AUTHASAS™
AUTHENTICATION AT YOUR SERVICE

Architecture Overview

Authasas Advanced Authentication®

Biometric Logon to Microsoft® Vergence

September 2010

Authasas
Advanced Authentication®

Asterweg 19D12
1031 HL Amsterdam
The Netherlands

www.authasas.com
info@authasas.com

t: +31 (0)26 373 61 70
f: +31 (0)20 524 13 68

© 2010 Authasas

Introduction

Securing access to medical applications and patient data remains a top priority for IT in healthcare. Sentillion has been providing Identity and Access Management solutions to healthcare organizations since 1998. They have revolutionized how medical providers access and manage clinical systems. In December, 2009, Sentillion was acquired by Microsoft® to deepen the company's presence in the growing market for healthcare IT systems. Through a partnership with Authasas® and Bio-key®, Microsoft® customers are provided a fully integrated systems which incorporates market-leading enterprise biometric authentication with Microsoft® Vergence.

The purpose of integrating Authasas® with the Vergence Authenticator is to provide biometric fingerprint authentication as a replacement for the Windows® and/or Vergence Password. Users are able to authenticate to Vergence by using a combination of username + biometric, or through the use of active or passive proximity badge + biometric. By leveraging technology from Bio-key®, interoperability and compatibility is provided for over 50 biometric readers. Through the integration of Authasas Advanced Authentication® with Bio-key's Web-key® technology, a powerful One-to-Many biometric solution provides both identification and authentication; and eliminates the requirement for a username at logon.

Several implementation options available to support combinations of:

- Dedicated workstations and laptops
- Kiosk and shared workstations
- 1:1 Biometric authentication / verification
- Proximity card + biometric authentication
- 1:n Biometric identification/authentication

Solution Overview

For the purpose of this document, the reader is assumed to possess a fundamental understanding of the Microsoft® Vergence Clinical Workstation. This solution overview and architectural descriptions will focus on the implementation of biometric authentication using Authasas Advanced Authentication® with Bio-Key® BSP (Biometric Service Provider) and Bio-key® Web-key® technologies.

Vergence Authenticator Overview

Vergence Authenticator provides strong authentication that allows you to control access to user workstations, secure the desktop when not in use, and provide single sign-on and context management among Vergence-enabled applications (CCOW-compliant applications and applications accessed through a Vergence Bridge®.

A workstation that is using the Vergence products to accomplish these activities is called a Vergence-enabled desktop.

Authasas Advanced Authentication Overview

Authasas Advanced Authentication® is a software solution that enhances the standard user authentication process by providing an opportunity to log on with various types of authenticators including biometric fingerprint, smart cards, contactless/proximity cards, and USB Flash drives.

Authenticators are more secure than passwords, because they do not complicate logon procedure, but allow users to give up passwords and thus keep access to their information secure. Authasas Advanced Authentication® gives users an opportunity to use hardware authentication devices and retains an opportunity to log on by password (on permission from the system administrator). Authasas® provides a biometric fingerprint authentication module to the Vergence Authenticator.

Bio-key Overview

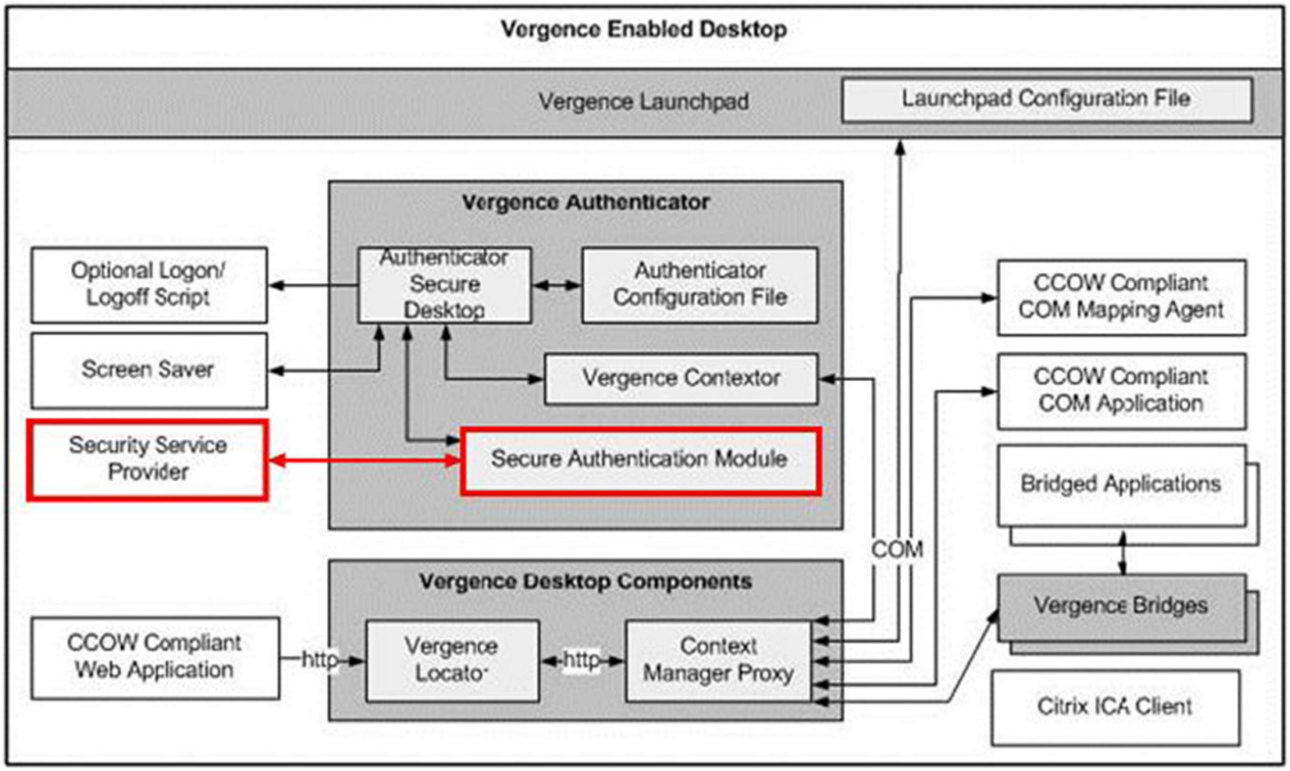
BIO-key's patented Vector Segment Technology™ (VST) with True User Identification (TUI™) is a fingerprint algorithm and database development toolset that allows you to tightly integrate biometric verification and/or identification into new or existing applications and middleware.

BIO-key International's implementation of the Biometric Service Provider (BSP) is based on BIO-key's patented Vector Segment Technology™ (VST™), the industry's fastest, most accurate and reliable fingerprint algorithm.

BIO-key's BSP provides an easily implemented, BioAPI compliant interface for applications. It supports both verification and identification modalities. BIO-key® has taken great efforts to extend this BioAPI to include user identification. Additionally this API's user enrollment and identification screens can be easily customized for a streamlined and seamless application experience.

Architectural Design

The following diagram represents the Vergence application on a client workstation.


Vergence Enabled Desktop
Vergence Launchpad
Launchpad Configuration File
Vergence Authenticator
Optional Logon/ Logoff Script
Authenticator Secure Desktop
Authenticator Configuration File
Screen Saver
Vergence Contextor
Security Service Provider
Secure Authentication Module
CCOW Compliant COM Mapping Agent
CCOW Compliant COM Application
Bridged Applications
COM
Vergence Desktop Components
Vergence Bridges
CCOW Compliant Web Application
http
Vergence Locato
http
Context Manager Proxy
Citrix ICA Client

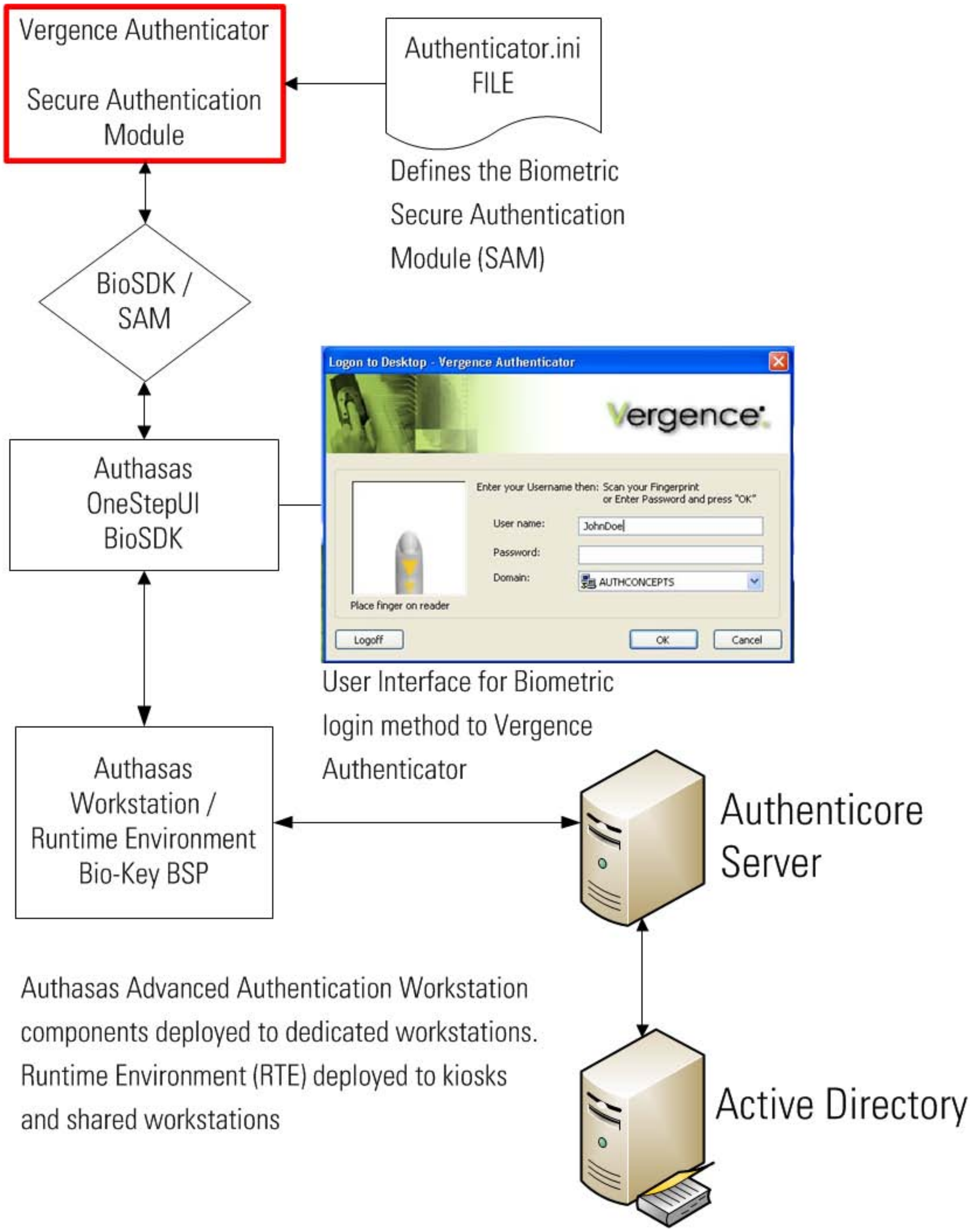
Secure Authentication Module (SAM) – Gathers user credentials, authenticates user credentials with security services, and changes user passwords, depending on the identification and authentication technologies used.

Authasas Advanced Authentication® is a Security Service Provider and is integrated with Vergence through interfaces provided via the Secure Authentication Module.

As a critical component to the overall security of the Vergence Enabled Desktop, biometric matching technology for verifying a user's identity is unparalleled in accuracy, guarantying a positive match before granting access the system or application. The interface is user-friendly and delivers high performance to the healthcare personnel who demands immediate access to patient data and clinical applications.

Despite the additional layer of security implemented by this system, authentication to the Vergence Desktop takes less time than traditional password-based authentication.

The following diagram outlines the Authasas interface to the Vergence Secure Authentication Module, including the client and user interface components and backend server components required to support username + 1:1 fingerprint authentication as well as proximity card + fingerprint.



Defines the Biometric Secure Authentication Module (SAM)

Logon to Desktop - Vergence Authenticator

Enter your Username then: Scan your Fingerprint
or Enter Password and press "OK"

User name: JohnDoe

Password:

Domain: AUTHCONCEPTS

Place finger on reader

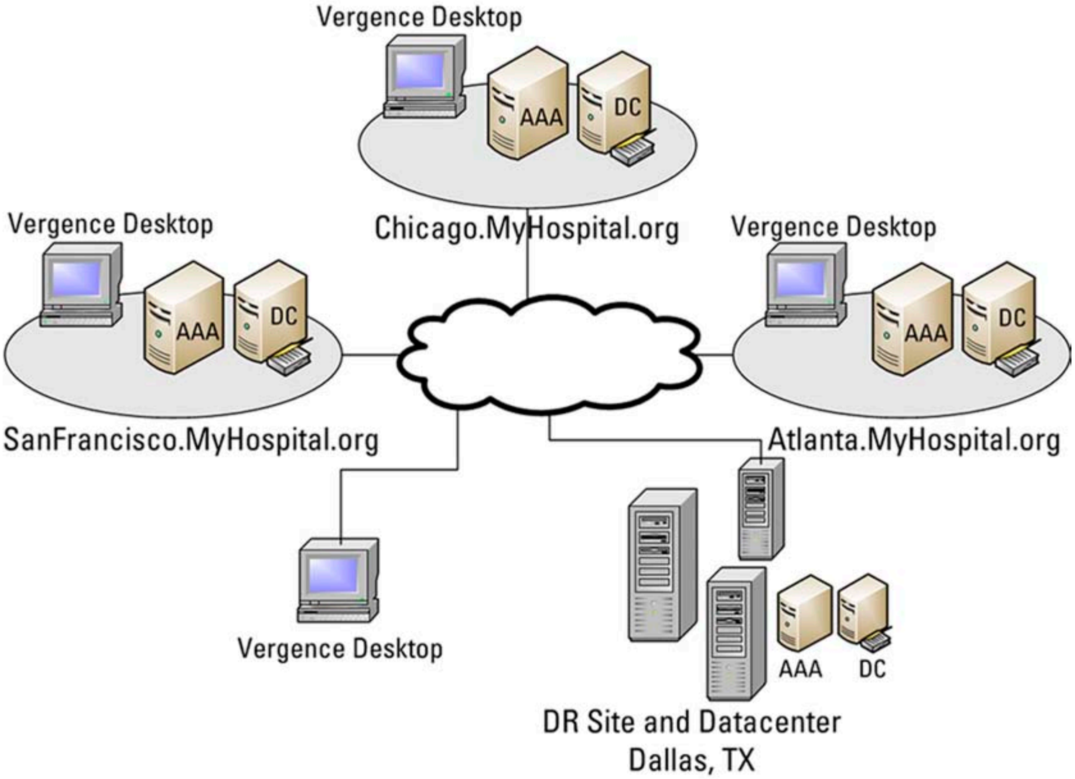
User Interface for Biometric login method to Vergence Authenticator

Authasas Advanced Authentication Workstation components deployed to dedicated workstations. Runtime Environment (RTE) deployed to kiosks and shared workstations

In addition to speed and accuracy, the biometric authentication system's architecture allows for a distributed deployment for fault tolerance and high availability. The Authasas® infrastructure components leverage the Microsoft® network architecture, and minimize the dependence on proprietary systems to deploy to large and small networks.

Authasas® can support a small deployment of a few hundred users on a single site, and can scale to support tens of thousands of users across dozens of sites.

The following diagram describes the Authasas® Backend Server integration into a Microsoft Network. Just as each site would be supported by a domain, controller, so would each site be supported by an Authasas Advanced Authentication® (AAA) server.



All biometric data is stored in Active Directory for availability at each site, however authentication requests will be managed locally to each site and fail over to a remote or DR site should the local server become unavailable.

Remote workstations will authenticate to the AAA server in closest proximity to the DC to which Windows authentication would occur.

One to Many Biometric Identification

Advanced Functionality

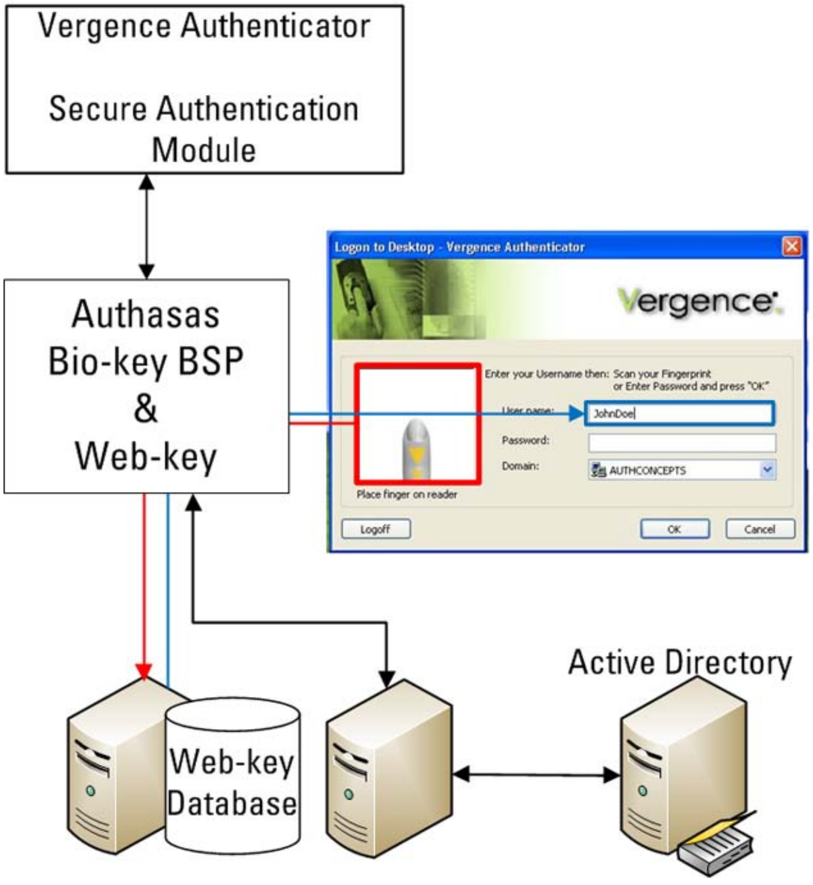
The previous sections describe the architecture for the standard Vergence user lookup and authentication for users in Active Directory. In those examples, the user provides the username or presents a proximity card with the stored username, then provides a fingerprint to the system. Since Active Directory does not provide the type of indexing that would be required to perform 1:n biometric lookup, this functionality can be obtained (as an upgrade) through the integration of Bio-key® Web-key® into the deployment design.

Leveraging BIO-key's Intelligent Image Indexing™ Technology, WEB-key® delivers the speed and accuracy required to perform millions of fingerprint matches per second. Web-key® will biometrically identify the user by matching the fingerprint against templates stored in the Web-key® database. Web-key will provide the user's identity to Authasas®, and Authasas® will perform the biometric authentication to the Vergence Enabled Desktop.

This 2-tiered approach provides the user with a secure and simple method of accessing the Vergence Desktop with performance and accuracy never before available in an identity management solution.

1:n Architectural Design

The workflow depicted to the right provides a single step logon process for the end user, while performing two-step identification and authentication process before authenticating the user to the Vergence Desktop.



Enter your Username then: Scan your Fingerprint or Enter Password and press "OK"

User name: JohnDoe

Password:

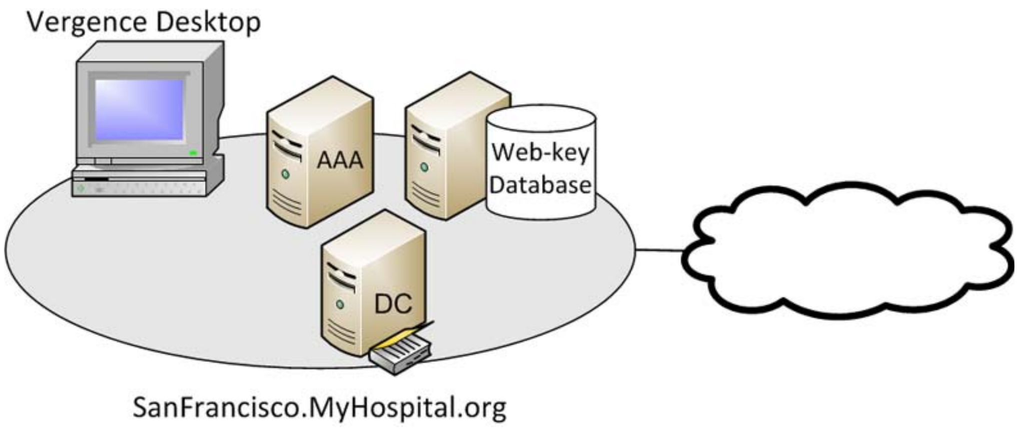
Domain: AUTHCONCEPTS

Place finger on reader

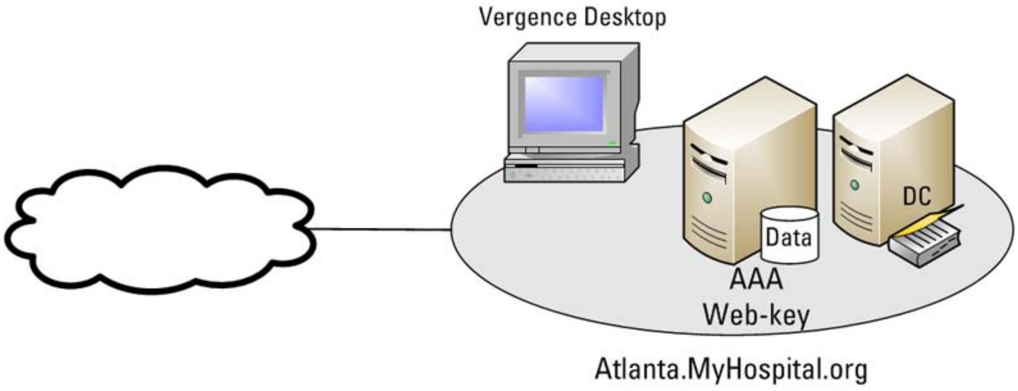
The Web-key® server may be deployed as a stand-alone server supporting multiple Authasas Advanced Authentication® servers, or both server components may be installed on the same server to consolidate hardware.

The following diagram depicts the same distributed network architecture, and includes examples of the three methods of implementing Web-key for 1:n matching and logon.

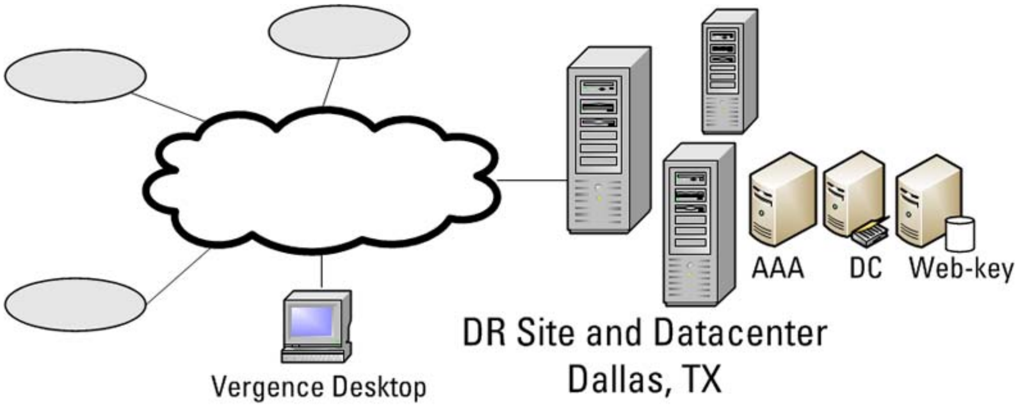
1. Dedicated Servers on local Site



2. Combined Servers on local Site

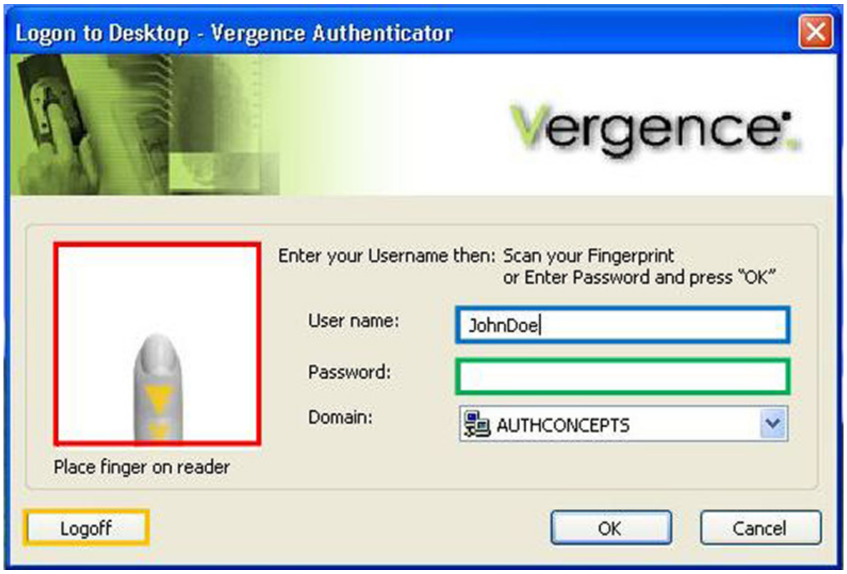


3. Dedicated Server at Datacenter servicing multiple sites



End User Experience

As depicted in diagrams throughout this document, the biometric user interface is a simple to use, one-step integration into the Vergence Authenticator via the OnestepUI.dll. Users are presented the same interface regardless of whether the Vergence Enabled Desktop is deployed in personal workstation (dedicated) mode, or in shared workstation (kiosk) mode. Since both modes are supported in the same deployment, the user experience will be simplified by only having to be familiar with a single user interface.



Enter your Username then: Scan your Fingerprint
or Enter Password and press "OK"

User name: JohnDoe

Password:

Domain: AUTHCONCEPTS

Place finger on reader

Animated biometric prompt: displays feedback as user presents fingerprint, and helps users to visualize their finger placement and quality of the image.

Username: depending on deployment strategy, this field may be

- Manually filled in by user
- Automatically populated by proximity card (SentillionGina.dll)
- Automatically populated buy 1:n match using Web-key

Password – this field remains usable to ensure backup or alternative login method via password is available.

Logoff – button remains available to support Vergence User-Switching. *Displays Shutdown option at Windows Logon.*

Conclusions

The fingerprint biometric authentication solution delivered by the partnership between Microsoft® and Authasas® + Bio-Key® delivers a highly usable biometric solution that scales to fit healthcare networks of all sizes. By providing multiple options for logon behavior and support for proximity cards as well as One-to-Many biometric matching, the combined solution may be tailored to suit the unique requirements of each healthcare organization.

The solution architecture is flexible, designed to be tailored to leverage existing Microsoft network architecture. Hardware support and interoperability allows each organization to leverage existing biometric fingerprint readers, and allows for reader selection from over 50 supported devices.

Deployment and support services are provided to ensure that the project is deployed within schedule and budget.

AUTHASAS™
AUTHENTICATION AT YOUR SERVICE

Trademarks

Microsoft, Active Directory, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Bio-key, Web-Key, Vector Segment Technology (VST), True User Identification (TUI), and Intelligent Image Indexing are either registered trademarks or trademarks of Bio-key International, Inc. in the United States and/or other countries.

Authasas, Authasas Advanced Authentication are either registered trademarks or trademarks of Authasas in the United States, The Netherlands, and/or other countries.

© 2010 Authasas. All rights Reserved