How To Design Authentication and Access Architecture For Apps In A Modern Organisation

A comprehensive White Paper for CIOs and System Architects looking to build a flexible and bulletproof SSO cloud-based architecture

by Tomasz Onyszko

Co-owner and a CTO of Predica. Tomasz is an internationally recognized expert in the field of Identity and Access Management. Microsoft has awarded him multiple Most Valuable Professional status awards. He is also a remarkable keynote speaker at international conferences (TechEd Europe, The Experts Conference, Microsoft Technology Summit).
TABLE OF CONTENTS
INTRODUCTION
Most companies have extensive on-premises infrastructure supporting its users and applications. In this infrastructure configuration, Active Directory (AD) or Lightweight Directory Access Protocols (LDAP) directories are the center of user authentication and authorization strategies.

Built over time, these directories become a central point in security control and application access for users. For on-premises applications AD\LDAP, directories authenticate user information and authorization, mostly based on groups.

Companies adopted LDAP or Kerberos-based authentication based on the Active Directory as a common way of providing central authentication and authorization for users within applications. These applications function on Windows-based applications, but are also incorporated deeply within Java, PHP, and many other application environments.

Applications integrated with Active Directory or central LDAP directory provide a user authentication path. The same credentials are authenticated in multiple applications. It can also achieve single sign-on based on Kerberos protocol.

This approach worked well and still does for the on-premises environment. For desktop or web based applications, integration with AD or LDAP provides a convenient way of authentication and for the IAM team. It is a single point for final authorization where information (groups) needs to be managed.

AD also guards company network access, remote access solutions like VPN, and many other aspects of company infrastructure.

This all changed as the internet rapidly gained users. The rise of mobile devices further compounded the problem across wide distributed networks.

Due to the rapid expansion of the internet and the rise of mobile computing cloud service, SaaS applications are rapidly growing. Most organizations use multiple SaaS applications for productivity, communication, and a variety of other tasks that aid users.

The approach towards building authentication and authorization services, must change. Services like central AD and LDAP are still necessary. But these services don't scale well when going outside company firewalls. Organizations with mobile users and SaaS applications must build a new authentication and authorization strategy.

Modern architecture of authentication and access control for applications need to provide a secure and seamless user experience when the user is accessing an application:
· On-premises
· In the cloud infrastructure (IaaS)
· SaaS applications.

These elements are essential to a modern company’s IT infrastructure.

Managing customer and client communication is the key element in building a competitive business advantage. And this relationship in applications takes the form of digital consumer identity, which organizations need to be ready to gather, manage and consume within applications.

This whitepaper introduces architecture patterns that companies can use to build modern authentication and authorization solutions for applications. It illustrates how organizations can transform their current on-premises environment with modern, cloud and SaaS to serve its employees, business partners and consumer identities.

This transformational architecture will provide a solution that:

· Provides secure access with single sign-on to both applications on-premises and in the cloud, based on the foundation of existing Active Directory infrastructure.

· Enables organizations quickly to adopt applications and services like Software-as-a-Service (SaaS) or move to the cloud providers from on-premises infrastructure.

· Builds a foundation for managing B2B and B2C relationships with external entities.

· Provides additional protection for digital identities used by users to access applications.

Let’s take this journey together.
WHERE ARE WE?
Most organizations rely on Active Directory as a central authentication and identity information store for on-premises applications. Applications are deployed in on-premises networks and are protected within those boundaries.

To provide authentication, these organizations use a set of technologies to utilize AD in this context, either using native Windows Authentication on Windows platform (which uses Kerberos or NTLM underneath) or LDAP.

This approach works well within an on-premises network. When the user is working outside of its perimeter network things get complicated. Windows authentication or LDAP-based applications were never designed to work outside of an organization perimeter network.

To provide application access for users working outside of perimeter networks, organizations typically use several different solutions:

- Allowing application access only over VPN to bring the user to the perimeter network. This extends on-premises perimeter reach to the user location. Users need to be equipped with additional client software and in many cases additional equipment to provide stronger authentication when accessing on-premises network.

- Application publishing over reverse proxy application gateways or remote access solutions like Citrix. These solutions stand between the user and the published application, while handling authentication process as the user would be on-premises.

This traditional approach solves immediate application by providing users with the means to work. However, it is not addressing all the needs which exist in modern organizations right now:

Did you know?

LDAP was never designed to be an authentication protocol. It is a directory data access protocol. It was never intended for credentials protection. LDAP without SSL sends user credentials over networks in clear text.
- Users and applications still are attached to on-premises identity store. It is just being exposed or used by the underlying infrastructure to make it somehow available in the external network.

- Application access is not simple and convenient; usually, it comes with a need for additional software or hardware.

- SaaS application access is still not provided. Organizations still need to maintain it separately.

- Relationships with external entities, either business partners or consumers requires additional efforts like the creation of accounts for them within company resources. This is troublesome and provides some security risks.

This application authentication and access management architecture are what is present in most companies. It works pretty well for administrators. They have to manage users in the single identity store. They know how to use it as it is based on their daily credentials, and developers learned how to utilize AD for this purpose.
SAAS AND CLOUD INFRASTRUCTURE AHEAD
Why introduce change?

The introduction of cloud infrastructure, cloud services and software as a service (SaaS) changed this picture.

Applications might reside right now outside of company perimeter network or be moved to the extended location which is cloud Infrastructure as a Service (SaaS) in Microsoft Azure or Amazon Web Services.

User stores are dispersed. Each SaaS application used within the organization is introducing a new one. Collaboration scenarios with other businesses or customers are creating the need to incorporate external identity stores into a picture. These users also want to extend their identity and express it in applications without the need for creating additional accounts.

Application integration becomes a major need. Using more external applications or using cloud platform for application creation invokes another need, that of user identity being easily available and ready to use outside of perimeter networks. Cloud platforms can also use solutions like VPN to connect to the organization network environment. However, this is not a conclusive solution. It is just augmenting a solution.

Your organization should incorporate modern solution architecture for this problem, allowing it to expand and use applications on-premises, in cloud infrastructure and provides as SaaS.

You need to build an architecture which easily extends to another environment and uses digital user identity as a central point of focus to bring all elements together. Architecture should be easy to use and consume within the applications and APIs.

Identity is a new control plane.
(Alex Simons, Microsoft)

Identity is what is needed for your modern organization when the next new application is introduced.
PEERING THROUGH THE CLOUDY SKY
In most of the organizations, the need to modernize its authentication and authorization services arises first with a major move into the SaaS services. When an organization is making a decision to use SaaS application company-wide, a question arises: “How can we get our users’ identities there?” It is not that this need was not present before. Most companies were using SaaS software on a smaller scale before. (It is a first major use case which affects a significant number of users within the organizations which brings this question to CIO or CSO table.) rephrase this sentence!!!

Control doesn’t mean blocking!

Luckily, we don't need to re-invent the wheel. The move towards cloud infrastructure and SaaS apps has resulted in some solutions we can use to build our cloud identity solutions.

Companies like Microsoft have built such capabilities into their infrastructure to make it easy to onboard their current customers into cloud services.

But we are not limited to the choice provided only by platform vendors like Microsoft. There is an entire class of services and software focused on providing a way to promote our user’s digital identity as a first class citizen in the cloud. It is called Identity as a Service (IdaaS) and it is a growing part of the IT services ecosystem.

Companies like Ping Identity, Okta or Auth0, are providing services which are making it easy to extend the reach of our current identity stores into the cloud services environment.

Typically, these solutions require your organization to implement directory synchronization between your on-premises directory and IdaaS directory. It doesn't mean that all your user information is being transferred there; you are in control what is being synchronized.

When user information is transferred into cloud directory, you need to enable your users to sign into this service.

What you need to consider when selecting an Identity as a Service provider is:

- **What tools you can use to bring your current user’s identity into this solution.** Usually, there is a tooling provided to you by a solution vendor to provision users from your on-premises directory into IdaaS user repository. You should take a look at what this tool provides regarding capabilities and match it with your infrastructure. Typical use cases are synchronization of users from multiple AD forests into single IdaaS tenant – consider those
• **How user authentication solution is provided.** Solutions in this area are usually similar between various IdaaS providers, but implementation might be different. Options provided usually are to use authentication through agents deployed on-premises or to use federation services approach. Consider this and check what infrastructure will be required!

• **Application support and ease of adding new applications!** Each of IdaaS services provides built-in support for some applications. These are pre-defined application configurations to work with this provider. It saves time and makes it easier to deploy the service. Match your applications being used with those provided in given IdaaS! Check how easy it is onboard your new application when it is not one of the standards provided by the vendor.

### Peek into cloud identity service – Azure AD

Let’s look at the very common case of companies using Office 365 collaboration service provided by Microsoft.

With each instance of Office 365, deployed customers are effectively getting their new Identity as a Service instance created in the form of the Azure Active Directory.

The main reason for that is to provide access to Office 365 services itself. Azure Active Directory, however, is one of the modern IdaaS offerings, and it is not limited to providing access to Office 365 alone.

It supports standard protocols like SAML and OpenID Connect which enable it to be used with other SaaS applications.

On-premises users are synchronized into cloud service with a Microsoft-provided tool – Azure AD Connect. This tool allows information to be synchronized from on-premises directory to Azure AD and in some cases like devices or groups to synchronize it back to the on-premises environment.
User authentication can be delivered through on-premises service or in the cloud, with choices of:

- **Cloud user**: user account and password reside in the IdaaS and are not synchronized from the on-premises AD

- **Synchronized user with password hash**: user is synchronized from on-premises and its password hash travels with it. The user is authenticated in the cloud but with the same credentials as for its on-premises AD account.

- **Federation services deployed on-premises**: the user is authenticated on-premises through federation services (on-premises identity provider), which provides proof of authentication (token) to Azure AD.

- **Pass-through authentication**: the user is authenticated on-premises in local AD through the channel established with Azure AD Connect. In this option, all authentication happens on-premises, but the user experience is the same as when the user is logging on as cloud user.

User authenticated to Azure AD can benefit with access to any application which is integrated with Azure AD or was configured as such by organization administrators. It might also include third party applications not provided in service itself or developed by the organization.

The user can access these applications through a web panel or on mobile devices through native applications. It is a typical element of Identity-as-a-Service offerings.

Administrators benefit from Azure AD with granular control over applications available for users and single point of control for user access to SaaS applications.
Identity and protocols – what fuels applications?

The Web is fueled by applications and what allows us to work with these applications are standards. It is same for identity implementation. If we want to make it easy to use we need to rely on standards.

Currently, there are two major standard protocols for authentication for users.

**Security Assertion Markup Language (SAML)** is an XML-based, open standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. It provides a means to authenticate the user within the application and provide authorization information based on a trusted identity provider model. SAML was mainly designed for enterprise use, and it requires 1:1 trust configuration between the given application or its instance and identity provider. (http://saml.xml.org/)

**OpenID Connect** is a modern, simple identity layer and protocol based on OAuth 2.0, which allows the application to verify the identity of an end-user based on the authentication performed by an Authorization Server (aka Identity provider). It is designed to be used in internet web environment and easily consumed with REST interfaces. (https://openidconnect.net/)

**OAuth 2.0** is not strictly authentication protocol. It is an open standard for authorization of access to resources. In many cases, it is used for user authentication, though this was not its original purpose. That is why OpenID Connect layer was created on top of OAuth 2.0 protocol flow. (https://oauth.net/)
MODERNIZE IT ON THE INSIDE
With Identity as a Service (IdaaS) solutions, an organization can quickly adopt cloud solution and start to manage user access to SaaS applications. It is easy as most of SaaS applications are adjusted to modern authentication protocols and ready for such scenarios.

Most of the organizations already have some systems and applications which are running on-premises and were not built or configured to use services which reside outside of the perimeter network.

Not all new applications are also deployed as cloud services. Organizations will still deploy on-premises applications. This will happen because there is still value in on-premises applications and some organizations are still not allowed to move data to the cloud, mostly due to regulation requirements.

Even within on-premises environment, companies can still benefit from modernization of authentication and authorization services.

How?

Using the same architecture approach as with cloud identity as a service, organizations can deploy internally identity provider services and adjust applications to use those services as a source of authentication and authorization information.

With this approach a company can benefit in following way:

- **Provide SSO experience for users while working with multiple applications**: Using common service providing user authentication and supporting a range of federation protocols can enable a single sign-on experience for users. It will greatly benefit users who are struggling with a growing number of applications and credentials to manage.
· **Prepare the organization for future infrastructure change:** Even if the organization is not considering it at the current moment, all the trends show that infrastructure becomes a commodity. In the future, it might be changed in the same way as a provider of other services. Decoupling application from underlying authentication infrastructure through identity provider service is making them ready for such a move.

· **Lower cost of applications maintenance and development:** Using standard-based and well defined common architecture for user authentication through identity provider service is lowering cost of deploying, and in the case of custom application, development of software.

This architecture can be easily expanded to the internet and users from organization working outside of the perimeter network. Through publishing application and identity provider service for external networks, an organization can enable users to access the application securely with authentication provided through Identity provider.

It means using the same credentials as on-premises and the same authentication methods. It can be made more secure with additional security measures like multi-factor authentication (MFA) or conditional access policies.

Publishing to external networks service like identity provider allows us to extend our user's digital identity reach the IdaaS service. This is the concept of hybrid identity where on-premises authentication service is extended to the cloud through IdaaS service and its capabilities.
How can I implement Identity provider on-premises?

That might be the first question to ask: what does it take to build such a service for the organization?

The identity provider can be established using various software provided from commercial vendors and also available as Open Source software.

In an Active Directory based environment the simplest choice might be to use Active Directory Federation Service (AD FS) provided as part of Windows Server operating system. AD FS is a great choice because it is provided within the license of OS and it is also a good solution. AD FS has some limitation. For example, it can utilize as authentication source only AD or in Windows Server 2016 also LDAP directories. It is however excellent software if it suits the organization’s needs.

If the organization needs more flexibility with authentication options, supported protocols and advanced features, it might consider other options like Ping Identity, ForgeRock or Auth0 (which can be deployed on-premises).

Choice of the solution should be made based on analysis of business scenarios, technical requirements, and the cost of operation of each software option.
Will it solve all my problems?

No, it won’t. There still be some applications which are not ready or cannot be adjusted to work with such a service as an identity provider and will use a standard approach for user authentication based on AD, LDAP or some custom solution.

The fact that it will not address all of the problems should not prevent the adoption of these services and approach. Building common authentication and access management infrastructure within the company will help the organization to manage the problem with access to applications and not to make it worse.

Clearly defining a policy for application supporting specific protocols and architecture, which is built within the company, will provide guidelines as to how new applications need to be incorporated into the environment.

But if this architecture gets unfolded even further, there is a solution which can help us address and modernize access to even more applications. Let’s look further into this topic.
CLOUD INCEPTION
The Identity provider service deployed on-premises and adopted as a standard for application authentication and authorization helps with providing SSO and access for an application which supports such solutions. It also extends user identity to an external network and helps build a hybrid identity solution with IdaaS services.

IdaaS services will help to provide easy and unified access to SaaS applications. These are mostly first class citizens taking full advantage of modern authentication schemes.

Most organization will still have plenty of applications which are based on standard, on-premises authentication methods. Can we do something to introduce these legacy applications into the same schema and make it easy to access for our new breed of mobile users?

Modern services are providing a solution for at least one class of these legacy applications – Kerberos-enabled applications.

Kerberos, as a protocol, was never meant to be used on the Internet. It requires communication with a trusted key distribution center over a network with multiple opened ports. It simply was not designed for it.

It is an excellent protocol for authentication, and if correctly implemented and configured with application, it provides the benefit of secure single sign-on access. There are plenty of applications already using Kerberos through Windows authentication.

Kerberos authentication is not limited to Windows platform and is widely adopted also with Java and other non-Windows-based application environments.

It is however limited to the on-premises network unless it is proxied through some service acting as a go-between with on-premises and the external network.

**Azure Active Directory Web Application Proxy**

When an organization builds hybrid identity architecture with on-premises AD identity service extended into external networks with Azure AD IdaaS, it can benefit from one more service, which enables Kerberos-based applications to be first class citizens in this architecture.

This service is called Azure AD Web Application Proxy (Azure AD WAP).

How does Azure AD WAP fit into our modern authentication scheme? Azure AD WAP is a publishing service, which allows the organization to publish its internal application through the Azure platform infrastructure to the outside world.
The On-premises Application can be published to the external network, not through the company's own network infrastructure but through Azure infrastructure, connected with the on-premises network through the Application Proxy Connector service.

The Application Proxy Connector service is an on-premises deployed service, which enables application traffic to be published through Azure AD WAP.

In the general concept the Azure AD WAP performs here as a well-known reverse proxy service.

From the authentication services perspective Application Proxy service has one great capability. It can pre-authenticate users with Azure AD, and when the request is routed towards the On-premises Application proxy connector service, this service can request a Kerberos ticket on behalf of the user in the on-premises Active Directory.

Using Application Proxy service, we can enable Kerberos-based applications in our architecture with access to on-premises, using the hybrid identity model we have just built.
Our identity architecture is becoming more complete.
Predica, as with many other companies, is gathering a lot of data. This data is made available for our users through reporting services based on Microsoft SQL.

On a daily basis, our users work on Azure AD joined computers. Azure AD is also the main identity service used for application access. When deploying on-premises versions of SQL Server and Reporting Services, we had to face a challenge in how to handle user access and provide a seamless experience for users when accessing reports.

The solution we used was to publish the SQL Reporting Service through Azure AD Application Proxy. The Application proxy connector deployed on-premises is publishing our SQL Reporting Services web interface to the Internet.

When the user is accessing this website, it has to be authenticated with Azure AD. Given that, the application proxy connector exchanges user access token with the on-premises Kerberos ticket, enabling seamless access to the application.

To add a little twist to this architecture, we have to mention that we are not using an on-premises AD DS in this setup. Our entire infrastructure is based on the cloud service. SQL Server and reporting services are deployed on Azure Infrastructure as Service (IaaS) virtual machines and are part of the Azure AD Domain Services domain.

The Azure AD Domain Services is a service, which provides a subset of capabilities of the normal Active Directory, but based on the content of Azure Active Directory. Its main purpose is to provide authentication and authorization for infrastructure in Azure (lift and shift scenarios).

In our case, we have enabled this service to deploy on-premises software in Azure IaaS with our users being able to access it using their identity from Azure AD. It was possible because of Azure AD Application Proxy services capabilities to translate the Azure AD authentication token into an on-premises Kerberos ticket.
MIND BUSINESS PARTNERS AND CUSTOMERS
With the modern architecture of identity services, we can provide our users with easy access to applications and services. Proper design will allow us to build authentication services for users to access on-premises and SaaS applications in the easy and secure way with SSO provided.

To complete modern workplace requirements picture, we should also consider how our architecture can address two additional requirements:

- Provide easy to use way to collaborate between organizations (B2B)

- Allow our organization to maintain a relationship with our customers within services and applications (B2C).

Let's see how we can incorporate these scenarios in our architecture using capabilities provided by Identity as a Service platform.

**Business to Business collaboration**

Business to business (B2B) collaboration scenarios is becoming more common scenarios. Companies need to share not only information but access to applications.

In the past, using only on-premises solutions, this requires additional management overhead on managing trust relationship between directories or maintaining and managing additional user accounts for B2B users. This kind of approach also created ongoing security problem with controlling access of guest users to company resources.

This challenge is addressed by Identity as a Service solution like Azure AD built by Microsoft.

Azure AD as identity service is providing a dedicated scenario for collaboration between different entities using this identity service.

Azure AD B2B collaboration enables one organization to enable identities from another Azure AD tenant with access to applications handles within organization Active Directory tenant.
This collaboration is supported by dedicated service flow, where the company can invite selected individuals from another tenant to sign in to its tenant with access only to specified services and applications, like Office 365 or Dynamics CRM online.

In this scenario not only can a guest business user get access to the application in our organization, but the organization providing this access is in control of what and how a guest user can access. Guests obtain access only to assigned applications while organization sharing application is in control of security policies like enforcing multi-factor authentication when the application is being accessed.

**Business to Consumer collaboration**

Doing business with consumers requires maintaining a relationship with them. Managing consumer relationships in applications requires having a view on their identity and being able to express it in applications and services built by the company.

And still the need for managing consumer identity within business application comes up. It is a new area for most of the organizations. Consumer identity in the best case is handled with entries in organization databases and directories. It is gathered, processed and stored multiple times in dispersed repositories.
Modern needs are different. Consumers are using multiple digital identities, and they want to use those in relationship with businesses. Our identity architecture needs to address this and provide our consumers a way to use their identity, projected by one of their existing accounts into our company applications.

Our solution should allow this identity to be shared among all the applications we are building and delivering to our customers. It needs to support building a relationship with the customer.

It is what modern Identity as Service offerings promise. Multiple services enable the business organization to start no-time service, which will handle multiple social authentication providers and expose them to our services and applications.

IdaaS providers will handle social logins of the consumer, establish and maintain a directory of these identities and allow it to be used in our applications. At the same time they will handle all the security and management aspects of these interactions.

There are some existing identity services providing such capabilities – Microsoft Azure AD B2C, Auth0, Okta. Microsoft Azure AD B2C is an example of IdaaS service provided as part of Azure services which allows organizations to quickly build applications and services for consumers, and where all identity handling is done on the service provider side.
IT’S A WRAP
Modernizing security infrastructure, which authentication services are a part of, might seem like a mundane IT change. But it is so much more than that.

Business has become mobile and dynamic. Users are mobile, and organizations will have to start to provide services in a more dynamic way while maintaining relationships as part of business. These are relationships with employees, business partners, consumers. In the world of services and applications, this relationship is now defined by digital identity. Users identity is a new control plane which allows business to manage this relationship using devices, services, and applications.

Digital identity is free to roam between those elements and cannot be tied down to a single infrastructure element.

Delivering modern authentication infrastructure based on architecture patterns and solutions shown is allowing companies to build a foundation for future changes and transformation. From a business perspective it dynamically adjusts to changes in the requirements or situation.

It frees organizations to decide where and how they will locate and maintain services and applications, without worrying how to provide users access in a simple and secure way.

It simply works.

With Identity as a Service, companies can also externalize one of the most complex tasks – how to manage digital identity and provide authentication and access control in an easy and secure way within a hostile internet environment. Companies providing these services have resources and skills to constantly update their capabilities and deal with the complex tasks of providing security and protecting against threats.

That's why these services will be playing an increasingly important part in the changing business ecosystem where consumer relationships are the mainstay of success.

This white paper is intended to guide you through the process of understanding the definition of modern authentication infrastructure. It does not explain all technical details of implementation. These can be found in the product documentation. It also will depend on business requirements and current company infrastructure.

At Predica we believe in the value of digital identity as a business enabler and a key for building successful environments for modern organizations. It builds organizational advantage and provides the flexibility needed to win in a dynamic business world.
WHO IS PREDICA?
We are a group of highly skilled IT, business and MVP experts, ready to share the 30 years of combined experience in supporting IT Professionals and major corporations from around the world.

14 MICROSOFT AWARDS
Benefit from an excellent support from an award-winning Microsoft partner.

650 PROJECTS FINISHED
We’ve helped transform businesses while reducing their costs, increasing productivity and agility.

147 SATISFIED CLIENTS
We aim to deliver transitions that are equally painless for our clients, their employees AND the end-user.

5 AREAS OF EXPERTISE
We’ve developed a proven methodology and toolsets to accelerate deployment timelines.