



Trusting Mobile Users

At-A-Glance

What Mobile Users Want:

- Convenience – users want it to be easy to logon with their mobile device to get access to the resources they require

What Organizations Need:

- Reduced risk – mitigate threats from mobile devices that enter the enterprise
- Simple provisioning of authentication solutions in a distributed environment

Providing Strong Authentication for Convenient, Secure Mobile Access:

- Mobile soft tokens available for leading handset operating systems
- Servers for simple provisioning and management
- Support for Open Authentication (OATH) standards

Delivering Business Benefits

- Trust the identity of users connecting via their mobile devices and effectively manage their access
- Reduce operational costs associated with issuing, provisioning and managing physical tokens

How to Manage and Authenticate Users on Mobile Devices

As more and more work is done on the go with laptops, smartphones and tablets, enterprises are struggling to trust the identity of their distributed users and effectively manage their access. A strong identity assurance solution that can help enterprises ensure their users are who they say they are is one of the best ways to start to secure informational assets.

A complete solution must include a way to authenticate users who are not only logging on via their desktop, but also their mobile devices. Most people don't want to carry anything extra with them, so mobile tokens that can be quickly and easily installed on a mobile device they already have can enable enterprises to effectively secure that mobile access.

The Challenges Posed by Mobile Users

Due to the increasingly distributed, mobile and varied user population, the idea of a defensible perimeter is gone. It has been replaced by the need to allow users to access resources using many different devices, which to further complicate things may or may not even be owned by the enterprise. Most organizations are struggling to support access by all the devices that employees bring into the enterprise (BYOD). They need a way to verify the user of a device is and then manage their access; they also need to ensure it's done in a way that's convenient for the user, so it doesn't hamper productivity.

What IT Teams Need to Authenticate and Trust Users on Mobile Devices

While physical tokens and other one-time-password devices increase security, they add one more thing employees need to remember and worry about. Enterprises need a way to seamlessly integrate strong authentication into existing workflows. Mobile tokens that can be quickly and easily downloaded onto an employee's existing mobile device are an effective way for enterprises to trust the identity of the user and securely connect them to the corporate virtual private network (VPN).

HID Identity Assurance Portfolio delivers the strong authentication enterprises need to trust their users and enable them to connect to the VPN via their mobile devices.

- Mobile soft tokens (4TRESS AAA or 4TRESS AS) can be pushed out over the network and quickly downloaded by users, with replacement for life with a current maintenance contract. Users simply type in a number (their token) when they want to connect via their mobile device to corporate resources. Mobile Soft Tokens are available on leading handset operating systems, including RIM BlackBerry®, Apple® iOS (for iPhone® and iPad), Google Android, Windows Mobile, and many other Java 2 Platform, Micro Edition (J2ME) enabled devices.

- Our servers simplify the overall management of the solution, supporting user self-provisioning and enabling enterprises to automate the way tokens are provisioned and de-provisioned to keep their security in force.
- Support for the Initiative for Open Authentication (OATH) HMAC-Based One-Time Password (HOTP) algorithms ensures interoperability with existing authentication infrastructure.

The Business Benefits of Deploying Authentication for Mobile Identities

Soft Tokens provide unique benefits for organizations that want to leverage devices that their users are already carrying, including smart phones, PDAs, and laptops. Soft Tokens provide businesses a simple and efficient solution for the distribution, activation, and reuse of tokens for strong authentication via mobile devices. They deliver:

- Strong security to protect access via mobile devices to enterprise resources.

- Reduced operational costs – enterprises can use the software to reduce their provisioning costs, since they don't need to issue or ship a physical token. Self provisioning and the web self-help desk can help reduce expensive calls to IT and support.
- Smooth migrations from existing one time password (OTP) infrastructures to help enterprises leverage their current authentication investments.
- Simple, convenient user experience – they don't have to remember passwords or change them every month for VPN access, they can simply type in a number (token) and get connected.



Learn about HID Global's green initiatives
hidglobal.com/green



HID Global

North America: +1 949 732 2000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +49 6123 791 0
Asia Pacific: +852 3160 9800
Latin America: +52 477 779 1492

ActivIdentity

Americas: +1 510 574 0100
US Federal: +1 510 574 0100
Europe: +33 (0) 1 42 04 84 00
Asia Pacific: +61 (0) 2 6208 4888

hidglobal.com actividentity.com

ASSA ABLOY

An ASSA ABLOY Group brand

© 2012 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, and the Chain Design are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

© 2012 ActivIdentity. All rights reserved.

20120910-OTPMobile-authentication-uc-en-ai