wwGate™ 1.0

September 2013

Gerry Texeira, Eric Scace, Jessica Schilling

Who should read this white paper:

IT professionals and managers specializing in data security and risk management.

This paper assumes the reader is familiar with basic concepts of authentication, identity management, and single sign-on for web-based applications.

wwGate integrates patented WWPass® hardware or software based cryptographic authentication with X.500 directory services to provide a single sign-on service for Security Assertion Markup Language (SAML) compliant web-based business applications. wwGate eliminates the need for usernames and passwords, eradicating the associated vulnerabilities while simultaneously simplifying user log-in. The WWPass PassKey® credential — compliant with NIST SP Level of Assurance 3 standards — further increases resistance to outside attack.

Deployment of wwGate on the VMware vSphere® appliance and user rights administration are straightforward for the experienced IT professional. User on- and off-boarding typically requires less than 15 minutes.

Targeted toward populations of 50-10,000 users, wwGate 1.0 integrates with Microsoft® Active Directory® to support the following popular SAML-compliant cloud-based apps in addition to Juniper® VPN authentication:

- Google® Apps for Business™ and Education™
- Salesforce.com®
- Dropbox™ for Business

wwGate advantages at a glance

Increases security of SAML-compliant web-based business applications by replacing username/password authentication with patented WWPass hardware-based cryptographic two-factor authentication.

Gives users a simpler, faster sign-on for these applications, as well as other key enterprise services such as VPN.

Simplifies administration of user access rights by integrating with X.500 standard directory services.

Acronyms in this document

AD	Microsoft Active Directory
IdP	Identity Provider
LDAP	Lightweight Directory Access Protocol
RP	Relying Party (*note: In SAML, a Relying Party is referred to as a Service Provider)*
SAML 2.0	Security Assertion Markup Language 2.0
SP	Service Provider *(SAML term for a Relying Party)*
SPID	WWPass Service Provider Identifier
SSO	Single Sign-on
UPN	AD UserPrincipalName
wwGate	wwGate
VPN	Virtual Private Network

1 What is wwGate?

wwGate 1.0 integrates WWPass' hardware or software based cryptographic authentication with X.500 directory services to provide SAML-compliant single sign-on (SSO) solutions for compatible web-based business applications.

To log in, the user employs a personal PassKey® in place of a username. The PassKey is a cryptographic token available in convenient Smartphone, USB and NFC (near-field communications), and CAC (common access card) form factors. With the addition of an AccessCode, the PassKey serves as a strong two-factor authentication solution. When combined with the enterprise's own X.500 directory services, allows the enterprise to achieve NIST SP 800-63-1 Level of Assurance (LoA) 3 or 4 standards for authentication and data protection.

The PassKey is anonymous: It contains no personal identifying information, certificates, or other identity attributes. Working together with WWPass cloud-based servers and encrypted, fragmented, globally-dispersed cloud storage, the user's PassKey provides a single-credential, secure, and anonymous method for high-assurance authentication into any enabled VPN, web or PC-based application. It provides an unprecedented convenience for the user, who now carries one device to quickly login to anything.

For the IT team, wwGate's integration with Active Directory provides a familiar administration interface for centrally managed user access rights. User on-boarding and off-boarding take only a few minutes to complete. wwGate runs as a virtual appliance on an enterprise's VMware vSphere infrastructure — a virtualization technology already familiar to many IT professionals. wwGate's design simplifies deployment and reduces user rights management costs.

For compliance and security staff, wwGate offers the peace of mind of two-factor authentication using hardware-based cryptographic credentials. A simple, seamless user experience ensures ease of adoption and continued use. Risk management professionals can also rest easy knowing that if a PassKey is lost or stolen, corporate data security is in no way compromised. A simple web-based utility allows the user or authorized IT administrator (acting as the user's recovery agent) to invalidate the lost PassKey and create replacements.

2 How does wwGate work?

wwGate interacts simply with both the user and IT administrator. Under the hood, the combination of wwGate, WWPass cloud services and the X.500 directory services implement SAML's Identity Provider (IdP) function.

2.1 What the user sees

1. User enters the URL of the desired web app (such as mycompany.salesforce.com) into a browser. This web app is the Relying Party (RP).
2. A dialog appears on the user's display, asking for confirmation to authenticate into the web app by presenting the PassKey and entering an AccessCode.

- The dialog notifies the user if thePassKey or AccessCode are not correct.

3. After the user successfully provides a valid PassKey and associated AccessCode and confirms desire to authenticate into the target web app, the dialog box disappears.

   - If the user is authorized to use the app, the app returns the appropriate welcome page.
   - If the user is not authorized to use the app, the app returns the appropriate “access denied” page.

2.2 Under the hood

The user’s seamless experience with wwGate via the WWPass PassKey is backed up by powerful behind-the-scenes technology.

For purposes of clarification, the following SAML-defined roles are performed within the wwGate architecture as defined below:

- **SAML SP (aka RP)** The target web app.
- **SAML user agent** The user’s web browser.
- **SAML IdP** The combination of wwGate, AD and WWPass services. The wwGate appliance implements the SAML message interchanges with the web app and user’s browser.

While the combination of wwGate, WWPass authentication service and AD perform the SAML Identity Provider role, each of these systems has a specific mission:

- WWPass authenticates the user’s base identity[i]. Base identity individuates the user from all other machines and people — without containing any personal information about the user.
- AD acts as an authoritative attribute provider, holding the user’s access rights and other personal identifying information.
- wwGate binds the attributes obtained from AD to the user’s session, delivering a SAML security assertion to the RP.

See the figure on the next page for a depiction of the wwGate authentication workflow in action according to the steps below:

1. User enters URL of web app into browser.
2. The RP redirects the browser connection to wwGate.
3. wwGate communicates with WWPass front-end servers via SSL to request two-factor authentication of the user. WWPass servers communicate with a browser plug-in on the user’s machine to present dialogs prompting the user for PassKey and AccessCode, and to confirm desire to authenticate into the web app.

Supported functionality and requirements

Virtualization VMWare vSphere v5.0 and above

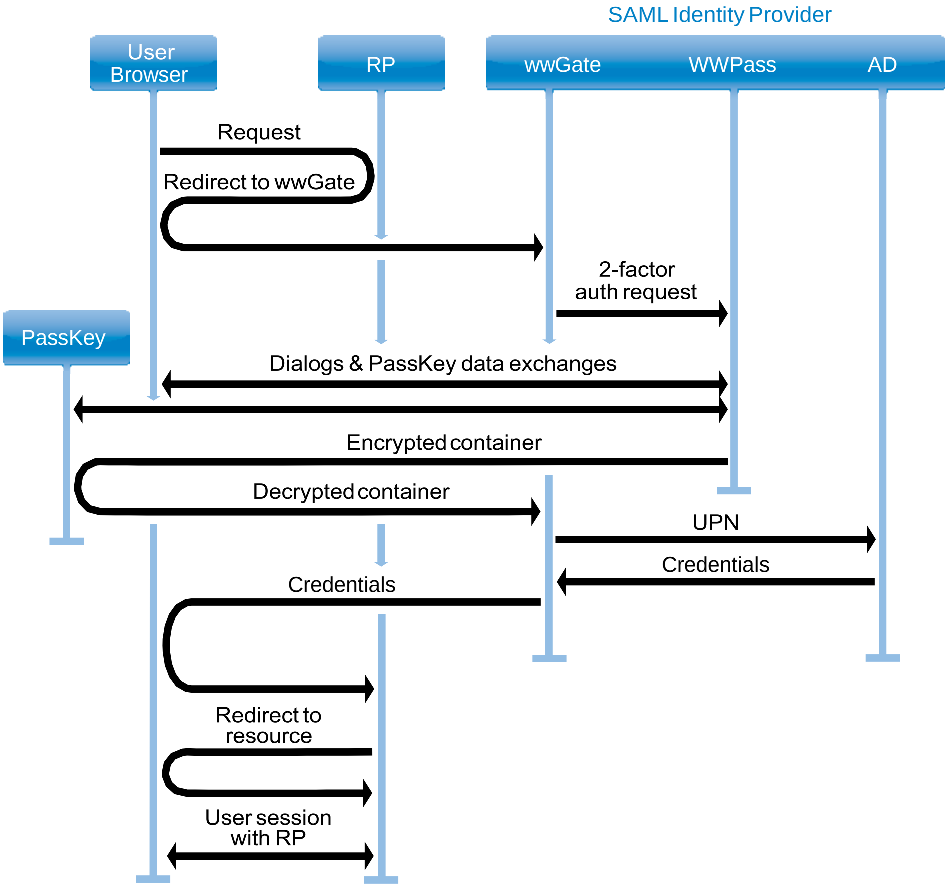
Directory stores Microsoft Active Directory 2003/2008/2012

Supported browsers Internet Explorer® 8, 9 and 10 (32-bit and 64-bit); Chrome™ 20+; Mozilla Firefox® 14+; Opera™ 16+; Safari® 5
Note: Web browser and internet connectivity are required to activate a WWPass KeySet and authenticate into WWPass-enabled applications

Supported federation protocol SAML 2.0

Minimum requirements 10 GB storage space; 1 GB RAM (minimum); 1 64-bit Intel® or AMD® processor

wwGate Authentication Workflow



Note: All communications between WWPass servers, wwGate and the user's machine employ encrypted SSL sessions.

4. WWPass servers verify that the user's PassKey is valid and that the AccessCode is correct. If so, WWPass servers reassemble an encrypted data container from WWPass fragmented, globally-dispersed storage[ii]. These servers deliver the data container to the user's machine for decryption (under the control of the user's PassKey), and the user's machine transmits the decrypted container to wwGate.

5. wwGate removes the user's UPN from the decrypted data container and transmits it to AD in order to verify whether the user's security object is enabled or disabled.

6. AD replies to wwGate with account and user attributes. If the account is disabled, wwGate rejects authentication.

7. wwGate transmits the attributes in a SAML XHTML form to the browser.

8. User's browser transmits a SAML Request Assertion Consumer

Service message containing the credentials to the web app.

9. Web app authorizes the user to access the app, and then redirects the browser to the appropriate welcome or “access denied” landing page.

2.3 For the IT admin: adding and removing users

Because wwGate integrates so tightly with existing Active Directory records, adding and removing users is speedy and simple:

- During user on-boarding, the administrator binds the newly created AD UserPrincipalName (UPN) with the user’s PassKey via a wwGate utility. User access privileges continue to be administered via AD’s admin tools. Creating a web SSO typically takes less than 15 minutes.
- The administrator off-boards a user by deleting or disabling the user’s AD security object, thereby invalidating the UPN. No actions are required with either wwGate or the user’s PassKey, since neither contains personally identifiable information or security certificates.

3 Is wwGate a good match for your organization?

While wwGate reduces authentication vulnerabilities in a wide range of enterprise settings, it is best suited for environments with the following characteristics:

- 50 to 10,000 individual users
- Employing any of the following RPs (SAML SPs):
  - Google Apps for Business/Education
  - Salesforce.com
  - Dropbox for Business

Users may be on an internal network, VPN, or the public internet when working with the RP. For Juniper VPN systems, users authenticate with the same PassKey into both the VPN and the RP — an added convenience.

For settings outside these parameters, please contact **sales@wwpass.com** to discuss customized solutions best suited for your needs.

4 Why deploy wwGate?

As organizations employ an increasing number of off-site and web-based services in order to meet business needs, SSO methods become essential. A 2013 Gartner Inc. report proposes that by 2017, more than 50% of enterprises will choose cloud-based services as the delivery option for new or refreshed user authentication implementations up from less than 10% today.

Requiring users to maintain separate username/password combinations for each such service not only is inconvenient, but also exposes the organization to increasing security threats. According to the *2013 Data Breach Investigations Report* 76% of network intrusions exploited weak or stolen credentials — the highest percentage of all categories of breaches reported. In scenarios such as these, the victims' reliance on duplicate or otherwise weak username/password combinations represents a significant contributing factor to successful attacks.

SSO systems make the user's life more convenient by reducing the number of log-in credentials to be learned. SSO systems also simplify administration of users' access rights to multiple applications using centralized user administration. But if the SSO system itself relies on a username/password for authentication, security vulnerabilities are amplified when those credentials become compromised — and even more so if the compromised username/password belongs to an administrator.

While a variety of competing solutions exist within this space, WWPass' unique combination of:

- strong two-factor authentication
- a single, anonymous, hardware-based cryptographic PassKey
- encrypted, fragmented, globally-distributed cloud storage, and
- extensibility to other directory systems

offers an ideal combination of user convenience, IT admin ease of installation and maintenance, and opportunities for multifaceted future expansion and integration.

Finally, because the user's PassKey neither stores personally identifiable information nor retains any application-specific data, it may be used for authentication into an unlimited number of applications both within and outside the organization. An application cannot obtain from the PassKey — or from WWPass secure storage — any information about other activities of a user. For example, additional WWPass-enabled solutions such as the following can be accessed using a single PassKey while keeping the information within each solution siloed:

- 1- and 2-factor website log-in
- Desktop PC authentication (using WWPass Security for Desktop)
- Email digital signing and encryption (using WWPass Security for Desktop)
- VPN authentication, including Juniper VPN Appliance
- Encrypted cloud storage (using Personal Secure Storage)

Free WWPass-provided SDKs allow website and other application developers to similarly integrate PassKey authentication and secure cloud storage services.

4.1 The future of wwGate

wwGate 2.0, will include support for LDAP and openLDAP servers, expanding even further the range of integration possibilities for smaller enterprises as well as organizations currently using multiple directory systems. SAML single log-out is scheduled for a future release.

What if your company's directory system or critical app isn't supported? WWPass welcomes inquiries for supporting alternative X.500 directory systems and other web applications in order to ensure that ongoing development of wwGate continues to be driven by the needs of the market. Please contact **sales@wwpass.com** for more information on how we can integrate with your needs.

5 Ready to take the next step?

With user security concerns at the forefront of consumer and business consciousness, there's never been a better time to invest in safeguarding your enterprise. To learn more about wwGate, or to obtain a customized solution and quote for your organization, please contact **sales@wwpass.com**.

About WWPass

WWPass solves the information security infrastructure's biggest deficiency by conveniently, yet securely, protecting both users and data. With just one self-managed PassKey, the user easily authenticates into any number of enabled local or cloud-based applications — no more username/ password combinations to remember! WWPass' patented authentication and cloud storage technologies keep both the application's data and user's identity separated and hidden from all other applications, preserving both user and application privacy. By integrating WWPass technology into their applications, organizations protect two critical assets: their data and their users.
Learn more at wwpass.com.

WWPass Corporation
1155 Elm Street
Manchester, NH 03101
+1.603.836.4932 or
+1.888.997.2771
wwpass.com

[i] Towards a Trustworthy Digital Infrastructure for Core Identities and Personal Data Stores by Hardjono, Greenwood and Pentland
https://www.wwpass.com/wp-content/uploads/hardjono-greenwood-coreid.pdf

[ii] How WWPass Works
https://www.wwpass.com/wp-content/uploads/WWPass_Authentication_How_It_Works.pdf