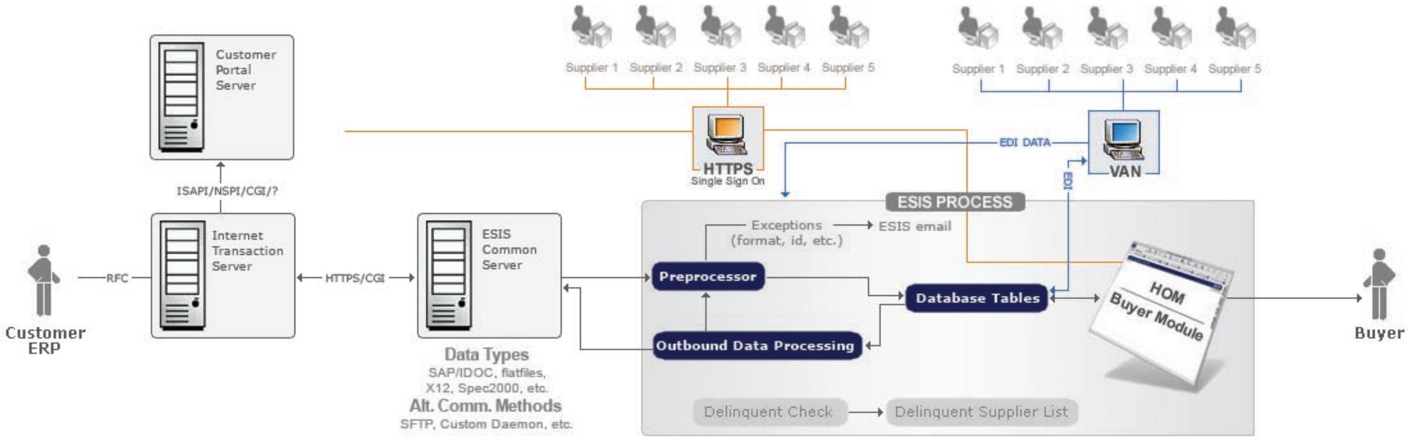
ESIS

Supply Chain Solutions That Work

The ESIS Single Sign On Portal Solution

While intended to increase efficiency, the growing number of proprietary supplier portals is causing an unforeseen problem-significant costs are being added to supply chains across all industries. The reason? Suppliers must currently log onto numerous Internet portals in order to perform their daily business tasks.



There is a better way. The solution is to provide a method to share login authorizations across portals so the supplier only has to log in once to have access to all their documents on different sites. As a supplier logs in to a given portal, that portal contains links to other portals. When a link is clicked, a window to the remote site opens. The supplier's authentication is taken care of between the two portals, so the supplier is automatically authenticated to the remote portal via the local link.

From a supplier's perspective, the user opens a web browser client and visits an Internet portal, either ESIS' HOM or one of their customers' proprietary portal sites. During the course of their business on this initial site, the user finds that he or she must view a document on another portal. Previously, they would need to manually open a new web browser window in order to visit the second site. They would also be required to log in an additional time to this second portal. If the supplier has to do business on more than one or two portals, login management can become very troublesome and decrease their productivity. Consider the all-too-common scenario where a supplier customer service representative must access scores of customer portals in the course of a single day.

With the advent of the ESIS Single Sign On System, the supplier no longer has to manage different logins on all of their customers' portals. The user simply clicks a special link to one of the other portals and the authentication is taken care of behind the scenes. This speeds up the user's workflow and therefore increases their daily productivity.

Technical Options

There are numerous ways in which the ESIS Single Sign On System can be implemented. One is by using a browser cookie that is shared between portals to authenticate the user. This may be the hardest to implement technically, but is also the most seamless to the user. The secondary portal automatically reads the shared cookie, and the user is granted or denied access automatically. Both portals must recognize the cookie format and the information contained within it for this system to work.

Another method is by using a session ID to track the unique user. When visiting the secondary remote portal, the session ID is transferred via URL to the new server. This server then queries the original portal to find out which user corresponds to that particular session ID. The original server responds with the information, and the remote portal makes its authentication decisions based on this server-to-server communication.

User identities can also be passed by way of links or buttons that are generated dynamically on the original portal site. After logging in to the primary portal, the user is presented with links or buttons that will send them to various secondary portals, either in a new window or another frame. Clicking one of these objects passes authentication information to the remote site via either a HTTP GET or POST request. The remote site receives the authentication information and grants or denies access to the user. This method requires that the two portal sites have some way of reconciling their own proprietary ways of authentication. This can be achieved by tables hosted locally on each site, or by sending queries from server to server to request this information as needed.

The Shared Cookie Option

Pre-Reqs: Servers have DNS aliases that point to the other company's domain name (example: esis.honeywell.com and honeywell.esisinc.com).

How It Works: Client logs in to server A. HTTP cookie is set after successful authentication. Client then visits server B under the DNS aliased name using server A's domain. Server B then reads server A's cookie and processes the authentication automatically. Permissions are granted accordingly and the client then proceeds to browse the protected content on server B.

The Session ID Option

Pre-Reqs: Secure pipeline for sharing information established between servers A and B.

How It Works: Client logs in to server A. Client authenticates with server A, and a session ID is assigned by the server. This session ID is a unique alphanumeric value, possibly encrypted, which is passed to each page that the client visits. The programs on server A are able to identify the particular client by virtue of this unique ID.

When the client chooses to visit server B, the session ID is transferred via either GET or POST methods from the client to server B. Server B receives the information and contacts server A. Server A then responds with the identity of the client that corresponds with that particular session ID. Server B then uses that information to authenticate the client and grant the appropriate permissions.

The Intra-Server Form Submission Option

Pre-Reqs: Either a secure pipeline for sharing information established between servers A and B, or lookup tables reside locally on each server. These tables would contain information that correlates a local user ID with one on the remote server. These tables would need to be refreshed whenever this information is changed on either server.

How It Works: Upon successful authentication on server A, a secure communication pipeline is used to gather authentication information for the client from other servers in the partnership. The client is then presented with a page of links or form-submit buttons to visit these other servers (collectively referred to as server B). This page is dynamically generated by server A so that it contains encrypted authentication information for the other servers.

If links are used, the authentication information is encoded into the URL, possibly encrypted. When clicked upon, these links open either a new browser window or use another frame in the current window to display information from server B. When server B receives the request for a document, it decodes the authentication information contained in the URL and automatically logs the client in. The remote page is then displayed without necessitating the client to authenticate to server B.

If form-submit buttons are used, then the authentication information is contained within the HTML code of the page as hidden form inputs, possibly encrypted. Clicking one of these buttons on server A will submit the information to an authentication program on server B. Server B then processes this information and logs in the client automatically. The remote document is then displayed to the client, either in a separate window or in a particular frame in the current window.

Trading Partner Benefits

Having a single sign on facilitates a supplier's ability to do business with the buying organization, thus leading to more sales for the supplier and a more efficient supply chain for the buyer. Easy access to spec sheets, diagrams, and other proprietary information on the buyer's portal will help prevent supplier confusion and lead to more accurate order fulfillment and fewer incorrect shipments. In addition to creating efficiencies on both ends, this technology generates good will with the supplier.