日日是Oracle APEX

Oracle APEXを使った作業をしていて、気の付いたところを忘れないようにメモをとります。

2020年3月12日木曜日

APEX_JWTパッケージを使わずJWTを生成する

Oracle APEXに標準でAPEX_JWTという、Java Web Token (RFC 7519)を扱うパッケージが提供されています。ただし、APEX_JWTパッケージは署名アルゴリズムとして、"HS256" - HMAC SHA-256だけをサポートしています。これ以外のJava Web Ticketを作るために、一番追加作業が少ない手順を考えるために、とりあえずAPEX_JWTで作れるJWTをPL/SQLで実装するとどうなるか、というのを書いてみました。

```
set lines 1000
set serveroutput on
declare
  l_now       timestamp;
  l_secret    varchar2(32) := 'secret!';
  l_username  varchar2(32) := 'TESTUSER';
  l_jwt       varchar2(32767);
  l_jwt_token apex_jwt.t_token;
  l_jwt_t     apex_t_varchar2;

  l_header_json json_object_t;
  l_header_str  varchar2(200);
  l_header_base64 varchar2(400);
  l_payload_json json_object_t;
  l_payload_str  varchar2(200);
  l_payload_base64 varchar2(800);
  l_token varchar2(1000);
  l_hmac varchar2(1000);

  -- Unix時間の取得
  function unixtime(p_timestamp in timestamp)
  return pls_integer
  is
    l_date date;
    l_epoc number;
  begin
    l_date := sys_extract_utc(p_timestamp);
    l_epoc := l_date - date'1970-01-01';
    return l_epoc * 24 * 60 * 60;
  end unixtime;

  -- Base64のデコード
  function from_base64(t in varchar2) return varchar2 is
  begin
    return utl_raw.cast_to_varchar2(utl_encode.base64_decode(utl_raw.cast_to_raw(t)));
  end from_base64;

  -- Base64のエンコード
  function to_base64(t in varchar2) return varchar2 is
    l_base64 varchar2(32767);
  begin
    l_base64 := utl_raw.cast_to_varchar2(utl_encode.base64_encode(utl_raw.cast_to_raw(t)));
    l_base64 := replace(l_base64, chr(13)||chr(10), '');
    return l_base64;
  end to_base64;
begin
  -- 共通で使用する現在時刻
  l_now := current_timestamp;
  dbms_output.put_line('Current Timestamp = ' || l_now || ', unixtime = ' || unixtime(l_now));

  -- APEX_JWTパッケージを使用しJWTの作成
  -- Using Oracle APEX provided package APEX_JWT
  l_jwt := apex_jwt.encode (
    p_iss      => 'sqlplus',
    p_aud      => 'APEX',
    p_sub      => l_username,
```

```
    p_iat_ts   => l_now,
    p_exp_sec  => 10,
    p_signature_key => sys.utl_raw.cast_to_raw(l_secret));
  -- 生成したJava Web Token
  l_jwt_t := apex_string.split(l_jwt, '.');
  dbms_output.put_line('APEX_JWT.encode ============================');
  dbms_output.put_line('Header    = ' || l_jwt_t(1));
  dbms_output.put_line('Payload   = ' || l_jwt_t(2));
  dbms_output.put_line('Signature = ' || l_jwt_t(3));

  -- JWTをデコードし、内容を確認する。
  l_jwt_token := apex_jwt.decode (
    p_value         => l_jwt,
    p_signature_key => sys.utl_raw.cast_to_raw(l_secret) );
  --
  dbms_output.put_line('APEX_JWT.decode  ===========================');
  dbms_output.put_line('Header    = ' || trim(l_jwt_token.header) );
  dbms_output.put_line('Payload   = ' || trim(l_jwt_token.payload) );
  dbms_output.put_line('Signature = ' || trim(l_jwt_token.signature) );

  -- ヘッダーを手作業で生成する。
  dbms_output.put_line('Hand made ==================================');
  l_header_json := json_object_t();
  l_header_json.put('alg','HS256');
  l_header_json.put('typ','JWT');
  l_header_str := l_header_json.to_string();
  l_header_base64 := to_base64(l_header_str);
  dbms_output.put_line('Header    = ' || l_header_str);
  dbms_output.put_line('Header    = ' || l_header_base64);

  -- ペイロードを手作業で作成する。
  l_payload_json := json_object_t();
  l_payload_json.put('iss','sqlplus');
  l_payload_json.put('sub',l_username);
  l_payload_json.put('aud','APEX');
  l_payload_json.put('iat',unixtime(l_now));
  l_payload_json.put('exp',unixtime(l_now)+10);
  l_payload_str := l_payload_json.to_string();
  l_payload_base64 := to_base64(l_payload_str);
  dbms_output.put_line('Payload   = ' || l_payload_str);
  dbms_output.put_line('Payload   = ' || l_payload_base64);

  -- シグネチャを手作業で作成する。
  l_token := l_header_base64 || '.' || l_payload_base64;
  l_hmac := utl_raw.cast_to_varchar2(utl_encode.base64_encode(dbms_crypto.mac(
    utl_raw.cast_to_raw(l_token),
    dbms_crypto.HMAC_SH256,
    utl_raw.cast_to_raw(l_secret)
  )));
  l_hmac := trim(translate(l_hmac, '+/=', '-_ '));
  dbms_output.put_line('Signature = ' || l_hmac);
end;
/
```

上記の実行結果は以下のような感じです。時刻が毎回変わるため、同じ結果は生成されないです。

```
Current Timestamp = 12-MAR-20 04.29.05.616729 PM, unixtime = 1583998145
APEX_JWT.encode ============================
Header    = eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
Payload   = eyJpc3MiOiJzcWxwbHVzIiwic3ViIjoiVEVTVFVTRVIiLCJhdWQiOiJBUEVYIiwiaWF0IjoxNTgzOTk4MTQ1LCJleHAiOjE1ODM5OTgxNTV9
Signature = fgjlxE-JLcZdcvU4D_vqP9xX29G8lgC6w4zzifWCPuU
APEX_JWT.decode  ===========================
Header    = {"alg":"HS256","typ":"JWT"}
Payload   = {"iss":"sqlplus","sub":"TESTUSER","aud":"APEX","iat":1583998145,"exp":1583998155}
Signature = fgjlxE-JLcZdcvU4D_vqP9xX29G8lgC6w4zzifWCPuU
Hand made ==================================
Header    = {"alg":"HS256","typ":"JWT"}
Header    = eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
Payload   = {"iss":"sqlplus","sub":"TESTUSER","aud":"APEX","iat":1583998145,"exp":1583998155}
Payload   = eyJpc3MiOiJzcWxwbHVzIiwic3ViIjoiVEVTVFVTRVIiLCJhdWQiOiJBUEVYIiwiaWF0IjoxNTgzOTk4MTQ1LCJleHAiOjE1ODM5OTgxNTV9
Signature = fgjlxE-JLcZdcvU4D_vqP9xX29G8lgC6w4zzifWCPuU
```

Base64変換はこちらの記事、Base64の変換結果から改行を除く方法はこちらの記事、Unix時間の取得はこちらの記事、それ以外にはこちらの記事も参考にさせていただきました。ありがたいことです。もちろん、RFC 7519とRFC 4648も。

完

Yuji N. 時刻: 16:35

共有

‹ ホーム ›

ウェブ バージョンを表示

自己紹介

Yuji N.

日本オラクル株式会社に勤務していて、Oracle APEXのGroundbreaker Advocateを拝命しました。
こちらの記事につきましては、免責事項の参照をお願いいたします。

詳細プロフィールを表示