



Secure Web Sign-On with SafeEnterprise™ SSL iGate

Replacing user log-on with two-factor token authentication

Implementation White Paper

By Chris Holland, Senior Product Manager

This white paper describes the recommended method to implement Credential Forwarding, a feature of the SafeEnterprise SSL iGate solution, with Core Web based applications to create a seamless and secure solution for internal, remote, wireless, and partner access.

Introduction

Instant Private Web (IPW) solutions like the SafeEnterprise SSL iGate provide a secure environment to deploy Web based applications – allowing companies to leverage the cost and access benefits of web deployments over traditional fat client applications and enjoy stronger and easier to use security than a VPN.

The SafeEnterprise SSL iGate solution consists of an appliance, management software and USB tokens (the SafeNet iKey). Together with Web based application software it creates a secure, easy to access, manage and deploy web-based solution. SafeEnterprise SSL iGate brings the customer added confidence over the privacy of his data by ensuring that only people with an iKey (employees, partners, customers etc...) can access the system. The SafeEnterprise SSL iGate also creates an instant SSL connection between the remote users and the appliance – so that regardless of the medium (home network, customer network, wireless LAN etc...) the data is kept private. The benefits of a web deployment of any application – portability, freedom from VPNs, access into partner networks – can be confidently enjoyed with the added security assurance that an SSL and iKey based system brings. The mechanisms and technology implemented provide very strong authentication, not only ensuring that authorized people are accessing the system – but also eliminating the need for password management.

Credential Forwarding

Although it appears seamless to users, authentication with a SafeEnterprise SSL iGate solution is typically accomplished in two steps:

1) This step requires authentication to the SafeEnterprise SSL iGate system. This is done via a challenge-response scheme between the appliance and the iKey. The underlying technology utilizes the HMAC-MD5 algorithm using a different shared secret stored on each iKey with a copy stored in the appliance. The response computed on the client side is compared with another response on the appliance. If they match, then the user passes on to the second step where the user needs to be identified to the Web application. There are generally two types of method for authenticating to a Web based application – using either (1) the built in user account management and log-in solution of that application or (2) utilizing some other existing Network based authentication method (see Figure 1).

With the first method, the Credential Forwarding feature of the IPW solution passes the user name and a pass phrase to the Web application server using custom HTTP headers. This information is included with each HTTP request from the client thereby allowing the application to know, with each request, who is accessing the system. This can allow an end user to access a user-specific (portal) page on the application without requiring a separate login to the default application login screen.

IPW Credential Forwarding Solutions

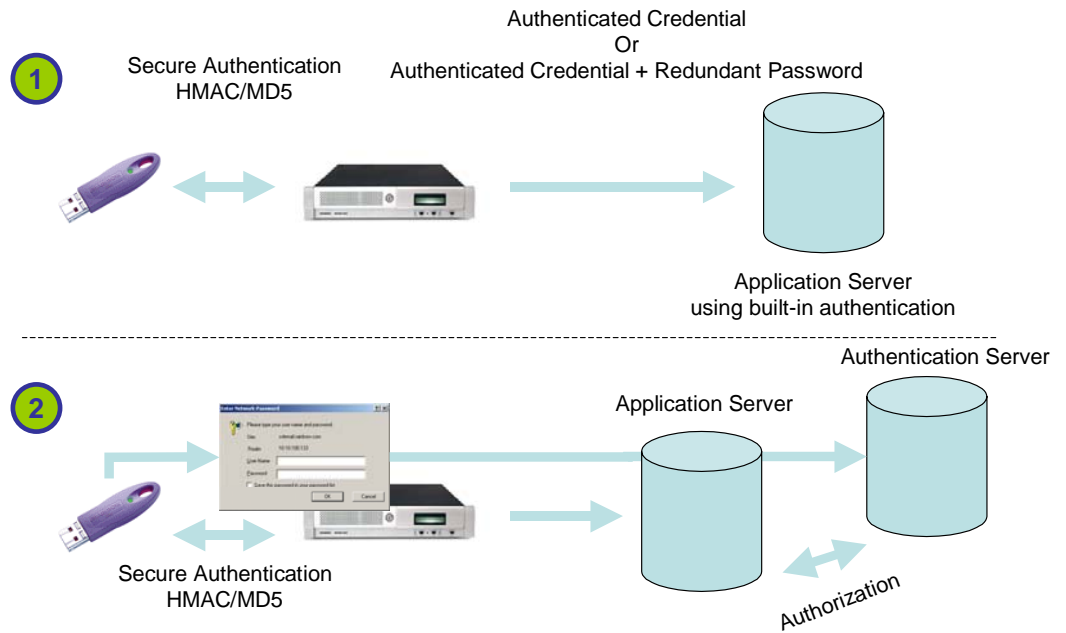


Figure 1: Credential Forwarding

2) This step relies on an NT server for authentication to the Web application. Users not already authenticated to the network (typically remote or partner users) are presented with a familiar dialog box in which to enter their domain credentials. The Credential Forwarding feature of the SafeEnterprise SSL iGate eliminates this step by intercepting the login request and securely responding to the request with the correct credentials of the key holder. In this case the domain credentials are securely stored in the iKey and are managed entirely by the users (i.e. holders of the iKey). In this manner, users have a simple and seamless experience when using the iKey to access the application securely from any browser.

Both methods can be used together to allow support for both trusted users with domain credentials and partner users who most likely do not have accounts on the domain but still require simple, secured and custom access to the Web based application.

Either of these methods provides the administrator with the benefit of authorized and confidential access to the information stored within the application without having to administer unwieldy, unpopular and complex password maintenance routines.

While it is not necessary, administrators may still use the iGate without Credential Forwarding – essentially requiring users to authenticate twice – once

with the iKey into the SafeEnterprise SSL iGate system and then a second time directly in to the Web based application. This configuration may be used as a temporary step toward complete integration and in the meanwhile provides the benefit of two-factor authentication and the secure transmission (SSL) across any network medium.

Solutions Overview

When a Web based application is being used with its own built in authentication mechanism the appliance is configured to forward to the server the username and a password. Some applications require both a username and password, while others may be configured to require only a trusted username, assuming that when a request reaches it – the user has already been authenticated. When the SafeEnterprise SSL iGate is used, the need, in general, for an additional authentication solution is redundant. While theoretically no longer needing a username/pass phrase pair, in practice some applications still require both pieces of information. In these instances, the recommended approach is to configure the Web based application so that all users share the same common pass phrase. The SafeEnterprise SSL iGate simply forwards each user name with the same redundant pass phrase to the applications access control mechanism.

An alternative approach to using a redundant pass phrase, if it is required, is to configure the registered pass phrase for each user as the iKey serial number. This provides a unique username/pass phrase pair for each user. This methodology is considered unnecessary since the SafeEnterprise SSL iGate is already providing very strong authentication independently. Figure 2 shows the steps managed by the SafeEnterprise SSL iGate between the client browser and the Web based application.

*Implementing Credential Forwarding with an applications'
built in authentication*

IPW Credential Forwarding

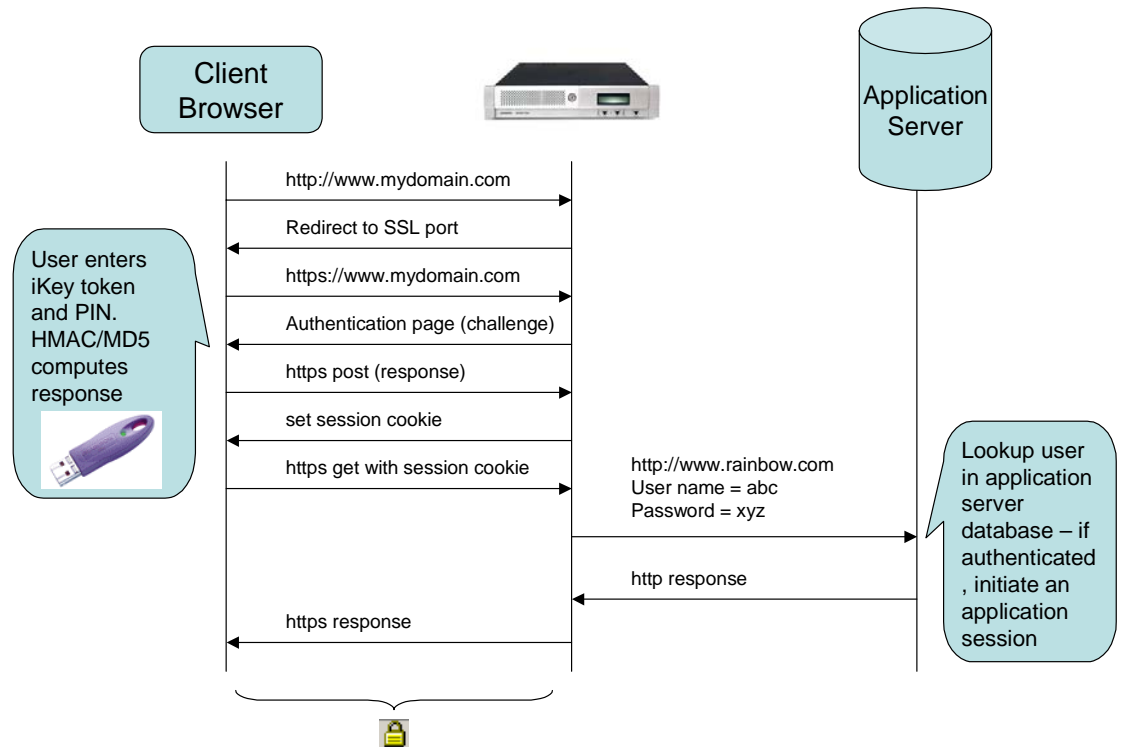


Figure 2: Interaction with Web based application

An alternative access control implementation is when the application server is relying on a separate third party authentication mechanism, such as an NT server. A user is either already authenticated to the network domain by virtue of having already “logged-in” to the network, or, in the case of a remote access (employee / partner / customer) is presented with a Windows like pop up dialog box in order to enter their credentials. In this scenario, since the control of the password is maintained by a 3rd party system these credentials are held securely in the iKey itself. Once the SafeEnterprise SSL iGate has authenticated a user with an iKey, it intercepts the request for domain credentials that is generated to authenticate the user, and securely places the stored credentials directly from the iKey into that form – thus relieving the user from the need to log-in to the application directly. This process is transparent to the end user and to the administrator. In this mode – no changes are required to the application or the user database.

Using Credential Forwarding the SafeEnterprise SSL iGate can be integrated with a Web based application to authenticate users quickly and securely. For customers using the built in authentication scheme, the solution consists of making modifications to the ASP or other types of login processing script to make use of the forwarded credentials.

The following steps summarize how changes can be implemented to create a seamless integration and complete overall solution:

1. The user pass phrase is configured to be either
 - a) a common phrase for all users – used in this example
 - b) the least-significant 8 bytes of the user's assigned iKey serial number¹
2. The application scripts are modified to retrieve the user name and pass phrase from the HTTP header when HTTP requests are received and no current session is open (i.e. no cookie present in the request).

If the user name / password pair in the HTTP header matches that stored in the Web applications' authentication database, a login session may be created without sending the default authentication page to the client browser.

An added feature of the SafeEnterprise SSL iGate is that when the iKey is removed – all sessions open and active across the system are terminated and client side information can be destroyed.

The following custom HTTP headers are automatically present in a default configuration and should be used on the server side as the authenticated credentials:

HTTP_IGATE_USERID
HTTP_IGATE_IKEYSERIALNUMBER

In the case where a common pass phrase is required, then the solution can be configured to support another custom header, which will return that phrase. In this case a variable might be created as follows...

HTTP_IGATE_appnamePASSWORD

Where there are multiple applications, using this scheme it is possible to support different "common" pass phrases for each application.

The following is sample code that can be used to implement credential forwarding in an IIS 5.0 environment.

```
!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
```

```
<html>  
<head>  
  <title>SafeEnterprise SSL iGate Credential Forwarding</title>  
</head>  
  
<body>
```

¹ This method is not recommended since it is burdensome on the administrator while providing only a limited incremental benefit in terms of security.

iGate 2.2 Credential Forwarding

This is an example on the user credential forwarding available in iGate version 2.2.

The ASP code used was tested on IIS/5.0

Prerequisites

- IIS 5.0 with example website setup
- this** default.asp in the root directory of the example website
- iGate setup and administered for client authentication to your test website
- iGate configured for protection of the test website
- user account administered in Access Control Manager (ACM)
- iKey assigned to user

It is recommended to implement and test the user authentication with iKey prior to evaluating and implementing the user credential forwarding.

Overview

During authentication, two server variables will be set. These can be extracted via ASP using the following commands:

```

Request.ServerVariables(" HTTP_IGATE_USERID ")
Request.ServerVariables(" HTTP_IGATE_IKEYSERIALNUMBER ")

```

ServerVariable	Content
HTTP_IGATE_USERID	The username as administered in the Access Control Manager (ACM).
HTTP_IGATE_IKEYSERIALNUMBER	The serial number of the iKey assigned to the user HTTP_IGATE_USERID in the ACM.

Your logon information

<p>Note: The following will only succeed on your live example website!</p>
<p>So in this example you logged in as user
<%
strUserID = " " & Request.ServerVariables("HTTP_IGATE_USERID") & "
"
Response.Write strUserID
%>
</p>

<p>The serial number of your iKey is
<%
strSerialNo = " " & Request.ServerVariables("HTTP_IGATE_IKEYSERIALNUMBER")&
"
"
Response.Write strSerialNo
%>
</p>

<p>Note:If you logon using username and password, the server variable
<i>HTTP_IGATE_IKEYSERIALNUMBER</i> will be empty</p>

<p>As this information is now available for your ASP code,
you can use to pass it on to backend systems (e.g. Crystal Reports) or to proprietary
login scripts.</p>

<hr>

For comments, suggestions and questions, please contact Christian
Huesch, TS EMEA, SafeNet Ltd.

<p>Version 1.0; last edited 4/Dec/2002 at 15:27:38; created by TS
EMEA, CRH</p>

<hr>

</body>

</html>

Summary

Credential Forwarding offers an excellent opportunity for companies to replace hard to manage complex passwords with token-based authentication. See www.safenet-inc.com/igate for more information on SafeEnterprise SSL iGate.

SafeNet Overview

SafeNet (NASDAQ: SFNT) is a global leader in information security. Founded more than 20 years ago, the company provides complete security utilizing its encryption technologies to protect communications, intellectual property and digital identities, and offers a full spectrum of products including hardware, software, and chips. ARM, Bank of America, Cisco Systems, the Departments of Defense, and Homeland Security, Microsoft, Samsung, Texas Instruments, the U.S. Internal Revenue Service, and scores of other customers entrust their security needs to SafeNet. For more information, visit www.safenet-inc.com.



www.safenet-inc.com

Corporate Headquarters: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: +1 410.931.7500 or 800.533.3958 eMail: info@safenet-inc.com

Phone USA and Canada (800) 533-3958
Phone Other Countries (410) 931-7500
Fax (410) 931-7524
E-mail Info@safenet-inc.com
Website www.safenet-inc.com

2004 SafeNet, Inc. This document contains information that is proprietary to SafeNet, Inc. No part of this document may be reproduced in any form without prior written approval by SafeNet. SafeNet shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretation thereof. The opinions expressed herein are subject to change without notice.

Australia +61 3 9882 8322
Brazil +55 11 6121 6455
China +86 10 8266 3936
Finland +358 20 500 7800
France +33 1 41 43 29 00
Germany +49 18 03 72 46 26 9
Hong Kong +852 3157 7111
India +91 11 26917538
Japan +81 3 5719 2731
Japan(Tokyo) +81 3 5719 2731
Korea +82 31 705 8212
Mexico +52 55 5575 1441
Netherlands +31 73 658 1900
Singapore (1) +65 6274 2794
Singapore (2) +65 6297 6196
Taiwan +886 2 6630 9388
UK +44 1932 579200
UK (Basingstoke) +44 1256 345900
U.S. (Massachusetts) +1 978.539.4800
U.S. (New Jersey) +1 201.333.3400
U.S. (Virginia) +1 703.279.4500
U.S. (Irvine, California) +1 949.450.7300
U.S. (Santa Clara, California) +1 408.855.6000
U.S. (Torrance, California) +1 310.533.8100

Distributors and resellers located worldwide.