



## DigitalPersona Product Brief

# Strong RADIUS Authentication with DigitalPersona® Pro

An introductory technical overview to the DigitalPersona solution for Two-Factor RADIUS Authentication.

December 2010

DigitalPersona Pro is a leading centrally-managed suite of security solutions that protects data and controls access to PCs and applications. It simplifies management of solutions like disk encryption, strong authentication, single sign-on, and more thus helping achieve compliance and lower security-related IT costs.

This document is intended to provide a high-level, technical overview of how DigitalPersona Pro's RADIUS authentication module works.

# Strengthening authentication for RADIUS access

## Introduction

With DigitalPersona Pro, you can improve the security of existing Virtual Private Networks or other RADIUS applications (such as Citrix, Outlook Web Access, and others) by adding authentication based on one-time passwords.

At a high level, adding two-factor authentication to an existing RADIUS solution requires the following steps:

- IT has to provide users with the means to generate the one-time-password (OTP)
- Users have to provide the one-time password together with their logon credentials at logon into the RADIUS application
- The one-time password has to be validated “in real time” when a user tries to log on

## Generating one-time passwords

DigitalPersona Pro supports a variety of methods for users to generate the OTP required at logon. It supports virtually any device or method that is based on OATH-compliant one-time passwords.

A typical example of supported devices include dedicated hardware tokens, of the type users typically carry attached to their key fobs. Leading token providers such as Vasco® or Quest® use OATH-compliant algorithms to generate the one-time password in their devices.



In addition, DigitalPersona Pro lets users use a broad set of smartphones as one-time password generating devices. On those devices, the one-time code is typically generated by a dedicated application that runs on the phone. Examples of supported smartphones include:

- BlackBerry®
- iPhone®
- Windows® phones
- Palm® smartphones

Finally, DigitalPersona Pro allows Administrators to configure the system so that the one-time password is automatically generated on the user’s PC, typically upon successful user authentication using some form of strong identity methods that DigitalPersona Pro supports.

For example, IT Managers may leverage the fingerprint readers that come built-in on many laptops and require users to provide their password AND swipe their finger in order to submit their credentials and an OTP generated “on-the-fly”.



Overall, DigitalPersona Pro offers market-leading flexibility in the deployment and configuration of methods users can leverage to generate and provide the one-time password. This allows Administrators to choose the configuration that best fits their needs and

their organization’s preferences in terms of balance between security and usability.

**Submitting one-time passwords**

DigitalPersona Pro supports different user experiences that largely depend on the one-time password generation system the IT Manager chooses to deploy.

With dedicated tokens or smartphones, users are typically prompted to type the one-time password on a dedicated dialog box that appears during the logon process.

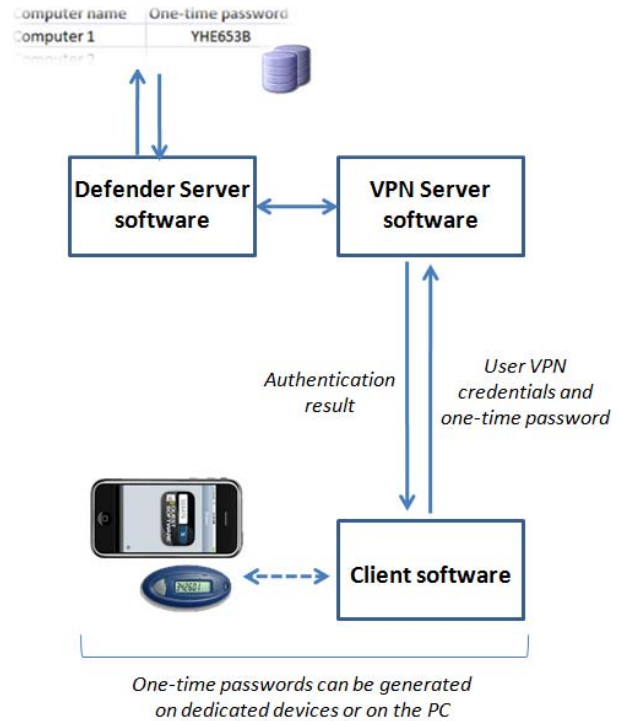
When the one-time password is automatically generated on the user’s computer, the IT Manager can leverage DigitalPersona Pro’s Password Management functionality to require user authentication (e.g. with password and fingerprints, smartcards, or any other combination of supported credentials) and then automatically submit RADIUS credentials and the one-time password.

**Validating one-time passwords**

The security value of adding one-time passwords to RADIUS applications largely depends on the fact that the one-time password is validated “on-the-fly” during the user logon process.

Regardless of whether it is automatically generated on the user’s computer and then submitted, or manually typed by the user based on the output of a smartphone application or a hardware token, the one-time password is sent from the managed computer to the RADIUS application together with the user’s credentials.

Digitalpersona Pro’s RADIUS plug-in routes the one-time password to the DigitalPersona Defender Security Server for validation. The Defender server validates the one-time password by tying it to the user for which the authentication request was submitted.



**Figure 1 - Example of OTP validation with RADIUS VPN authentication**

In the case of a successful one-time password validation, a positive confirmation is provided to the RADIUS application that then verifies the user credentials. Upon successful authentication, the corresponding feedback is sent to the client and the secure communication channel is established.

**More questions? Contact us**

DigitalPersona is looking forward to hearing from you and answering your questions. Contact your Account Manager or [sales@digitalpersona.com](mailto:sales@digitalpersona.com) to learn more.