ARTIGO: 11595
dart + crypto + hmac + aqueduct

Dart

```
import 'dart:convert';
import 'package:convert/convert.dart';
import 'package:crypto/crypto.dart';


var key = "my key";
var message = "my message";

// use sha1 algorithm
var hmac = new Hmac(sha1, UTF8.encode(key));

// conver message, or use bytes from body request if is webserver
var bytes = UTF8.encode(message);

// calcule hash
var digest = hmac.convert(bytes);

// encode hash to base64
var calculedHash = BASE64.encode(digest.bytes);
```

Aqueduct

```
class ApiController extends HTTPController {


  // prepare controller to handler original bytes from request
  @override
  void willDecodeRequestBody(HTTPRequestBody body) {
    body.retainOriginalBytes = true;
  }

  @httpPost
  Future<Response> send() async{

    // get post signature
    var signature = request.innerRequest.headers.value("Hub-Signature");

    var apiKey = "my api key";
    var hmac = new Hmac(sha1, UTF8.encode(apiKey));
    var bytes = request.body.asBytes();
    var digest = hmac.convert(bytes);

    var calculedSignature = BASE64.encode(digest.bytes);

    // check signature
    if(calculedHash != calculedSignature){
        return new Response.unauthorized();
    }

    // do anything

    return new Response.ok({ "message": "my message" });
  }
}
```