LoRaWAN Keys and IDs Overview
RM1xx Series

Application Note v1.0

INTRODUCTION

This document provides the following:

- Overview of the various keys used within LoRaWAN
- Suggestions on managing the keys during development when reloading them multiple times onto an RM1xx module

OVERVIEW

LoRaWAN allows for its packets to be both signed and encrypted by the use of keys known to both the node (module/sensor) and the LoRaWAN network/application server. The following are the keys:

- Network Session Key (NwkSKey)
- Application Session Key (AppSKey)

In addition, each device on the network has a unique device address (DevAddr).

These keys are known only to the individual node (RM1xx module) and the network/application server. This means that another node or man-in-the-middle is not able to decode the packet payload.

The following two methods are used to deploy these keys:

- Over-the-Air Activation (OTAA)
- Activation by personalization (ABP)

With either of these methods, the same keys are loaded into both the module and network server that allows end-to-end data security.
OVER-THE-AIR ACTIVATION

Over-the-Air activation (OTAA) uses an application ID (AppEUI) and an application key (AppKey) along with a device ID (DevEui) to derive the network session key (NwkSKey), application session key (AppSKey) and the device address. A device address (DevAddr) is assigned by the network. OTAA is the preferred method because of its security advantages including regeneration of the session keys and simplifying network management.

<table>
<thead>
<tr>
<th>Name</th>
<th>RM1xx Command</th>
<th>Length</th>
<th>Setup Required in Network Server</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppEui</td>
<td>at+cfgex 1010</td>
<td>8</td>
<td>Check with server provider</td>
<td>Application Identifier – Uniquely identifies the application globally</td>
</tr>
<tr>
<td>DevEUI</td>
<td>at+cfgex 1011</td>
<td>8</td>
<td>Check with server provider</td>
<td>End Device Identifier – Uniquely identifies the device globally</td>
</tr>
<tr>
<td>AppKey</td>
<td>at+cfgex 1012</td>
<td>16</td>
<td>Check with server provider</td>
<td>Application key used to derive the session keys</td>
</tr>
<tr>
<td>NwkSKey</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AppSKey</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DevAddr</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following screenshot (Figure 1) shows an example ABP setup on the RM186. Note the use of ATZ after the at+cfgex commands. This is important and the keys do not take effect until after the ATZ. A smartBASIC program can be loaded before or after setting the keys.

```
at 0
10 0   RM186
00
at+cfgex 1011 "0016a4A2F4774E"
00
at+cfgex 1010 "70E3D57ED601922"
00
at+cfgex 1012 "09770016a40000400770016a4000064"
00
atz
00
```

*Figure 1: OTAA setup example*
ACTIVATION BY PERSONALIZATION

Activation by personalization (ABP) uses both session keys directly, along with the DevAddr, to sign and encrypt the data packets. These must be configured both on the node (RM1xx module) and on the network server.

<table>
<thead>
<tr>
<th>Name</th>
<th>RM1xx Command</th>
<th>Length</th>
<th>Setup Required in Network Server</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppEui</td>
<td></td>
<td></td>
<td>Check with server provider</td>
<td>Application Identifier – Uniquely identifies the application globally. Assigned by network server</td>
</tr>
<tr>
<td>Dev EUI</td>
<td></td>
<td></td>
<td>Check with server provider</td>
<td>End Device Identifier – Uniquely identifies the device globally. Assigned by network server</td>
</tr>
<tr>
<td>AppKey</td>
<td>at+cfgex 1013</td>
<td>16</td>
<td>Yes</td>
<td>Not used with ABP</td>
</tr>
<tr>
<td>NwkSKey</td>
<td>at+cfgex 1013</td>
<td>16</td>
<td>Yes</td>
<td>Network session key – Specific to the end device</td>
</tr>
<tr>
<td>AppKey</td>
<td>at+cfgex 1014</td>
<td>16</td>
<td>Yes</td>
<td>Application session key – Specific to the end device</td>
</tr>
<tr>
<td>DevAddr</td>
<td>at+cfgex 1015</td>
<td>4</td>
<td>Yes</td>
<td>End device address – Identifies the device within the current network</td>
</tr>
</tbody>
</table>

The following screenshot (Figure 2) shows an example ABP setup on the RM186. Note the use of ATZ after the at+cfgex commands. This is important and the keys do not take effect until after the ATZ. A smartBASIC program can be loaded before or after setting the keys.

![Figure 2 ABP setup example]

MANAGING KEYS AND IDs

Laird’s UWTerminalX has a useful Automation feature than can be used to store the commands for setting the session keys or identifiers. Right-clicking on the main UWTerminalX screen brings up a menu. From this menu, select Automation (Figure 3).

The biggest benefit of using the Automation feature is removing errors when manually typing keys/IDs multiple times.
Once you select the Automation option, you can set and save commands that can then be sent to the terminal. This feature can be used for any AT command. In the example below, I’m using `ati 4` to identify the MAC address of the module as well as set the various LoRa IDs (Figure 4).

- `At&f 1` can be used to clear the file system, deleting any loaded smartBASIC programs without deleting any stored keys.
- `At&f 256` can be used to delete any stored keys without deleting any loading smartBASIC programs.
**MULTITECH CONDUIT NOTES**

If you are using the Multitech Conduit AEP gateway as a networks server rather than just a packet forwarder, the following set-ups should be used.

*Note:* Different terminology is used on the Conduit.

**OTAA Setup**

To set up OTAA, follow these steps:

1. From the LoRa Network Server setup page on the Conduit, configure the following settings:
   - Where the EUI is the application EUI (AppEUI) as configured on the RMxx using at+cfgex 1010
   - Where the key is the Application key (AppKey) as configured on the RM1xx using at+cfgex 1012

2. Make sure to replace the EUI and key used in the following screenshot with your own.

![Figure 5: Multitech Conduit LoRa configuration example](image)

**ABP Setup**

To set up ABP, follow these steps:

1. To manage ABP nodes on the Multitech Conduit AEP gateway, you must SSH into the gateway and use netcat.
   ```
   # nc -u localhost 6677
   ```

2. Add nodes using the following:
   ```
   node add [DevAddr] [APPEUI] [DEVEUI] [NwkSKey] [AppSKey]
   ```

3. List exit nodes with the following:
   ```
   Node list
   ```

![Figure 6: Multitech Conduit Netcat example](image)
REFERENCES

The following additional references are available:

- Interfacing with LoRoWAN – RM186

- Interfacing with LoRoWAN – RM191

- Connecting to a Multitech Conduit Gateway

- Conduit AEP: LoRa Use with Third-Party Devices

- UWTerminalX
  https://github.com/LairdCP/UwTerminalX/releases

REVISION HISTORY

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Notes</th>
<th>Approver</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>19 Dec 2016</td>
<td>Initial Release</td>
<td>Mark Duncombe</td>
</tr>
</tbody>
</table>