Customer Authentication Authority

The Foundation of Consistent Digital Experiences

WHITE PAPER

TABLE OF CONTENTS

INTRODUCTION

When customers embark on a user journey with your brand, the registration process is often their first impression—or at least a very early one. If that process is cumbersome, users will abandon it and you'll likely never get the chance to turn them into a customer. The sign-on process is also critical to get right. If customers are forced to remember several different passwords for one company—a different one for each digital property they interact with—they'll abandon you. Fewer customer sign-ons mean less frequent customer activity, smaller wallet share and decreased revenue.

While streamlining these processes may seem like a simple goal within a broader digital transformation initiative, complexities can quickly arise. For instance, your applications may have been developed by different teams and have varying sources of data about customers, including customer sign-on credentials. Or, only a patchwork of applications may be based on secure identity standards.

In addition, some enterprises have centralized customer identity systems that were built in house over time to meet tactical identity challenges, or are commercial off-the-shelf solutions designed for the on-premises era of workforce-only identity. In most cases, these legacy identity systems simply aren't equipped to deliver the extraordinary digital experiences required to make a good first impression on your customers and to help you stay competitive. They may lack standards support, needed security features or even simple capabilities like social login. They might not be able to handle peak sign-on demand after product launches and end up costing you millions in lost opportunities when customers try to sign up and receive a "sorry, something went wrong" error.

> **67% of customers say their standards for good experiences are higher than they've ever been.[1]**
>
> **-SALESFORCE**

Customer identity and access management (CIAM) has evolved to meet today's identity intricacies. Enterprises recognize the need for a strategic platform for managing digital identity for millions of customers, not just their workforce and partner identities. Modern customer identity platforms offer options for how you deploy to the cloud: IDaaS, hosted private clouds, private clouds, on-premises or hybrid. They consider the plethora of devices, customer use cases and rich profile data required to deliver seamless experiences. Of course, they should also help protect that valuable customer data from breach, fraud or privacy violations. Trying to address these scenarios with legacy solutions built for employees is a recipe for failure.

When it comes to smoothing out the beginning of your user journey and streamlining sign-on and registration processes consistently across all digital channels, one of the most important functions a modern customer identity solution has is serving as an authentication authority. An authentication authority enables you to give your customers consistent sign-on and registration experiences on any app, regardless of whether that app is custom or standards-based.

CIAM authentication authorities enable features that deliver extraordinary customer experiences such as social login, social registration, user-friendly multi-factor authentication (MFA), passwordless authentication and more. They are able to deliver these capabilities no matter the use cases, diverse digital properties, and performance and scalability SLAs required by the enterprise. Read on to gain an understanding of the range of capabilities you can leverage, as well as the use cases CIAM authentication authorities support and the issues they solve.

1 "State of the Connected Customer," Salesforce, accessed July 7, 2020, https://www.salesforce.com/form/pdf/state-of-the-connected-customer-2nd-edition/

WHAT IS A CUSTOMER AUTHENTICATION AUTHORITY?

A customer authentication authority is a centralized service provided by customer identity and access management (CIAM) platforms. The goal of the authentication authority is to provide customers with consistent sign-on and registration experiences across all applications. For enterprises that have numerous customer-facing applications, a customer authentication authority is a specialized solution that can simplify the often-complex and disjointed architectures within enterprise application portfolios.

Below are examples of some of the complexities enterprises may face, and the approach a customer authentication authority takes to solving them.

Application Silos

Large enterprises tend to have several—often dozens or more—customer-facing applications. These applications might have come into existence via mergers and acquisitions, disparate app teams or one-off initiatives. Often they have different methods of registering and authenticating users. Some may be connected to a legacy IAM system owned by IT. Others may have their own home-built, simple login and registration process. Still others may fall under various identity solutions. As a result, these applications can vary in their support for standards and capabilities.

A customer authentication authority has the ability to direct authentication for any application. It supports common customer identity standards such as OAuth, OpenID Connect and SAML, and can even connect with custom apps that don't support standards at all. It provides a one-stop shop for authentication across your enterprise, ensuring that customers have consistent capabilities, consistent security and consistent credentials, no matter which application they are trying to access.

Diverse Use Case Requirements

With such a diverse set of applications, many combinations of use cases may be required to achieve consistent single sign-on (SSO). A brand might have a popular digital property that they wish to use as an identity provider (IdP) for all other digital properties. An authentication authority can ensure that a centralized session created when a user signs on that popular app will work to access all other applications that are acting as service providers (SPs).

An authentication authority can direct users to the appropriate place to sign on, no matter where a customer enters their digital application ecosystem. If a customer first lands on an SP app, the authentication authority will redirect them to the appropriate IdP to authenticate—that's SP-initiated single sign-on. Or, links within the popular identity provider app may direct users to the appropriate service provider application—that's IdP-initiated single sign-on.

A common IdP-initiated use case can be found in online banking. After signing on to a banking web app, you often have links for services such as bill pay, loyalty points, stock trading, transfers and more. These options are often other applications. If the banking

web app acts as the IdP when you sign on, then the other sections of the site (separate apps) are able to recognize that session. This example exemplifies just how invisible these processes should be to the end user, because a customer should never know that all those links at the top of their banking website are separate applications.

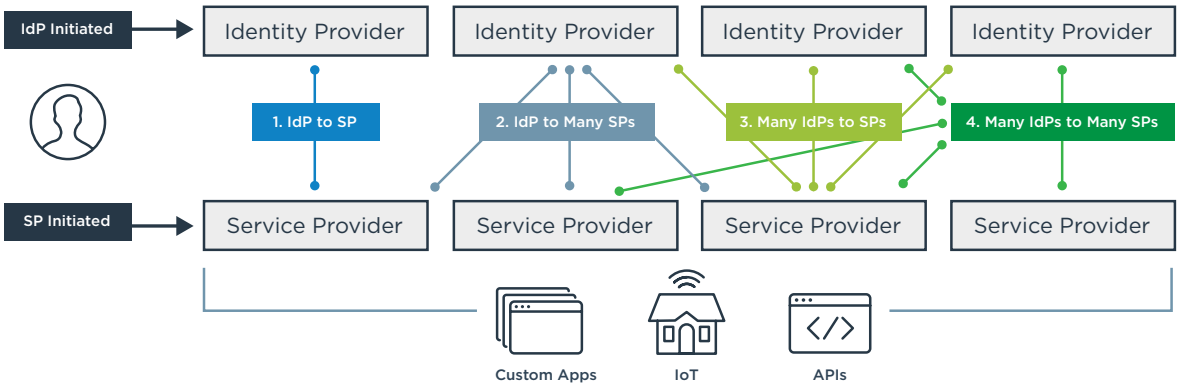
Many enterprises may have even more complex setups than the ones described above, such as:

- multiple sign-on options for customers
- social login or passwordless for some apps but not others
- an IdP serving as an authentication source for one SP or many SPs
- multiple IdPs, each connected to different sets of SPs
- IoT devices or APIs (as well as users) authenticating

To handle such use case diversity, an authentication authority often has to change its role from IdP to SP as necessary to receive, translate and pass along tokens and assertions. For example, say a user visits the URL for a service provider app. That app sends them to the authentication authority, which directs them to a SAML IdP to authenticate.

The authentication authority is acting as a service provider as it receives a SAML assertion from the IdP. It may need to translate that SAML assertion to an OpenID Connect ID token so the target app can understand it. After it does that, it changes its role to an IdP and the target app becomes the SP as it passes along the translated OpenID Connect ID token.

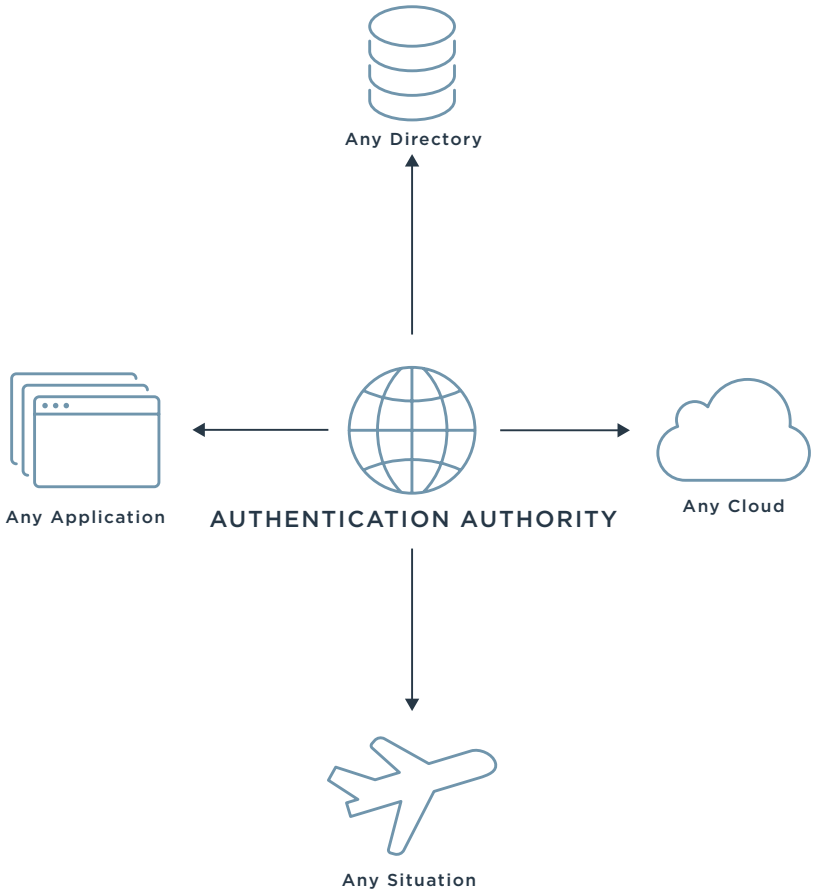
No matter the use case complexity, an authentication authority can act as a central operator to direct authentications across all of your digital properties.



Cloud Optionality

The diversity of enterprise application portfolios may span various private clouds, SaaS and on-premises environments. In some cases, customers may prefer the simplicity of a hosted, multi-tenant identity-as-a-service (IDaaS) solution. For some apps, enterprises will want control over their own up-time, security and user data. In those situations, managing identity in their own private cloud might be the best solution. If an enterprise prefers the control of a private cloud, but doesn't want to manage the environment, a hosted, single-tenant private cloud might be the way to go.

There is no one-size-fits-all solution. That's why it's critical that modern authentication authorities give customers multiple cloud deployment options. Whether they want IDaaS, on-premises, private cloud, hosted private cloud or a combination of those, an authentication authority should be able to cohesively direct sign-ons across all environments.



BENEFITS OF A CUSTOMER AUTHENTICATION AUTHORITY

The benefits of a customer authentication authority can be split into a few broad categories: benefits to customers, benefits to IT and identity administrators, and benefits to application teams and business units.

Benefits to Customers

Customer demands of a brand are simple. Customers expect enterprises to deliver delightful experiences and protect their data. An authentication authority helps to check both of these boxes in the context of registration and login.

Authentication Consistency	Authentication authorities ensure that customer credentials, registration requirements such as password policies, account recovery and other authentication experiences are consistent, no matter which digital property they are trying to access.
Protect Customer Data	Though customers may not always notice when security is present, they will notice if lack of security causes a breach, or if the security processes during sign-on or registration add too much friction. An authentication authority ensures a consistent balance of security and convenience across all apps that reduces the risk of breach.
Pixel-perfect Authentication Design	Brands put a lot into pixel-perfect applications and web properties. The same level of care should go into authentication and registration UIs. An authentication authority ensures pixel-perfect and consistent registration and sign-on interfaces across all apps.
Authentication Options	Customers may prefer different ways to sign on or register—using a form, with social media providers, with other IdPs, without passwords, etc. An authentication authority ensures that options you choose to offer customers are consistent across all channels.
Fraud Protection	Hackers don't target only enterprises, they also target customers directly with phishing scams and other attacks. Many customers prefer protection from such attacks with capabilities like user-friendly multi-factor authentication (SMS, email or push notifications from custom mobile apps). An authentication authority can deliver these capabilities to protect customers from fraud.

Benefits to IT and Identity Administrators

Central IT needs to maintain control over their identity solution. They need to decide how much risk they're willing to accept, what types of use cases they want to enable and how to strike the perfect balance between security and convenience. An authentication authority helps meet these needs while enabling application teams to take control of certain aspects of identity to save IT time.

Centralized Security	Application teams are generally not security or identity professionals. IT, IAM professionals or security professionals should control the authentication within their enterprise. An authentication authority grants them that centralized control.
Enable App Teams	Even though IT maintains centralized control over security, an authentication authority ensures that app teams are enabled to control the user experience and to embed authentication into their applications. This way, IT isn't bogged down maintaining identity integrations to numerous applications.
Balance Security and Convenience	An authentication authority enables IT to define the levels of risk they're willing to accept across their application portfolio. With capabilities like adaptive authentication and robust policies, they can ensure that the level of assurance (LOA) about the user's identity always exceeds the level of risk associated with an authentication event.
Cloud Deployment Options	Many organizations are on a long journey to get more of their infrastructure to the cloud. No matter where you are along that path, an authentication authority should provide you with multiple cloud deployment options—IDaaS, private cloud, hosted private cloud, on-premises or hybrid—to help you move more of your footprint to the cloud in a manner that meets your needs.

Benefits to Application Teams and Business Units

Application teams and business units care about new users and speed to market. An authentication authority must check IT's security boxes, while not slowing down critical launch timelines of app teams.

Faster Time to Launch	By exposing easy-to-use APIs, documentation, customizable interfaces and other developer-friendly elements, an authentication authority ensures that the complexities of identity will not slow down application launches.
Control Identity Experience	While IT controls security and authentication flows behind the scenes, business units and app teams are empowered to create the perfect registration and sign-on experiences for their applications and plug those experiences into the authentication authority's sign-on and registration flows.
Take Security Off Their Plates	Application teams are not security experts. Not only would worrying about security slow down their launches, it would likely result in security holes in the authentication process. An authentication authority removes security from app teams and puts it in the hands of IT and built-in best practices—so application teams don't have to worry about it.

CAPABILITIES OF A CUSTOMER AUTHENTICATION AUTHORITY

When determining where to get started on your journey, strong identification and authentication is the logical place to start. Ensuring that all access is authenticated access is the bedrock of strong cybersecurity. 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.

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), adaptive authentication and passwordless 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 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 these additional factors and, as such, is one of the simplest ways to strengthen your security.

For customers, not just any form of MFA will do. Employees may not mind carrying around a USB drive hard token, but it is very unlikely that a customer would be so willing. But customers have shown they are willing to accept other additional authentication factors, such as push notifications or soft tokens from custom apps, SMS or email one-time passwords (OTPs), and third-party authentication apps such as Google Authenticators.

Unfortunately, they are not equally effective at preventing phishing attacks. NIST has deprecated SMS usage because of the ability of attackers to hijack phone numbers via a variety of methods. Using email OTPs is easy for a dedicated fraudster to overcome since customer credentials that grant access to their email are often shared with many other websites.

	Mobile Push	Mobile OTP (Soft Token)	Auth App (e.g. Google Auth.)	SMS OTP	Email OTP	Voice OTP
Customer Experience	Great	Okay	Bad	Okay	Bad	Bad
Security Level	Very High	High	High	Low	Low	Low

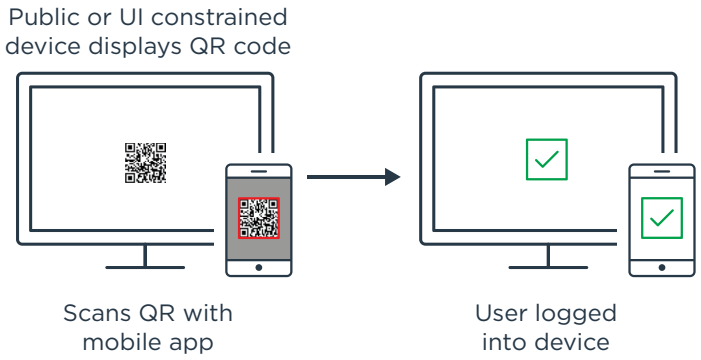
In the customer use case, the most convenient and secure option is when an MFA push notification gets sent to a trusted device and the user simply needs to approve it. Often, this is done by leveraging an authentication authority's mobile SDKs. Not only is user experience enhanced, but customers are able to leverage device features such as built-in biometrics.

Customers are as diverse as their preferences for authentication factors. Some may not download your mobile app at all—and you can't force them too. Some may prefer email or SMS OTPs. Any MFA is better than no MFA at all. An authentication authority will allow you to deliver MFA options so that you can give as many customers as possible the most secure, convenient MFA methods.

Passwordless Authentication

Since second authentication factors are often more secure than passwords, why do you need a password at all? You often don't. Combined with the fact that passwords can add a lot of friction to user experiences, many companies are opting to remove them entirely and give their customers a completely passwordless experience. In this situation, all that is required is a username or other identifier, and then the trusted device or second factor the user has set up can be used to verify their identity and sign them on.

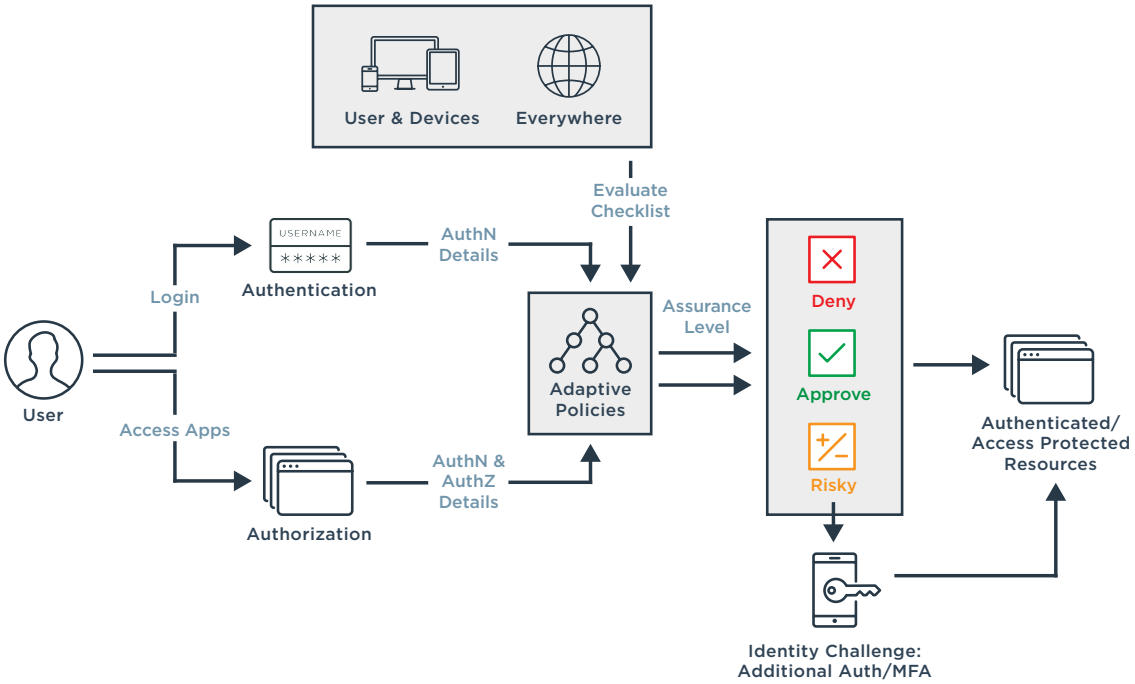
In some cases, usernames aren't even required and a user can simply sign on by scanning a QR code from their mobile device. This is a great use case for UI-constrained or public devices—imagine trying to log in to a streaming service in a hotel room with the TV remote control. Why not just use the streaming services app that you're already logged into, scan a QR code, and never have to type anything into the TV with the remote control.



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.

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.



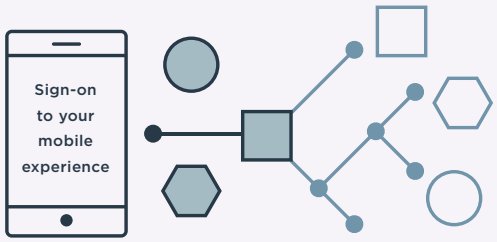
Conversely, if the adaptive authentication system has high confidence in the user's identity based on the repetitive and consistent nature of the access request, it may require fewer factors over time. For example, a user may initially be prompted for a second factor each time they request access to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

Authentication Policies

Authentication policies control both the flow the user sees when authenticating and the factors that are 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. Below are just a few ways—there are many, many others—that authentication policies can help balance security and convenience for customer use cases.

Give a Little Control to Apps

Allow apps to send preselected variables along with a token to control the authentication flow. This could be used if central IT wants to allow an app to deem itself as "high risk" or "low risk" depending on the function of the application.

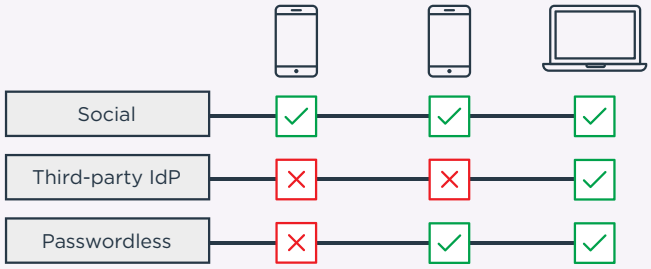


Review Previous Authentications

If a user has an active session with an app that requires a higher level of security, that session can persist to lower-risk apps without requiring another authentication. However, a session for a lower-risk app will not grant a user access to a higher-risk app.

Control Authentication Methods

Some authentication methods, such as passwordless authentication or social login, may be more appropriate for some apps than others. Authentication policies allow you to choose which authentication methods are available to which apps.



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

An authentication authority allows you to provide convenient SSO to your users. As the name suggests, single sign-on allows a user to authenticate once to gain access to all available resources. For the customer-facing use case, customers are often perplexed by a brand experience forcing them to sign on again and again—leaving them feeling annoyed and frustrated.

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. In the sections below, we have attempted to cover the majority of scenarios and business benefits when sending and receiving these standard tokens.

2. SSO to proprietary systems

In an ideal world, every application and service would accept standard identity tokens, but unfortunately that is not the world we currently live in. While most large service providers support standards, many of the smaller ones do not. Custom applications that aren't standards-based will continue to be a reality for the foreseeable future. An authentication authority has to be able to address them.

Identity and Attribute Handling

Many organizations have multiple user directories or identity stores because of mergers and acquisitions, or have pools of identities that are seen as "different" from 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 directories or other data sources for this information.

Authentication Orchestration

The term "authentication orchestration" 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 allows you to build simple, single-responsibility policies, and 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 authentication authority capabilities and the degree of control needed over the workflows and policies.

Data-driven Dynamic Policies

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

Conditional Sources of Authentication Factors

This 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 through 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 that you would like to integrate into your authentication workflows and policies. It's also 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 OpenID Connect. 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.

OpenID Connect Support to Third-party Providers

Both SAML and OpenID Connect are widely supported standards for customer applications. 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. It does support the ability to integrate login from a third party, but typical OpenID Connect 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 application has the identity token, it can create a session for the user and the user can do whatever they need. A nice security benefit of this flow is that the client application never actually sees the user's credentials and the identity token was never in a URL, which is often logged and can present a potential vulnerability for long-lived tokens.

OpenID Connect and OAuth Support

While OpenID Connect is built on top of OAuth, an 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.

In a typical use case, the application itself requests both an identity and an 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 session's 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.

WHAT'S BEYOND AUTHENTICATION

There is more to customer identity than authentication. While great first impressions with registration and streamlined interactions with sign-on experiences are critical pieces of the process, they're just the beginning of your customer journey. To truly stay competitive, you have to ensure that customer experiences remain seamless and secure even after the customer signs on.

A Unified Customer Profile

Creating a unified customer profile is often a logical next step. A unified profile serves several important purposes in customer identity use cases:

Storing Rich Customer Profiles

With employees, the types of attributes required to be stored about them are more predictable. With customers, the only limits are the imaginations of the team developing the customer apps. If a customer app needs to store a customer's favorite colors, preferences or any other data related to a customer's profile, they should not be limited by the availability of custom fields in a user store. The same goes for the type of data stored. An app team may prefer to store preferences as a JSON Blob, and that should not be a limitation.

Often, making these types of updates to a legacy user store is impossible. Even when it is possible, it can involve risky migrations that could affect any app connected to the repository. Database admins may hesitate to modify schemas based on app teams needs, which either leaves them having to yet again splinter the customer identity into their own data silo, or forgo storing the data and sacrifice a piece of their desired customer experience.

A unified profile from a customer identity solution allows application developers to store whatever data they need to about a customer, in whatever form they want—structured or unstructured—without the need for risky migrations.

A Source of Truth about Your Customers

Once companies have a rich customer profile, one of the most advantageous things they can do is expose it to all of their applications—ideally through REST APIs. Doing this allows every application to leverage customer data collected by any other application. This creates many opportunities for cross-sells and more personalized multi-channel experiences.

Scale and Performance

Another key tenet of a unified profile is its performance and scalability. Customer deployments may consist of tens or even hundreds of millions of identities. The data stored in a customer profile may be frequently read from the repository by numerous applications during authentication and beyond.

Like an authentication authority, giving customers deployment options that range from IDaaS and private hosted clouds to on-premises and hybrid can help ensure that an enterprise has the control they need to meet scale and performance SLAs for mission-critical applications responsible for many millions in annual revenue.

This becomes extremely critical during demand spikes that may result from marketing campaigns or product launches that represent significant investment by an enterprise.

Securing Customer Data

It's the authentication authority's job to project customers from fraud, but it's the unified customer profile's job to protect them from breach. When customer data is stored in a single place, it becomes a target. It has to be protected from both external and insider threats.

Capabilities such as data being encrypted in every state, alerts that let administrators know about suspicious admin activity or privilege escalations, tamper-evident logs and many other features of CIAM unified profiles can help protect your customer data from breach.

CONCLUSION

A globally trusted single source of identity can bring tremendous value to an organization and put you on the path to amazing and secure digital customer experiences.

When you can configure combinations of local and remote identities, as well as leverage flexible authentication and authorization policies, you gain the ultimate flexibility. You're able to manage your 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 seamlessly give your customers access to applications regardless of whether those applications are on-premises, cloud-based or third party.

To learn more about the Ping **Customer***360* customer authentication solution–and why we're trusted by more than 60% of the Fortune 100–please visit https://www.pingidentity.com/customer360.

Ping Identity is pioneering Intelligent Identity. We help enterprises achieve Zero Trust identity-defined security and more personalized, streamlined user experiences. The Ping Intelligent Identity™ platform provides customers, employees, partners and, increasingly, IoT, with access to cloud, mobile, SaaS and on-premises applications and APIs, while also managing identity and profile data at scale. Over 60% of the Fortune 100 choose us for our identity expertise, open standards leadership, and partnership with companies including Microsoft and Amazon. We provide flexible options to extend hybrid IT environments and accelerate digital business initiatives with multi-factor authentication, single sign-on, access management, intelligent API security, directory and data governance capabilities. Visit www.pingidentity.com. #3498 | 07.20 | v03