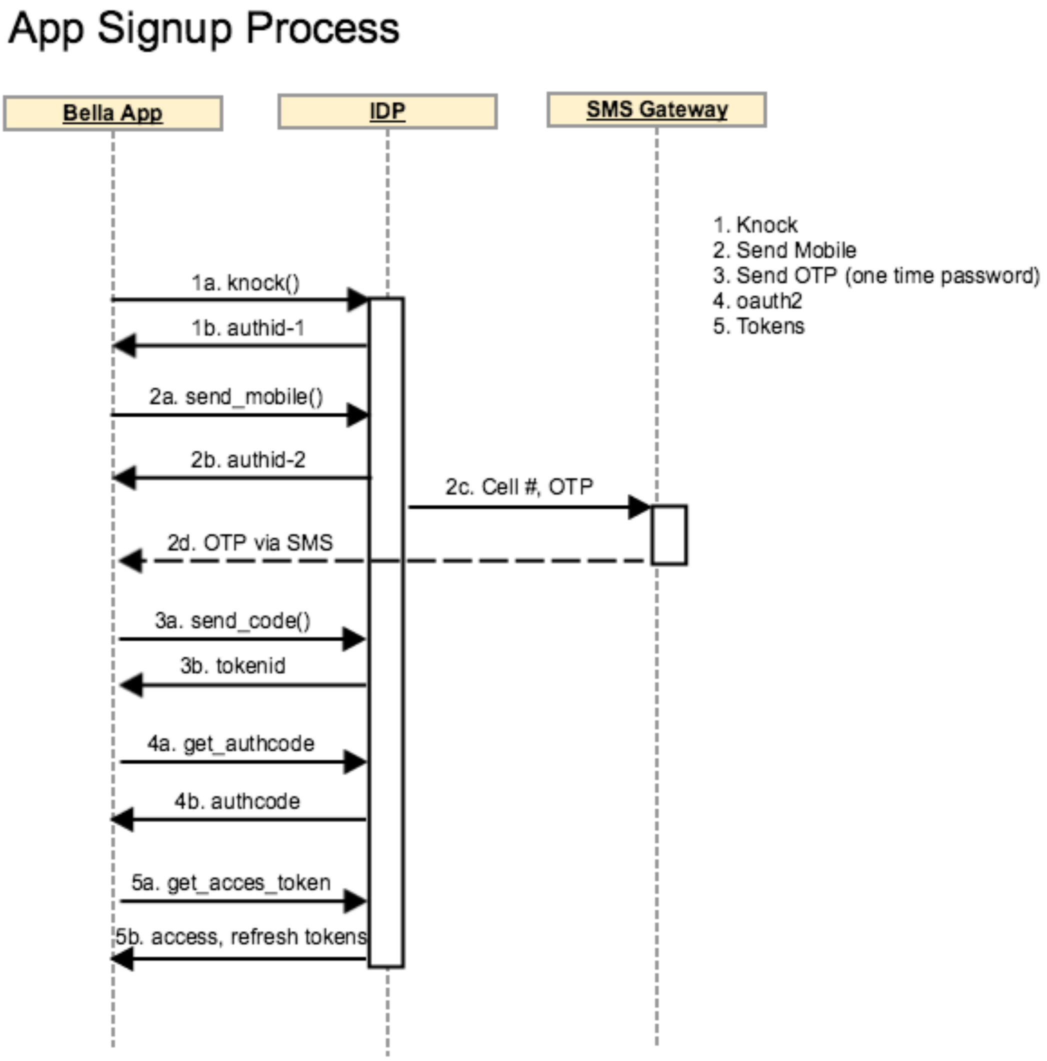
IDP - App Communication Processes

In this document are detailed six distinct communication processes which occur between IDP and the app. The first process, the signup, is the most lengthy and has five stages, while the remaining five processes are relatively simple and short.



Environments

Replace ${IDP_HOST} with the hostname for the environment you want to use:

Environment	Host
Production	`secure.bagus.io`

Test	`secure-test.bagus.cc`

Signup Process

Main Steps

In the diagram to the left and below in sections are detailed the five major steps of the app's signup process. In the HTTP output in the code blocks, certain strings such ass access tokens have been replaced with $STRINGNAME types of variables.

Other Steps, Future Signins

Not included in this description is how IDP passes off newly acquired information about the new user to Relevate and StoreBox. This occurs after the final tokens are distributed.

For the life of the refresh token, the app can communicate with IDP simply by submitting its refresh token and getting a fresh access token which it uses to authenticate. Once the refresh token has expired the user must go through the entire process again.

HTTP Headers

Following HTTP headers must be included in **all** requests to the IDP.

Header name	Description
X-correlation-id	Uniq correlation id as UUID
X-device-id	The devices dev id, if no id use hostname
X-mobile-nr	Users full mobile nr (with prefix 47)

1. Knock

Request: The app sends a request for an authid to IDP

Response: IDP responds with the first authid with which the app may identify itself

Request

```
POST
https://${IDP_HOST}/secure/json/authenticate?realm=/ap
p HTTP/1.1
Host: ${IDP_HOST}
X-correlation-id: ${CORRELATION_ID}
X-device-id: ${DEVICE_ID}
X-mobile-nr: ${MOBILE_NR}
Content-type: application/json
Accept: application/json
{}
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Content-API-Version: resource=2.0
Content-Type: application/json;charset=UTF-8
Date: Wed, 15 Feb 2017 15:47:26 GMT
Expires: 0
Pragma: no-cache
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=$JSESSID-1; Path=/; HttpOnly
Set-Cookie: authZPath=03; Path=/;
Domain=.prod.bella-idp.local
Set-Cookie: authZPath=03; Path=/; Domain=.bagus.io
Set-Cookie: AWSELB=$ELBID; Path=/; Domain=.bagus.io
Content-Length: 579
Connection: Close
{
    "authId": "$AUTHID-1",
    "callbacks": [
        {
            "input": [
                {
                    "name": "IDToken1",
                    "value": ""
                }
            ],
            "output": [
                {
                    "name": "prompt",
                    "value": "Phone Number:"
                }
            ],
            "type": "NameCallback"
        }
    ],
    "header": "Phone Validation Login",
    "stage": "ABPhone2",
    "template": ""
}
```

2. Mobile

Request: The app sends IDP the phone's number along with the authid so IDP recognizes who's sending it

Response: IDP sends the app a second authid. The previous one may now be discarded.

IDP - SMS Gateway: IDP sends the phone number along with a one time password (OTP) to the SMS gateway

SMS Gateway - Phone: The SMS gateway sends the OTP to the phone via SMS

Note: the third and fourth steps are not detailed in the code to the right, since it is communication that isn't directly between IDP and the app.

Request

```
POST
https://${IDP_HOST}/secure/json/authenticate?realm=/ap
p HTTP/1.1
Host: ${IDP_HOST}
X-correlation-id: ${CORRELATION_ID}
X-device-id: ${DEVICE_ID}
X-mobile-nr: ${MOBILE_NR}
Content-type: application/json
Cookie: JSESSIONID=$JSESSID-1; Path=/; HttpOnly;
authZPath=03; Path=/; Domain=.prod.bella-idp.local;
authZPath=03; Path=/; Domain=.bagus.io; AWSELB=$ELBID;
Path=/; Domain=.bagus.io
Accept: application/json
{
    "authId": "$AUTHID-1",
    "callbacks": [
        {
            "input": [
                {
                    "name": "IDToken1",
                    "value": "$MOBILENUM"
                }
            ],
            "type": "NameCallback"
        }
    ],
    "stage": "ABPhone2"
}
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Content-API-Version: resource=2.0
Content-Type: application/json;charset=UTF-8
Date: Wed, 15 Feb 2017 15:47:26 GMT
Expires: 0
Pragma: no-cache
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=$JSESSID-2; Path=/; HttpOnly
Content-Length: 880
Connection: Close
{
    "authId": "$AUTHID-1",
    "callbacks": [
        {
            "input": [
                {
                    "name": "IDToken1",
                    "value": ""
                }
            ],
            "output": [
                {
                    "name": "prompt",
                    "value": "Enter OTP"
                }
            ],
            "type": "PasswordCallback"
        },
        {
            "input": [
                {
                    "name": "IDToken2",
                    "value": 0
                }
            ],
            "output": [
                {
                    "name": "prompt",
                    "value": ""
                },
                {
                    "name": "messageType",
                    "value": 0
                },
                {
                    "name": "options",
                    "value": [
                        "Submit OTP",
                        "Request OTP"
                    ]
                },
                {
                    "name": "optionType",
                    "value": -1
                },
                {
                    "name": "defaultOption",
                    "value": 0
                }
            ],
            "type": "ConfirmationCallback"
        }
    ],
    "header": "Please enter your One Time Password, or
request a new one",
    "stage": "HOTP2",
    "template": ""
}
```

3. OTP

Request: The OTP, now received in an SMS on the phone, is entered into the app, which sends it along with the second authid to IDP

Response: IDP, satisfied that the app belongs to the phone whose number it received, sends the app a tokenid which will be used by OAuth

Request

```
POST
https://${IDP_HOST}/secure/json/authenticate?realm=/ap
p HTTP/1.1
Host: ${IDP_HOST}
X-correlation-id: ${CORRELATION_ID}
X-device-id: ${DEVICE_ID}
X-mobile-nr: ${MOBILE_NR}
Content-type: application/json
Cookie: JSESSIONID=$JSESSID-1; Path=/; HttpOnly;
authZPath=03; Path=/; Domain=.prod.bella-idp.local;
authZPath=03; Path=/; Domain=.bagus.io; AWSELB=$ELBID;
Path=/; Domain=.bagus.io
Accept: application/json
{
    "authId": "$AUTHID-1",
    "callbacks": [
        {
            "input": [
                {
                    "name": "IDToken1",
                    "value": "$SMSCODE"
                }
            ],
            "type": "PasswordCallback"
        },
        {
            "input": [
                {
                    "name": "IDToken2",
                    "value": 0
                }
            ],
            "type": "ConfirmationCallback"
        }
    ],
    "stage": "HOTP2"
}
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Content-API-Version: resource=2.0
Content-Type: application/json;charset=UTF-8
Date: Wed, 15 Feb 2017 15:47:34 GMT
Expires: 0
Pragma: no-cache
Server: Apache-Coyote/1.1
Content-Length: 164
Connection: Close
{
    "successUrl": "https://${IDP_HOST}:443/",
    "tokenId": "$TOKENID-1"
}
```

4. OAuth 2.0

Request: The app sends its new tokenid to IDP. On an application level, OAuth 2.0 receives the tokenid instead of OpenAM.

Response: OAuth on IDP validates the tokenid and sends the app an authcode

The client code embedded in the location header is going to be used in the next step to request the access token

Request

```
POST
https://${IDP_HOST}/secure/oauth2/authorize?realm=/app
HTTP/1.1
Host: ${IDP_HOST}
X-correlation-id: ${CORRELATION_ID}
X-device-id: ${DEVICE_ID}
X-mobile-nr: ${MOBILE_NR}
Cookie: secureToken=$TOKENID-1
Content-type: application/x-www-form-urlencoded
nonce=$NONCE&csrf=$TOKENID-1&decision=allow&redirect_u
ri=https%3A%2F%2F${IDP_HOST}%2Fsecure%2Fbella.html&res
ponse_type=code&client_id=app-client&scope=storeboxid+
account_number+identity+phone
```

Response

```
HTTP/1.1 302 Found
Accept-Ranges: bytes
Cache-Control: no-store
Date: Wed, 15 Feb 2017 15:47:34 GMT
Location:
http://${IDP_HOST}:80/secure/bella.html?scope=identity
%20phone%20account_number%20storeboxid&iss=https%3A%2F
%2F${IDP_HOST}%2Fsecure%2Foauth2&client_id=app-client&
code=$CLIENTCODE
Pragma: no-cache
Server: Restlet-Framework/2.3.4
Set-Cookie: JSESSIONID=$JSESSID-3; Path=/; HttpOnly
Vary: Accept-Charset, Accept-Encoding,
Accept-Language, Accept
Content-Length: 0
Connection: Close
```

5. Tokens

Request: The app sends IDP its new authcode

Request

Response: IDP (OAuth 2.0) sends back an access token and refresh token. The app will use these to continue communication and to get a new access token when it expires, respectively.

```
POST
https://${IDP_HOST}/secure/oauth2/access_token?realm=/
app HTTP/1.1
Host: ${IDP_HOST}
X-correlation-id: ${CORRELATION_ID}
X-device-id: ${DEVICE_ID}
X-mobile-nr: ${MOBILE_NR}
Content-type: application/x-www-form-urlencoded
Authorization: Basic $APPCLIENTID
Cache-control: no-cache
code=$CLIENTCODE&redirect_uri=https%3A%2F%2F${IDP_HOST
}%2Fsecure%2Fbella.html&response_type=code&grant_type=
authorization_code
```

Response

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: no-store
Content-Type: application/json
Date: Wed, 15 Feb 2017 15:47:34 GMT
Pragma: no-cache
Server: Restlet-Framework/2.3.4
Set-Cookie: JSESSIONID=$JSESSID-4; Path=/; HttpOnly
Vary: Accept-Charset, Accept-Encoding,
Accept-Language, Accept
Content-Length: 248
Connection: Close
{
    "access_token": "$ACCESSTOKEN",
    "expires_in": $EXPTIME,
    "nonce": "$NONCE",
    "refresh_token": "$REFRESHTOKEN",
    "scope": "identity phone account_number
storeboxid",
    "token_type": "Bearer"
}
```

Refresh Access Token

Request: The app requests a new access token and authorizes this with its refresh token.

Response: IDP responds with both a new refresh token and a new access token.

Request

```
POST
https://${IDP_HOST}/secure/oauth2/access_token?realm=/
app HTTP/1.1
Host: ${IDP_HOST}
X-correlation-id: ${CORRELATION_ID}
X-device-id: ${DEVICE_ID}
X-mobile-nr: ${MOBILE_NR}
Content-type: application/x-www-form-urlencoded
Authorization: Basic $APPCLIENTID
Cache-control: no-cache
redirect_uri=https%3A%2F%2F${IDP_HOST}%2Fsecure%2Fbell
a.html&response_type=code&refresh_token=$REFRESHTOKEN&
grant_type=refresh_token
```

Response

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: no-store
Content-Type: application/json
Date: Thu, 16 Feb 2017 09:16:48 GMT
Pragma: no-cache
Server: Restlet-Framework/2.3.4
Set-Cookie: JSESSIONID=$JSESSID-5; Path=/; HttpOnly
Vary: Accept-Charset, Accept-Encoding,
Accept-Language, Accept
Content-Length: 201
Connection: Close
{
    "access_token": "$NEWACCESSTOKEN",
    "expires_in": $EXPTIME,
    "refresh_token": "$NEWREFRESHTOKEN",
    "scope": "account_number identity phone
storeboxid",
    "token_type": "Bearer"
}
```

Show Token Info

Request: App requests information about the token.

Response: IDP responds with a payload containing information such as StoreBox id, access token, expiry of access token, account number and identity code.

Request

```
GET https://${IDP_HOST}/secure/oauth2/tokeninfo
HTTP/1.1
Host: ${IDP_HOST}
X-correlation-id: ${CORRELATION_ID}
X-device-id: ${DEVICE_ID}
X-mobile-nr: ${MOBILE_NR}
Authorization: Bearer $ACCESSTOKEN
```

Response

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: no-cache, no-store
Content-Type: application/json
Date: Thu, 16 Feb 2017 09:16:52 GMT
Server: Restlet-Framework/2.3.4
Set-Cookie: JSESSIONID=$JSESSID-6; Path=/; HttpOnly
Vary: Accept-Charset, Accept-Encoding,
Accept-Language, Accept
Content-Length: 370
Connection: Close
{
    "access_token": "$NEWACCESSTOKEN",
    "account_number": "$ACCTNUM",
    "client_id": "app-client",
    "expires_in": $EXPTIME,
    "grant_type": "refresh_token",
    "identity": "$IDNUM",
    "phone": "$MOBILENUM",
    "realm": "/app",
    "scope": [
        "identity",
        "phone",
        "account_number",
        "storeboxid"
    ],
    "storeboxid": "$STOREBOXID",
    "token_type": "Bearer"
}
```

Show User Info

Request: App requests user information.

Response: IDP responds with some of the same data as show tokeninfo did. Included are StoreBox id, sub, identity and account_number.

Request

```
GET https://${IDP_HOST}/secure/oauth2/userinfo
HTTP/1.1
Host: ${IDP_HOST}
X-correlation-id: ${CORRELATION_ID}
X-device-id: ${DEVICE_ID}
X-mobile-nr: ${MOBILE_NR}
Authorization: Bearer $ACCESSTOKEN
```

Response

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Content-Type: application/json;charset=UTF-8
Date: Thu, 16 Feb 2017 09:16:54 GMT
Server: Restlet-Framework/2.3.4
Set-Cookie: JSESSIONID=$JSESSID-7; Path=/; HttpOnly
Vary: Accept-Charset, Accept-Encoding,
Accept-Language, Accept
Content-Length: 167
Connection: Close
{
    "account_number": "$ACCTNUM",
    "identity": "$IDNUM",
    "phone": "$MOBILENUM",
    "storeboxid": "$STOREBOXID",
    "sub": "$MOBILENUM"
}
```

Sign Out

Request: App submits signout request, providing its access token to identify itself.

Response: IDP sends a confirmation of the signout request and finishes of with a close connection call.

Request

```
POST
https://${IDP_HOST}/secure/oauth2/token/revoke?realm=/
app HTTP/1.1
Host: ${IDP_HOST}
X-correlation-id: ${CORRELATION_ID}
X-device-id: ${DEVICE_ID}
X-mobile-nr: ${MOBILE_NR}
Content-type: application/x-www-form-urlencoded
Authorization: Basic $APPCLIENTID
token=$ACCESSTOKEN
```

Response

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Content-Type: application/json;charset=UTF-8
Date: Thu, 16 Feb 2017 09:16:58 GMT
Server: Restlet-Framework/2.3.4
Set-Cookie: JSESSIONID=$JSESSID-8; Path=/; HttpOnly
Vary: Accept-Charset, Accept-Encoding,
Accept-Language, Accept
Content-Length: 2
Connection: Close
{}
```

Delete User

Request: The app sends a DELETE request to IDP.

Response: IDP confirms the request and proceeds with the DELETE.

Request

```
DELETE https://${IDP_HOST}/user HTTP/1.1
Host: ${IDP_HOST}
X-correlation-id: ${CORRELATION_ID}
X-device-id: ${DEVICE_ID}
X-mobile-nr: ${MOBILE_NR}
Authorization: Bearer $ACCESSTOKEN
```

Response

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Date: Wed, 15 Feb 2017 16:01:13 GMT
Server: Restlet-Framework/2.3.4
Vary: Accept-Charset, Accept-Encoding,
Accept-Language, Accept
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Connection: close
Set-Cookie: SERVERID=03; path=/
Cache-control: private
{}
```