Ping Identity

GLOBAL AUTHENTICATION AUTHORITY

The Foundation of a Zero Trust Architecture

WHITE PAPER

TABLE OF CONTENTS

03 INTRODUCTION

Understanding Zero Trust

04 THE GLOBAL AUTHENTICATION AUTHORITY

Localized Authentication vs. Global Authority

Additional Benefits of a Global Authentication Authority

07 CAPABILITIES OF A GLOBAL AUTHENTICATION AUTHORITY

Support for Multiple Authentication Methods & Policies

FIDO2: The Latest Defense Against Phishing Attacks

Single Sign-on (SSO) to All Applications

Identity and Attribute Handling

Authentication Orchestration

Identity and Session Token Issuance Use Cases

Inbound Federated Authentication Use Cases

Authorization Policies

Token Mediation

18 CONCLUSION

References

INTRODUCTION

As part of their digital transformation, many organizations have realized the need to revamp their existing identity systems. Whether those systems were built in house over time to meet tactical identity challenges, or commercial off the shelf solutions built for the on-premises era of workforce-only identity, current needs aren't being met in a strategic fashion. Legacy identity systems simply aren't able to keep up with needs for rapid integration, deployment flexibility and enterprise scale.

Today's enterprises maintain hybrid IT and multi-cloud infrastructures, and are in need of a strategic platform for managing digital identity for their employees, partners and customers. This platform must also support organizations who are starting to move from their existing security architecture to one that involves the principles of a Zero Trust ecosystem. As the notion of a network perimeter becomes a relic of the past, security leaders must adopt new security philosophies and methods. Zero Trust provides a framework to increase security in an increasingly open and connected world.

When it comes to establishing your Zero Trust foundation, the natural first step is implementing a global authentication authority. Regardless of where you are in your digital transformation journey, putting a centralized authentication authority in place will get your identity revamp on solid footing, increase your security posture and deliver tangible business value.

While there is no single prescriptive way to transition to an authentication authority, capabilities like directory synchronization and token mediation can provide a starting point while you bring the rest of your systems up to date. Read on to gain an understanding of the range of capabilities you can leverage, as well as the use cases they support and the issues they solve.

Understanding Zero Trust

The previous security approach of "trust, but verify" has lost its relevance and effectiveness. In light of digital transformation initiatives that rarely conform to a perimeter-based security model, many organizations are adopting the Zero Trust philosophy of "never trust and always verify."

Zero Trust (as originally defined by Forrester in 2013) assumes all network traffic—both internal and external—is not to be trusted. The book *Zero Trust Networks* reiterates that all network traffic should be assumed to be hostile. The authors' definition of Zero Trust further adds that every device, user and network flow must be authenticated and authorized, and policies must be dynamic and calculated from as many data sources as possible.1

To achieve this, you need to provide a consistent way for your customers, employees and partners to authenticate to their on-premises, cloud and SaaS resources. But this is easier said than done. Enabling this access requires accounting for multiple standards, custom app requirements and other complex authentication use cases. At the same time, you must give equal priority to user convenience and risk management.

Just like Rome wasn't built in a day, your Zero Trust adoption will also take well-orchestrated planning and implementation to achieve. And the logical place to start is by building a solid foundation.

BENEFITS OF A GLOBAL AUTHENTICATION AUTHORITY

Implementing a Zero Trust approach requires the ability to verify users, applications, devices and data flows. All access must be authenticated to ensure security. To make Zero Trust access possible, you need controls for intelligent authentication and authorization. A centralized, or global, authentication authority provides them.

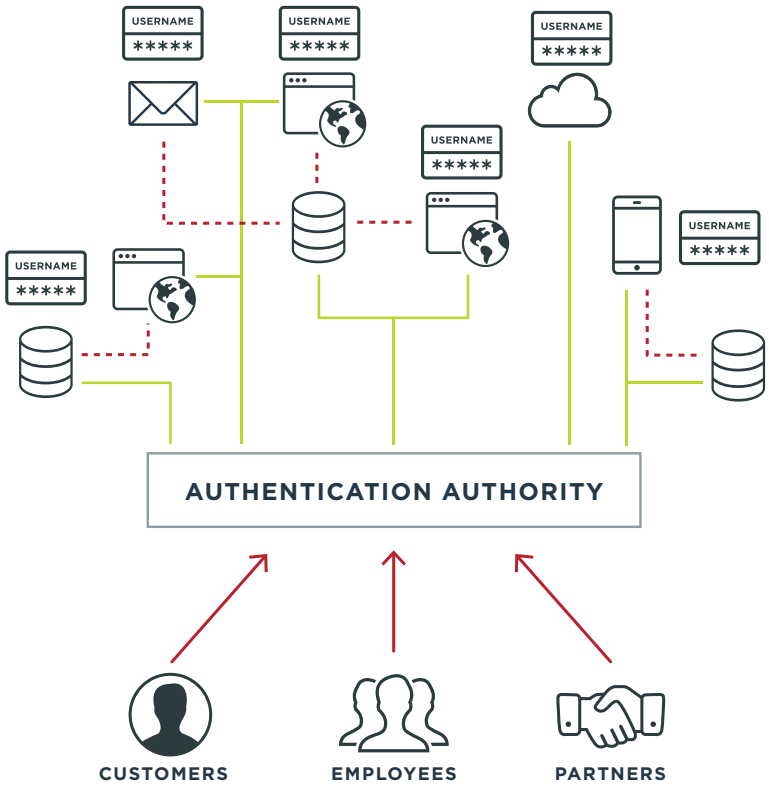

Figure 1: An authentication authority allows you to secure and control access to resources across all of your domains and platforms.

A global authentication authority allows you to secure and control access to resources across all of your domains and platforms, from public and private clouds to legacy on-premises environments. With support for all identity types, user populations, apps and environments, a global authentication authority gives you the ability to identify high-risk behaviors without unnecessary friction so you can strike the perfect balance between security and convenience.

Able to authenticate across a broad range of SaaS, on-prem and cloud resources, a global authentication authority orchestrates complex authentication flows to continuously provide identity, device and context data for identity validation. You're able to leverage attributes from multiple sources of data to establish and fulfill diverse policy requirements.

Localized Authentication vs. Global Authority

Localized Authentication	Global Authentication
Tightly Coupled Applications & Authentication When your applications and authentication are tightly coupled, you can't change authentication methods or authentication sources without having to update and re-release the application.	**Decoupled Applications & Authentication** The use of standard tokens to communicate identity, session and other needed information allows applications the freedom to use different authentication methods and sources without requiring application code changes.
Disjointed User Experience When each application must rely on its own authentication method, your users must authenticate independently to each application. Given that the average enterprise has about 130 apps deployed, this is frustrating at best. When each of those authentication methods is also unique, your users have an even more inconsistent and disjointed user experience.	**Consistent User Experience** Providing a central authentication service means users have the same authentication experience across all of your applications. You can also extend your authentication authority to partners and other third-party applications.
Greater Risk of Breach & Outages As your applications grow in number and move beyond the corporate data center, the number of authentication providers and data stores starts to proliferate. These systems and stores all have varying degrees of resiliency, compliance and security, leading to difficulty assessing and maintaining your overall availability, security and compliance posture.	**Increased Availability & Security** Global authentication authorities are designed for scale, resilience and security. Having a properly implemented authentication authority means that as your applications extend to new cloud environments and technologies you can remain confident in the availability and security of your authentication process, and that you comply with relevant regulations and directives.
Separate & Siloed Data Stores As more applications move to the cloud, you're likely accumulating separate and siloed stores of user information for each application, leaving you with an inability to share data across applications. These stores often fall short of addressing increased security risks, compliance requirements and performance needs.	**Consolidated Identity Stores** All identities can be consolidated into the global authentication authority, providing a single source of truth that can be leveraged by both current and future applications whether on premises or in the cloud. The consolidated underlying store also simplifies assessing and ensuring compliance with data residency and data locality requirements.

Additional Benefits of a Global Authentication Authority

Once you move beyond the limitations of localized authentication to a centralized and global authentication authority, you're also able to:

- **Enable Single Sign-on (SSO) for Application Access:** Using standard tokens to communicate identity, session and other information means that users only need to authenticate once and allows multiple applications to use the same information. You're able to provide convenient SSO to standards-based apps, mobile and SaaS apps, and APIs, regardless of identity provider (IdP) or service provider (SP).

- **Centralize Access to SaaS Applications:** The ability of an authentication authority to issue standard tokens and federate to relying parties means it can allow users to access both third party and enterprise SaaS applications regardless of where the applications are located.

- **Create Flexible & Reusable Authentication Policies:** Applications often have different authentication needs that fall into well-defined categories. Having the authentication activity performed by a central authority allows these authentication policies to be re-used by applications with similar needs, accelerating release cycles.

- **Integrate Partner & Social Identities:** In addition to locally stored identities, an authentication authority can accept identities from both partner and social identity sites using standard identity tokens. This allows seamless onboarding of partner and social identities without requiring users to re-register.

CAPABILITIES OF A GLOBAL AUTHENTICATION AUTHORITY

When determining where to get started on your Zero Trust journey, strong identification and authentication is the logical place to start. Ensuring that all access is authenticated access is the bedrock of Zero Trust. By deploying global, adaptive authentication, you're able to use this capability as the central policy and administration authority for risk signals and policy decisions.

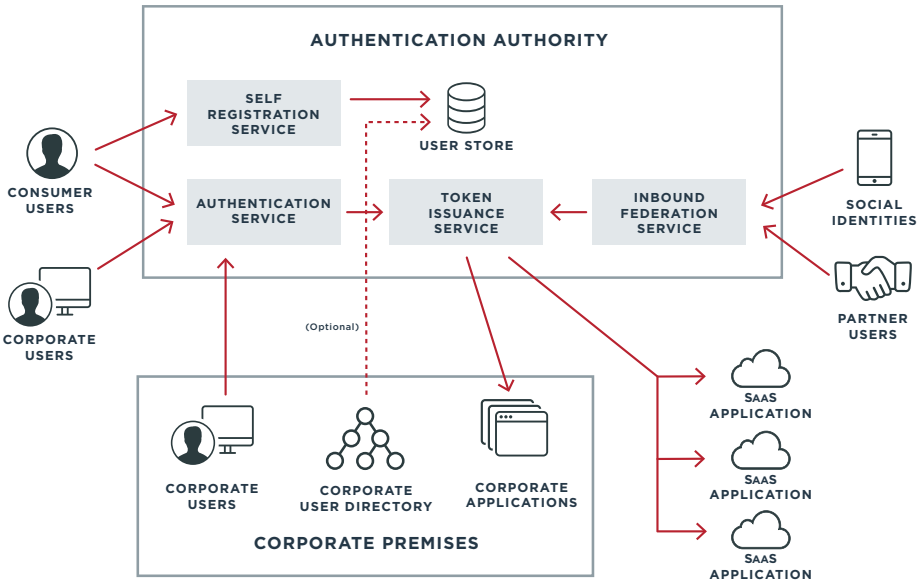

Figure 2: A global authentication authority allows you to secure and control access to resources across all of your domains and platforms, with support for all identity types, user populations, apps and environments.

Support for Multiple Authentication Methods & Policies

Among the many advantages of an authentication authority is its ability to support a host of local authentication methods and policies, including basic authentication, multi-factor authentication (MFA) and adaptive authentication.

Basic Authentication

Basic authentication relies on the traditional username and password combination. It provides a security barrier between users and resources, but this barrier has become increasingly fragile. While familiar to users, basic authentication suffers from significant weaknesses, including its vulnerability to credential stuffing and phishing attacks.

Credential stuffing entails using automated bots to play lists of stolen usernames and passwords against your login form. Authentication authorities have gotten better at developing built-in defenses against these attacks. But the botnet authors have simultaneously done an impressive job of keeping up, resulting in a seemingly never-ending tug-of-war between the attackers and the authentication authority providers.

Basic authentication is also highly susceptible to phishing attacks. Attackers have figured out how to leverage easy-to-use attack proxies such as Modlishka to create very convincing phishing sites and dupe users into thinking they're logging into a legitimate resource.

Multi-factor Authentication (MFA)

To overcome these vulnerabilities and prevent account takeover, basic authentication can and should be paired with additional authentication factors. This is known as multi-factor authentication. Adopting MFA allows you to require those additional factors and, as such, is one of the simplest ways to strengthen your enterprise security.

Some common forms of additional authentication include SMS, OTP, out-of-band push notification, biometrics and physical tokens. But while these factors improve overall security, they are not equally effective at preventing phishing attacks. SMS usage has been deprecated by NIST because of the ability of attackers to hijack phone numbers via a variety of methods. Further, If a user believes they are logging into a legitimate website, they have no reason not to also enter OTP codes into the phishing site, respond to push notifications, use the fingerprint scanner, etc.

What's needed is an additional security layer above the authentication layer that can determine whether the authentication request is or isn't coming from a legitimate website, and a standard called FIDO2 provides it.

FIDO2: The Latest Defense Against Phishing Attacks

FIDO2, an open authentication standard developed through a joint effort between the FIDO Alliance and the World Wide Web Consortium, is the overarching term for FIDO Alliance's newest set of specifications. FIDO2, or simply FIDO, provides even more protection against phishing attacks by combining the capabilities of WebAuthn and CTAP to determine if an authentication request is coming from a legitimate website vs an imposter phishing site.

WebAuthn is the protocol that browser-based applications use to invoke authentication via either CTAP or platform-based authenticators. It's supported by stable releases of Chrome, Firefox and Edge, and is available as an experimental feature in the desktop Safari technology preview release.

> FIDO2 reflects the industry's answer to the global password problem and addresses all of the issues of traditional authentication.[2]

CTAP, which stands for client to authenticator protocol, allows a user-controlled roaming authenticator to interoperate with a client platform, such as the WebAuthn enabled browsers. The authenticators communicate with the platform via one of three methods: BLE, NFC or USB.

The FIDO2 combination is particularly resistant to phishing because of mutual registration. You must register the authenticator with each application domain you want to use it for. The application domain is registered with the authenticator after the user confirms the registration. Then the authenticator creates a public/private key pair and sends the public key back in the registration response so that the application can know that it's really the authenticator that's responding to the authentication request it issues.

During subsequent authentication requests, the registered domain is checked against the domain that the authentication request is coming from. If that domain does not match the registered domain, the authentication request will fail. The failed request raises a red flag, signaling to the user that they may be attempting to login to a phishing site.

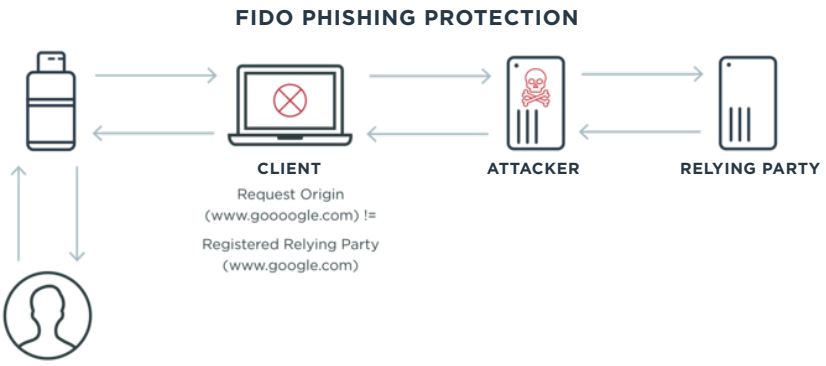

Figure 3: FIDO2, the latest version of the FIDO standard, ensures authentication requests originate from the domain where the authenticator was registered, preventing attackers from using phishing sites like www.goooogle.com.

Adaptive Authentication

Taking MFA a step further, adaptive authentication both improves security and minimizes user friction. By relying on a variety of contextual factors, adaptive authentication is able to establish a greater level of assurance that a user is who they claim to be. These factors might include IP address, geolocation, device fingerprint, time of day and similar contextual variables.

Adaptive authentication can analyze the user, device and requested resource in tandem to evaluate the risk profile of the request and adapt the authentication requirements accordingly. For example, if the risk is deemed to be low, no additional authentication is needed. But if the risk appears high, additional authentication factors will be required. When the user last authenticated, the health of their device and the reputation of their IP address can all be used to determine if a user should be granted access to a resource, denied access or prompted to provide additional proof of their identity.

Machine learning can also be used to build a model of what constitutes "normal" behavior for a given user. If a user performs a suspicious operation such as accessing a brand-new application or requesting access to a resource from an unfamiliar geolocation, the adaptive authentication system can recognize this anomalous behavior and require additional authentication factors to provide a greater level of assurance in the user.

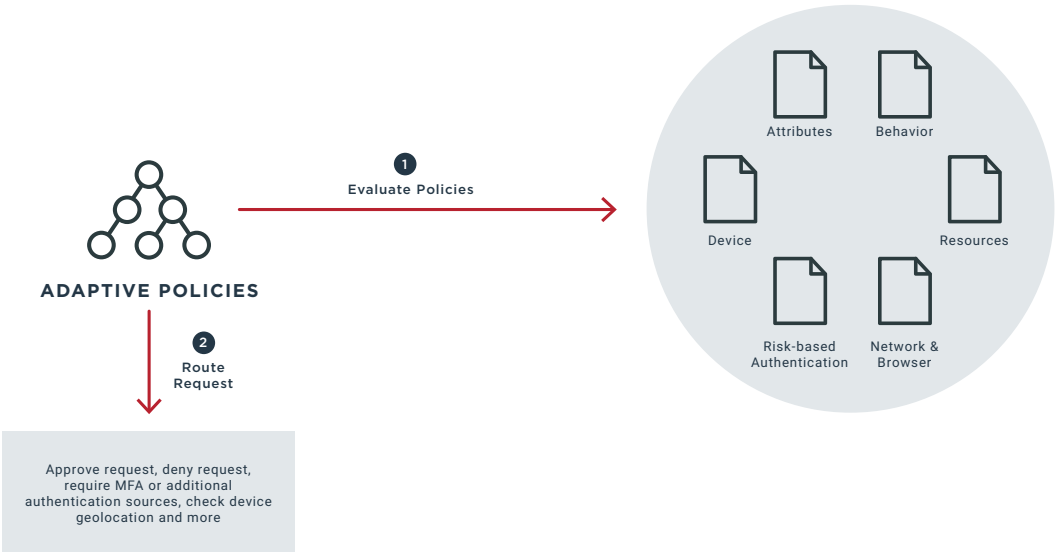

Figure 4: Adaptive authentication evaluates policies to determine if additional factors are needed to access resources.

Conversely, if the adaptive authentication system has high confidence in the user's identity based on the repetitive and consistent nature of the access request, it may require fewer factors over time. For example, a user may initially be prompted for a second factor each time they request access to applications.

But if that same user routinely accesses the same applications and from the same computer at the same time of day, they may be required to enter a second factor less frequently, until ultimately they're prompted for an additional factor only one time per month. The subsequent reduction in friction makes for a better user experience and often translates to improved satisfaction and productivity.

Authentication Policies

Authentication policies control both the flow the user sees when authenticating, as well as the factors that will be required during the authentication flow. Specific authentication policies are typically assigned by administrators based on the application being accessed. Applications with low security requirements may allow authentication via social identity providers or simple username and password. Applications with greater security requirements may require MFA, or request that remote identity providers perform specific user authentication before allowing federated access to the application.

Administrators may also be able to configure additional authentication policies based on the manner in which authentication is being requested. For example, when using OAuth or OpenID Connect, administrators may assign authentication policies based on the client ID of the application requesting an authentication.

Single Sign-on (SSO) to All Applications

A global authentication authority allows you to provide convenient SSO to your users. As the name suggests, single sign-on allows a user to authenticate once and gain access to all available resources. Remember that with Zero Trust there is no inside or outside, and the default is to never trust. If you don't provide SSO, your users need to re-authenticate to every application they want to access, which hurts productivity and usability.

In the context of an authentication authority, there are numerous SSO use cases. These use cases fall into two main categories: SSO to standards-based systems and SSO to proprietary systems.

1. **SSO to standards-based systems.**

   The development of open, interoperable standards for providing single sign-on between enterprises, and between enterprise to cloud, has been one of the most transformative technologies in the last 15 years. Both service consumers and service providers can now leverage these standards to easily send and receive identity and attributes without having to learn, implement and test proprietary protocols, or having to simulate SSO by storing usernames and passwords and screen scraping to emulate human input. We have attempted to cover the majority of scenarios and business benefit when sending and receiving these standard tokens in the sections below.

2. **SSO to proprietary systems.**

   While in an ideal world every application and service would accept standard identity tokens, that is unfortunately not the world we currently live in. While most of the large service providers support standards, many of the smaller ones do not. As of 2019, Gartner says that only 30% of application providers support modern identity protocols like SAML, OAuth2 and OIDC over proprietary approaches. By 2022, that number is expected to grow to just 60%.[3]

Given that reality, the ability of an authentication authority to support SSO via custom connectors to proprietary applications that are important to your business should be a factor in your selection process.

Identity and Attribute Handling

Many organizations have multiple user directories or identity stores because of mergers and acquisitions, or have pools of identities that were seen as "different" than the regular identities.

An authentication authority should be able to connect to a variety of identity sources and user directories when authenticating a user. These directories could be LDAP, RDBMS or other formats.

If the authentication authority is part of a larger IDaaS or CIAM offering, it may provide the ability to onboard and store identities and their attributes locally.

Once a user is authenticated, you will typically want to add additional attributes or user claims to their identity or federation token. The authentication authority should allow you to leverage multiple directory or other data sources for this information.

Authentication Orchestration

A term that people investigating authentication authorities may have recently become familiar with is Authentication Orchestration.

The term can be a bit confusing, as there is no firm dividing line for when flexible authentication policies turn into actual authentication orchestration. However here are some key capabilities and benefits that authentication orchestration provides. Understanding these and deciding which ones are important to you will help in your choice of authentication authority solutions.

Workflow Enablement

Authentication orchestration allows you to easily build conditionally executed flows involving one or more authentication policies in the sequence of your choosing. This chaining of policies allow you to build simple, single-responsibility policies, then bundle them together to create more complex scenarios. The creation of workflows and policies may be either UI based or may involve writing in a policy language depending on the capabilities of the authentication authority and the degree of control needed over the workflows and policies.

Data Driven Dynamic Policies

These policies are not statically defined and always performing the same actions. They base their actions on data gathered from both the authentication process as well as third parties. This flexibility allows these policies to cover a wide range of scenarios and integrate well into existing corporate environments.

Conditional Sources of Authentication Factors

Allows users the choice between different logically equivalent authentication factors based on the capabilities of their authentication device, while still leveraging the same authentication policy. This choice can be automatically driven by the policy choosing a "preferred" device from the available set, driven by a user-controlled authentication selector, or other methods.

Inclusion of Multiple Attribute Providers or Claim Sources

While in most cases you want to have a single source of truth for an identity and the claims or entitlements associated with it, sometimes this is not possible. A flexible authentication authority will allow you to gather the needed information from multiple sources at authentication time. Gathering this information at login time can prevent multiple applications from having to reach out at runtime to the information sources, decreasing overhead and increasing scalability.

Flexible Inclusion of External Trust or Risk Factors

No matter how much functionality your authentication authority provides, there will always be something new or novel that you would really like to integrate into your authentication workflows and policies. It's also pretty much a given that the outputs from these external providers will vary widely. Whether it's a risk or reputation score, a vector of trust, or an arbitrary set of claims data should not matter.

Identity and Session Token Issuance Use Cases

After an authentication authority successfully authenticates a user, it communicates this fact to other applications by issuing identity and/or session tokens. Identity tokens are typically standards-based such as SAML or JWT. Third parties will generally define their own sessions after receiving these tokens. For internal use, the tokens may have enough information to be used to control user sessions, or a separate token may be issued.

Workforce SAML Federation to External SaaS providers

Allowing employees to access external SaaS applications such as SalesForce, Github, Concur, Workday and ADP is probably the most common use for an authentication authority. The remote application is typically web based and accessed through a user's browser. In this scenario the authentication authority will generally create a SAML token. These tokens are signed and optionally encrypted and contain attributes identifying the user, the intended recipient and any other attributes needed by the remote application for authorization or personalization.

The authentication and token issuance can either be **SP Initiated,** or **IDP Initiated.** SP or service provider-initiated SSO is kicked off by a user visiting a SaaS application without having a session there. In this case the SP will either determine the authentication authority associated with the user from the resource being accessed, or will ask the user for their email address or for some other information that can determine their authentication authority. The user is then redirected to the authentication authority as part of an authentication request.

The authentication authority, acting in the role of IDP (identity provider) will authenticate the user with the relevant authentication policy, determine if the user meets any applicable authorization policies and then, if successful, will generate a SAML identifying the user. Finally, the user is redirected back to the service provider along with the SAML token. After validating the SAML token and checking its own authorization policies, the SP will then let the user into the requested application.

Workforce SAML Federation to Enterprise Applications

Often times within corporations, there are separate pools of applications and identities that cannot be combined. Typically this is after mergers and acquisitions, but can also occur when local-use-only applications need to be made available to a wider geographic audience.

In these cases it may make more sense to set up federations between the divisions containing users that want to access the applications and the applications themselves. This is no different techncially than the federation to SaaS providers and is often easier given that both sides reside in the same organizational structure.

OpenID Connect Support to SaaS Providers

While the majority of SSO to SaaS applications is done via SAML, more and more applications such as SalesForce are supporting the newer OpenID Connect standard. With OpenID Connect, applications that want to obtain an identity token register as clients with the authentication authority. The two parties are the authorization server (AS) and the relying party (RP), which correspond to the SAML identity provider and service provider respectively.

OpenID Connect does not support the concept of IDP-initiated SSO so all authentication flows start with the relying party. A user visits the RP without credentials and then is redirected to the authentication authority which is acting as the OpenID Connect authorization server or AS. The user authenticates and is then redirected back to the RP with what is known as an authorization code, which is a temporary token. The RP then calls a token endpoint on the AS, authenticates itself and presents the authorization code to the AS. The AS then returns an ID token identifying the user.

Once the client SaaS application has the identity token, it can create a session for the user and the user can do whatever they need to. A nice security benefit of this flow is that the client application never actually sees the users credentials and the identity token was never in URLs, which are often logged and can present a potential vulnerability for long-lived tokens.

OpenID Connect or SAML Support for Mobile Application Access to SaaS or Other External Resources

In addition to providing web-based applications, many SaaS providers also provide mobile applications for their users so they can work with the SaaS provider from anywhere. An authentication authority can provide enterprise and consumer users of these applications an authentication experience similar to what they see for web applications, including self-registration, single sign on, forgotten password support and more. The SaaS provider can use the same authentication mechanisms and authentication authorities they use for web-based users.

Most mobile applications either embed browser toolkits or call out to system-supplied browsers so that users can interact with web pages. As such these applications can support using either SAML or OpenID Connect from the authentication authority, although OpenID Connect is more common. For use of OpenID connect the only difference would be that the client application would be the mobile application vs. a web application.

Some mobile applications may be native applications, which do not use or embed HTML browsers into themselves. Since these applications cannot redirect users to the authentication authority, they need to collect a user's credentials—such as username and password—and submit them directly to the authorization server.

This direct submission is permitted by OpenID Connect via the Resource Owner Password Credentials grant type. It is generally used as a last resort only since the client application could reuse or leak the credentials and, if this happens, the authentication authority has no way of knowing whether the user has initiated this authentication or not.

OpenID Connect and OAuth support for Enterprise Application Access

As most people know, OpenID Connect is built on top of OAuth. The important distinction is that OpenID Connect is an authentication protocol, while OAuth is an authorization protocol.

An OpenID Connect ID token identifies a user, but does not determine whether a user is allowed to access a given application or resource. Conversely an OAuth access token has specific scopes associated with it that applications and API gateways can check to determine

if access is allowed. However, the access token generally does not contain any information as to who the user is. That information is communicated by another mechanism such as a Kerberos ticket, a web access management session cookie or is associated with the access token and read via an application lookup.

In a typical use case, the application itself requests both an identity and access token for a user from an authentication authority and then passes on the access token to APIs that it needs to call on behalf of the user to get or set information related to the application or user.

Session Token Issuance and Pairing with Access Control System

The authentication authority may issue itself an internal session token for the purpose of single sign-on. If this token has been issued the user will not be challenged for subsequent authentication requests within the lifetime of the token unless the relying party specifically requests a fresh authentication or the sessions level of authentication is not sufficient to meet any requirements specified by the relying party.

If the authentication authority is paired with an access control system, such as the combination of PingFederate and PingAccess, the session token may also be used to access applications within the domain of the enterprise and can be scoped to individual applications to limit the potential impact of a token hijacking attack. Additionally, the authentication authority and access control systems can standardize the parameters for session creation, lifetime and timeouts for resources in both systems.

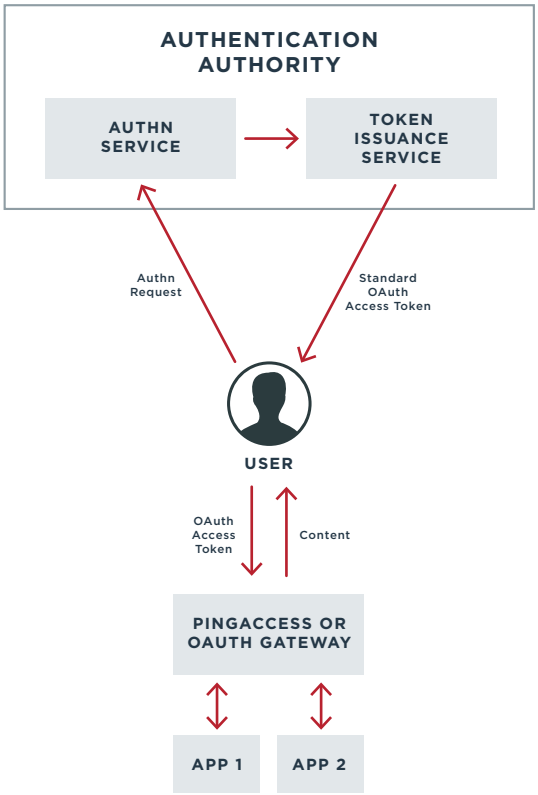

Figure 5: An authentication authority can be paired with an access control system.

Inbound Federated Authentication Use Cases

In addition to issuing standard identity and session tokens, the authentication authority can be configured to accept them as well. This is a key capability of an authentication authority as it allows the acceptance of partner and third-party identities without those identities having to be explicitly added to the local identity store.

Once the authentication authority has received and validated the token it will issue its own tokens for the user. This allows enterprises to easily grant partner access to both enterprise applications and multi-tenant applications that need to be accessed under the context of the enterprise running the authentication authority.

Federated Business Partner or Business Customer Access to Enterprise Applications

Partners can be supported in a variety of ways. The enterprise that owns the applications can stand up a catalog of applications available to partners. Many authentication authorities provide tools that make it easy to set up these catalogs.

The authentication authority can also allow partner users to directly link to applications by supporting SP-initiated SSO. A persistent cookie that points to the partner site can be placed in the user's browser after a user initially federates into the authentication authority from their home IDP. After this, or other means of IDP discovery when the user attempts to access a target application, the authentication authority will know what partner site the user originates from and where to get them authenticated.

Federated Workforce Access to Enterprise Applications after Merger or Acquisition

User repositories and application domains often stay separated for a significant period of time after mergers and acquisitions. In these scenarios, federation may be the best solution to provide employees of different business units with access to enterprise-wide applications via SSO. Logically, the configuration—including the need for IDP discovery—is very similar to the partner use case, with the only real difference being the span of applications employees can access.

Social Identity Access to Enterprise Applications

For a number of applications the enterprise may want to provide access via social identities like Google or Facebook as well as other local or federated identities. Authentication authorities can easily support giving users a list of supported social identity logins as well as providing a local authentication option.

Federated Partner Access to Third-party SaaS Applications

From an authentication authority perspective, allowing partner users to access third-party SaaS applications is the same as allowing them to access enterprise applications. The complication can occur when partner users try to directly access SaaS application resources without going through either their company's portal or the partner portal associated with the authentication authority.

Some SaaS providers associate tenant tags with resources and applications or issue their own IDP discovery cookies, allowing them to determine which enterprise account to associate with the request. Those who do not have these mechanisms may require user interaction to determine what enterprise to associate the user with, and by extension, what authentication authority to redirect them to.

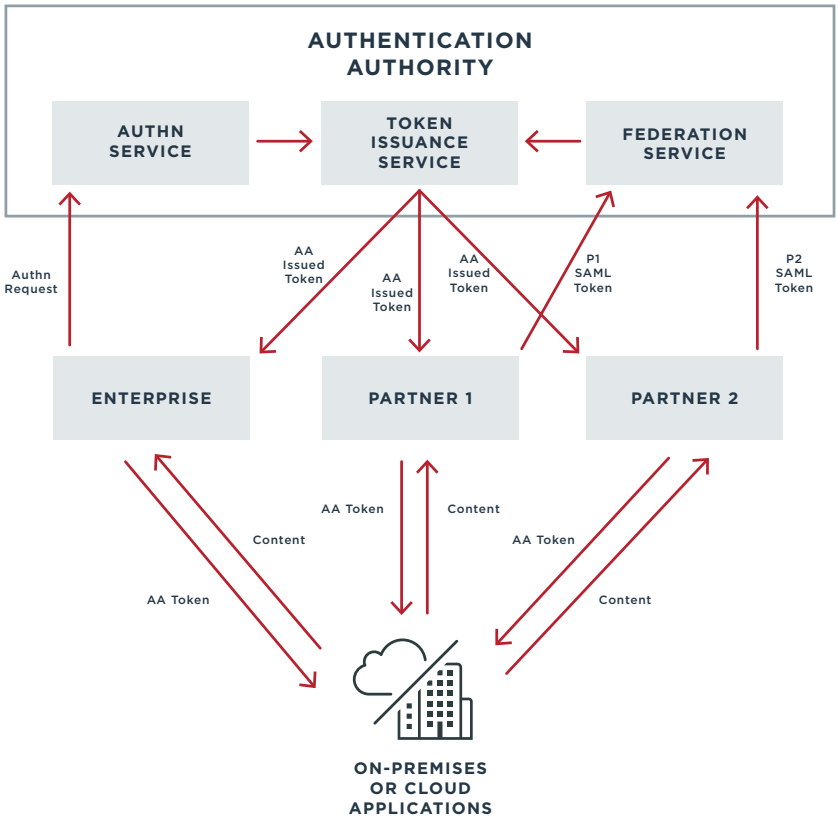

Figure 6: An authentication authority can orchestrate both workforce and partner access to applications.

Authorization Policies

Authentication authorities may also allow the creation and use of authorization policies in certain scenarios. Typically, this is done when generating SSO access tokens for specific applications. In these scenarios, a user's group membership or other entitlements can be checked before the authentication authority issues a SAML token or an OAuth access token with a requested scope.

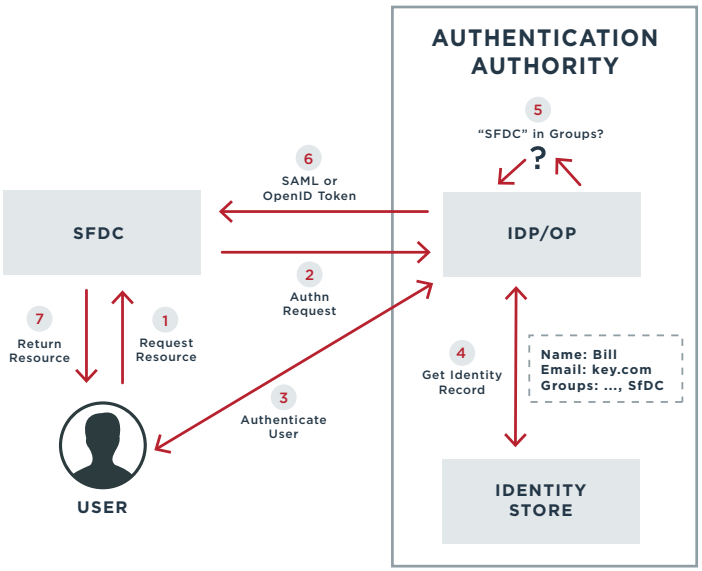

Figure 7: An authentication authority may allow the creation and use of authorization policies.

Token Mediation

When an existing token-based access control system is in use, fully retrofitting that mechanism to accept standards-based tokens may not be feasible in the early stages of moving to a centralized authentication authority.

As shown in the diagram below, token mediation allows an authentication authority to exchange a standards-based token for a proprietary security token used by a third-party web access management (WAM) system. The access request is transparent to the user, allowing PingAccess to transparently manage access to systems using those WAM tokens. The request is also transparent to the protected application, which handles the access request as if it came from the user directly. Once token mediation has occurred, the token used for accessing the application is cached for continued use during the session.

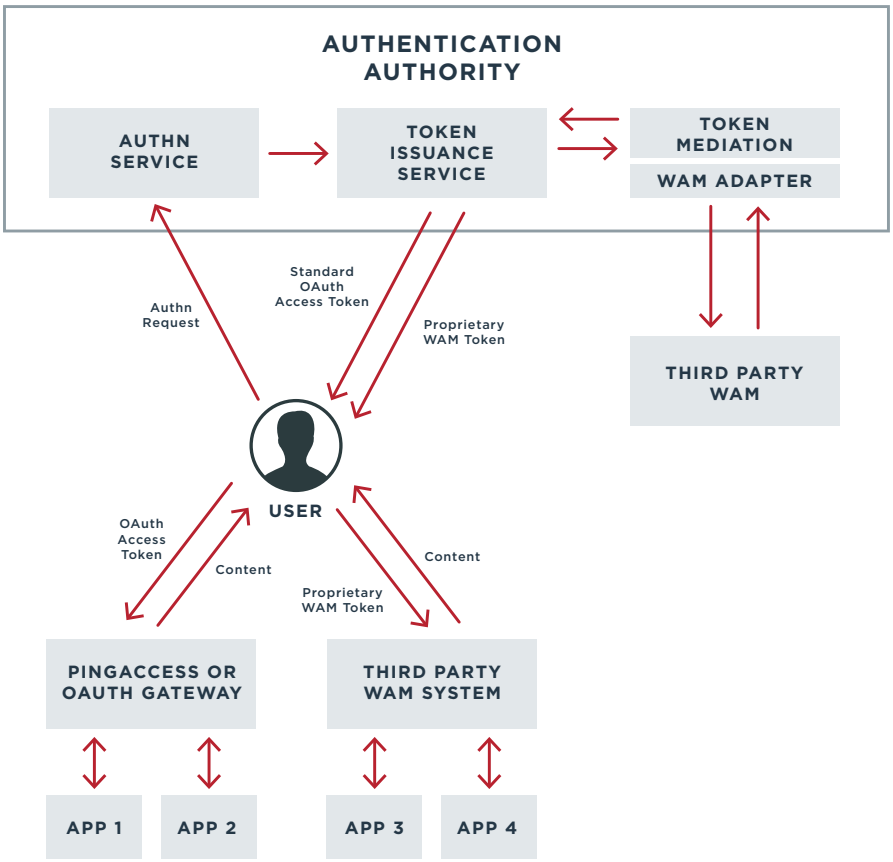

Figure 8: Token mediation allows an authentication authority to exchange a standards-based token for a proprietary security token used by a third-party WAM system.

Another use case for token mediation is at the edge of a domain. An opaque access token can be swapped for a signed JWT token, which will then be presented to downstream microservices. This internal only token allows the services to determine access rights and entitlements directly from the token, without the performance overhead of having to query the issuing authority directly.

CONCLUSION

A globally trusted single source of identity can bring tremendous value to an organization and put you on the path to Zero Trust.

When you can configure combinations of local and remote identities, as well as leverage flexible authentication and authorization policies, you gain the ultimate in flexibility. You're able to manage your employee, partner and customer identities as best suits your needs.

With the ability to accept, issue and transform a variety of standard and proprietary tokens, you can also securely give your users access to on-premises, cloud-based and third-party applications, all while minimizing friction.

To learn more about Ping's global authentication offerings, please visit www.pingidentity.com.

References

[1] Barth, Doug and Evan Gilman. 2017. Zero Trust Networks. O'Reilly Media, Inc.

[2] The FIDO Alliance. "Moving the World Beyond Passwords." Accessed July 5, 2019. https://fidoalliance.org/fido2/.

[3] Kelly, Michael, Abhyuday Data and Henrique Teixeira. Magic Quadrant for Access Management. Gartner. Aug 12, 2019.