

How to Use the Wireless

Welcome! The following general SSIDs are provided:

- **Hackerhotel** (WPA2 802.1X, 2.4GHz and 5 GHz)
- **Hackerhotel-open** (open/OWE, 2.4 GHz and 5 GHz)
- **eduroam** (2.4 GHz and 5 GHz)
- **spacenet** (2.4 GHz and 5 GHz)

You can use **hacker / hacker** or **guest / guest** when using MS-CHAPv2 inside TTLS or PEAP, or choose any username/password combination when connecting with PAP inside TTLS.

The SHA256 fingerprint of the server's certificate is:

2D:15:22:89:AE:FE:5A:7C:76:D8:23:1D:42:D9:DE:1E:88:17:08:F6:73:46:E1:ED:99:7C:D8:56:A3:09:92:4D

The subject CN on the certificate is radius.eventinfra.org. It is signed by Let's Encrypt for your convenience, though the fingerprint is the thing to check.

Note that this setup is only slightly more secure than open wireless but not by much; e.g. it relies on X.509. Remember that X.509 was chosen at a time when people wanted to protect against credit card theft on the internet by common criminals, not against entities with considerable resources.

Extra: by default inbound traffic to your device is only allowed from the event-network. Use **outboundonly / outboundonly** to only allow outbound traffic from your device, giving you basic protection and a way to save battery usage. Alternatively, use **allowany / allowany** to allow any inbound traffic to your device from the internet (and event-network).

EventInfra.org