

SchoolBOX WS

Jurn Wubben

Websocket communication between the SchoolBox device and the associated server.

November 07, 2025

Contents

1. Messages	3
1.1. Heartbeat	3
1.1.1. Server	3
1.1.2. Device	3
1.2. Registration	3
1.2.1. Server	3
1.2.2. Device	3
1.3. Authentication	3
1.3.1. Server	3
1.3.2. Device	3
1.4. Session	3
1.4.1. Server	3
1.4.2. Device	3
2. General flow	4

1. Messages

1.1. Heartbeat

1.1.1. Server

- {"c": "ping"}
- {"e": 0, "info": "Pong missed"}

1.1.2. Device

- {"c": "pong"}

1.2. Registration

1.2.1. Server

- {"c": "reg_pin", "d": {"pin": 1234}} // Pin is a random integer. Length doesn't really matter, as long as it fits on the screen.
- {"c": "reg_ok"}

1.2.2. Device

- {"c": "reg_start"}

1.3. Authentication

1.3.1. Server

- {"c": "auth_nonce", "d": {"nonce": "random_string"}} // Should be a long, random generated string.
- {"c": "auth_ok"}
- {"e": 1, "info": "Invalid packet, wrong ID."}
- {"e": 2, "info": "Invalid signature."} // the info doesn't matter
- {"e": 3, "info": "Logged in at other place."} // the info doesn't matter

1.3.2. Device

- {"c": "auth_start", "d": {"id": "id"}} // Id that is provided with registration.
- {"c": "auth_validate", "d": {"signature": "HMAC hash of nonce"}}
 - The HMAC is a SHA256 with the password as the key, and the nonce as the data.
 - The returned signature is encoded as hex.
 - [Example implementation in JS.](#)^o

1.4. Session

1.4.1. Server

- {"c": "session_start", "d": {"text": "Question?"}}
- {"c": "session_stop"}

1.4.2. Device

- {"c": "session_vote", "d": {"vote": 1}} // Vote is an integer in the range of 1..5

2. General flow

