Dokumentace k API WebMeeting

verze z 9. 11. 2020

Marek Skalka, skalka@ipcc.cz

I. Popis rozhraní

Všechny dostupné metody naleznete v dokumentaci rozhraní WebmeetingInterface na adrese https://admin.webmeeting.cz/docs/

II. Jak poslat požadavek na server?

Pro zaslání jakéhokoliv požadavku je potřeba

- adresa serveru (`'https://admin.webmeeting.cz/api'`),
- login uživatele,
- sdílené tajemství pro podepisování požadavků (`api_request_secret`) a
- sdílené tajemství pro ověřování odpovědí (`api_response_secret`)

Každý uživatel má vlastní dvojici těchto tajemství.

Požadavek se posílá jako POST požadavek na adresu serveru takto:

```
POST /api/ HTTP/1.1
Host: admin.webmeeting.cz
Accept: */*
Content-type: application/json
Authorization: SaltedChecksum: d7a5f859724ffe606a8ddcc293b811905f6d5df6022cb8059e3088…
Content-Length: 198

{"action":"createMeeting","login":"loginklienta","name":"Uvodni porada",
"time_begin":"24.09.2020 11:00","speaker_name":"Elroy Geddes",
"description":"Popis uvodni porady","type":2,"timestamp":"2020-09-23
10:23:11","client":"loginklienta"}
```

Tělo požadavku je JSON obsahující atributy action (název volané funkce), všechny parametry volané funkce, atribut timestamp s aktuálním časem a atribut client s loginem uživatele.

Krom toho se z tohoto JSONu se spočítá hash metodou HMAC algoritmem SHA1 se sdíleným tajemstvím pro podepisování požadavků, například takto:

```
$saltedChecksum = hash_hmac("sha256", $json, $api_request_secret);
```

a pošle se v hlavičce jako Authorization jako SaltedChecksum.

Hodnota atributu client specifikuje klienta, na jehož účtě se operace provádí, hodnota atributu login specifikuje klienta, který přes API posílá požadavek a jehož tajemstvími se podepisují zprávy (nahřazený účet). Pro uživatele jednajícího vlastním jménem je parametr login a client shodný.

III. Jak zpracovat odpověď ze serveru

Odpověď serveru vypadá takto:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Authorization: SaltedChecksum: ba2f8e65c0e692a01e350fad40f6297447b93d8de5d3aca924e5af…
Date: Thu, 21 May 2020 12:56:52 GMT
Content-Length: 58

{"response":4667,"server_timestamp":"2020-09-23 10:22:27"}
```

1. Ověříme, že HTTP kód odpovědi je 200 nebo 201
   - pokud nikoliv, ale HTTP kód odpovědi je 400, viz níže
2. Ověříme, že tělo odpovědi je JSON
3. Spočítáme hash příchozí zprávy metodou HMAC algoritmem SHA1 se sdíleným tajemstvím pro ověřování odpovědí, např.:
   ```
   $hashComputed = hash_hmac("sha256", $body, $api_response_secret);
   ```
4. Ověříme, že námi spočítaný hash se shoduje s hashem z HTTP hlavičky odpovědi Authorization: SaltedChecksum
5. Ověříme, že odpověď obsahuje hodnotu indexovanou "server_timestamp" a ta obsahuje aktuální čas ± tolerance
6. Z hodnoty odpovědi indexované "response" získáme návratovou hodnotu volané funkce.

Pokud je HTTP kód odpovědi 400 a tělo odpovědi je JSON, v těle odpovědi pod klíčem error můžeme získat popis chyby a pod klíčem code její chybový kód.