Wireless Internet Connectivity for Embedded Devices

Wi-Fi Easy Setup
Cooee

April 2013

IMPORTANT NOTE

The Cooee™ Protocol may not work with some Access Points or Setup Clients. Please review the caveats presented on Page 24

Cooee! (IPA /ku:'i:/) is a shout used in Australia,
usually in the Bush, to attract attention,
find missing people, or indicate one's own location.

-- Wikipedia

The Wi-Fi Setup Problem

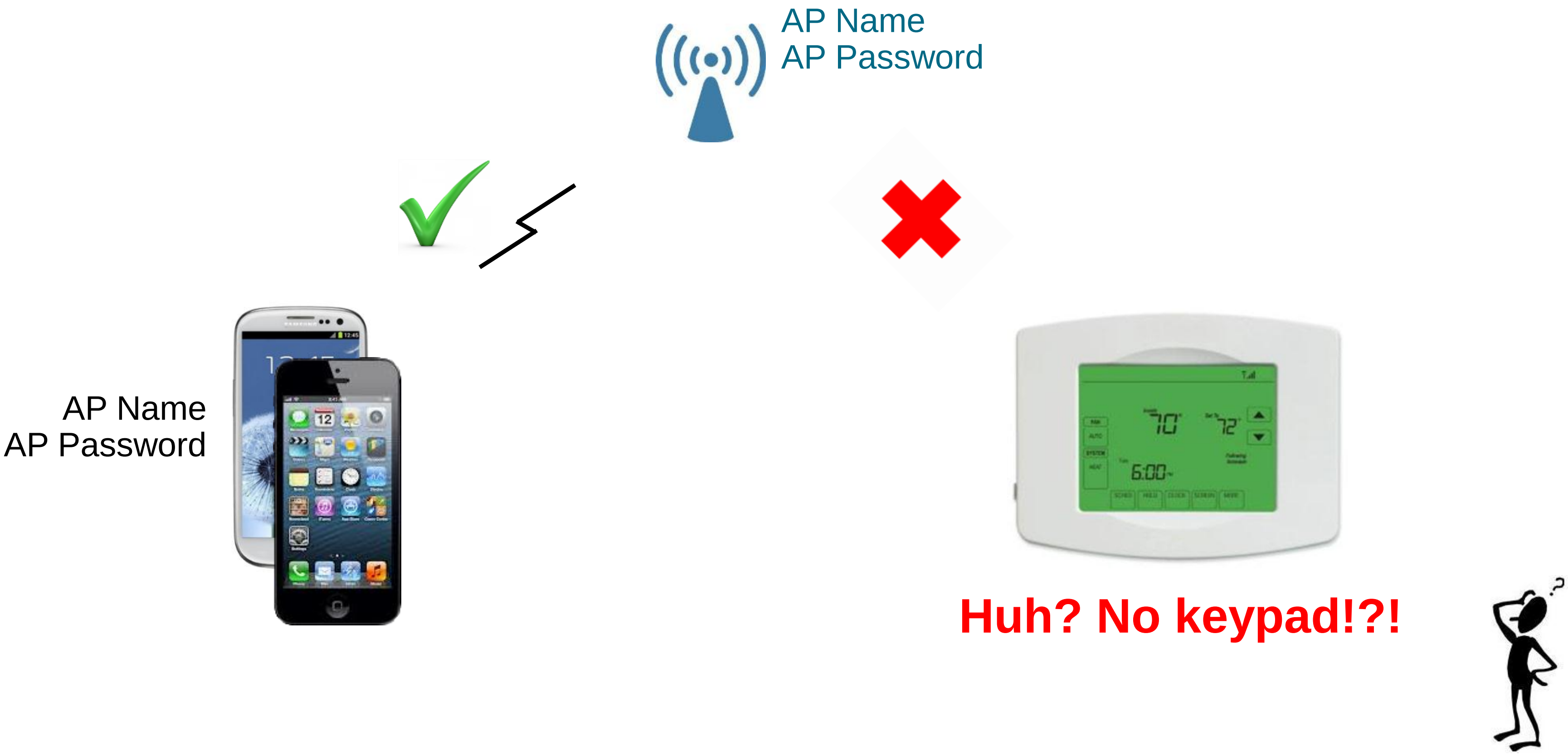
- **All Wi-Fi clients require setup information to**
  - Connect to a Wi-Fi access point : AP Name (SSID) / Password (Passphrase)
  - Find devices and advertise services on a network (once connected)
- **Sophisticated clients (phones, tablets, laptops)**
  - Great user interface (keyboard, display) to enter AP Name / AP Password
  - Lots of memory to run a network discovery protocol eg. mDNS/Bonjour
- **Deeply Embedded WICED Devices**
  - Minimal user interface (buttons, LEDs)
  - Low memory (typically ≤128kB)

PROBLEM STATEMENT

How does a user enter an AP Name / AP Password into a WICED device easily, and then how does the device find other devices or advertise services on the network?

How Does a User See the Problem?

- My Phone is already on the home Wi-Fi network
- I know the password for the home network
- How do I enter this information into the device?



AP Name
AP Password

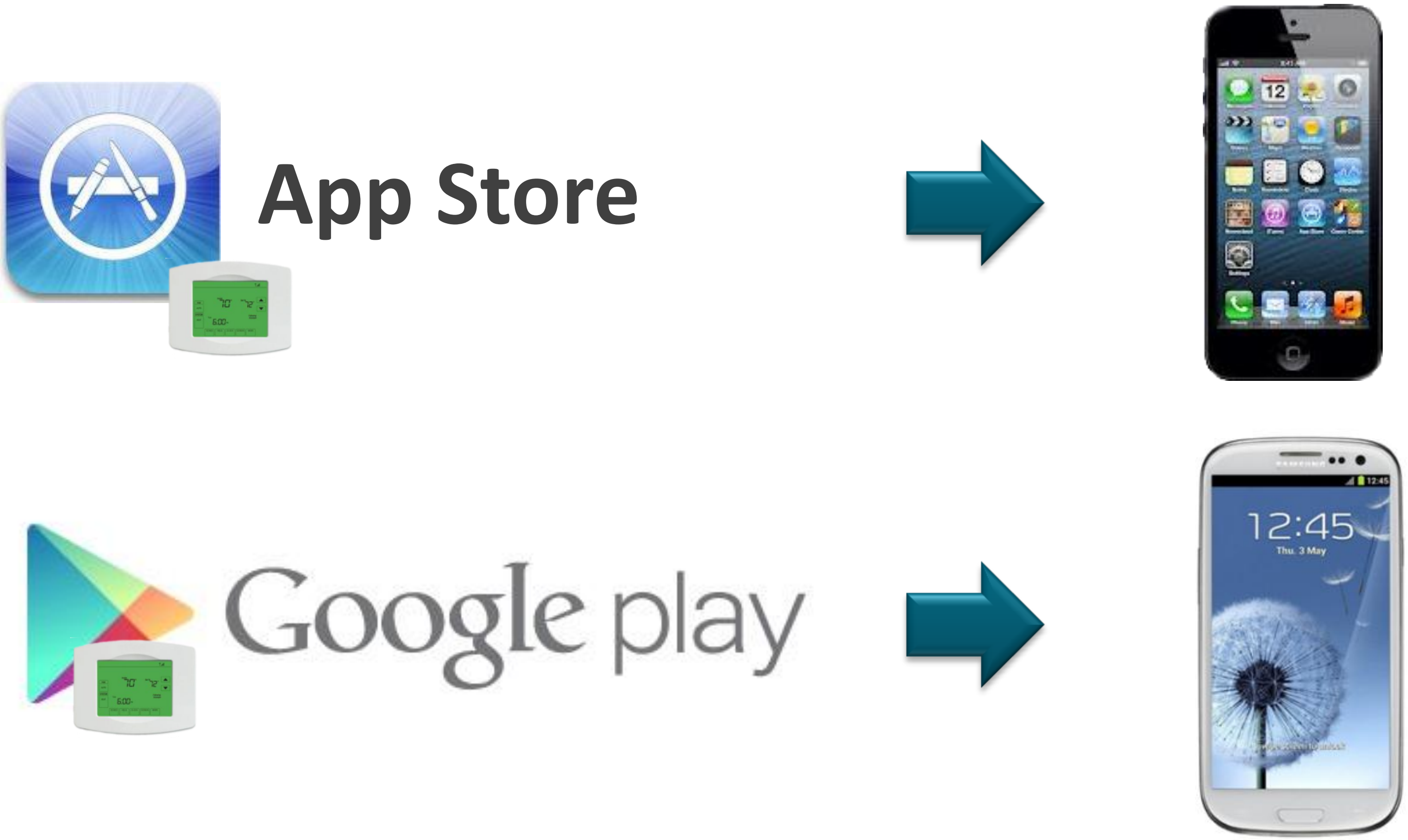
AP Name
AP Password

Huh? No keypad!?!

Wi-Fi Easy Setup in 4 Steps using Cooee

User Experience

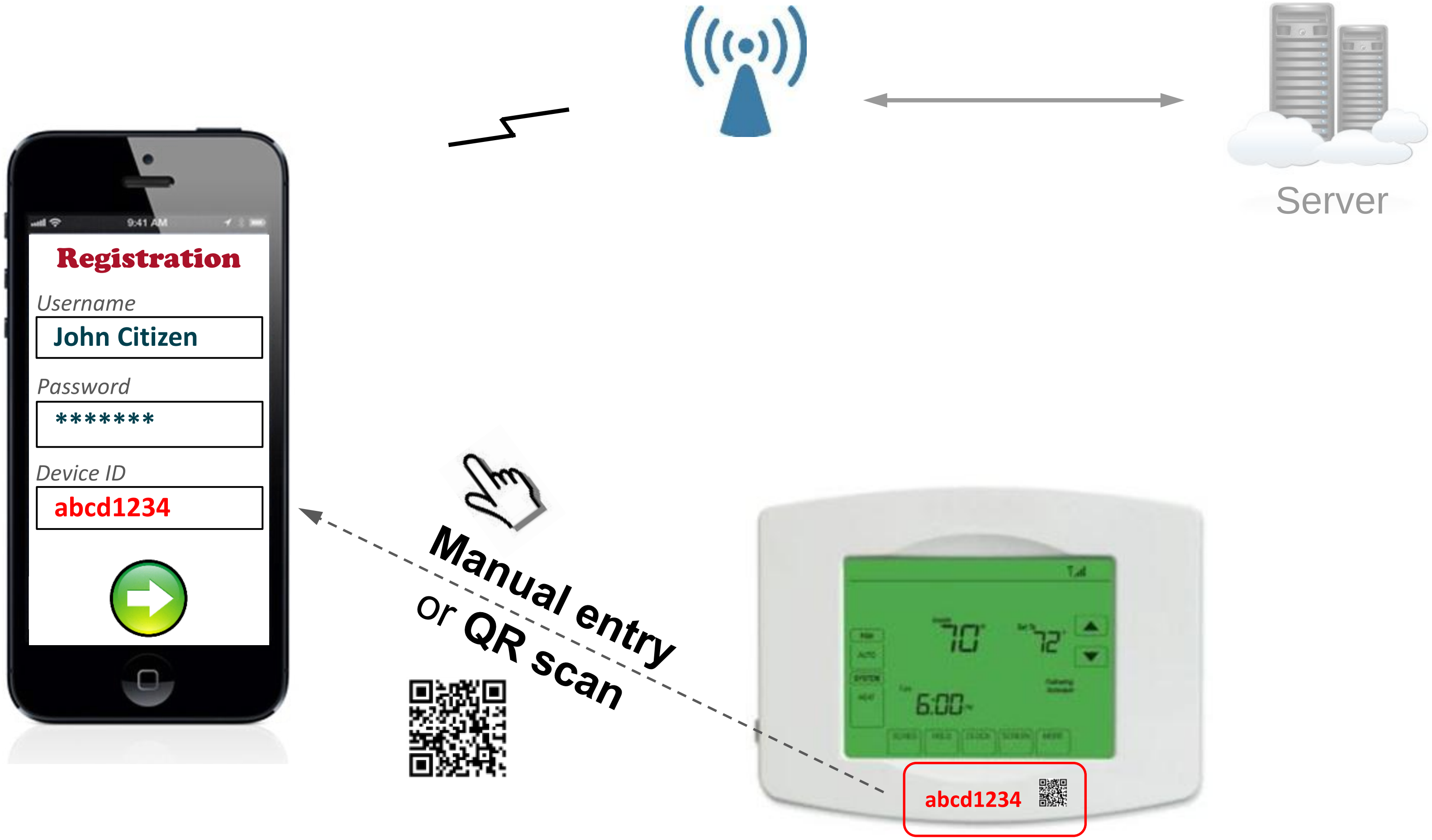
Step 1 Download an App for the Device



Wi-Fi Easy Setup – Cooee™

User Experience

Step 2 Register the Device



Registration

Username

John Citizen

Password

****

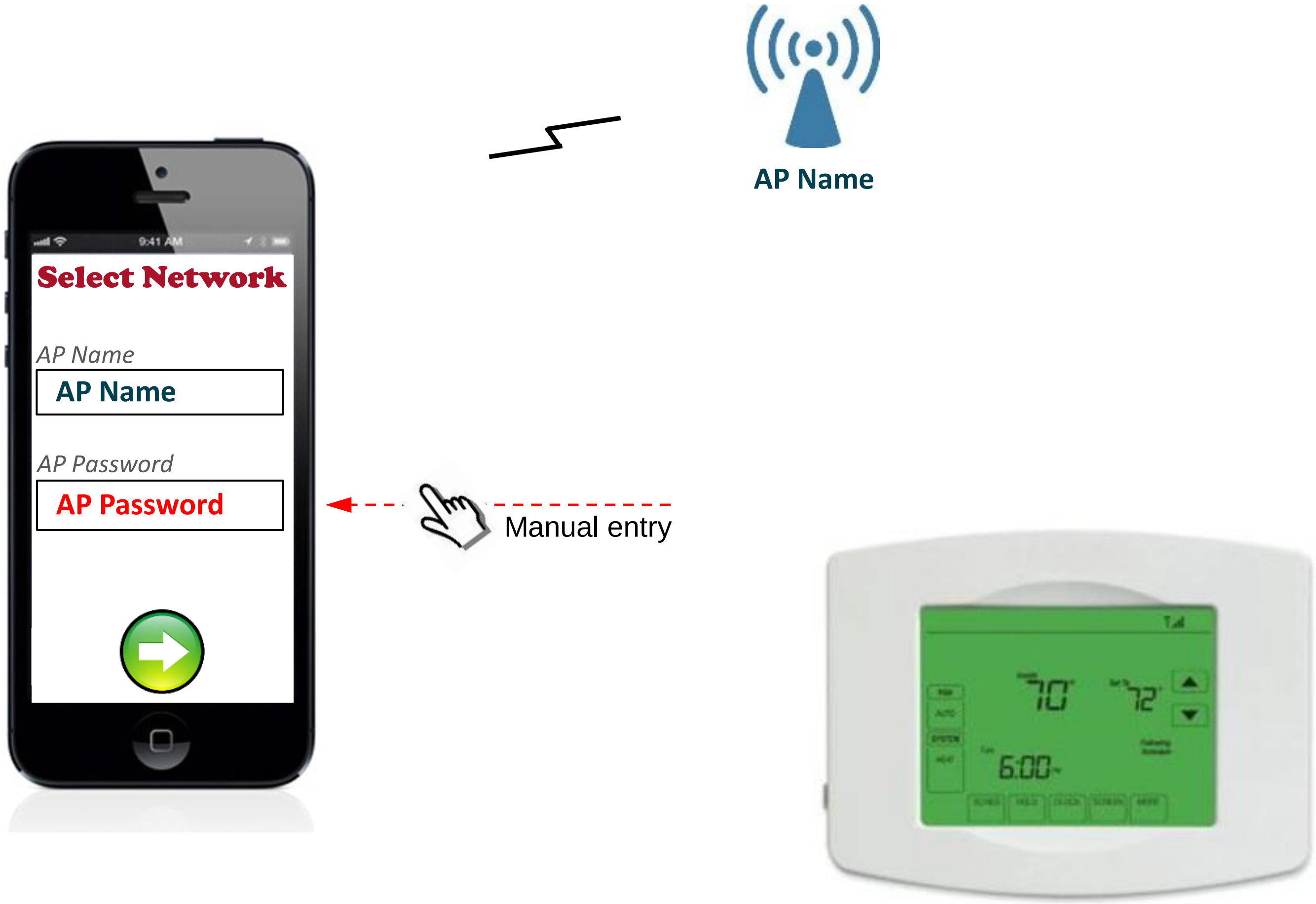
Device ID

abcd1234

Wi-Fi Easy Setup – Cooee™

User Experience

Step 3 Type the AP Password



Select Network

AP Name

AP Name

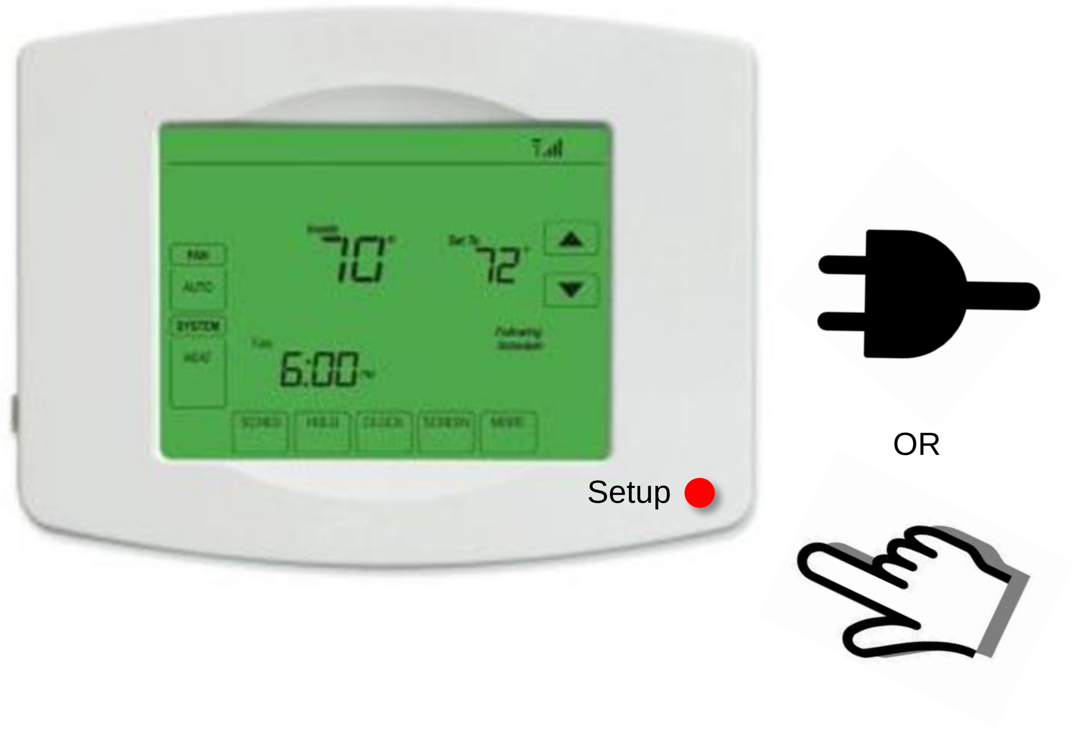
AP Password

AP Password

Wi-Fi Easy Setup – Cooee™

User Experience

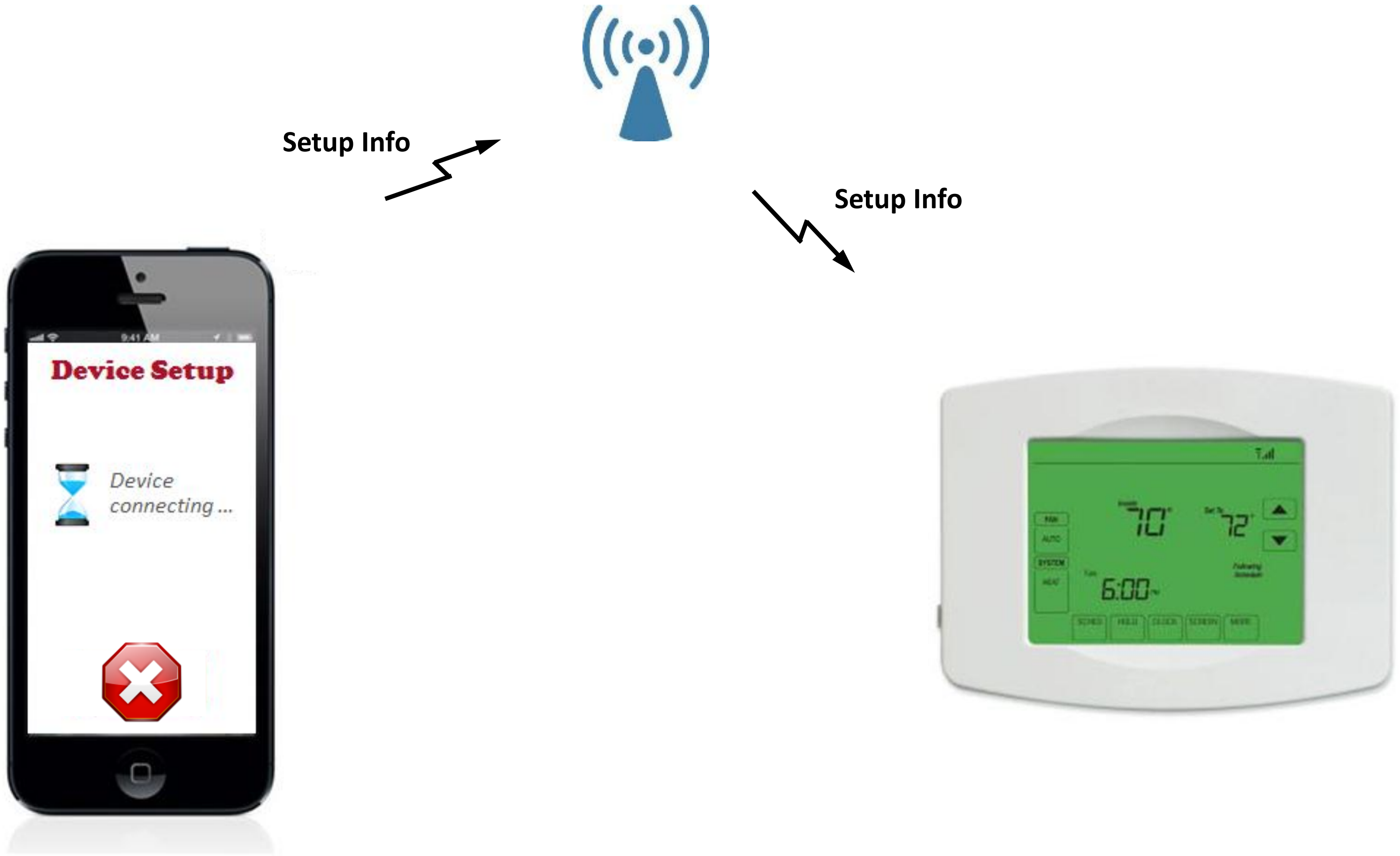
Step 4 Power on the device OR press Setup



Wi-Fi Easy Setup – Cooee™

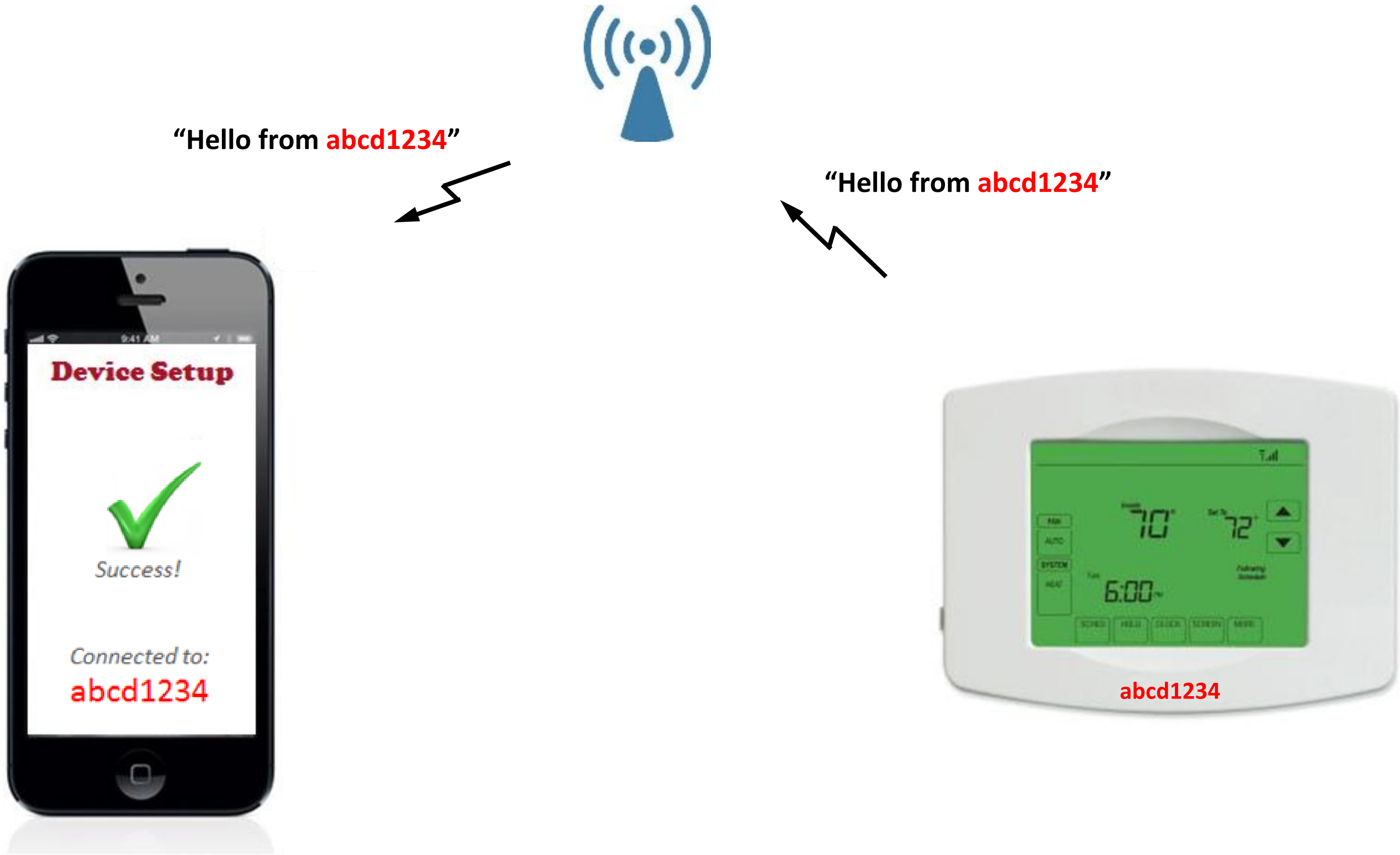
User Experience

… wait for the Device to connect …



Wi-Fi Easy Setup: Done!

… the Device is connected!



“Hello from abcd1234”

“Hello from abcd1234”

Wi-Fi Easy Setup in 4 Steps using Cooee
(Behind the Scenes)

Wi-Fi Easy Setup – Cooee™

User Experience : Behind the Scenes

Step 1 Download an App for the Device

App Store

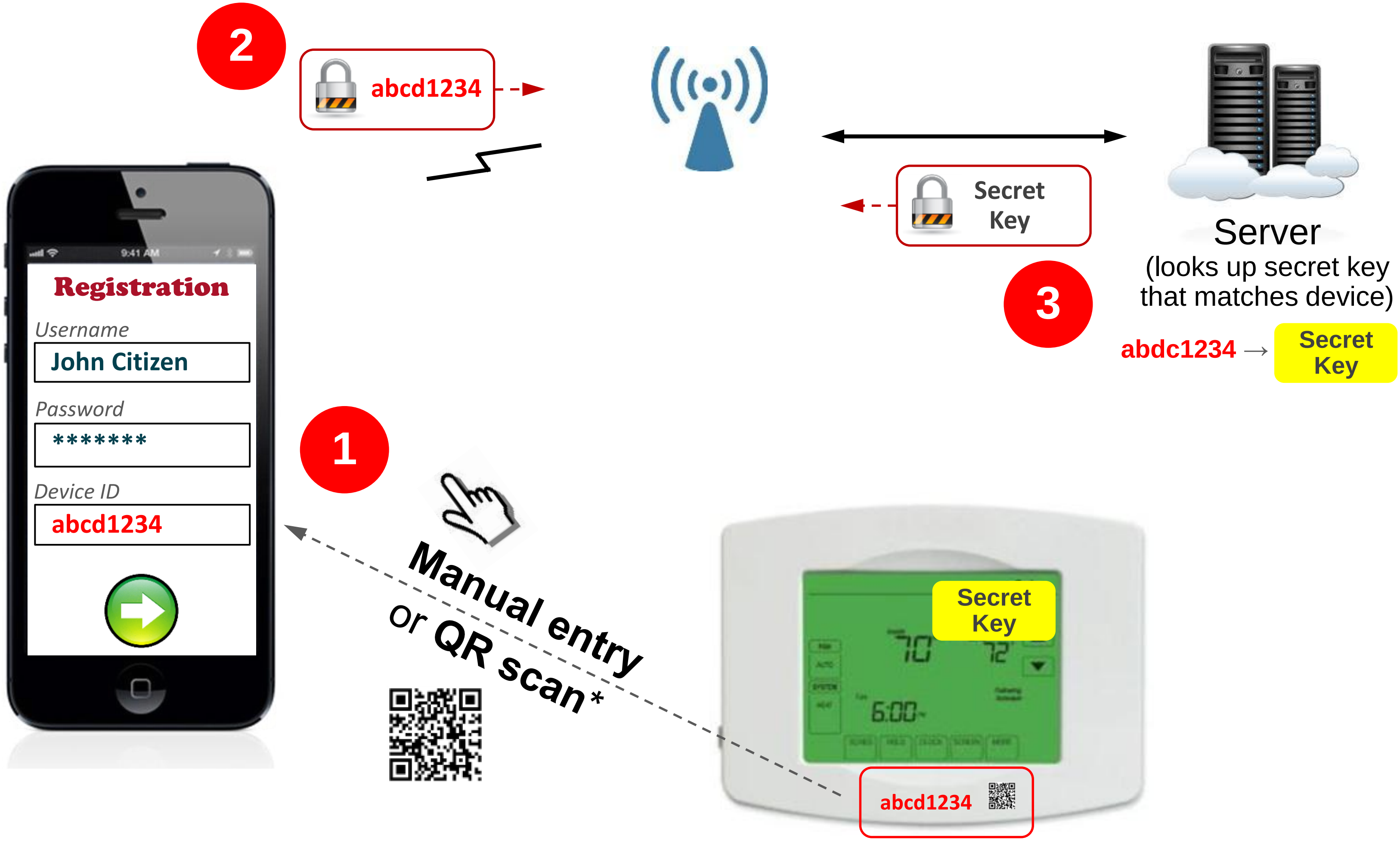
Google play

(no tricks here)

Wi-Fi Easy Setup – Cooee™

User Experience : Behind the Scenes

Step 2 Register the Device & retrieve the Secret Key



Registration

Username: John Citizen

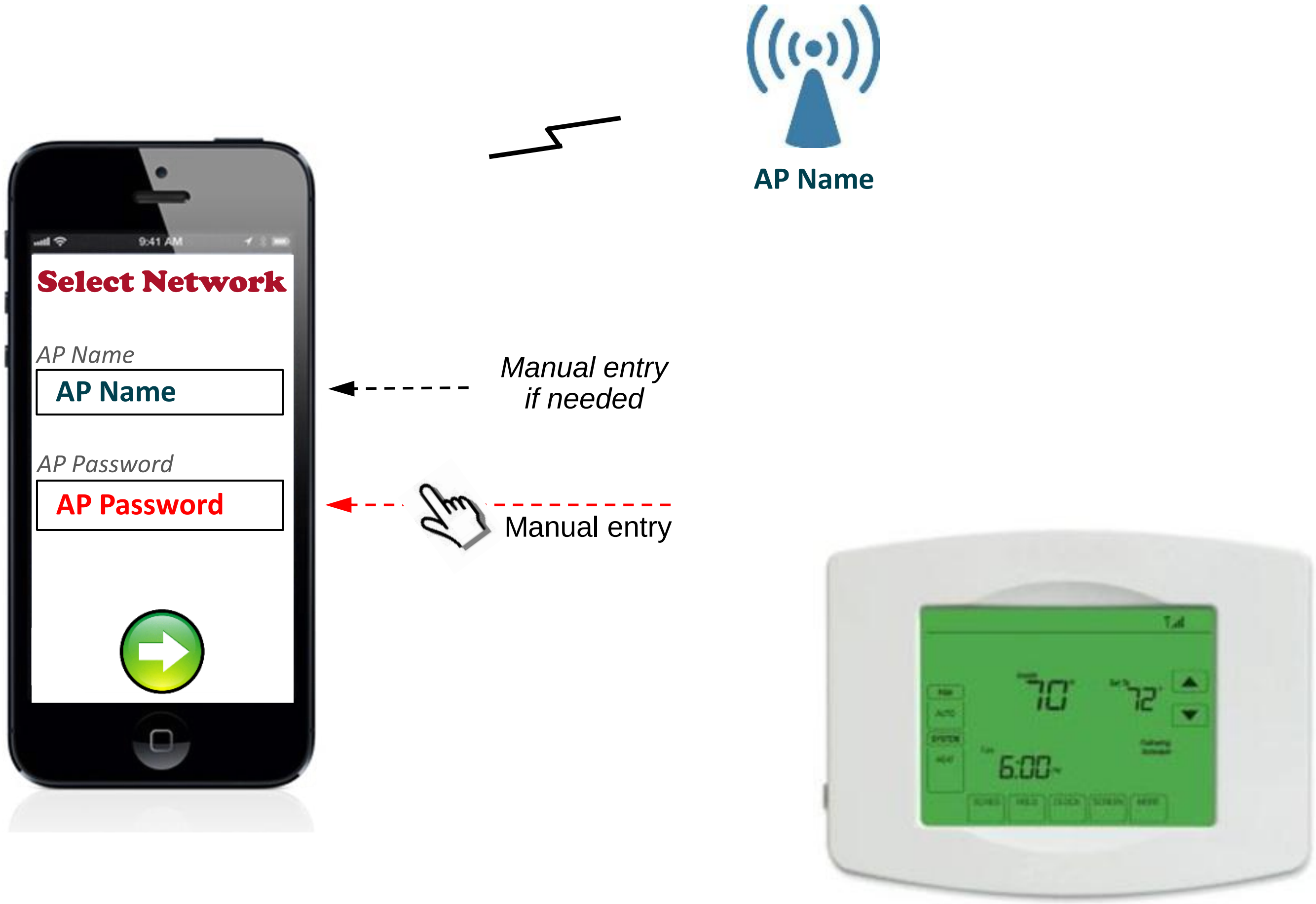
Password: *******

Device ID: abcd1234

Wi-Fi Easy Setup – Cooee™

User Experience : Behind the Scenes

Step 3 Type the AP Password



AP Name

Select Network

AP Name

AP Name

AP Password

AP Password

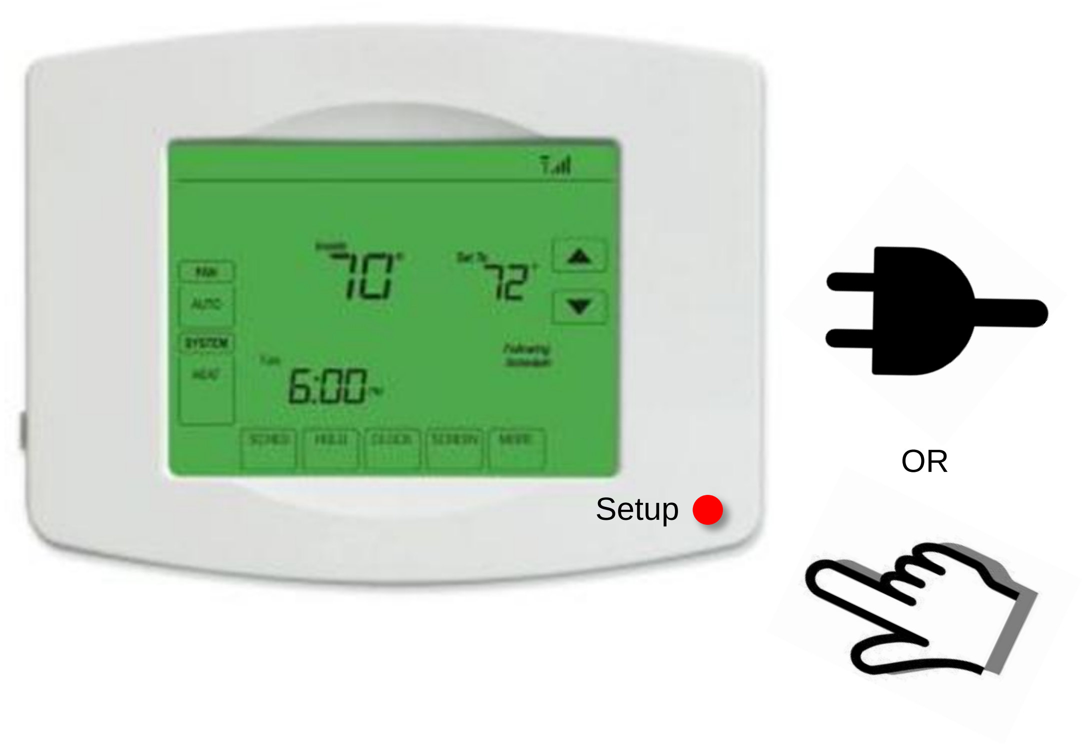
Manual entry if needed

Manual entry

Wi-Fi Easy Setup – Cooee™

User Experience : Behind the Scenes

Step 4 Power on the device OR press Setup

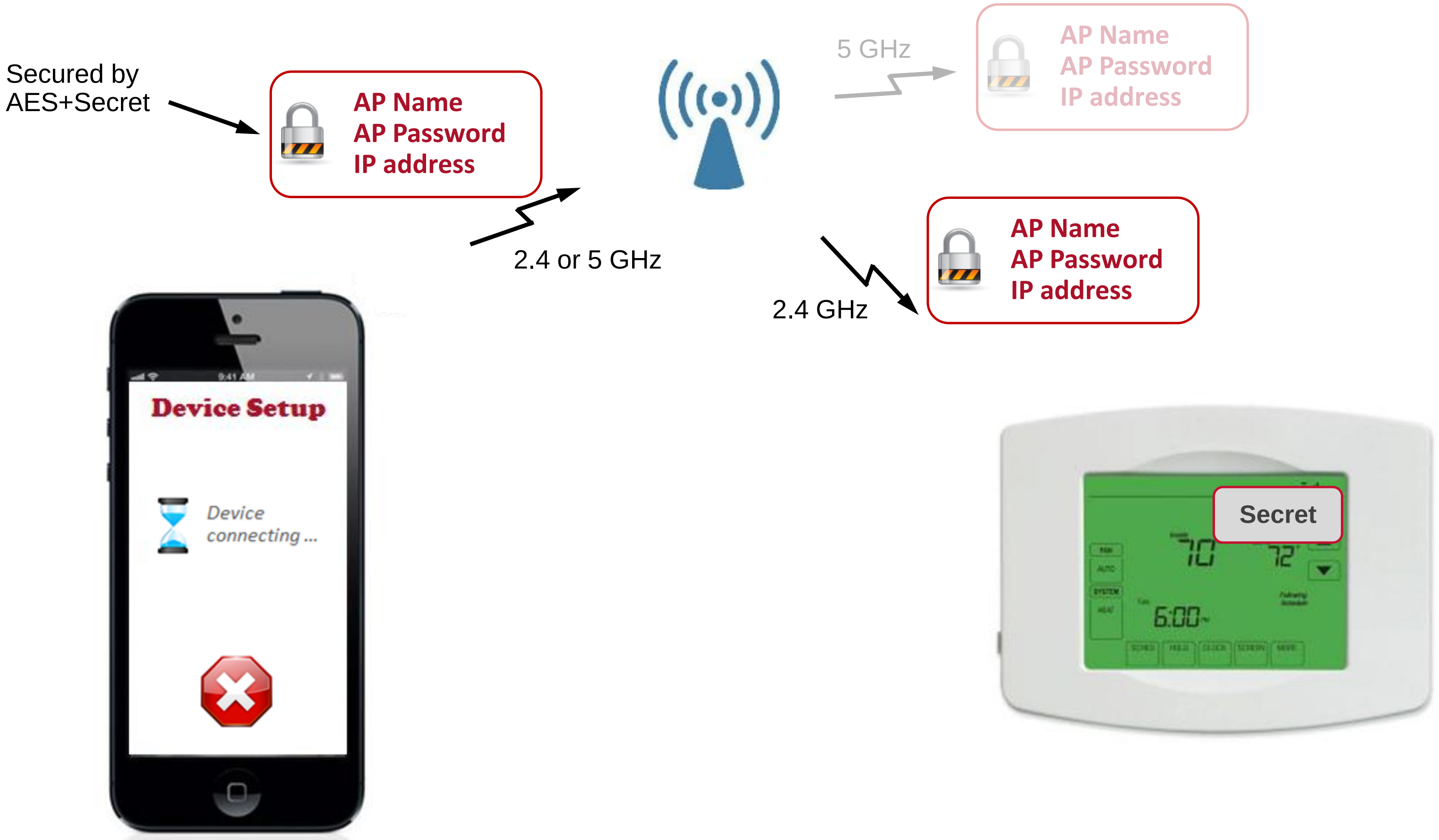


(no tricks here either)

Wi-Fi Easy Setup – Cooee™

User Experience : Behind the Scenes

… wait for the Device to connect …



Secured by AES+Secret

AP Name
AP Password
IP address

2.4 or 5 GHz

5 GHz

AP Name
AP Password
IP address

2.4 GHz

AP Name
AP Password
IP address

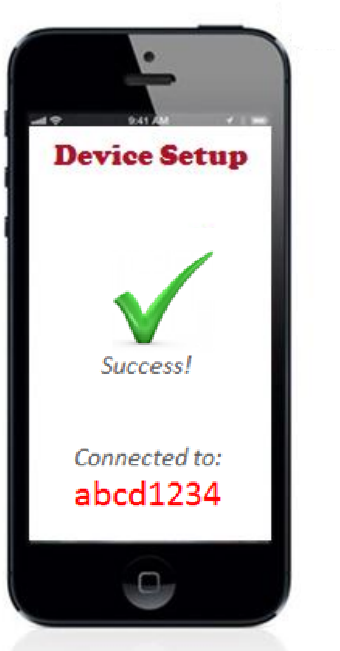
IP address: 192.168.1.100

Wi-Fi Easy Setup. Done!

… device is connected & ready for additional setup!

"Hello 192.168.1.100,
I am abcd1234
at 192.168.1.103"

"Hello 192.168.1.100,
I am abcd1234
at 192.168.1.103"

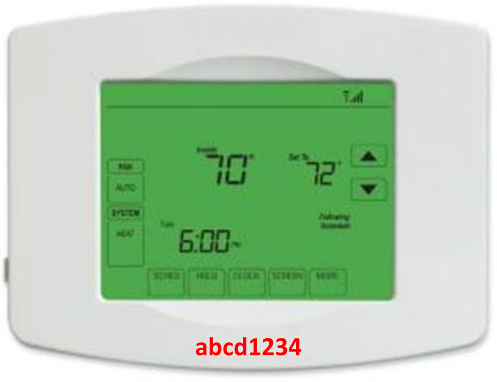


Device Setup

Success!

Connected to:
abcd1234

IP address: 192.168.1.100



IP address: 192.168.1.103
Connected!

Summary

Cooee makes device setup EASY FOR USERS

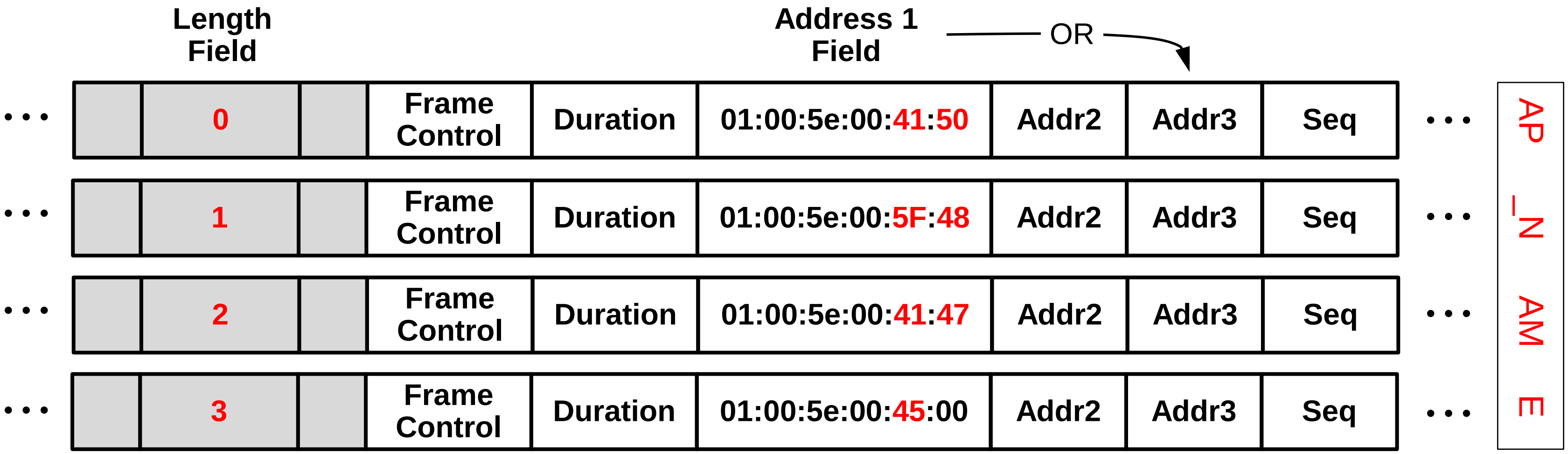
- **Consistent User Experience Across ALL Mobile Platforms**
  - iOS, Android, WinPhone, Blackberry, etc
- **Fast Setup Time**
  - Wi-Fi connection in 100's milliseconds
  - DHCP time is AP dependent (may be up to a few seconds)
- **Requires Trivial Incremental Memory Usage**
  - RAM : < 1kB
  - Flash : 3 kB (or 12kB if device app does not already use AES)
  - Does not require mDNS for setup, since the IP address of the setup client is sent as part of the Cooee message

Technical Q&A

How is Setup Information Encoded?

- The Setup Client App encodes information in the LS-bytes of consecutive multicast addresses.
  - Data packet are sent to IP multicast addresses that are directly mapped by the Network stack into 802.11 multicast addresses

    ie. 802.11 Address 3 for phone-to-AP, 802.11 Address 1 for AP re-broadcast
- An EXAMPLE (without the Cooee security algorithm applied to setup data)
  - The lower 2-bytes of the **Address 1** field contain the ASCII text: AP_NAME
  - The **Length Field** denotes the packet number in the block of packets
    - The setup client app sends real data packets of varying lengths with dummy data
    - Information is encoded in the Address field of the packet and NOT the data field. Recall the data field is encrypted using Wi-Fi security making it unreadable by the device.



		Length Field				Address 1 Field					
• • •		0		Frame Control	Duration	01:00:5e:00:41:50	Addr2	Addr3	Seq	• • •	AP
• • •		1		Frame Control	Duration	01:00:5e:00:5F:48	Addr2	Addr3	Seq	• • •	_N
• • •		2		Frame Control	Duration	01:00:5e:00:41:47	Addr2	Addr3	Seq	• • •	AM
• • •		3		Frame Control	Duration	01:00:5e:00:45:00	Addr2	Addr3	Seq	• • •	E

Why Register the Device with a Server?

- **Device registration with a server is useful for THREE reasons**
  1. It provides device vendors with a means of connecting with end users
  2. It provides users with a way to remotely access their device
  3. **SECURITY** : It overcomes a serious security issue with the setup process …

- **What if an attacker obtains the Secret Key for a device?**
  - The attacker can decode the transmission and obtain the Wi-Fi Network Password
    - ➢ **BAD!**
  - Packets can be recorded
    - The transmission could also be recorded, and the Secret obtained from the device at a later date for packet decoding in the comfort of the attackers home

- **The Implication?**
  - The device compromised the security of the user’s Wi-Fi network!
  - Legal ramifications and bad publicity for the device vendor

KEY TAKEAWAY

For maximum security, each device must have a unique ID and secret. Device registration with a server is the only way to meet this requirement.

Wi-Fi Easy Setup – Cooee™

What about Session Overlap?

- **Can my neighbor take over my device if we happen to setup our devices at exactly the same time?**
- **This can NEVER happen!**
- **Explanation**
  - The transmitter (phone) MAC address of Cooee messages sent by your neighbour is different to your transmitter (phone) MAC address
  - The WICED device locks onto packets from a unique MAC address
  - If it locks onto your neighbours address, the device will fail to decrypt the received Cooee message (since the Device Secret is incorrect)
  - The device then restarts the setup process and locks onto packets from the other (ie. probably your) MAC address
  - This process continues until the device setup completes
- **Setup is FAST**
  - The message transfer process takes 100’s milliseconds. So even if there is overlap, the setup latency impact to the user is minimal

What are the Caveats?

1. **IGMP Snooping**
   - On some corporate networks, multicast traffic may be blocked.
     BUT most APs do NOT block multicast packets by default
2. **5GHz / 2.4GHz Bridging (if a dual band AP is used)**
   - If the Wi-Fi setup client is connected on the 5GHz band **AND** the AP is not setup to bridge the 5GHz and 2.4GHz interfaces, then multicast packets will not be rebroadcast on the 2.4GHz band.
     BUT most APs bridge 5GHz and 2.4GHz interfaces by default
   - If a client is not already connected to the 2.4GHz interface, some APs may decide not to forward multicast packets received on the 5GHz interface to the 2.4GHz interface
     BUT most APs forward multicast packets by default
3. **Multicast to Unicast Conversion**
   - Some APs are known to convert multicast packets to unicast packets

How to resolve these issues? (if they occur)

- The WICED device can ALSO receive packets sent by the Wi-Fi setup client (phone) to the AP! For this to work, the phone & WICED device must
  - be on the same radio band (eg. 2.4GHz)
  - use compatible 802.11 modulation schemes e.g. 802.11b/g/n 1x1, 20MHz

Cooee Message Protocol Details

Cooee Message Block (1)

Message Block*

Header	**Mandatory Elements**	**Optional Elements**

* Prior to encryption

Header

4 bits	12 bits	8 bytes
Ver	**Message length***	**Security Nonce**

* Header length + Ciphertext length + MIC length

Mandatory Elements

AP SSID	**≤ 32**	**e.g. My AP Name**

Wi-Fi Key(s)*	**≤ 4x13**	**e.g. WEP Key(s) or WPA2-PSK**

* Key(s) = WEP key(s) or PSK

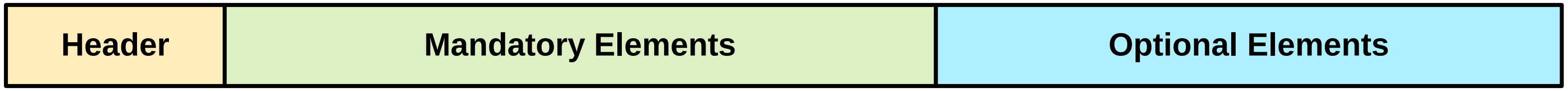
Server Address*	**4 or 16**	**e.g. IPv4 or IPv6 Address**

* IP address of transmitter or other server

Type	**Length**	**Value**
1 byte	1-byte	(length determined by length field)

Cooee Message Block (2)

Message Block*



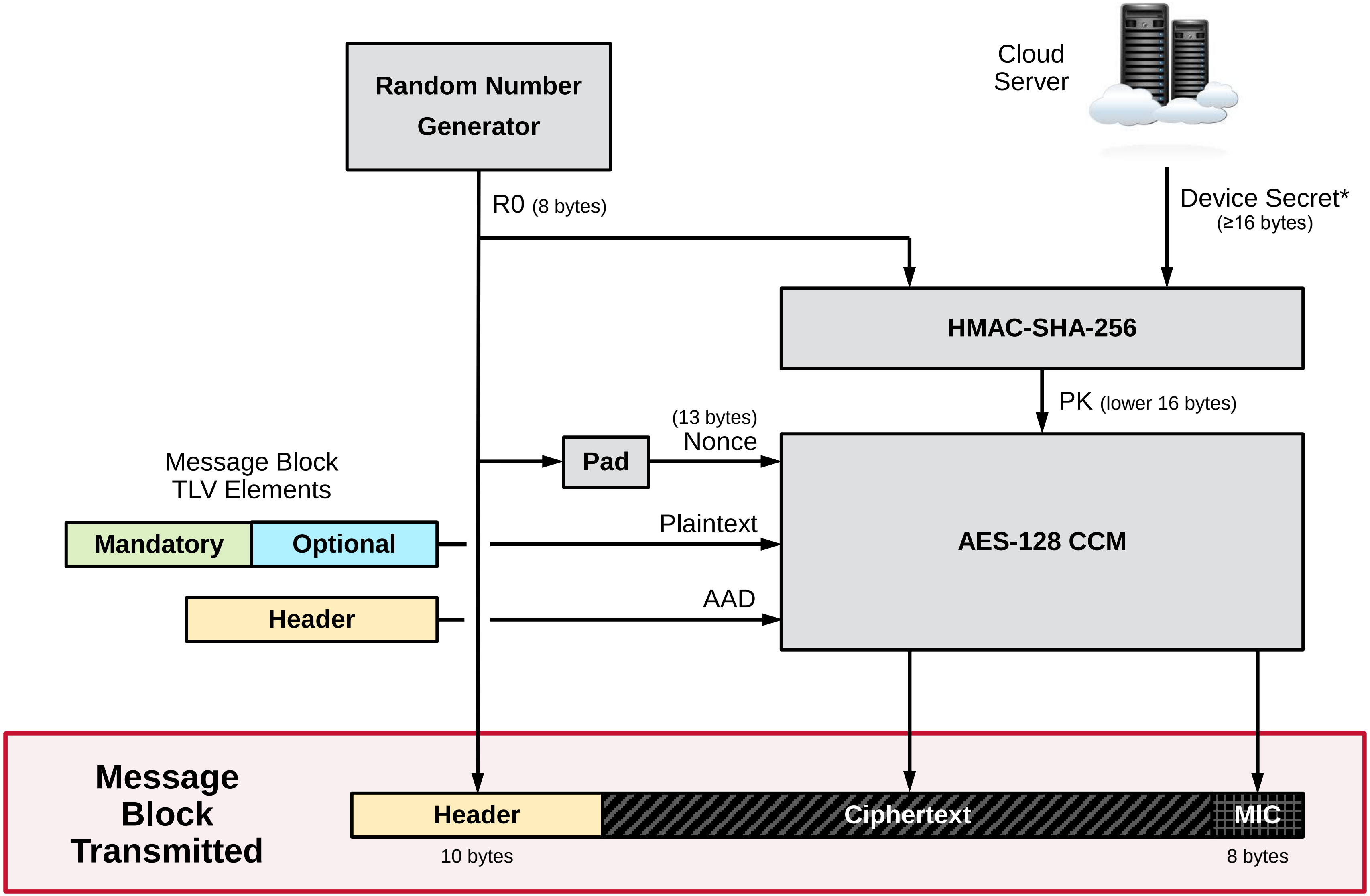
Header | Mandatory Elements | Optional Elements

* Prior to encryption

Example Optional Elements

Type 1 byte	Length 1-byte	Value (length determined by length field)
Server URL	16	api.myserver.com
Comm Protocol	5	HTTPS
ISO Time	17	2013-02-02T12:07Z
Device Name	13	Lounge Sensor
Device Name	22	Master Bedroom Speaker

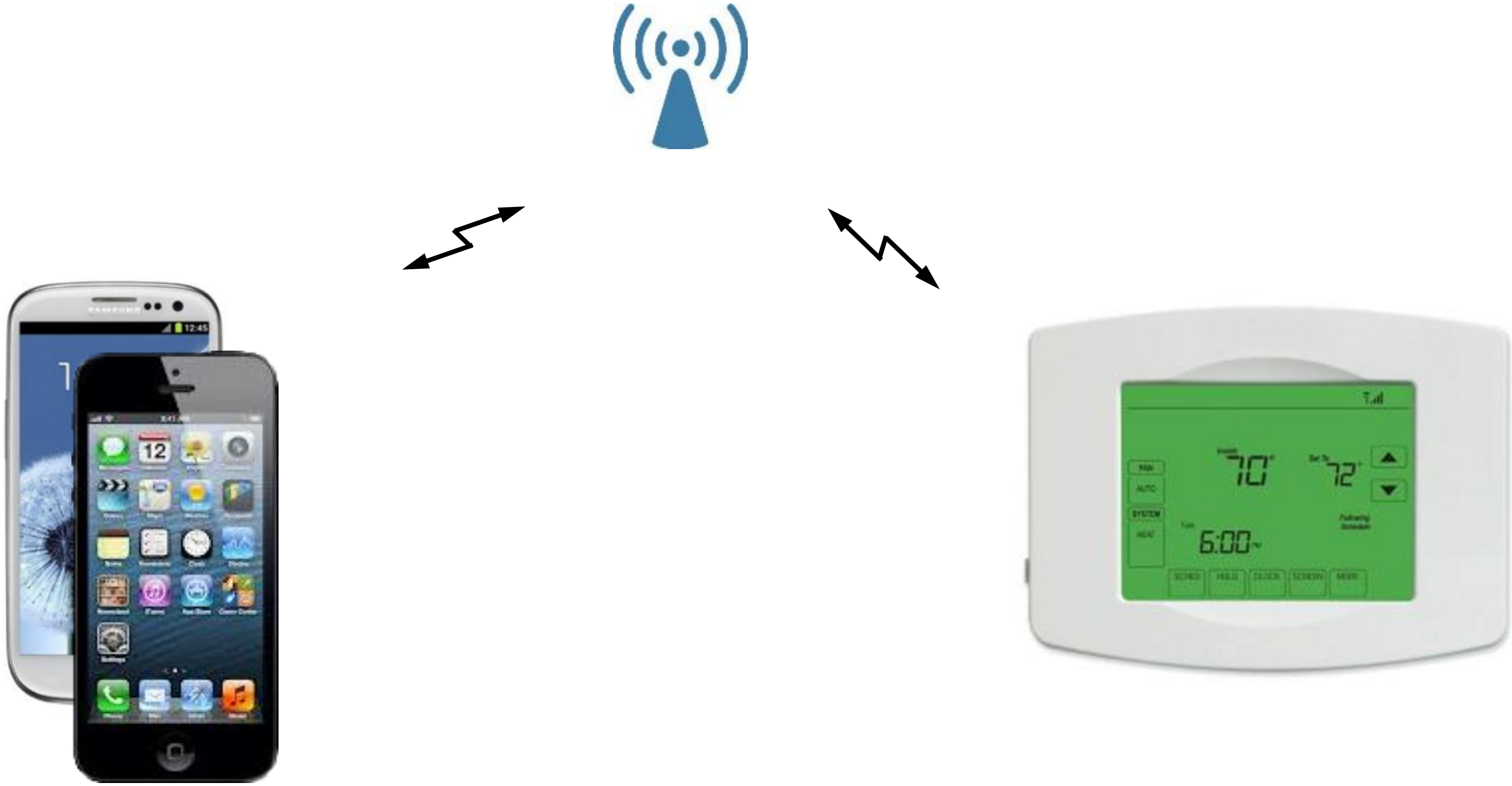
Cooee Security Algorithm



* A further improvement would instead send a hash of the secret together with the nonce used to generate the hash (instead of the secret itself)

Wi-Fi Easy Setup – Cooee™

Integration with Applications



Wi-Fi Setup Client

Broadcom can provide
an example setup client
App for Android & PC

WICED Device

Application calls a single
API function :

```
wiced_easy_setup_start_cooee()
```

Thank you