okta

Build your app or service right from the get go

Save with an identity solution that won't slow you down as you scale

Small and medium-sized businesses (SMB) often face tough decisions about where to spend funds, time, and mental bandwidth.

The process of building up your app or service involves not only, well, building the app or service, but also the foundational tech you need to support that process and your end result. You might use Twilio for communication or Stripe for online payments, because buying those tools gives time back to your team and removes the burden of building and maintaining SMS gateways and payment processing yourself.

One of the most important foundational elements is how you handle Identity and access management (IAM). Like other tools, there's a lot of options when it comes to deciding on an effective IAM solution:

- Build from scratch
- Purchase point solutions
- Invest in bundled features

Each path needs resources for the project to be successful, but what exactly those resources are may differ. You want solutions that can scale with you, can improve your security and time to market, make your users happy, and it's worth your investment. You need an option that extends, scales, and supports your business as it grows. If you need to replatform in the future, will your chosen solution scale, or will you have to take on more debt?

Very often, key areas may be overlooked. This whitepaper aims to provide valuable insight and practical guidance to help navigate the app building process and help make informed decisions about Identity that support your business for the marathon of success, not just the sprint to market.

How to build it right

Today it's a login box. But what will the market, users, and partners require of you tomorrow? How do you prepare when market expectations and technology are always changing?

There's more to choosing a robust Identity ecosystem to support your business than what products are available. Time to market, reliability, scalability, data, and security are all potentially affected.

okta

Don’t underestimate complexity of a complete Identity service

Identity is complex. Feature and system complexity can be underestimated and in a state of constant evolution. In-house development resources may be able to handle identity basics such as account creation, login, and password reset. However, advanced features like single sign-on (SSO) support, customer data partitioning, token authentication, multi-factor authentication (MFA), social login, and LDAP/Active Directory integration, require considerably greater effort to build and maintain.

When considering solutions, scour Identity and access management (IAM) company websites and consider products and features. What functionality will you need right away, or a year from now? If certain products or functionality are not included, could you build them with the team you have now without draining resources from core business? Will you need to hire specialists, or dedicate dev resources in the future?

Common Identity and access management requirements

IAM component	Description
Admin UI	Admin user interface for managing users, apps and APIs with scoped admin roles.
Authentication policies	Configurable policies and policy framework to control signin based on context such as user, app, group, geolocation, IP range, behavior, device, etc.
Build authorization server	Build authorization engine for business logic, including customizable scopes and claims.
Customer UI	Customer service or help desk UI to manage customer profile information with scoped admin roles.
Deploy directory with extensible profile/user/ groups/clients	A scalable user repository that provides a flexible user profile and groups. Includes Directory App server, Database, App Database, and Encryption.
Deploy token service	A scalable service to track each user session, with ongoing database maintenance and patching.
Directory/IDP integration	Create integrations with outside directories such as AD/ LDAP and support inbound federation via SAML, OIDC and WS-Fed for existing IDPs.
Gateway integration	Integrate with API gateways such as Apigee and Mulesoft.
SAML support and open protocols	Learn and amortize specs for SAML, OIDC, OAuth 2.0.
MFA	High availability, redundant MFA with multiple factor support (SMS, voice, email, Google Authenticator, biometrics, Push).

IAM component	Description
Operating system set-up, maintenance and lockdown	Customization of operating system and server software to eliminate security vulnerabilities.
Password storage and security	Hashing of passwords with most up-to-date algorithms and continuous maintenance as methods evolve.
Provisioning connectors	Custom-build, maintain and test API-based connectors to hand CRUD user functions and SCIM.
Provisioning engine	Engine for managing user objects in downstream services.
Registration, sign-in, account recovery, MFA screens	Building user interfaces and workflows, hosting of sign-in and registration pages.
Deploy token service	A scalable service to track each user session, with ongoing database maintenance and patching.
Reporting	Dashboard to see overall health of users and applications. Easy access to metrics and user reports for compliance purposes.
Social auth and profile sync	Broker authentication for any social identity provider, and sync profile attributes.
SSO connectors	Custom-build, maintain and test SSO connectors for third party apps.
Terminate SSL	Create and maintain a secure connection with any client over https. Manage a web certificate for a domain. Setup and maintain/patch strong SSL/TLS. Keep cryptography up-to-date.

Prepare for scope creep

As your business grows, users may demand greater functionality and rich features. The scope creep drive is, in some ways, a natural result of end users demanding more features, functionality, and seamless experiences. At the same time, it can be hard to predict future needs or user volumes when your applications first take off. Scope creep rates are high and, in some ways, expected — while rates vary, companies without project scope management experience scope creep with 66% of projects while companies with scope management experience scope creep with 39% of projects (31 Essential Project Management Statistics 2024, FounderJar). It's not impossible to fall victim to your own success if not prepared.

However, customers today are increasingly demanding greater functionality and security, which oftentimes increases the scope of projects. Additionally, companies quickly begin to build additional applications and may find themselves reinventing the wheel if development teams are not in constant communication. As a result, individual teams often underestimate the difficulty of building a complete, future-proofed identity service, which causes deadlines (and ROI) to slip.

okta

Get ready to maintain — and evolve

When planning out Identity, remember to include ongoing efforts to maintain, update, scale, and innovate.

Identity requirements are constantly evolving as well. Standards, requirements, and technologies may need ongoing expertise and budget to remain up-to-date. SAML and WS-Fed have evolved to more modern standards like OpenID Connect and OAuth 2.0. Elements within these standards have evolved as vulnerabilities have been found. Further, enterprise requirements such as deprovisioning access to APIs by revoking tokens may not have been initially contemplated in the standard. If you plan on having enterprise-sized customers, or already do, you will need to build and maintain enterprise-grade security that satisfies their compliance requirements.

Preparing for hosting it yourself

Open source solutions are appealing for their price point, but keep in mind they aren't always "free" — there will always be hidden costs when it comes to developer time to install software, try it and test it, find bugs, evaluate security and vulnerability of the components, and ongoing DIY maintenance and future-proofing. There's rarely a support service build-in to open source solutions: Maintenance and future-proofing is ultimately your responsibility. You, the company, are in charge and responsible for exposure to potential security risk related to lack of automatic updates and patching of vulnerabilities in open source code.

For information about what compliance requirements are applicable to your business and industry and whether you can use Okta's services to meet your compliance requirements, you should contact your legal counsel. Information about Okta's compliance with a range of industry-standard certifications and authorizations can be found here.

Even if your project avoids scope creep (or the need to scale and adapt with your user base), ongoing maintenance costs are a reality you will need to contend with. Providing seamless upgrades and maintenance to ensure uninterrupted service adds overhead, possibly quickly as the market shifts and changes. Maintenance alone has the potential to leech developer resources away from your core product.

okta

Align on developer resources

How you deploy developers can make your company excel. While Identity isn't your core business offering, as a foundational component that supports your entire business, it needs to be maintained like it is. For SMBs, where people often need to wear multiple hats, that means careful management of IT and developer talent.

Organizations can also underestimate the specialized technical expertise needed to build a secure and scalable identity function for their applications. It requires team members with diverse technical knowledge, including cryptography, database security, performance engineering, system engineering, and security auditing, as well as advanced data architecture to manage authorization. Specialist development resources are scarce, which means many organizations may have trouble finding the resources to get the job done in-house—particularly on a tight deadline, if a team realizes it doesn't have the resources while in the middle of a project.

Ask yourself how experienced and up-to-date is your team on security and DevSecOps? How do they plan to stay on top of the latest cryptographic trends?

Power tip

Whenever you're building, keep watching out for the common building pitfalls to avoid:

- Trying to keep doing what you have done in the past, using antiquated patterns or approaches
- Asking for way too much user effort and data upfront
- Believing you need embedded login (mobile or website) for the best user experience
- Believing your business customers have to authenticate with usernames and passwords
- Believing that you need to code everything to retain control

Alternatives to building

There are certainly benefits to the initially cheaper cost of DIY solution and maintaining control over portions of your stack. If you have time, if you have the talent, if you have capital. But if the overall cost of building doesn't make sense for your goals, offloading some of that burden onto a pre-built tool is the next logical step.

It all comes down to a balance of resources. Development teams have increasingly turned to pre-built tools to offload some of the burden of app development. Identity and access management presents developers with a broad range of challenges that a trusted identity layer can help offload easily. This is a sound strategy for companies of all sizes that want to accelerate time-to-market, reduce costs, focus development teams on core functionality, and realize a host of other benefits.

Unsure about must-haves or where to start with Identity? Read up our SMB Identity Checklist to get acquainted with the questions you need to ask when planning your Identity solution.

The potential pitfalls of buying are similar to those of building it yourself. Half-measures are the enemy, creating a scenario of not fully committing, only to realize it's not a tenable long-term solution. This often happens with point solution purchases, perhaps added later in the app development process or after dev resources have been spread thin. Unfortunately, tech debt can rack up quickly as tech silos are potential new points of failure built into your ecosystem. All those point solutions will, at some point, have to go through replatforming.

How to buy it right

1. **Lay groundwork**
   - Scope out your current, most immediate needs
   - Identify where you want to be in six months
   - Identify where you want to be in a year
   - Collectively agree on must-haves and components that accelerate your roadmap
2. **Research options**
   - Research Identity service providers
   - Effectively narrow your search
     - Check with peers, community boards, analysts, and customers.
   - Check that your top 3 potential providers can meet your must-haves list
3. **Test it! (at a small scale)**
   - Look at solutions that offer a quick way to ideate on and test them
     - Extra points if the solution offers you a pay as you go/grow route
   - Look at solutions with comprehensive getting started guide
   - Check for a strong community if something breaks or you have questions on the way

Pro buyers' tip

Don't forget to read customer success stories, or case studies. Generally available on providers' websites, these give detailed, personal insight into Identity development journeys, challenges, and solutions — including from business pivoting from building Identity in-house.

Proof of concept

If you're curious about what an IDaaS provider can do for you, jump into a free trial and spin up a POC. This is a fantastic way to get your hands on a product and gather data yourself. How quickly can devs spin it into a workable model and test it? How easy and available are resources and documentation to access and use? Are customer support or sales available to answer questions? Is the company otherwise enjoyable to work with?

Learn more

No matter where your Identity journey takes your business, knowledge is your strength. To save time and get up to speed, check out the checklist for SMBs with the top ways Identity can further support your business and how to plan for the future.

Curious about what we have to offer locally? We have a 30-day free trial you can try today.

Further questions? We have resources specially made to help SMBs below, and our Sales team is always willing to help and field questions you might have.

These materials and any recommendations within are not legal, privacy, security, compliance, or business advice. These materials are intended for general informational purposes only and may not reflect the most current security, privacy, and legal developments nor all relevant issues. You are responsible for obtaining legal, security, privacy, compliance, or business advice from your own lawyer or other professional advisor and should not rely on the recommendations herein. Okta is not liable to you for any loss or damages that may result from your implementation of any recommendations in these materials. Okta makes no representations, warranties, or other assurances regarding the content of these materials. Information regarding Okta's contractual assurances to its customers can be found at okta.com/agreements.

Resources

- Secure your Small Business with Identity
- Securing your workforce with MFA
- SMB Identity buyers' checklist
- Build vs. Buy: Customer Identity and Access Management

About Okta
Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.