# Design notes

These are our design notes from our first real design meeting. Below is an overview and a list of the important points we discovered during our design meeting which are important to keep in mind while reading.

We choose to focus on the **Lock down scenario**.

Topics discussed are:

* Installation
* Configuration
* Presets
* Multiple controllers (i.e. phones)
* Remote scenarios control within the home

**Important point: Do not depend on external services!**We only want to require a phone and a Wifi hotspot in an existing home.

**Important point: The app is just a remote!**The phone app, i.e. the controller, is just a remote used to trigger actuators and read sensor data, not something that can have running logic, active presets, which reacts to context changes and triggers actuators. The phone is a volatile device that moves, gets turned off, etc., and can thus not be relied on to handle active presets, as this would result in a very unpredictable home.

**Important point: An actuator is also a sensor!**  
This is more from object oriented point of view, but since an actuator also has to be able to report on its current status, just like a sensor does, it is both a sensor and an actuator to the controller.

## Installation

The workflow diagram below illustrates the main points, here are our assumptions:

The thingy has:

* A passive NFC tag and/or QR code for installation containing the thingies ad hoc Wifi’s SSID and passcode
* A physical reset/install mode button
* The phone app automatically transitions to the Configuration workflow from the installation workflow

**Regarding security during installation:** If a thingy has a random SSID (possibly hidden) and a passcode set when it is in install mode, it should be not be possible for an attacker to take control of the device before the user is able to run through the installation workflow.

**Challenge:** How to establish secure communication between the device and the T. By secure we want to prevent eavesdropping by encrypting communication and authentication of the user, and allow access to be delegated to multiple users. A possible idea is to create an encryption certificate that is used to encrypt traffic and authenticate the sender. The certificate can be shared other authorized users.



## Configuration

See workflow diagram below.

**Challenge 1:** A thingy is assigned a dynamic IP from the homes Wifi router/hotspot. We need a fast, consistent way to establish an IP communication channel with the device with only its MAC address available, i.e. resolve its IP based on its MAC address.

**Challenge 2:** How to dynamically generate an UI for a thingy’s specific settings and/or calibration.



## Presets

This was previously mentioned as macros, but we think Presets is a better name.

We imagined different levels of Presets, simple ones changes the state of a one or more thingies in a sequential order and checks sensors for specific states, and more advanced Presets that allow users to define conditions (sensor states) which must be met to proceed or use sensor state to branch to a different execution path. For this project, we do not thing it is required to implement/support more than the simple version.

See the diagram below for a Preset creation workflow.



## Multi-user scenarios / multiple controllers

We still miss a lot of details in regards to the multiple controllers issue, here are our notes so far (controller = phone app):

* State is on the individual thingies, no need to keep that in sync between controllers
* Configuration, presets, security tokens/certificates needs to be synchronized between controllers
* A peer to peer solution seems to be the optimal, with controller devices automatically synchronizing with each other when connected to the home Wifi and timestamping of data determine which dataset on controllers is the most current

## Remote scenarios within the home

We realized that even within a home there is a remote scenario, e.g. the kids should not be able to control the lights in the parents’ bedroom.

This brings up the question of an *owner* of a thingy within a home, or maybe a *primary owner*, i.e. the daughter might be the owner of the devices in her home, but the parents have access to them, but not her siblings.

Another discussion point is this, if I am in a room which is not “mine”, should I be able to control e.g. the lights, like I normally would by having physical access to the light switch? This would require us to have indoor tracking and this complicates and raises more challenges.

Our instinct is to keep things simple, so we will only handle the ownership issue, and keep indoor location context out of it.