delivery of the solution, the customer can use the IAM services to strong and positive business effect. The benefits that are derived from the solution extend across a wide range of business impacting areas:

- Supports delivery of a consistent customer service

  The solution fully conforms to industry preferred practices and the customer's own practices and standards. This situation helps enforce a consistent user experience for all user touch points with the enterprise, improved user satisfaction levels, and encourages further adoption and effective use of new services.

- Supports migration of user accounts

  The solution provides for *lazy* user migration process to minimize disruption and risk, updating and populating user details in new repositories as part of a login-time operation.

- Improves productivity and customer satisfaction

  Self-care functions provide customers with the option to perform account management functions quickly and easily without the need to call on third-party assistance. This means users get the access that they need straight away, and in the case of password resets, avoids any "dead time" as individuals wait for help desk calls to be answered and processed.

- Decreases costs

  The costs of running central administrative functions for user and account management are known to be a significant drain on the business. The delivery of this self-care function helps minimize costs for administration by reducing the requirement for support from help desks, and so on.

- Improves security controls

  The implementation of Q&A functionality, together with tightly marshaled, process-linked execution of user journeys for account maintenance, can deliver improved controls to the business, ensuring that procedures and policies are applied consistently.

- Enhances reporting capability

  The centralized components that are used for self-care functions provide an audit point for capturing and reporting on user account maintenance activity. When coupled with other sources of user activity data (for example, user repositories, Identity Management platforms, or SIEM tools), this function can deliver enhanced Identity and Access Intelligence for the business to use.

- Make the solution usable in the future

  The deployment of IBM Security Solutions with Pirean Access: One provides the customer with an enterprise class framework that can be further used as the needs of the business change. The flexible, framework-based approach allows swap-in/out of new user repositories, target systems, and authentication mechanisms quickly and easily, without the need for code development or new infrastructure deployments.

Summary

IAM solutions are reaching new and more interesting levels of maturity as project mandates evolve from those that are built around requirements for security and control to a new focus on enabling agile IT service delivery for the business in the competitive marketplace. Although these changes are impacting all IAM projects today, perhaps the most significant examples can be seen in B2C scenarios where organizations must look to find ways to transform and improve their digital service offerings to customers.

Concurrently, many of the IAM requirements for the modern enterprise are distinctly familiar. The online world continues to be built around identity systems and models that have inherent challenges in asking for the delivery of new services to wider customer audiences while still ensuring the privacy of customer information and balancing acceptable levels of risk for the organization. Customers, vendors, and system integrators must face these strategic challenges together to help build the right IAM solutions for tomorrow. With the IBM and Pirean technology approach that is described in this guide, we are seeking to deliver solutions for IAM that enable our customers to strike the right balance today, bringing IAM solutions that can demonstrate short-term and business-focused return on investment (ROI) while establishing the flexible framework that is needed to support solution evolution tomorrow.

Pirean is a *Ready for IBM Security Intelligence* Business Partner and the solution, *Pirean Access: One*, was validated with the *Ready for IBM Security Intelligence Validation Program*. More information about this program can be found at the following website:

http://www.ibm.com/partnerworld/gsd/scsolutiondetails.do?&solution=48272&lc=en&cd=BPAS&sbcd=

Other resources for more information

For more information about this approach to delivering innovative solutions for IAM with IBM and Pirean software, contact us through any of the following website:

- Find us on the web:

  http://pirean.com

- Follow us on Twitter:

  http://twitter.com/pirean

- Look for us on LinkedIn:

  http://www.linkedin.com/company/pirean-ltd

- Look for us on Google+:

  https://plus.google.com/+pirean/posts

Authors

This guide was produced by Pirean working with the International Technical Support Organization (ITSO).

Rob Macgregor is a Product Manager at Pirean Software. With over 30 years of IT experience, of which more than 10 have been focused on solutions for IAM, Rob has a wealth of experience in securing some of the world's leading brands. Joining Pirean in 2007, Rob was a Principal Consultant in Pirean's Professional Services business before joining the product team for Access: One. Rob's current role involves defining product strategy and working with clients and business partners to design and deliver leading solutions for IAM.

Colin Miles is the Chief Technology Officer at Pirean Professional Services. Colin has over 20 years of IT solution delivery experience, having progressed his career from software engineer to architectural and management leadership roles for many customers across a wide range of industry sectors, including Retail, Utilities, Manufacturing, and Financial Services. For the past 10 years Colin has had a specific focus on meeting the technical and business challenges for the implementation of IAM solutions. Having joined Pirean in 2008, Colin is responsible for the portfolio of new and existing products and services that are delivered by Pirean's consulting business.

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

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 IBM 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 on 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites 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-5124-00, was created or updated on September 15, 2014.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at
http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

Redbooks (logo) ®	Redbooks®
IBM®	Redguide™

The following terms are trademarks of other companies:

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