OneSpan

DATASHEET

AUTHENTICATION SERVER FRAMEWORK

HIGHLIGHTS

Authentication Server Framework is an API-based authentication platform that serves as a backend for OneSpan's strong authentication and e-signatures solutions.

This server solution is capable of processing large volumes of authentication requests and can support mass deployments in a variety of customer interfacing applications, including online banking, e-commerce, online gaming, and web portals, among others.

AUTHENTICATION SERVER FRAMEWORK

Integrate strong authentication into your applications

OneSpan Authentication Server Framework is a state-of-the-art API-based authentication platform that serves as a back-end for Digipass Strong Authentication tools. It automatically handles login requests, ensuring only properly authenticated users can access protected online applications and networks. In addition, OneSpan Authentication Server Framework can be used to validate e-signatures which are developed to protect your online transactions from Man-in-the-Middle attacks. The unique design, unlimited scalability and flexibility of OneSpan Authentication Server Framework make it a perfect fit for large deployments in a variety of customer interfacing applications such as online banking, e-commerce, online gaming, web portals, and others.

> "We are very pleased with the way the solution works. On the client-side, everything passes off quite smoothly. Also, on the server-side, we haven't experienced any problems. OneSpan Authentication Server Framework is well-integrated in our WebSEAL, so we are happy that our integration and security concerns are finished."
>
> **Erik Ladefoged**
> Lead Infrastructure Architect
> Jyske Bank

Native integration

OneSpan Authentication Server Framework can be customized and integrated into any existing application regardless of the operating system, data model, or architecture. The versatility of this API-based solution makes the entire two-factor security implementation effortless and cost-effective, ensuring the lowest possible impact on existing infrastructure and operations.

Unlimited scalability

OneSpan Authentication Server Framework makes it easy to add more users and/or applications without the need to rebuild the back-end infrastructure. There is no need to deploy and maintain additional or back-up servers.

High availability

With OneSpan Authentication Server Framework API, there is no need to worry about server downtime and service disruptions. Its high reliability ensures that your users can get secure access to the system when they need it.

Low total cost of ownership

OneSpan Authentication Server Framework is designed to accommodate all current and future OneSpan authentication and e-Signature technologies and devices. This provides your organization with the flexibility to follow new standards and developments in application and network security for virtually any operating system or platform.

OneSpan Authentication Server Framework is a cost-effective solution that leverages your IT investment and provides one centralized platform without any additional requirements for a separate authentication server or database. As such, no server farms and dedicated disaster recovery systems are needed.

OneSpan

DATASHEET

AUTHENTICATION SERVER FRAMEWORK

High security

OneSpan Authentication Server Framework is a single platform with secure key management and provisioning suitable for any security policy:

- End-to-end security chain from OneSpan manufacturing sites to customers
- Initialization secure room with a high level of both physical and logical security
- Secure encrypted transport Digipass key file (DPX) with an optional key ceremony for the customer's security officer(s)
- Optional Hardware Security Module (HSM)-compliant solution
- Optional hardware DPX file encryption
- One-time password and e-signature validation operates inside the HSM
- No sensitive information exposed outside of the HSM
- Compliant with FIPS standards

Integrations with strategic partners

OneSpan Authentication Server Framework is currently integrated into over 100 applications, including those in the portal, single sign-on, and banking markets, among others. Native integration significantly reduces the cost of strong authentication implementation and simplifies back-end deployment and management.

Support for multiple form factors

OneSpan Authentication Server Framework is a unique and flexible platform that supports multiple authentication devices and mechanisms. It works with all hardware and software-based Digipass authenticators, as well as with OATH-compliant devices (except OneSpan Authentication Server Framework HSM versions) and EMV-CAP smart cards. When combined with Digipass hardware and software authenticators, OneSpan Authentication Server Framework can provide end-to-end secure online provisioning and management of these authenticators.

The following form factors are supported in every implementation:

- One-button hardware authenticators
- PIN-protected hardware authenticators
- Matrix Cards
- Software-based solutions (Digipass for Web, Digipass for Mobile, Digipass for APPS)
- SMS delivery (Requires integration of an SMS gateway)
- USB authenticators
- Smart cards

Support for multiple authentication technologies

OneSpan Authentication Server Framework supports a range of authentication modes including:

- Time- and/or counter-based one-time passwords (response only
- Time- and/or counter-based challenge/response
- Time- and/or counter-based e-signatures
- Mutual authentication (between a user and a server)
- e-signature confirmation code
- Server-side PIN validation
- CHAP & Microsoft Response Authentication using Digipass dynamic passwords
- Knowledge-based authentication (secret question & answer scheme)

Other features include:

- Time- and/or event-based synchronization mechanisms
- Supports DES/3DES/AES/OATH encryption standards
- Integrated secure unlocking feature for locked users
- Centralized credential provisioning mechanism to be used with OneSpan Mobile Authenticator Studio and OneSpan Mobile Security Suite product line.
- Centralized OTP generation mechanism to offer SMS-based authentication
- Multi-thread and multi-task aware code
- On- and offline software-based Digipass provisioning
- Multi-device licensing based Digipass provisioning

TECHNICAL SPECIFICATIONS			
Support for most processors and platforms (32 and 64 bit)	• Windows NT/9x/Me/2000/XP/2003/2008/ Vista/Win7/Win8/Win10 • Linux • Sun Solaris Sparc / Intel • HP/UX • AIX • FreeBSD • AS/400 • Z/OS • Z/Linux		
Standards	• EMV CAP (2004, 2007) • EMV CAP E (2008) • OATH (HOTP, TOTP and OCRA based on HMAC-SHA1) (**)		
Hardware Security Modules	• Safenet ProtectServer and ProtectServer2 (K5 ARM and K6 Power PC architectures) • Thales nShield and nCipher netHSM (Power PC architectures) • Thales nShield Connect XC (Windows and • Linux 64 bit only) • IBM ICSF		
Languages	Windows: • C / C++ • Java • C# (.net)	Unix/Linux Systems: • C / C++ • Java	Mainframe: • C / C++ • Java • COBOL • PL1 • Assembler

** For other HSM support, please contact your local account representative*

*** Except VACMAN Controller HSM versions*

OneSpan

OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.

CONTACT US
For more information:
info@OneSpan.com
www.OneSpan.com