Authenticated Monetization API

Extends API: Monetization API

Current Version: 0.2

Used by: The Item Transaction API, Item Info API, Subscription Reward API v1&v2, Subscription Status API v2, Subscription Cancel API v2, Subscription Refund API v2, Subscription Sync API v2, Subscription Grace API v2.

Summary

An API interface that defines authenticated (but not encrypted) requests.

Request

The request body is replaced by the following:

Request Body

<securityHash>" "<jsonRequest>

where

- <securityHash> is a base-64-encoded SHA-1 HMAC hash of <jsonRequest> using <secret> as the hmac key. If the hash sent in the request doesn't match the hash calculated on the responder's end, the request should fail with <error-type> "unauthorized".
- <secret> is a shared secret unique between the "requester" and the endpoint url. The secret should be agreed upon between the team implementing the requester and the team implementing the responder (future versions of this API will hopefully obtain the secret using the DCOP auth service).
    - Monetization - when interacting with monetization, QA will have the secret "QA_secret_key" and production will have some other key created by monetization.
- " " is a space
- <jsonRequest> is the original reponse body as defined by Monetization API

Example Request Body

<jsonRequest>: {

- "system": "monetization"
- "requester": "btetrud"
- "t":1344385436
- "idOrigin": "facebook"
- "id": 23489
- "network": "f"
- "user":"c28k3fjj9"
- "items":[
    - {
        - "category":"item"
        - "id":"12"
        - "amount":1
    - }
-]

}

stringified <jsonRequest>:

```
{"system":"monetization","requester":"btetrud","t":1344385436,"idOrigin":"
facebook","id":23489,"network":"f","user":"c28k3fjj9","items":[{"category"
:"item","id":"12","amount":1}]}
```

secret: dummySecret

securityHash: G7sSpScpOgVc/GnZqSohRzpIvu0=

full request body:

```
G7sSpScpOgVc/GnZqSohRzpIvu0=
{"system":"monetization","requester":"btetrud","t":1344385436,"idOrigin":"
facebook","id":23489,"network":"f","user":"c28k3fjj9","items":[{"category"
:"item","id":"12","amount":1}]}
```

Response

The response body, <jsonResponse>, is extended in the following way:

- <error-type> has the standard type:** "unauthorized" - the request could not be authorized
- <error-message> for <error-type> "unauthorized" are not recommended in normal cases

Supplementary Info

Security Techniques used

- hashing rather than encryption for authentication but not privacy
- SHA-1 hash for speed yet reasonable security

Additional Examples

<securityHash>

Java:

```
// hmac based on RFC 2104 (unsure if this is true anymore)
    // returns base64 encoded string
    public static String sha1HMAC(String key, String message) throws
Throwable {
        SecretKeySpec spec = new SecretKeySpec(
            key.getBytes(),
            "HmacSHA1");

        Mac mac = Mac.getInstance("HmacSHA1");
        mac.init(spec);

        byte[] result = mac.doFinal(message.getBytes());
        byte[] empty = new byte[]{};
// don't do line separaters..
        org.apache.commons.codec.binary.Base64 encoder = new Base64(0,
empty);  // and don't chunk the result

        return encoder.encodeToString(result);
    }
```

Change Log

Note: all items in the change log are reflected in the canonical documentation above.

v0.2

- Removed the nonce parameter, as it doesn't actually serve any security related purpose for authentication hashes

v0.1

- Created from the Item Transaction API v1.0