

Build vs. Buy

Rethinking authentication in the era of FIDO





Contents

Build vs. buy: An overview of the pros and cons	3
The third option: A hybrid approach	4
Why partner with OneSpan	5
Trusted authentication platform	5
Ability to navigate key and device complexities	6
Future-proof approach	6
Streamlined deployment	6
Conclusion	7

The information contained in this document is for information purpose only, is provided AS IS as of the date of publication, and should not be relied upon as legal advice or to determine how the law applies to your business or organization. You are responsible for obtaining legal advice from your own legal counsel. You should not act or refrain from acting on the basis of any of our content without first obtaining matter specific legal and professional advice. OneSpan accepts no responsibility for any loss or damage which may result from accessing or reliance on the content of this document, and disclaims any and all liability with respect to acts or omissions made by readers on the basis of our content. Our content may contain links to external websites and external websites may link to our content. OneSpan is not responsible for the content or operation of any such external sites and disclaims all liability associated with such websites.



Build vs. buy: An overview of the pros and cons

The decision to build custom software or buy off-the-shelf solutions is one of the most debated topics in the software industry. It's a choice that can define a business's operations, scalability, and long-term competitive advantage. Both approaches come with distinct advantages and challenges, and these differences help organizations make informed decisions aligned with their unique business objectives. In this white paper, we take a deeper look at the options in the context of FIDO-based (Fast Identity Online) authentication solutions.

Build

When organizations choose to build custom software, they gain the ability to tailor the solution to their exact requirements. This approach ensures the software aligns perfectly with internal processes and workflows, offering a competitive edge by addressing gaps that generic solutions cannot fill.

Building software also provides full control over the solution's development roadmap, enabling teams to introduce new features, manage integrations, and dictate the pace of innovation.

However, building software also presents significant challenges. The upfront costs are high, requiring substantial investment in time, money, and skilled resources. Development timelines can be long, delaying implementation and the realization of business benefits.

There is also an inherent risk of project failure if the initiative is not managed effectively, potentially resulting in wasted resources and sunk costs. Most importantly, it demands specialized technical expertise. Skilled developers and IT professionals who understand both the technology and the business context can be difficult and expensive to find or train.

Once deployed, custom solutions require continuous maintenance — regular updates, bug fixes, and performance optimization — all of which can divert focus away from an organization's core business activities.

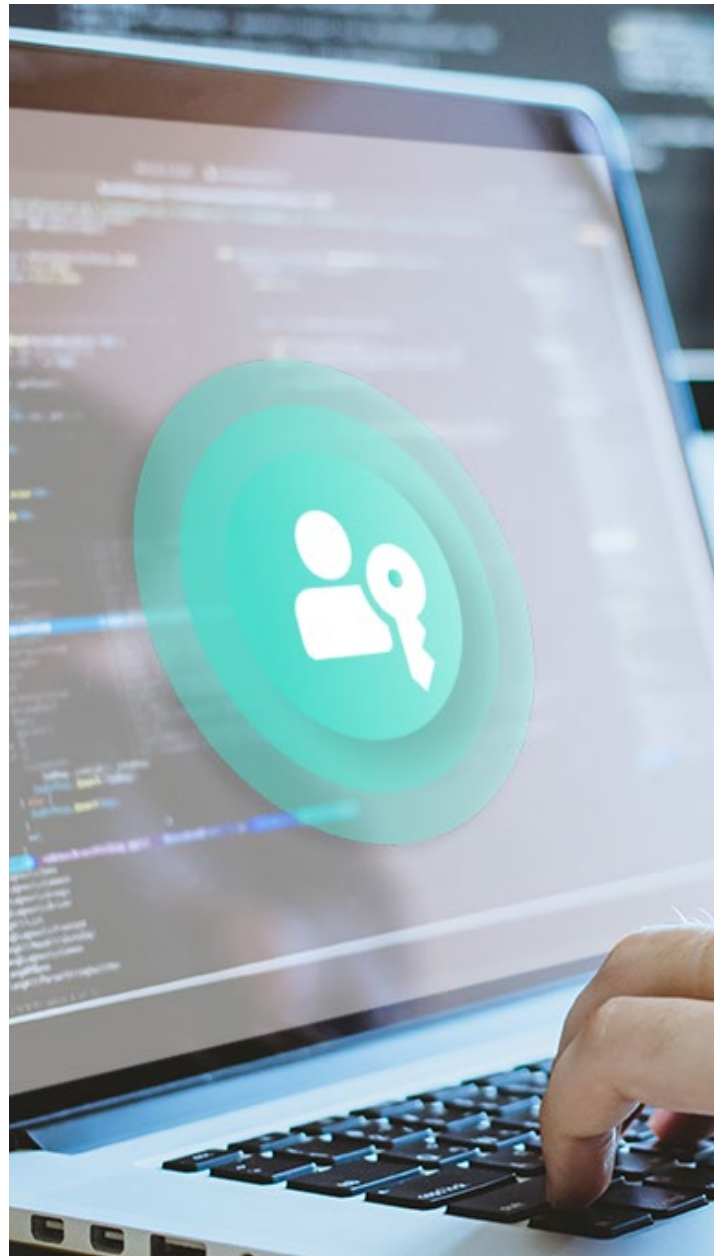
Buy

Buying off-the-shelf software offers a faster and more cost-effective route to implementation. Ready-made solutions, such as OneSpan's Digipass® S3 Authentication Software, require less setup time and a lower upfront investment, making them more predictable and easier to budget for.

These platforms often come with proven reliability, certifications, and a track record of successful implementations. Vendor support typically includes

ongoing updates, technical assistance, and maintaining compliance certifications. Subscription-based licensing models further simplify budgeting by providing predictable costs over time.

Still, buying software has its limitations. Off-the-shelf solutions may not perfectly fit every business's unique requirements, sometimes requiring customization or add-ons to close functional gaps. In certain cases, pre-packaged products may include unnecessary features that increase overall costs without adding measurable value.





The third option: A hybrid approach

There is another option beyond the binary build vs. buy decision. Consider a hybrid approach that combines off-the-shelf systems with custom-built components. This strategy balances cost-efficiency with flexibility, allowing organizations to focus internal resources on areas that create differentiation while leveraging proven technologies for foundational needs.

Think of it like building a house. While design choices and finishes can be fully customized, the framing, wiring, and plumbing — the critical underpinnings — follow established standards.

Similarly, that's what OneSpan offers. Businesses can innovate and enhance their brand experience as much as they wish, but the underlying authentication infrastructure must provide one fundamental outcome: proving who's there.

Every digital interaction should start with trust. Getting authentication right is not easy and getting it wrong can have serious consequences. Cybercriminals are constantly evolving, so it's crucial to anticipate vulnerabilities and maintain a secure, frictionless user experience. Doing so requires deep expertise in encryption, authentication, and compliance. That's precisely what OneSpan delivers.





Why partner with OneSpan

At OneSpan, we've consistently seen how blending custom development with our authentication platform provides an ideal balance between innovation and efficiency. By using Digipass® S3 SDKs and APIs for secure, passwordless authentication, organizations can achieve faster time to market, reduce costs, and enhance security — all while maintaining flexibility in design and user experience.

For instance, many customers have built bespoke, customer-facing applications to support unique features that differentiate their offerings. They then integrate authentication using Digipass® S3 Authentication Software, saving months of development effort and significantly reducing security risk.

This hybrid approach allows development teams to focus on delivering value to users, while OneSpan provides the secure foundation for authentication and identity verification.

Another major benefit is cost efficiency. Developing FIDO-based authentication capabilities in-house is resource-intensive and requires constant maintenance to keep pace with changing standards. Leveraging OneSpan's proven technology reduces that burden and ensures continuous compliance with the latest FIDO and privacy regulations. By avoiding the need to reinvent the wheel, organizations can redirect resources toward innovation and improving the customer experience.

Security and user experience are also enhanced through this model. OneSpan's deep expertise in FIDO standards, encryption, and adaptive risk-based authentication offers a level of reliability that's difficult to replicate internally. Integrating SDKs and APIs allows organizations to maintain full control over branding and user flow while benefiting from a proven, enterprise-grade security backbone.

The result is a seamless user journey where authentication feels native, fast, and secure. OneSpan modernizes authentication security by helping development teams replace outdated, password-based systems with FIDO passkeys, a modern standard leveraging cryptographic authentication that is inherently resistant to phishing and credential theft. The platform also eases compliance with global security standards while reducing costs by eliminating password management and account recovery overhead.

Built with rigorous quality and reliability standards, Digipass® S3 Authentication Software delivers scalable, high-performance authentication for enterprise environments. The platform meets FedRAMP High and DoD IL5 requirements (in partnership with UberEther) and is pending SOC 2 Type II certification, demonstrating OneSpan's commitment to enterprise-grade security and compliance. These capabilities stem from decades of experience and investment in authentication innovation, the kind of depth that is difficult to build internally from scratch.

Blending build-and-buy strategies promotes agility, allowing organizations to launch faster, reduce technical debt, and innovate continuously. Businesses can build differentiation where it matters most while relying on trusted components for the rest. With this pragmatic approach, technology serves business outcomes, not the other way around.

A trusted authentication platform

As organizations work to improve both security and user experience, passkeys have emerged as a powerful alternative to traditional passwords. OneSpan's modern approach to passkey implementation enables organizations to deploy secure, passwordless authentication with ease.

Through seamless integration, adaptive orchestration, and FIDO-based encryption, OneSpan empowers enterprises to deliver authentication experiences that are both scalable and user-friendly.

With full support for all FIDO protocols, OneSpan enables developers to integrate advanced authentication capabilities into their applications without building complex systems from the ground up. Using OneSpan's SDKs and APIs, organizations can reduce development time, lower costs, and meet privacy and regulatory compliance standards.

OneSpan's adaptive orchestration engine dynamically adjusts authentication flows based on contextual data such as device, location, and risk level — further streamlining the user experience. With its cloud-scale architecture, OneSpan allows global deployment of FIDO authentication, delivering robust security and a frictionless experience for millions of users. For organizations requiring hardware-based authentication, OneSpan also offers Digipass® FIDO2 security keys, a family of FIDO-certified hardware



devices that deliver the same secure, phishing-resistant authentication experience in environments where regulatory, operational, or physical security mandates hardware tokens.

By supporting both software and hardware authenticators within the same FIDO ecosystem, OneSpan provides enterprises with unmatched flexibility to deploy passwordless authentication across every user segment, from digital-first consumers to employees in regulated, high-assurance sectors.

Ability to navigate key and device complexities

Building a comprehensive, modern FIDO-based authentication system across platforms is a complex, resource-intensive endeavor. Many organizations underestimate the effort required until they are deep into development.

Digipass® S3 Authentication Software simplifies that process with a proven solution that includes an abstraction layer, scalable authentication infrastructure, and FIDO client integration. This reduces development cost and complexity, streamlines compliance, and provides seamless support for diverse use cases.

The result: Organizations can deliver secure, modern authentication faster, without the significant challenges of building from scratch. Examples include:

- Digipass® S3 Authentication Software seamlessly supports both device-bound and synced passkeys, providing enterprises with flexibility and strong security. Device-bound passkeys stay tied to a single device, reducing risks such as phishing and credential replay. Synced passkeys, meanwhile, enhance convenience by enabling secure authentication across multiple trusted devices.
- Backed by years of expertise managing both device-bound and synced passkeys, OneSpan's Digipass® S3 Authentication Software streamlines authentication and reduces password management and recovery costs. This proven approach helps organizations strengthen security practices, simplify administration, and enhance the user experience across every channel.
- Digipass® S3 Authentication Software also addresses key limitations in cross-device authentication, such as the inability of default passkey providers to sync credentials across Windows, Android, and iOS ecosystems. By leveraging out-of-band authentication, OneSpan enables seamless credential creation across devices; for example,

allowing a user to register on a laptop and generate a passkey on their mobile phone for app access.

Future-proof approach

- Digipass Intelligent Credential Detection further enhances authentication by identifying compatible devices and user credentials in real time. This feature empowers relying parties to deliver adaptive authentication journeys that optimize both security and user convenience.
- Digipass Granular Adaptive Policies eliminate the need for hard-coded algorithms, offering unmatched flexibility to customize authentication experiences for each user and device. This dynamic model modernizes authentication by creating secure, seamless, and context-aware journeys that adapt to every environment and risk scenario.
- Digipass Intelligent Passwordless Authentication enhances both security and usability by analyzing key protection, binding, user verification status, passkey provider, and certification level in real time. The platform then adapts authentication responses accordingly, granting access, triggering step-up verification, or denying access, to deliver a frictionless and secure process.
- Digipass SDKs and APIs simplify integration across web, mobile, and IoT applications, abstracting technical complexity and shortening deployment timelines. Developers can deliver FIDO-compliant authentication faster and more reliably without maintaining internal authentication infrastructure.
- The Digipass Quick Authentication feature revolutionizes the passkey process by minimizing network calls, dramatically reducing authentication latency and server load while improving user experience.

Streamlined deployment

Digipass® S3 Server delivers high-performance, low-latency authentication built for enterprise scale. Drawing on insights from large-scale global deployments, the platform supports modern containerized environments like AWS, Azure, and GCP, ensuring reliability, scalability, and zero downtime.

The Digipass® S3 adaptive authentication rules engine makes it simple to configure or update authentication policies, such as registration, verification, and contextual checks, without making code changes to apps or services. Policies can dynamically adjust based on device health, network signals, geolocation, and authenticator attributes, verifying that the user is who they claim to be.



Conclusion

Ultimately, the decision between building and buying depends on several factors: The complexity of business needs, available technical talent, time constraints, and scalability goals.

For many organizations, a blended strategy combining internal innovation with OneSpan's trusted authentication foundation provides the most effective balance between flexibility and control.

By aligning priorities and resources, businesses can make smarter technology investments that strengthen security, speed innovation, and enable long-term growth.

To learn more, [speak to one of our experts](#) about your specific needs and requirements.

About OneSpan

OneSpan is a global leader in digital security, trusted by thousands of enterprises across 100+ countries—including more than 60% of the world's 100 largest banks—to safeguard digital accounts, secure financial transactions, and prevent fraud. Our award-winning solutions provide passwordless authentication, digital transaction security, and advanced mobile application protection, helping organizations meet the highest security standards and global compliance requirements. As cyber threats grow more sophisticated, OneSpan delivers cutting-edge technology to safeguard customers, mitigate risks, and ensure trust in every digital interaction.

Learn more at
[OneSpan.com/security](https://onespan.com/security)

Contact us at
[OneSpan.com/contact-us](https://onespan.com/contact-us)



Copyright© 2025 OneSpan North America Inc., all rights reserved. OneSpan®, the "O" logo, Digipass®, Cronto® are registered or unregistered trademarks of OneSpan North America Inc. or its affiliates in the U.S. and other countries. Any other trademarks cited herein are the property of their respective owners. OneSpan reserves the right to make changes to specifications at any time and without notice. The information furnished by OneSpan in this document is believed to be accurate and reliable. However, OneSpan may not be held liable for its use, nor for infringement of patents or other rights of third parties resulting from its use.