imprivata®
OneSign

Passwords,
the weakest link
in your enterprise security

Password security and secure network access are major issues for most organizations. Add to this regulatory compliance—Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBA), and Basel II—and the problem is even more demanding.

For organizations that need to strengthen user logon security to local desktops and remote networks, Imprivata® OneSign™ and DIGIPASS® by VASCO® combine to replace network passwords with two-factor authentication that secures access for users regardless of whether they are online and connecting to the local network, offline and logging onto their laptop, or for VPN access from any computer—and, the solution is easy to use and cost effective.

- Imprivata OneSign is an appliance that provides user authentication and access management to IT networks, applications and IT/Building security that improves security access management, and compliance.

- Imprivata OneSign Authentication Management replaces static Windows and remote access VPN passwords with a broad range of strong authentication options, including integrated management for One-Time-Password (OTP) tokens, finger biometrics, smartcards, and building access cards.

- DIGIPASS by VASCO is a family of strong authentication devices that boosts security for Windows networks while providing unmatched user acceptance.

- As user acceptance is crucial for the success of security implementations, DIGIPASS tokens are extremely easy to use. The user simply presses one-button to generate a one-time password to remotely log into an application, website or network.

Together, OneSign and DIGIPASS help organizations effectively combat weak network logon by replacing static or paper based password systems for both local and remote network logon, and online/offline computer logon. Now, your organization can economically deploy a comprehensive, scalable, high performance two factor authentication solution for secure network access.

## ➔ Simplify the cost and complexity of managing network access security

Integrated VASCO DIGIPASS Token Management

OneSign enables customers to quickly set up, deploy, and manage any type of DIGIPASS—for both remote and local network authentication. No additional servers are needed.

Customers can enroll ANY DIGIPASS for network authentication use with OneSign. It's quick. It's easy. There's nothing else to buy.

OneSign's support for DIGIPASS includes a Web-based interface for token management, including:

- Importing DIGIPASS
- DIGIPASS assignment or self-enrollment
- Creating and assigning authentication policies
- DIGIPASS and PIN management
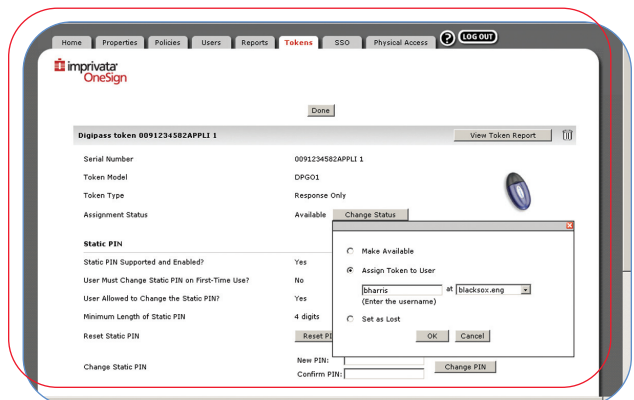
Assigning a DIGIPASS to a user

An unlimited number of DIGIPASS can be imported into OneSign at any time. Some DIGIPASS may support a static PIN feature of pre-set length that is used in conjunction with DIGIPASS security, and organizations have the option to use a static PIN or the primary network password as the second authentication factor.

For infrequent logins or if a user should lose their DIGIPASS, OneSign supports administrator-generated virtual DIGIPASS tokens. Administrator-generated virtual tokens can be sent to a user's mobile device in a text message (phone) or e-mail (PDA).

DIGIPASS users can be enabled for offline mode through policy. Other change status options include lost, available, or assigned to another user.

➔ Key Benefits

Single Authentication Management Platform

Combined, OneSign and DIGIPASS make authentication management flexible and easy. Secure network access can be deployed within hours without changing existing user directories. Policies are centrally managed and can be transparently applied in minutes. Users remain productive with minimal day-to-day management, and the user desktop experience is unchanged.

Easier Compliance and Reporting

With OneSign's built in monitoring, logging, and reporting, you can easily track which users logged in, when, and how. DIGIPASS specific reports show activity for defined periods of time. Detailed access logs and reports give organizations the ability to refine and strengthen security policies and enforce regulatory compliance across the enterprise.

Secure, Hardened Appliance

OneSign is shipped as a redundant appliance pair, pre-installed and ready to go for quick and easy deployment. Because the VASCO Controller is built in, there is no additional hardware or software to buy, install, integrate, or maintain.

Additionally, OneSign includes seamless real-time failover and can be restored from a back-up within minutes for disaster recovery.
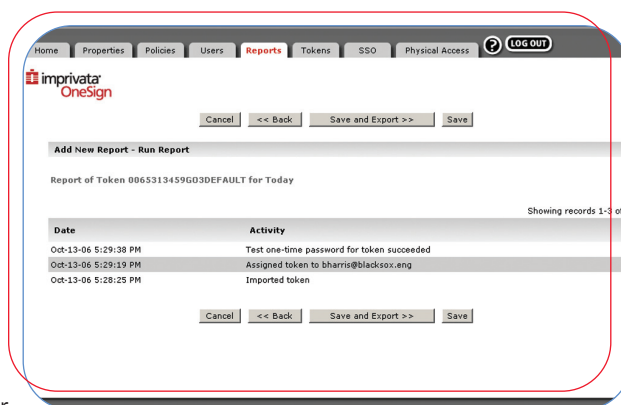
Generating and viewing a DIGIPASS activity report user

Lowest Cost Two-factor Authentication

OneSign's fast implementation, quick user adoption, and built-in support for multiple authentication methods delivers instant cost savings–and immediate financial return. As a self-contained appliance, OneSign delivers all the functionality needed to effectively implement and manage network authentication. There is nothing else to buy and no costly integration.

DIGIPASS tokens are cost effective. Long battery life results in reduced replacement costs and because DIGIPASS licenses never expire, you need not worry about budgeting for recurring license fee renewals other vendors charge for.

Seamless Upgrade to Single Sign-On and Integrated IT/Building Access

The power of Imprivata OneSign is that it's ALL in the box. Regardless of your initial start point, you can seamlessly enable additional capabilities as your needs evolve. With a simple license key, you can extend OneSign to seamlessly enable single sign-on to all enterprise applications and/or implement policy for allowing or denying network access based on a user's physical location and badge events, role, and/or employee status.

Imprivata OneSign Physical/Logical™ provides a radically easy, simply smart and uniquely affordable converged security solution for integrating network and building access systems for unified enterprise security management.

To learn more, visit www.imprivata.com, contact us at sales@imprivata.com, or call 1-877-663-7446.