AUTHASAS™
AUTHENTICATION AT YOUR SERVICE

Architecture Overview

Authasas Advanced Authentication®

Advanced Authentication to Oracle® Enterprise Single Sign-on Logon Manager

March, 2011

Authasas
Advanced Authentication®

Asterweg 19D12
1031 HL Amsterdam
The Netherlands
+31 (0)26 373 61 70

106 E. Sixth Street,
Suite 900,
Austin, TX 78701
USA
+1 (512) 322-5792

www.authasas.com
info@authasas.com

© 2011 Authasas

AUTHASAS™
AUTHENTICATION AT YOUR SERVICE

Introduction

Single Sign-on has become commonly accepted as the ultimate solution for the growing number of login and password-management challenges. Oracle ESSO-LM provides advanced technology, offering ease of use, cost savings and enhanced password security. Integrating single sign-on with advanced authentication provides the enterprise with the peace of mind that all managed user credentials are securely protected by industry standard, strong authentication methods.

The purpose of integrating Authasas Advanced Authentication with Oracle ESSO-LM is to replace the Windows password which protects all ESSO-LM managed credentials with several authentication methods that are both secure and easy to use. Such methods include, biometric fingerprint, PKI and non-PKI smart cards, contactless smart cards, and even Flash drive + PIN technologies. ESSO-LM will leverage the new strong authentication method(s) for initial authentication, as well as for any subsequent authentication required by a single sign-on secure workflow, or when configured for re-authentication to an SSO-enabled application.

Though Authasas Advanced Authentication supports dozens of device types and multiple strong authentication methods, there has been an increasing demand for biometric fingerprint authentication and card-based authentication.

Biometric logon has “come of age” recently, and Authasas has dedicated its R&D efforts to ensure the enterprise stability, scalability, and usability for biometric authentication. Including market-leading template matching algorithms and device compatibility provided by BIO-key’s Biometric Service Provider (BSP).

Contact and contactless smartcards dominate the physical security market, and companies are increasingly interested in leveraging this investment to secure logical access.

AUTHASAS™
AUTHENTICATION AT YOUR SERVICE

Solution Overview

For the purpose of this document, the reader is assumed to possess a fundamental understanding of the Oracle ESSO-LM software. This solution overview and architectural descriptions will focus on the implementation of biometric authentication using Authasas Advanced Authentication with BIO-key BSP in a Microsoft Active Directory environment.

Oracle® Enterprise Single Sign-on Logon Manager

Oracle® ESSO Logon Manager (ESSO-LM) provides interfaces to network and computer logons as well as sign-on to applications, enabling users to log in one time with a single password. Once users are logged in, whatever application they open is served the correct ID and password transparently and automatically. This eliminates the need for users to remember and manage multiple user names and passwords for their applications, while allowing administrators to centrally manage passwords. The Oracle ESSO Logon Manager Admin Console interacts with the Logon Manager and facilitates management and administration of ESSO attributes.

Oracle® ESSO Kiosk Manager (ESSO-KM) provides initial user authentication and automatic user sign-off to kiosk environments, enabling secure kiosk computing at any location within the enterprise. The system monitors and protects unattended kiosk sessions from unauthorized access.

Authasas Advanced Authentication

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 an authentication module to Oracle® Logon Manager.

AUTHASAS™
AUTHENTICATION AT YOUR SERVICE

Authentication Methods

Authasas Advanced Authentication® provides the framework which supports virtually any strong authentication method as an independent module. This design approach allows existing methods to be enhanced, and new methods to be implemented. Therefore providing a future-proof authentication infrastructure that adapts to new technology and enhancements to existing technology.

Authenticore® Servers deployed in a domain or forest are flexible in the authentication methods that they support. A single server may be dedicated to supporting a single authentication method, or configured to support multiple methods.

Users may be enrolled in multiple authentication methods and utilize any specific authentication method as required by policy. Therefore, as an example, allowing biometric fingerprint authentication to certain ESSO-LM enabled systems and a smartcard authentication method to other ESSO-LM enabled systems.

Solution Architecture

Authasas Advanced Authentication® leverages a similar architecture to Oracle® ESSO Logon Manager in an Active Directory or AD LDS infrastructure. Like ESSO-LM, all credential data is stored in the corporate directory for high availability and redundancy. In addition to the directory components, Authenticore authentication servers are deployed to dedicated or shared Windows servers to support multi-factor authentication. Authentication servers are deployed as required to support the microsoft network topology, leveraging Microsoft® Sites to distribute the servers for load balancing and redundancy.

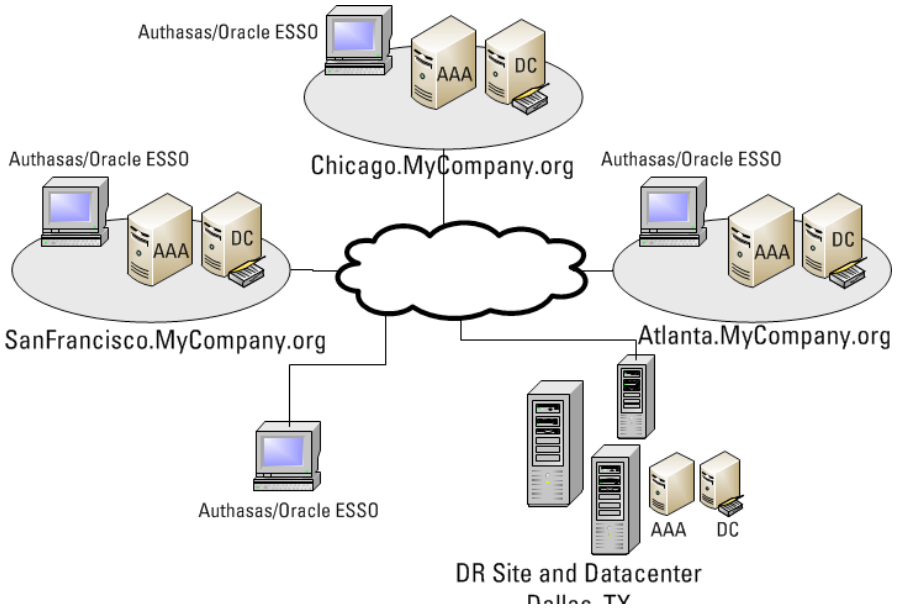
Authasas® Workstation provides the client components required to allow users to logon with a multi-factor method and device. These components are deployed to Windows® workstations, including VDI desktops. The Workstation components may also be deployed to terminal servers and Citrix XenApp / Xen Desktop servers to support strong authentication for hosted systems.

RTE (Run Time Environment) components may also be deployed independently on any system where strong authentication for Oracle® ESSO Logon Manager and Kiosk Manager is desired, but is not required for Windows® logon (GINA or Credential Provider).

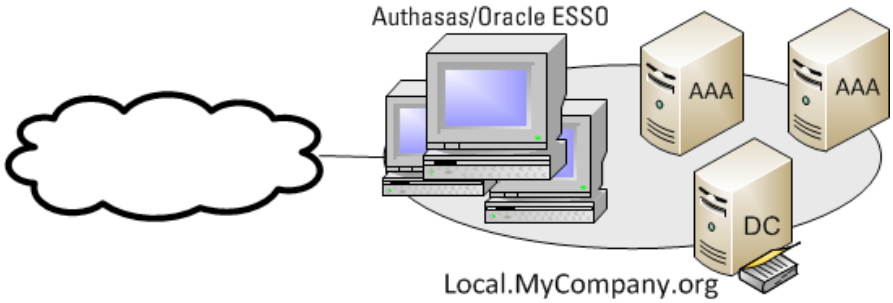
AUTHASAS™
AUTHENTICATION AT YOUR SERVICE

Deployment Topologies

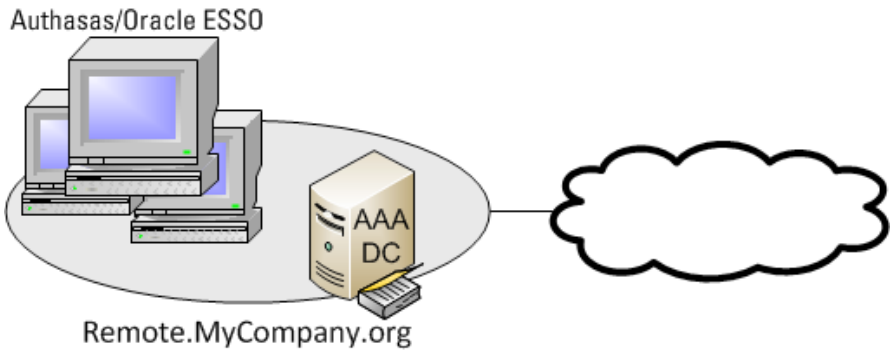
Distributed Enterprise Deployment, serving multiple sites + DR



Single LAN with redundant servers (shared or dedicated)



Small or remote site with authentication servers on DC's

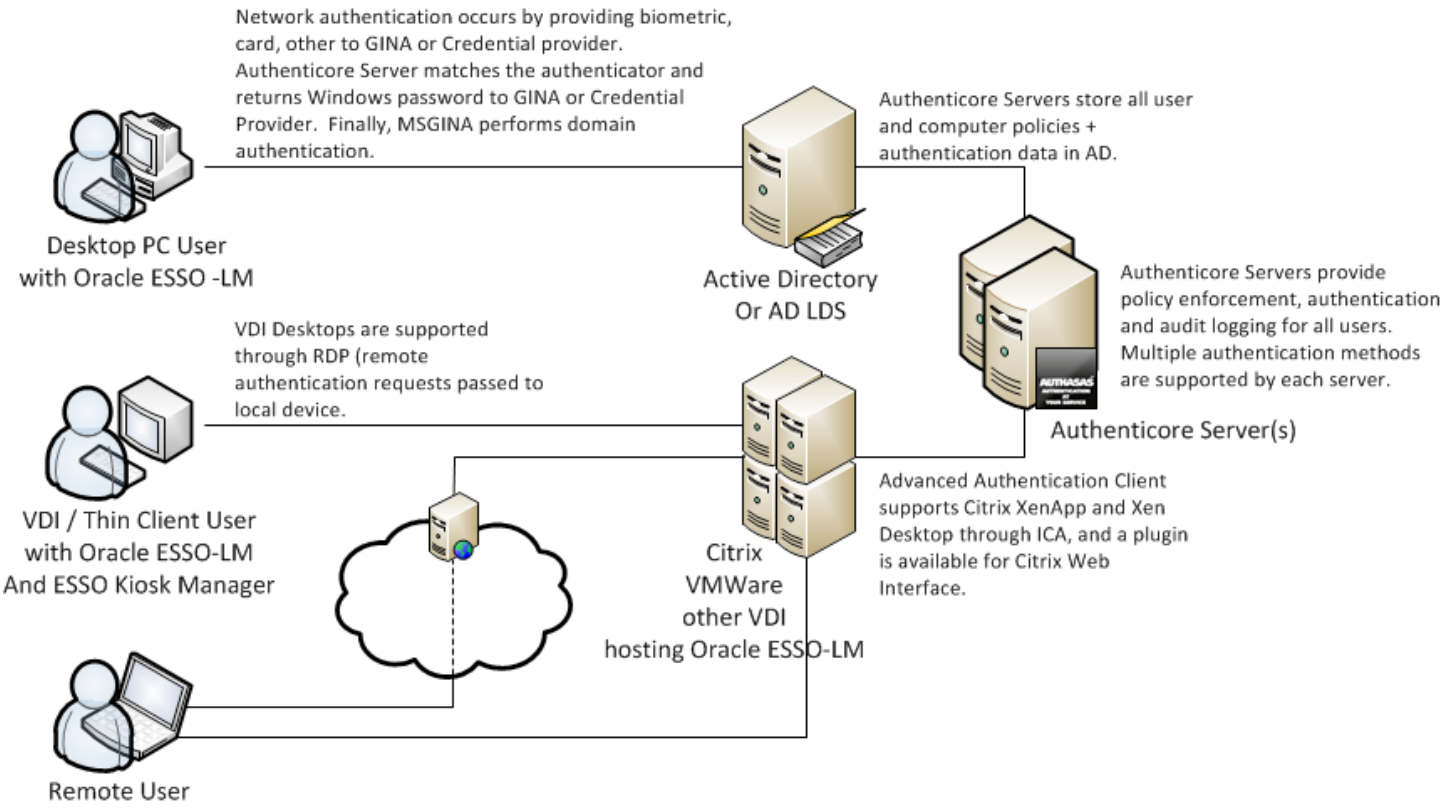


AUTHASAS™
AUTHENTICATION AT YOUR SERVICE

Client Architecture

Like Oracle®, Authasas develops technology based on a variety of client topologies. Today's users are often widely distributed and access network applications through many ways. Terminal Services and Citrix® have provided hosting options that centralize access to secured applications. Oracle® ESSO-LM and Authasas provide strong authentication to the hosting systems, as well as to the hosted applications themselves.

Virtualization has further centralized application hosting, and decentralized delivery. Authasas Advanced Authentication® supports remote authentication to Oracle® ESSO-LM from LAN and WAN connected systems and thin client terminals running Windows XPe and Windows Embedded Standard 7.

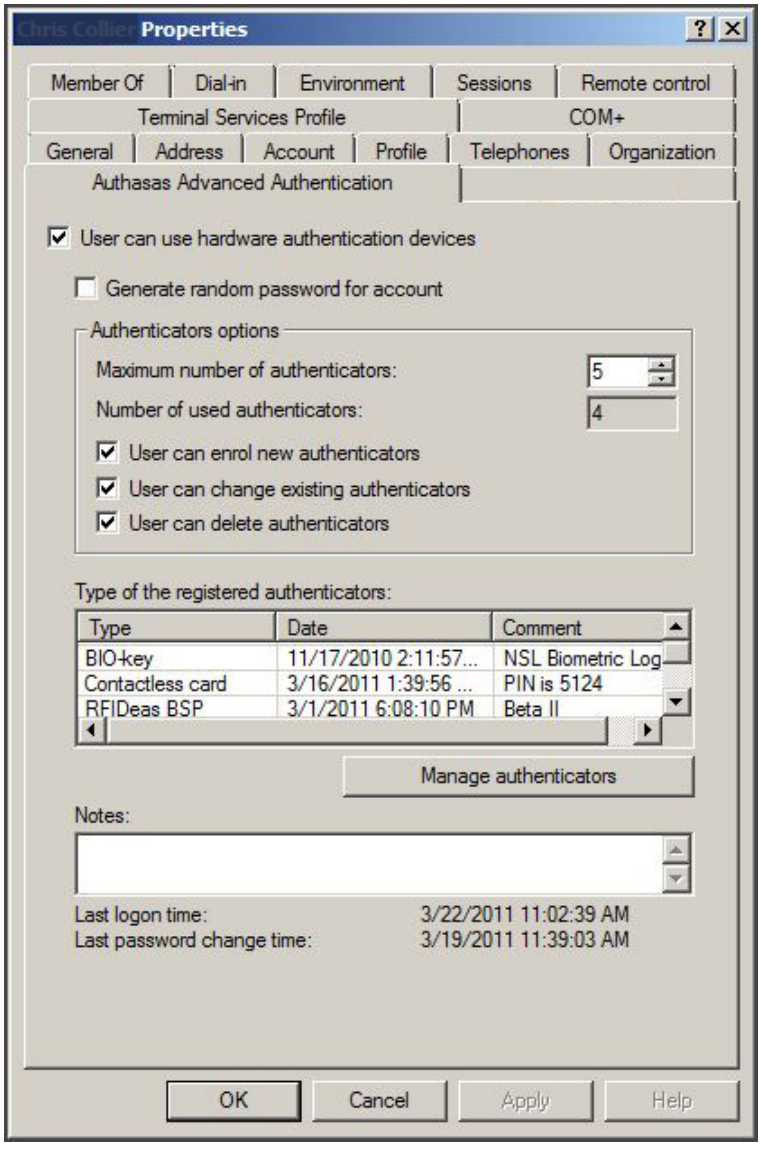


AUTHASAS™
AUTHENTICATION AT YOUR SERVICE

Administration

Both Authasas Advanced Authentication® and Oracle® ESSO Logon Manager leverage Microsoft® Directory Services and Lightweight Directory Services to store and manage user credentials. Oraclel® ESSO-LM manages application username and passwords, and Authasas® manages the strong authentication credentials and domain password.

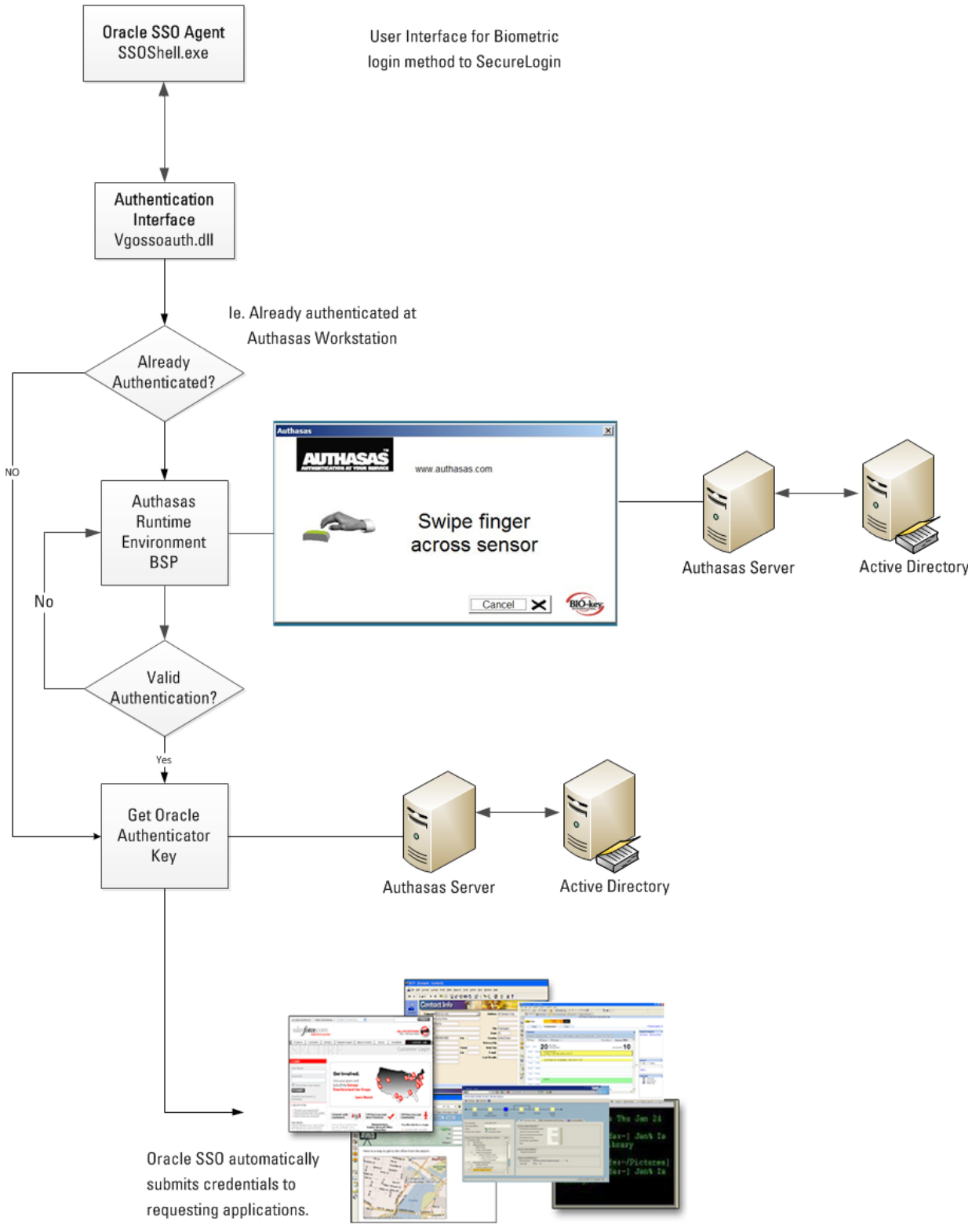
Authasas Advanced Authentication® provides Microsoft Management Console® Snap-ins to manage identity data stored in the directory . This allows for a high level of control from anywhere within the network to configure policies and perform routine credential management tasks such as centralized enrollment.



AUTHASAS™
AUTHENTICATION AT YOUR SERVICE

Workflow & Interface

The Diagram below outlines the workflow and required client interfaces to support biometric logon support to Oracle® ESSO Logon Manager.



Integration

Authasas® integrates with Oracle® ESSO Logon Manager through client-side interfaces as depicted in the previous diagram. This integration strategy provides the most flexible and minimally invasive method to a combined strong authentication single sign-on deployment. Localizing authentication requests to the client-side SSO solution, allows both Logon Manager and Authasas® infrastructures to deploy and scale infinitely.

Typical deployments are performed in phases to maximize acceptance of each technology, and to allow each technology to be used together, and independently as determined by unique requirements of separate user communities within the enterprise.

Adding, removing, and modifying strong authentication methods (i.e. biometric, smart card, contactless card, etc.) within Authasas Advanced Authentication® require no change to Oracle® ESSO-LM or the integration between both solutions. Further, multiple authentication methods may be deployed simultaneously with no modification to the Authasas® or ESSO-LM infrastructure. This allows one group of users, or one group of computers to authenticate via biometrics, while another group of users or computers authenticate using contactless smart cards.

Conclusions

The authentication solution delivered by the partnership between Oracle® and Authasas® delivers a highly usable authentication solution that scales to fit networks of all sizes. By providing multiple options for logon behavior and support for contact and contactless cards as well as biometric matching, the combined solution may be tailored to suit the unique requirements of each 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 hardware including support for over 50 biometric fingerprint readers, standards-compliant contact smart cards and readers, as well as virtually all contactless smart cards and readers.

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

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.

Oracle, is a registered trademark or trademarks of Oracle and or its affiliates in the United States and/or other countries.

© 2011 Authasas. All rights Reserved