In order to work with the Rest-API endpoints, the client application must first be authenticated and authorized. API-clients using endpoints in the public domain (e.g. Discovery) must have a valid WISE-KEY. The endpoints in the shared domain must have a valid user login as well. The steps below describe the authentication steps:

1. Generate a WISE-KEY using the API-KEY, API-ID and ApplicationName.
   An example of how this is calculated is given in the appendix.

2. For the shared endpoints where patron data is used, it is necessary to login with username and password:
   1. /patron/authentication
      For logging in as a patron the endpoint /patron/authentication is used. A token will be returned upon successful registration. This must be provided as an Authorization in the request header for the relevant endpoints.
      This authentication makes it possible to consult your own data as a patron.
   2. /login
      The endpoint /login is used for signing in as a user. A token will be returned upon successful registration. This must be provided as an Authorization in the request header for the relevant endpoints.
      This authentication allows the API-client to make requests to the Wise system as a staff user.

The token is valid for the current day till 23:59:59. It is not necessary to login again on the same day.