IndustrySafe Single Sign-On Specifications
Using SHA2 Encryption

1 Overview

IndustrySafe has developed a Single Sign-on (SSO) solution that allows a user to validate their identify using a client's user authentication system. Once the user has been authenticated by the client's system, that system passes the user's authentication credentials to IndustrySafe in the form of a token that has been encrypted using SHA2 encryption. The IndustrySafe login page validates the token and either logs the user into IndustrySafe or displays an error message.

2 Single Sign-on Process

IndustrySafe implements SSO by checking the HTTP header and request variables and validates key values in these variables to insure the referring system has properly validated the user's identification.

IndustrySafe uses the SHA2 encryption method to encrypt the validation token. In order for the token to be properly validated, the client must setup the encryption process to use the following two parameters which will be supplied by IndustrySafe.

- An Encryption Key
- A Salt Value

One the SSO process has been setup, the log in process will work as follows:

1. The user logs into the client's user validation system.

2. The user clicks on a link or is automatically redirected to the IndustrySafe Login Page with a query string containing the following values:

    - UID - the User's IndustrySafe User ID
    - Name - the user's full name
    - TS - the current UTC date and time in 12-hour format

- MAC - an encrypted version of the query string containing the previous three values with the SALT value appended to the end.

A sample query string would look like the following:

```
UID=gabes&Name=Gabe%20Smith&TS=2/9/2012%202:35:25%20PM&MAC=45485FD75BCF454071E9109407140
```

3. The IndustrySafe Login Page, takes the unencrypted version of the query string, adds the Salt value to the end and then encrypts it. The encrypted value is compared to the MAC value.
4. If the values match, the time stamp is checked to ensure that it is not more than 30 minutes old.
5. If the time stamp is valid, the user ID is checked to ensure that a matching user account exists in IndustrySafe.
6. If the user ID is valid, the user will be logged into IndustrySafe.

If there is a failure in steps 3, 4, or 5 the user will receive an error message and will not be logged into IndustrySafe.

3 SSO Process Flow Diagram