



DigitalPersona Product Brief

User identification with DigitalPersona® Pro

An introductory technical overview to DigitalPersona Pro user identification and shared PC logon functionality

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 DigitalPersona Pro's user identification functionality.

Introduction

Authentication vs. Identification

Generally speaking, authentication is the process of ensuring that a known user is indeed who he claims to be. Identification, on the other hand, is the process of recognizing an unknown user.

With no information other than the credential submitted into the system, an identification system must be able to associate the submitted credential to a specific user, and then verify its conformity with the user information stored in the database.

For the optimal balance between security and ease of use, DigitalPersona Pro Enterprise allows user authentication by leveraging credentials such as fingerprints, cards, and other methods. When a user wants to access business resources protected with DigitalPersona Pro, he is prompted to provide such credentials. This information is matched against the information stored in this user's records; in the case of positive matching, the user is granted access. DigitalPersona Pro's identification functionality extends this principle by allowing for identification of a user out of any subset of the users enrolled with DigitalPersona Pro. The system can seamlessly scale up to the entire Active Directory environment with virtually no deterioration in performance.

Authentication vs. Identification

At-a-glance

- **Authentication** – Verifying the identity of a known user, based on a set of credentials.
- **Identification** – Recognizing an unknown user, based on a set of credentials.

Why identification?

Strong authentication provides a highly accurate method of verifying that the person gaining access to applications, processes or property is who they say they are. The next step is to increase the number of individuals that can gain access to applications or resources, while still ensuring security and accuracy.

Identification enables users to quickly gain access to resources without having to first input or show their identity – thus completely replacing users' username and password with one or more strong authentication credentials.

The accuracy and speed of identification is particularly useful where there is the possibility of having groups of users accessing a shared resource, such as:

- Manufacturing or workplace entrances
- Learning locations and classrooms
- Kiosks in hospitals and clinics
- Workstations in call centers

DigitalPersona Pro's identification – how it works

When DigitalPersona Pro Enterprise is enabled with identification functionality, user identification is made possible by modifying how the system works. In this paper, we will focus on the case of a user identified based on his biometric characteristics – namely, his fingerprints.

The main changes to the normal authentication workflow include:

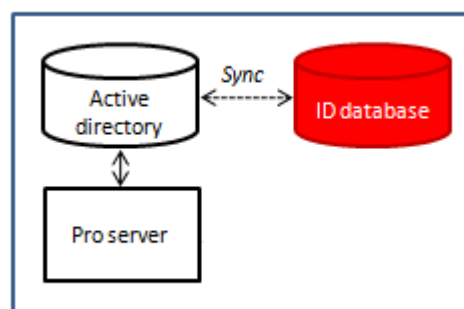
- A new fingerprint database is created within the DigitalPersona server.
- Users' fingerprint templates are indexed to "categorized" based on their characteristics.
- The process of matching fingerprint templates within the DigitalPersona Pro server is modified to take into account the presence identification functionality.
- Upon an identification request, a dedicated algorithm is run to associate a fingerprint template from an unknown user to the user that template belongs to.

In what follows, we provide a high level description of how the the DigitalPersona Pro server in an identification workflow works by describing the four items listed above.

Creation of an ID fingerprint database

For identification purposes, DigitalPersona Pro Enterprise copy all fingerprint templates stored in the Pro Active Directory user database. Specific users' fingerprint data can be excluded from the identification list if needed. The Pro ID Server maintains all fingerprint templates in memory to allow for high-speed identification.

At initial launch, DigitalPersona Pro Enterprise searches the entire user database in Active Directory and creates a first "snapshot" of the fingerprint template database. Then, every time user records in Active Directory change – for example, because users or fingerprints are added or removed – a notification is sent to allow for continuous synchronization of the AD and identification databases.



Indexing of fingerprint template information

The fingerprint templates stored in the ID database are indexed based on a patent-pending algorithm. The purpose of this categorization is to "group" templates based on a defined set of characteristics.

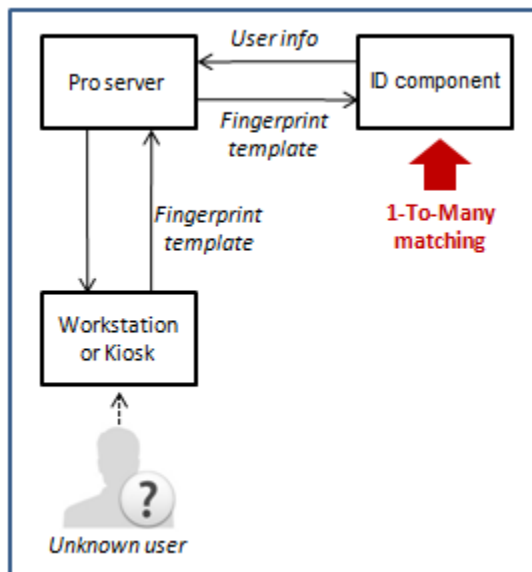
As in many other technology fields (e.g. webpage searches over the Internet), indexing is at the basis of high speed search and fast information retrieval. When all fingerprint templates are processed and indexed, the resulting indexing tables allow for fast searches of fingerprint templates, based on a given set of characteristics that is used as "input" of the search process.

Treatment of user authentication requests within the DigitalPersona Pro environment

When the user scans his finger on the fingerprint reader, the image of his fingerprint is processed on the local computer and fingerprint template information is extracted. The fingerprint template is then sent to the DigitalPersona Pro server over a protected channel.

In a standard DigitalPersona Pro environment, the server would perform user authentication by matching the fingerprint template received from the client software with the fingerprint template stored in Active Directory for a known, specific user.

When the identification functionality is enabled, Digit passes the identification request to the ID Server add-on.



User Identification through 1-To-Many matching

Within the identification component of DigitalPersona Pro Enterprise server, the identification process begins when a fingerprint template from an unknown user is received. The incoming template is processed to derive its key characteristics. This information is then used to “navigate” the indexing tables to find which template in the database best matches these characteristics.

Once this template is identified, the DigitalPersona Pro Enterprise server completes a reverse look-up to identify the user this template belongs to. The user information is then used to release the credentials associated to this user and grants access.

High performance for unparalleled experience

DigitalPersona Pro Enterprise’s identification functionality allows for the best user experience thanks to a unique combination of high speed and high accuracy. Depending on the processing power made available to the system, DigitalPersona Pro’s identification components can scale up to many thousands of users seamlessly.

Database size	Average identification time
2,000	0.2 seconds
20,000	0.5 seconds

For more information on system requirements, please refer to the DigitalPersona Pro Administration Guide or contact your DigitalPersona Account Manager.