



Saragosta

— it services —

IT Security Services



Password Management Self-Service

FastPassAD™: Enabling enterprise wide password synchronization

White Paper

Author: Richard Blackham

V1.0

Nov 2004

Saragosta IT Services Sp. z o.o.

Ilmet, Al. J. Pawla II 15 / 10-05, Warszawa
T: +48 22 697 79 70 E: Saragosta@saragosta.com

FastPassAD™: Enabling enterprise wide password synchronization

Abstract

The purpose of this document is to discuss options available for deploying a user self-service password setup and reset tool with a vendor agnostic backend functionality to push password changes from Active Directory. In particular the objective is to assist IT specialists planning identity and access management projects to gain the maximum ROI from a 'toe-in-the-door' approach where budgets may be limited. Selection of the best available technology is critical to successfully and seamlessly implementing a strategy that minimizes the impact on users and help desk personnel alike. The document also provides a brief overview of the roadmap envisioned for the development of the tool in cooperation with enterprise sized identity management solutions as well as an overview of the security issues that should be considered to maintain the integrity of a self-service tool based on Active Directory services.



FastPassAD™: Enabling enterprise wide password synchronization

Legal Disclaimer

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. However, because of the possibility of human or mechanical errors, IT InterGroup A/S does not guarantee the accuracy, adequacy, or completeness of any information in this publication, and is not responsible for any errors or omissions or the results obtained from use of such information.

Unless otherwise noted, the example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person, or event is intended or should be inferred.

IT InterGroup A/S does not endorse or accept any responsibility for the content or usage of links and references to any non-IT InterGroup A/S websites or technical documentation.

No part of this document may be reproduced, stored or transmitted in any form, by any means, or for any purpose, without the express written permission of IT InterGroup A/S.

IT InterGroup A/S, IT InterGroup, FastPass, **FastPassAD™**, their associated logos and all IT InterGroup product names and slogans are either registered trademarks or trademarks of IT InterGroup A/S. Other product or company names mentioned herein may be trademarks of their respective owners.

Saragosta IT Services, a member of the Saragosta Group represents IT InterGroup as solution provider and reseller in the Polish market as well as in the CEEMA region unless otherwise agreed.

Copyright © 2003-2004, IT InterGroup A/S. All rights reserved.

Last revised July 7, 2004.

IT InterGroup A/S

Gydevang 39
3450 – Allerød
Denmark
Tel: 0045 4810 0410
Fax: 0045 4810 0420
Email: info@itintergroup.com
URL: www.itintergroup.com

Saragosta IT Services Sp. z o.o.

Ilmet, Al. J. Pawla II 15 / 10-05
00-828 Warszawa
Tel: +48 22 697 79 70
Email: Saragosta@saragosta.com
URL: www.saragosta.com



FastPassAD™: Enabling enterprise wide password synchronization

Foreword

This paper sets out to show why password management projects can be key as enablers for generating the necessary appetite within an enterprise for full identity management projects incorporating:

- Role engineering
- ID Management
- Access management
- SSO to the portal environment
- Cross platform password synchronization
- Help Desk Integration

Whilst all, some or none of the above may apply to the type of project envisioned for your enterprise password management as a facilitator of fast ROI can play a critical role in the successful and speedy deployment of any of the functionalities listed above.

More especially, it has been seen by the author and IT InterGroup that the careful positioning of **FastPassAD™** as a tool capable of returning fast ROI can and does open the door to bigger and more far reaching projects.

Whereas the author would by no means wish to suggest that **FastPassAD™** could supplant the need for a full identity management deployment or replace the functionality of the enterprise provisioning tools, it can in some environments and in conjunction with data integration tools, prove itself a worthwhile low cost alternative.

FastPassAD™: Enabling enterprise wide password synchronization

Executive Summary

A smooth enterprise-wide rollout of **FastPassAD™** requires some analysis of the security practices in the organization and the management of the bottom line auditor requirements into the existing working habits of the administrators, help desk resources and user community.

Most organizations regard the implementation of new tools for empowering the users to setup and reset their own passwords through a challenge-response mechanism to be an assault on their IT competency rather than a means to enable better cost management at the help desk through more productive deployment of resources. The longer term aim once compliance with security auditor recommendations is under control may be for a deeper exercise in access rights and identity management. This could lead to more in depth analysis through role engineering and eventually a full identity management deployment.

Such organizations benefit most from a carefully planned role engineering analysis where group policies are carefully calculated to only give access through correct authentication and access levels.

Tools such as **FastPassAD™** offer a non-intrusive solution where the empowerment is with the user to set them selves up with their own challenge response mechanism for authentication via HTTP within the corporate LAN/WAN or HTTPS from the internet and to reset their passwords whilst leveraging all the features of Active Directory.

The biggest concern when deploying a new desktop tool which interfaces seamlessly with the directory (in this case Active Directory) is the impact on users. Should changes disrupt the work of users in any way, the help desk can be overwhelmed with calls and be unable to provide the necessary support. Since the objective here is to cut the calls to the help desk to fully exploit the ROI potential, education of the user population is a critically important factor for inclusion. Often, a new authentication strategy will include the requirement for domain migrations, upgrades from NT to Windows 2000/2003 which all implicitly include profile migrations, maintaining access to other resources, updating paths and links to new files and maintaining the required level of messaging and directory services as well as involving the deployment of desktop client software.

The deployment of web browser based **FastPassAD™** maintains the transparency to network and internet users alike and allows the organization to continue in the drive to improve services linked to Active Directory. Options exist with **FastPassAD™** for pushing password changes in Active Directory to other vendor systems, platforms and applications with an interceptor and dispatcher tool developed by IT InterGroup using the Microsoft .NET framework.

The combination of these utilities increases the breadth and scope of a password management project into supported systems including RACF, Domino, Open LDAP, Oracle, Unix, Linux, SAP and PeopleSoft. There is also an option to use a desktop reset tool for pushing the change to the Lotus Notes ID and this can and will be implemented in the GUI dependent upon customer requirements.

Pushing password changes on a 24 x 7 user self-service basis has proven benefits for cost management in respect of user and helpdesk productivity alike. The extremely light footprint of the **FastPassAD™** installation on the domain controller (DC) means that it is easy to uninstall and deactivate when a more full identity management project is rolled out. The installation amounts to less than 6 MB when deployed and is not to be confused with the all-enveloping installation of a Single Sign-On installation. **FastPassAD™** is equally at home with most of the enterprise Identity Management offerings from Tivoli, CA and BMC as a password reset tool and user validation engine for self-service profile management, assuring the enterprise of continued low cost of ownership.



FastPassAD™: Enabling enterprise wide password synchronization

Synchronization and Connectivity Architecture

Synchronization across multiple platforms is dependent upon connectivity to other platforms and the **FastPassAD™** v2.0 release due in Nov 2004 built on .NET uses a component type scalable architecture uses web services with an interceptor and dispatcher methodology.

Earlier versions of the tool used a number of different methods for connecting to target systems including:

- Direct to user database with SQL command on CLI
- Leverage the OS to authenticate
- Third Party LDAP (AD, IBM Directory Server, SunOne, etc.) authentication
- Linux open source authentication module (PAM).

The .NET re-write of **FastPassAD™** has created the demand for a roadmap that demonstrates the flexibility and scalability of the product as a synchronization engine to multiple platforms from multiple vendors.

Further development of the web services connector architecture is underway and currently supports the following platforms:

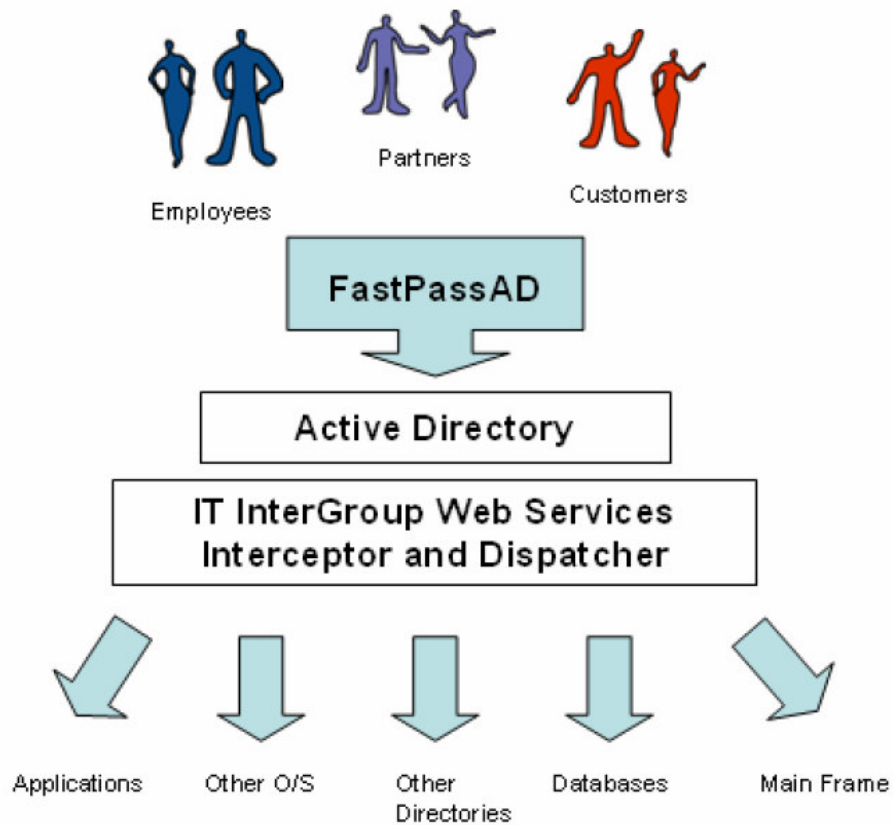
- Microsoft Active Directory
- Lotus Domino HTTP
- IBM RACF
- Open LDAP
- SunOne Directory Server
- IBM Directory Server
- Oracle
- MySQL
- Unix
- Linux
- NT4
- SAP
- PeopleSoft
- Lotus Notes ID file integration.



FastPassAD™: Enabling enterprise wide password synchronization

This diagram presents an overview of the how the user community might interact with AD and push password changes into other vendor platforms.

Authentication and Integration



FastPassAD™: Enabling enterprise wide password synchronization

State of Readiness

Considerations for the deployment of **FastPassAD™** should be based around the AD environment's state of readiness and the (DC) architecture.

- In many organizations, the existing Windows NT domain structure does not fit with the necessary minimum requirement. An optimized AD for domain and Organizational Unit (OU) structure
- should be created.
- It is also suggested that an analysis and cleanup of directory data be performed to remove obsolete users and group accounts. Without this, AD will contain polluted directory data.

Single-domain environments with only one DC are much easier installations to perform than multi-site deployments where localization issues and DC replication schedules are integral to maintaining authoritative data in the network. However provision is made in the installation for searching across DCs in order to locate the master repository, IIS and DC for the DLL installation.

Clustered DCs for load balancing are also supported and it is also important to note that all configurations are installed in the Registration database and are accessible to administrators for editing user settings such as localization of challenge questions as well as the maximum number of failed reset attempts and total number of challenge questions presented.

It is of course implicit that organizations be aware of which DC is the master repository and what the password policies are for the organization. This is not always the case and a 'state of readiness' audit is advised. IT InterGroup insist on the completion of documentation prior to installation where agreement is made with the customer regarding knowledge of the environment.



FastPassAD™: Enabling enterprise wide password synchronization

User Impact

User impact is the main concern in any enterprise infrastructure change. Should anything unexpected occur or anything look or operate differently, the time and resources required to address the issues and answer the questions can be significant.

Factor in the number of users across the network and consider the associated business impact, and it's clear that any organization planning a deployment must make minimizing user impact a primary objective.

The areas of concern include:

- User personal settings – users spend a large amount of time adjusting their profiles for everyday needs. Setup and reset functionality must be simple and reliable otherwise productivity suffers.
- Access to resources – users need to maintain access to the systems they work with throughout the deployment. Password changes must be reliably pushed to systems where they have access rights.
- Links to resources – when users are renamed the profiles should be updated to reflect the change and maintain continuity of global access.
- User collaboration – the existing user collaboration level (mail, calendars, shared folders, other systems) must be preserved.

Conversely, the benefits of a well planned design and deployment of a self-service tool for password management can remove doubt, reduce helpdesk intervention, increase security and ultimately enhance the opportunities for increased user productivity. This brings happiness to the user community, the ability for systems administrators to maintain critical platforms and relief to management.

ROI for Security Projects

Security based projects are notoriously difficult to justify through quantifiable financial gain because of differences in perspective existing in the industry. European corporations largely aim at measuring the success of a security project by the reduction in operating costs and a fast ROI, whereas their North American counterparts largely attempt to quantify the gain by justifying the costs associated with the protection of data.

Notwithstanding this fundamental difference in philosophy it is undermined by the fast ROI possible with the implementation of a password management project which satisfies auditors, corporate policy and regulatory authorities alike.



FastPassAD™: Enabling enterprise wide password synchronization

Staged Deployment Approach – An Example

Step 1 - FastPassAD™ - A Toolset Overview

FastPassAD™ targets the organization whose centralized enterprise user data repository is Active Directory. Experience has shown that as a first step to introducing new functionality to the user community corporate IT strategists find it easier to introduce the 'challenge-response' functionality for setup and password reset as a preliminary to widening the scope into other platforms and applications with password synchronization functionality.

Step 2 - The Notes Client - The Lotus Conundrum

In organizations where it is applicable synchronization with the Lotus Notes ID file on the desktop is now possible by pushing the new password to the ID file with a proprietary solution designed and developed by IT InterGroup. The code for this functionality sits behind the same GUI as the AD password reset screen so all passwords are reset/synchronized simultaneously.

Step 3 - The Backend - synchronization

IT InterGroup's web services interceptor and dispatcher module allows for synchronization with multi-vendor operating systems and application platforms by means of web services based connectors. Connectivity via the password synchronization component allows us to push password changes from Active Directory into environments such as RACF, NT4, AD, SunOne, Open LDAP, Domino, Oracle, Unix and Linux, PeopleSoft and SAP.



FastPassAD™: Enabling enterprise wide password synchronization

About IT InterGroup

IT InterGroup provides identity management and systems management solutions to organizations that rely on multi-vendor platforms. IT InterGroup's proven expertise in the directory space, and more particularly with Active Directory, helps customers improve security, productivity and availability. IT professionals choose IT InterGroup's solutions to administer, migrate, recover, audit and secure their critical systems. The company's customers and partners include TDC, Silkeborg Datacentral, Codan, IBM and Microsoft. IT InterGroup is a Danish company with offices in Allerød, Denmark. Their activities extend throughout the Scandinavian countries and into other parts of Europe.

About Saragosta IT Services

Saragosta Group is a young and dynamic IT consulting and services firm that delivers High Impact and High Value Services to Large and Medium sized Polish companies in Business Critical areas of consulting, IT solutions and IT services.

We have our base in Warszawa and are active across all of Poland. Through our extensive partner network, we are capable of supporting our customers both in Poland and internationally.

Saragosta Group has expanded its capabilities to provide our customers with a portfolio of high quality business critical solutions within consulting and IT services on top of Business Continuity Planning and Risk Management. Saragosta Group now consists of Saragosta Consulting and Saragosta IT Services.

The Saragosta Portfolio

Saragosta Group is a customer driven organization.

Our core competency lies in our ability to help our customers to meet their challenges.

This means that we are agile and adaptive in responding to our customers need and acquire new competencies rapidly through an extensive network and business partners. We maintain our own skills and competencies in the areas of IT Services and Consulting that are seen to be the most critical for our customers and their business and by continuously seeking to acquire new expertise in areas that are related to our core competencies.

The Saragosta Group portfolio includes key solutions and services within critical areas of Risk management and Business Continuity Planning as well as key infrastructure services managing information, applications, processes, users and workstations. The key activity areas are the following:

- **Business Continuity Planning**
- **Risk Management**
- **Strategy and Change**
- **Process Optimization**
- **Business Integration**
- **IT Management and Security**
- **Information Management**
- **E-commerce/Web solutions**
- **Solutions for Payment Systems for Banking**
- **Solutions for Anti-money laundering for Banking**

**For more information
contact Saragosta IT Services.**

E-mail : Saragosta@Saragosta.com

Telephone : +48 22 697 79 70

Address : Ilmet, Al Ilmet, Al. J. Pawla II 15 / 10-05, 00-828 Warszawa



FastPassAD™: Enabling enterprise wide password synchronization

Addendum

Nov 15 2004 – IT InterGroup announces the release of the .NET connector forSAP to coincide with MS IT Forum 2004 in Copenhagen.

