



ESSO: The Next Big Win for IT

A White Paper created by
Gregg LaRoche
Director of Product Management
Imprivata, Inc.

TABLE OF CONTENTS

Introduction.....	1
The Problems ESSO was Created to Solve.....	1
The Problem with Early ESSO Solutions.....	2
How Third-Generation ESSO Solves the Problems of Password Proliferation.....	3
How Third-Generation ESSO Delivers an Immediate, Significant ROI.....	3
The Broader Impact of Third-Generation ESSO.....	4
Imprivata OneSign: The Premier Third-Generation ESSO Solution.....	5

Every so often, a technology comes along that creates a true sea change in the marketplace. For example, virtual private networks (VPN) changed corporate networking forever by delivering a powerful combination of immediate return on investment (ROI), improved security, and greater user convenience. Indeed, by the time VPN technology reached its third generation, it radically altered the economics and capabilities of networking for companies of all sizes. The result? VPNs quickly became the de facto standard for remote connectivity.

More recently, Enterprise Single Sign-On (ESSO) has emerged with a similar potential to transform enterprise security. ESSO addresses one of the fastest-growing security issues facing corporations today—password proliferation and control. Like third-generation VPNs, ESSO solutions deliver an immediate, significant ROI while strengthening security and improving user convenience—and the benefits of ESSO span areas as diverse as user productivity, access control, help desk costs, and regulatory compliance. This white paper takes a closer look at ESSO, the problems it solves, and how it will fundamentally change the way corporations address their security needs.

The Problems ESSO was Created to Solve

Every technology solution is developed to solve a problem. In the case of early VPNs, the problem was the prohibitively high cost of deploying, operating and maintaining a private corporate data network. Only the largest companies could afford them, and without a private network, remote users were at the mercy of slow, costly, and insecure modem connections.

For ESSO, the problem is too many application passwords. Passwords have become a nightmare for many organizations. Once a relatively simple, effective and affordable way to ensure that only authorized users could gain access to important business applications, passwords have become a source of frustration, friction and increasing cost for many enterprises.

What changed?

Corporate computing environments became more complex. The number of business applications in those environments has multiplied, leading to a corresponding increase in the number and type of passwords required to access them. As a result, the average user now has to remember more than seven passwords. To make matters worse, in today's heterogeneous environments, the user must often recall several different types of passwords, each with its own "syntax" of alphanumeric characters and symbols.

As passwords have proliferated, it has become increasingly difficult for users to remember them. And when users forget passwords, what do they do? They get locked out of the applications they need to perform their work, they get frustrated, and they call the IT help desk for assistance. According to Forrester Research, more than 30% of all help desk costs are password-related. With the cost of a single help desk call at \$25 to \$40, the cost of password problems can quickly add up to hundreds of thousands of dollars per year for even mid-sized companies. And that's not even factoring in the cost of lost productivity when users are locked out of needed applications due to forgotten passwords.

What's worse, the negative impact of password proliferation extends to the very area that passwords are supposed to help: security. Faced with a growing number of passwords to remember, users often resort to writing them down and leaving them in plain view where a nefarious person can find them and use them to gain unauthorized access. Suddenly, every desktop in the organization is another point of vulnerability in the corporate security armor.

In an effort to strengthen desktop security, many organizations have instituted strong password policies. These policies mandate the use—and frequent changing—of passwords that, in the interest of preventing password theft, are intentionally complex and difficult to remember. This also exacerbates the problem, resulting in password policy non-compliance, increased security risk, and spiraling help desk costs.

More recently, another factor has increased the urgency among enterprises to solve the password proliferation problem: the law. The US federal government has enacted several laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Act of 1999, and the Sarbanes-Oxley Act of 2002, that require organizations to have processes in place to safeguard the privacy of client, patient, and employee information.

The Problem with Early ESSO Solutions

The first generation of ESSO solutions took a centralized approach. A central location, i.e. meta-directory, stored all credentials, then acted as an inline proxy to distribute the credentials when requested. While this approach had the advantage of centralized management and auditing, it often required organizations to make changes to the code of each application to be supported with ESSO. This made ESSO deployment slow, difficult, and costly. First-generation ESSO solutions relied on heavy scripting and building custom connectors to each application. Although these features gave users flexible and customized solutions, they were difficult to maintain and expensive to update, even making some applications impossible to support.

The second generation of ESSO solutions took the opposite approach; all ESSO software resided on the client. By tackling ESSO from the client side, these second-generation solutions had limited support for simple client/server and enterprise applications, and no support for Java applications. And, their ability to fulfill ESSO needs was restricted. Although they were non-intrusive, requiring no changes to application software, client-side ESSO solutions lacked one critical feature that earlier solutions provided: centralized control. Without it, IT organizations lacked the ability to control ESSO policy, account termination, auditing, and more. This increased security risks, since user compliance could not be assured.

Although first-and second-generation ESSO products found customers, their high implementation costs and complexity kept them from gaining widespread acceptance in the marketplace.

Third-generation ESSO solutions combine the strengths of their predecessors while overcoming their limitations, offering:

- Centralized control for stronger security, easier administration and maintenance
- Non-intrusiveness, with no application changes required
- Universal application support (including legacy, client/server, and Web)

In doing so, third-generation ESSO solutions have made single sign-on:

- Affordable for enterprises of any size
- Faster and easier to deploy enterprise-wide
- Easier and more efficient to administer and maintain
- More convenient for users
- More secure

Just as enterprises quickly embraced more mature VPN solutions once the barriers to adoption had been cleared, organizations are rapidly adopting third-generation ESSO as the de facto standard for identity management, desktop security, and compliance with information privacy regulations.

How Third-Generation ESSO Solves the Problems of Password Proliferation

Today's ESSO solutions solve the problems associated with password proliferation in a variety of ways:

- By enabling the use of a single strong password or authentication for all applications
- By reducing the number of password-related help desk calls
- By relieving users from shouldering the burden of password policy implementation
- By supporting compliance with federal and industry regulations

How Third-Generation ESSO Delivers an Immediate, Significant ROI

There are many ways to calculate the return on an investment. In evaluating the ROI impact of ESSO, enterprises should factor in three kinds of costs: the cost of deployment compared to other solutions; the existing costs that the ESSO solution seeks to reduce; and projected future costs that the ESSO solution will help the enterprise to minimize or prevent entirely.

ESSO offers low deployment costs

The right ESSO solution will cost much less than its competition to deploy, for several reasons:

- The best ESSO solutions work with virtually any application—legacy, client, or Web with no scripting or custom-coding required. This eliminates months of work and the associated costs of having skilled programmers write code to SSO-enable every application in the enterprise.
- Because the best ESSO solutions are distributed solutions, organizations can deploy them quickly and easily across the enterprise at multiple sites and all levels from a central location, again saving time and money.
- User training costs are low with ESSO because the authentication process is completely automated. Unskilled users can learn to work with the best ESSO solutions instantly and usually without any training.

ESSO reduces existing costs

The more complex the corporate IT environment and the more applications in use, the higher the costs associated with password problems. The right ESSO solution reduces these existing costs in several ways:

- ESSO reduces the number of costly, forgotten password-related help desk calls. With each user having only one password to remember, enterprises can expect to see an immediate, significant, and ongoing drop in the volume of help desk calls. With each call costing \$25 or more, the savings can add up very quickly.
- ESSO reduces IT resource requirements. With fewer password resets to handle, IT organizations can reduce or shift personnel to other, more productive assignments.
- ESSO increases user productivity. With only one password to remember, user lockout is greatly reduced, thereby making users more productive.

ESSO minimizes or prevents additional costs

Any accurate ROI calculation also has to consider incremental, future costs that ESSO can help organizations avoid. For example:

- ESSO can keep the cost of SSO-enabling new applications and upgrading existing applications low. Because the best ESSO solutions are non-intrusive, there are no custom coding costs associated with adding new applications or upgrading existing ones.
- With the right ESSO solution, administrative and maintenance costs are low. Ongoing operating costs remain low because administration and maintenance can be centralized and performed via Web browser without any specialized expertise.

The Broader Impact of Third-Generation ESSO

In addition to its direct impact on enterprise security and the costs associated with password proliferation, ESSO is affecting enterprises in other notable ways:

- Enterprises get a clearer picture of application access and usage. This visibility helps organizations improve license management, and ensure that users have appropriate access privileges.
- ESSO can be a driver for a better security policy for an organization. By creating a single system entry point, organizations can easily implement strong authentication, which in turn improves overall security.
- In the identity management arena, ESSO is one of the few technologies that provides a quick return on a low investment, while integrating very easily with other identity management services.

Imprivata OneSign: The Premier Third-Generation ESSO Solution

Imprivata OneSign is an affordable, non-intrusive appliance that provides third-generation ESSO for Web, client/server and legacy applications. Through a unique, centralized approach to password management, OneSign makes secure ESSO services quick to deploy, convenient to use, and easy to administer. As a result, customers benefit from increased productivity, higher user compliance and lower help desk costs. OneSign makes it simple and practical for companies of all sizes to adopt and enforce password policies.

OneSign features include:

- Non-intrusiveness. Organizations can implement OneSign without changing existing applications or modifying user logon behavior.
- Plug and go installation. OneSign is packaged in a secure, 1U rack-mounted device (with redundant unit) that requires nothing extra to buy or install.
- Password policy support. Customers can configure support for unique passwords and change passwords automatically in the background.
- Security policy support. Enterprises can assign different security policies to different users or groups of users.
- Shared credentials support. Customers can organize applications into groups that share a common credential store.
- Shared workstation support. Multiple users can sign on to a shared workstation without logging out of the desktop.
- User logging. Security officials can perform audits to determine which user is accessing what application and when.
- Self-updating agent. This feature simplifies deployments and updates without additional administrative overhead.

The whole point of using passwords is to keep data, applications, and other IT resources secure. While password proliferation often results in user behavior that increases security risks and support costs, the implementation of a proper ESSO solution can reduce those risks considerably. For IT organizations everywhere, that means implementation of third-generation ESSO which like third-generation VPNs represents another big win.

For more information on OneSign, please visit <http://www.imprivata.com> or contact Imprivata at 877-ONESIGN.



10 Maguire Road Suite 210
Lexington, MA 02421
v 781 674 2700
f 781 674 2760

www.imprivata.com
1.877.ONESIGN