Verify the phone number of a user

It is possible to verify that a user has access to read sms messages sent to a phone number.

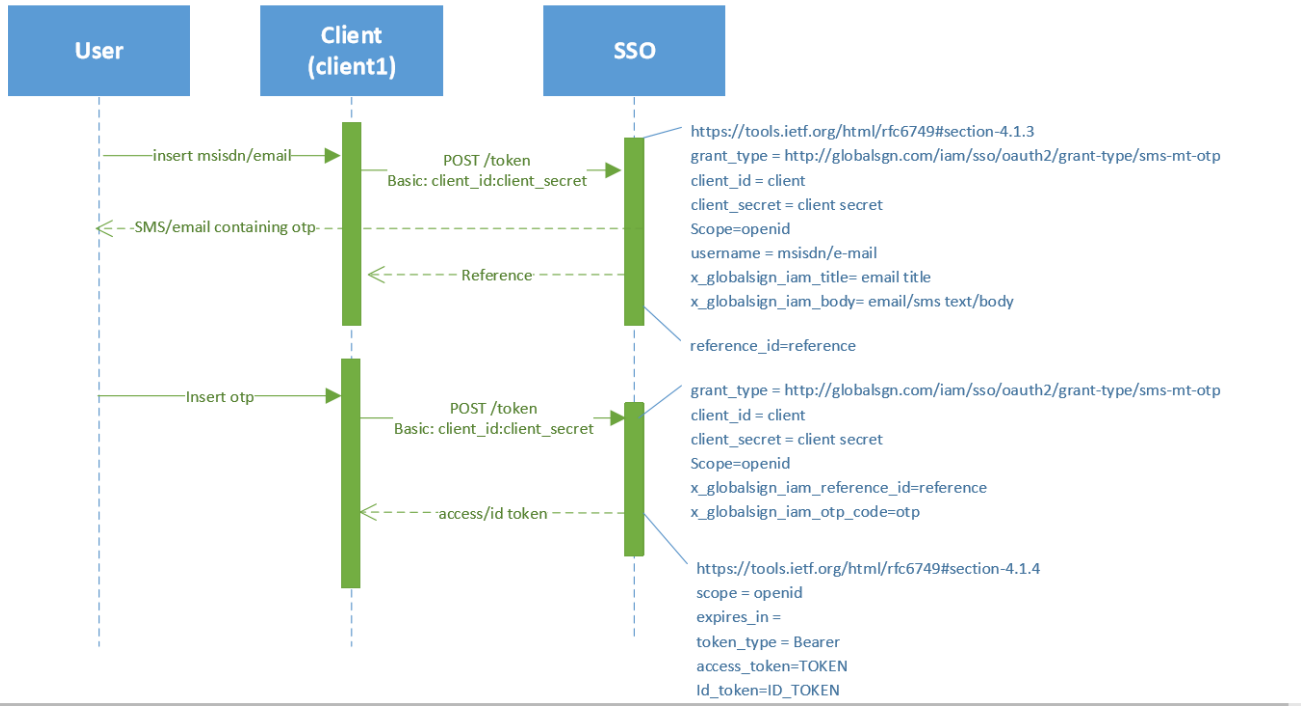
Applications can use the Ubisecure SSO infrastructure for sending the SMS message and verifying the code entered by the user.

The message displayed to the user in the SMS message together with the code can be dynamically defined at the time of the call.

Combined with an additional factor, this could be used by applications to add a second level of verification to a transaction prior to a high value or high risk event.

Technically the API uses the token request endpoint and a Ubisecure specific OAuth grant type.

Process flow



Step-by-step guide

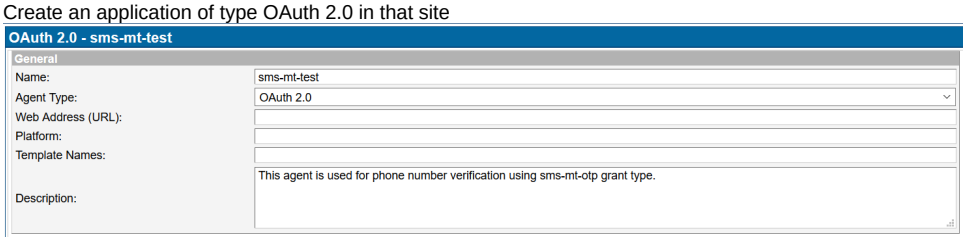
To configure Ubisecure SSO to support phone number verification:

1. In Ubisecure SSO Management, configure a new method of the type Unregistered SMS. In these screenshots, the name of the method is ubikey.sms.5
2. Add the URL of the SMS service to the configuration string. A GET request will be made to this address. If HTTP Response 200 is received, the message is deemed to have been sent successfully. {mobile} will be replaced with the phone number and {challenge} with the text to be shown in the message, including instructions and code.

Configuration String setting for SMS service
`smsUrl=http\://sms-sending-service.example.com/sendsms.asp?to\={mobile}&message\={challenge}`

3. Enable the method ubikey.sms.X on a site
4. Create a group called Unregistered SMS Users, assign membership based on the ubikey.sms.5 method just created.

5. Create an application of type OAuth 2.0 in that site



6. Activate the application using the following metadata. sms-mt-otp is disabled by default and can be used only if specified in the metadata. Because this flow is direct from the application to the server, without a user agent (browser), no return_uri is required

Metadata for phone number verification by SMS

```
{"grant_types":["http://globalsign.com/iam/sso/oauth2/grant-type/sms-mt-otp"]}
```

7. Press **Activate** to generate a client_id and secret required to make and verify requests. Save the client_id and secret safely in the calling application. An activated application will look like this:

8. Select the **Allowed To** tab and Add the group Unregistered SMS Users.
9. An authorization policy is not required. If used, attributes sent in the Authorization policy will appear in the id_token received in the verification response.

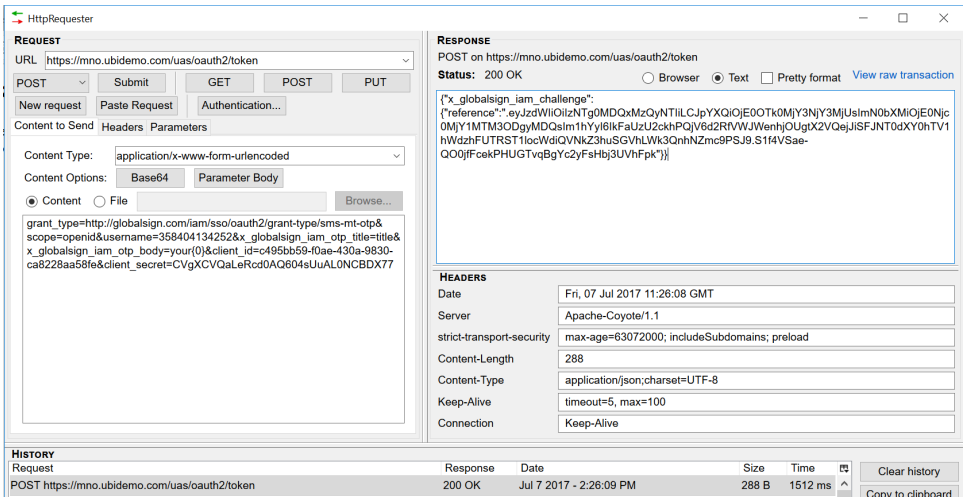
To send a verification code to a user:

1. Create a POST request to the /uas/oauth2/token endpoint of the Ubisecure SSO Server. The Content-Type must be application/x-www-form-urlencoded.
   The user phone number is sent in the username parameter.

POST body required for first token request

```
grant_type=http://globalsign.com/iam/sso/oauth2/grant-type/sms-mt-
otp&scope=openid&username=358404134252&x_globalsign_iam_otp_body=your%20otp%20code%20is%20{0}
&client_id=c495bb59-f0ae-430a-9830-ca8228aa58fe&client_secret=CVgXCVQaLeRcd0AQ604sUuAL0NCBDX7
```

   An example using the HttpRequester browser extension is shown here:



2. The response contains a x_globalsign_iam_reference_id value that must be stored and used again later when verifying the code:

Response to authorization request

```
{
    "x_globalsign_iam_challenge": {
        "reference": ".
eyJzdWIiOiIzNTg0MDQxMzQyNTIiLCJpYXQiOjE0OTk0MjY3NjY3MjUsImN0bXMiOjE0Njc0MjY1MTM3ODgyMDQsIm1hYyI6IkFaUzU2c
khPQjV6d2RfVWJWenhjOUgtX2VQejJiSFJNT0dXY0hTV1hWdzhFUTRST1locWdiQVNkZ3huSGVhLWk3QnhNZmc9PSJ9.S1f4VSae-
QO0jfFcekPHUGTvqBgYc2yFsHbj3UVhFpk"
    }
}
```

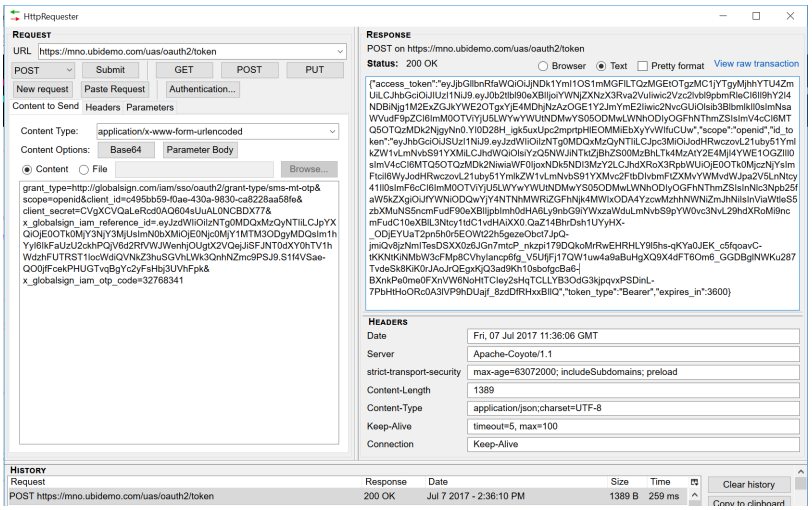
To verify a code collected from the user:

1. Create a POST request containing the x_globalsign_iam_reference_id together with the code collected from the user.

POST body required for second token request

```
grant_type=http://globalsign.com/iam/sso/oauth2/grant-type/sms-mt-otp&scope=openid&client_id=c495bb59-
f0ae-430a-9830-
ca8228aa58fe&client_secret=CVgXCVQaLeRcd0AQ604sUuAL0NCBDX77&x_globalsign_iam_reference_id=.
eyJzdWIiOiIzNTg0MDQxMzQyNTIiLCJpYXQiOjE0OTk0MjY3NjY3MjUsImN0bXMiOjE0Njc0MjY1MTM3ODgyMDQsIm1hYyI6IkFaUzU2c
khPQjV6d2RfVWJWenhjOUgtX2VQejJiSFJNT0dXY0hTV1hWdzhFUTRST1locWdiQVNkZ3huSGVhLWk3QnhNZmc9PSJ9.S1f4VSae-
QO0jfFcekPHUGTvqBgYc2yFsHbj3UVhFpk&x_globalsign_iam_otp_code=32768341
```

An example using the HttpRequester browser extension is shown here:



2. The response will contain an access_token and id_token

Response

```
{
    "access_token":
"eyJjbGllbnRfaWQiOiJjNDk1YmI1OS1mMGFlLTQzMGEtOTgzMC1jYTgyMjhhYTU4ZmUiLCJhbGciOiJIUzI1NiJ9.
eyJ0b2tlbl90eXBlIjoiYWNjZXNzX3Rva2VuIiwic2Vzc2lvbl9pbmRleCI6Il9hY2I4NDBiNjg1M2ExZGJkYWE2OTgxYjE4MDhjNzAzOGE1Y2JmYmE2Iiwic2NvcGUiOlsib3BlbmlkIl0sImNsaWVudF9pZCI6ImM0OTViYjU5LWYwYWUtNDMwYS05ODMwLWNhODIyOGFhNThmZSIsImV4cCI6MTQ5OTQzMDk2NjgyNn0.YI0D28H_igk5uxUpc2mprtpHlEOMMiEbXyYvWIfuCUw",
    "scope": "openid",
    "id_token": "eyJhbGciOiJSUzI1NiJ9.
eyJzdWIiOiIzNTg0MDQxMzQyNTIiLCJpc3MiOiJodHRwczovL21uby51YmlkZW1vLmNvbS91YXMiLCJhdWQiOlsiYzQ5NWJiNTktZjBhZS00MzBhLTk4MzAtY2E4MjI4YWE1OGZlIl0sImV4cCI6MTQ5OTQzMDk2NiwiaWF0IjoxNDk5NDI3MzY2LCJhdXRoX3RpbWUiOjE0OTk0MjczNjYsImFtciI6WyJodHRwczovL21uby51YmlkZW1vLmNvbS91YXMvc2FtbDIvbmFtZXMvYWMvdWJpa2V5LnNtcy41Il0sImF6cCI6ImM0OTViYjU5LWYwYWUtNDMwYS05ODMwLWNhODIyOGFhNThmZSIsInNlc3Npb25faW5kZXgiOiJfYWNiODQwYjY4NTNhMWRiZGFhNjk4MWIxODA4YzcwMzhhNWNiZmJhNiIsInViaWtleS5zbXMuNS5ncmFudF90eXBlIjpbImh0dHA6Ly9nbG9iYWxzaWduLmNvbS9pYW0vc3NvL29hdXRoMi9ncmFudC10eXBlL3Ntcy1tdC1vdHAiXX0.QaZ14BhrDsh1UYyHX-_ODjEYUaT2pn5h0r5EOWt22h5gezeObct7JpQ-jmiQv8jzNmITesDSXX0z6JGn7mtcP_nkzpi179DQkoMrRwEHRHLY9l5hs-qKYa0JEK_c5fqoavC-tKKNtKiNMbW3cFMp8CVhyIancp6fg_V5UfjFj17QW1uw4a9aBuHgXQ9X4dFT6Om6_GGDBglNWKu287TvdeSk8KiK0rJAoJrQEgxKjQ3ad9Kh10sbofgcBa6-BXnkPe0me0FXnVW6NoHtTCIey2sHqTCLLYB3OdG3kjpqvxPSDinL-7PbHtHoORc0A3lVP9hDUajf_8zdDfRHxxBIlQ",
```

```
    "token_type": "Bearer",
    "expires_in": 3600
}
```

3. The id_token signature should be verified and elements compared closely to the request to ensure that this is the response to the request. The id_token shown above contains more information:

    a. sub - subject - MISISDN phone number that the code was sent to)
    b. iss - issuer - The IDP that issued this token
    c. aud - audience - who this id_token is intended for (the client_id of the application)
    d. exp - expiry time - when this token expires
    e. iat - issued at - when it was issued
    f. auth_time - authentication time - when the user was authenticated
    g. amr - the authentication method used - Authentication Context Declaration Reference value from the methods settings screen (SAML equivalent of AuthnContextDeclRef)
    h. azp - Authorizing party - in this case the same as the recipient
    i. session_index - identifies the session on the IDP
    j. ubikey.sms.5.grant_type - value returned from the authentication policy if no Authentication Policy is set.

id_token contents (excluding header and signature)

```
{
  "sub": "358404134252",
  "iss": "https://mno.ubidemo.com/uas",
  "aud": [
    "c495bb59-f0ae-430a-9830-ca8228aa58fe"
  ],
  "exp": 1499430966,
  "iat": 1499427366,
  "auth_time": 1499427366,
  "amr": [
    "https://mno.ubidemo.com/uas/saml2/names/ac/ubikey.sms.5"
  ],
  "azp": "c495bb59-f0ae-430a-9830-ca8228aa58fe",
  "session_index": "_acb840b6853a1dbdaa6981b1808c7038a5cbfba6",
  "ubikey.sms.5.grant_type": [
    "http://globalsign.com/iam/sso/oauth2/grant-type/sms-mt-otp"
  ]
}
```

4. If the number entered by the user was incorrect or the code expired, an error code will be returned. The example below shows the error when an expired code is used.

Error response

```
{"x_globalsign_iam_challenge": {"reference": ".
eyJzdWIiOiIxMjMiLCJpYXQiOjE0Nzk5OTYzMzA5MDgsImN0bXMiOjg4Njg4NzYzNzY2MjAzNCw
ibWFjIjoibGlxSWRtdHdlakVuSmxoRm1yd0Y4Y0N4N0pNUzM4Vm05WW51LXhRUExscGc4ckduMFJO SktPSE55Uk9sU3NvS2RWdkpoUT09In0.
Usdl9RhGnlH6KJATWFfakYEFTyo1bl7jDvZ5SydWT4"},"error": "invalid_grant", "error_description": "OTP Expired"}
```

The validity time (timeout) of the OTP in minutes is set in Unregistered SMS authentication method settings.

Related articles

- Create a directory user mapping for SMS OTP
- Verify the phone number of a user
- Verify the email address of a user