This document describes the technical design for redirecting users to school systems from Gateway.

### Assumption

* The school system is installed in a secured school network environment.
* This is not a mutual authentication design, that is, the users cannot go back to Gateway from the school system.
* The data in the school system is not highly sensitive
* https is enabled on the school system.
* esf\_global\_id is used as the key to identify users.
* The logon users need to have Gateway logon account.
* SHA256 is used as the encryption algorithm for data exchange.
* School changes the secret text regularly. (e.g. at least twice a year)

### Configuration parameters (SGA is able to set these up in Gateway)

name: the name of the school system to be shown to users

icon: the icon to be shown

URL: e.g. school.edu/auth.php

secret text: 8-character-long private key for matching the key in the school system

user type: the types (parent/staff/student/guest) who can access the link

enabled: Yes/No

Gateway IP addresses: read-only

### Security

When a user clicks on the link in Gateway, he is redirected to the school system by the URL [https://school.edu/auth.php?g=esf\_global\_id&h=SHA-hashed[esf\_global\_id+serect\_text+esf\_global\_id]. The receiving end at the school, auth.php in this case, has to verify whether this request is valid by hashing esf\_global\_id+serect\_text+esf\_global\_id and compare it with the h parameter in the URL. The school system also has to check whether the requests are from Gateway servers by matching the IP addresses showing on the configuration parameters. They should redirect the users to an error or logon page when the verification is failed.

### User Interface



When the users logon to Gateway, they can find the School-based Systems tab under My Panels. There lists the icons of the linked systems. The icon is the URL to [https://school.edu/auth.php?g=esf\_global\_id&h=SHA-hashed[esf\_global\_id+serect\_text+esf\_global\_id].

### Application Program

Below is the sample code in PHP that verifies the authenticity of the URL request. They should be placed in the beginning of auth.php.

if (!in\_array($\_SERVER['REMOTE\_ADDR', $GATEWAY\_IP\_ADDR\_ARRAY)) {

 header(‘error\_page\_not\_from\_gateway’);

 die;

}

if (hash(‘sha256’,$\_GET[‘g’].$YOUR\_SECRET\_TEXT.$\_GET[‘g’])!==$\_GET[‘h’]) {

 header(‘error\_page\_faked\_url’);

 die;

}