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.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

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.

Name	RM1xx Command	Length	Setup Required in Network Server	Notes
AppEui	at+cfgex 1010	8	Check with server provider	Application Identifier – Uniquely identifies the application globally
Dev EUI	at+cfgex 1011	8	Check with server provider	End Device Identifier – Uniquely identifies the device globally
AppKey	at+cfgex 1012	16	Check with server provider	Application key used to derive the session keys
NwkSKey				
AppSKey				
DevAddr				

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 *smart*BASIC program can be loaded before or after setting the keys.

```
ati 0

10    0     RM186
00
at+cfgex 1011 "0016a4AEFAF7748E"
00
at+cfgex 1010 "70B3D57ED0001922"
00
at+cfgex 1012 "00770016a4000004007700l6a4000004"
00
atz
00
```

Figure 1: OTAA setup example

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0600

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.

Name	RM1xx Command	Length	Setup Required in Network Server	Notes
AppEui			Check with server provider	Application Identifier – Uniquely identifies the application globally. Assigned by network server
Dev EUI			Check with server provider	End Device Identifier – Uniquely identifies the device globally. Assigned by network server
AppKey			No	Not used with ABP
NwkSKey	at+cfgex 1013	16	Yes	Network session key – Specific to the end device
AppSKey	at+cfgex 1014	16	Yes	Application session key – Specific to the end device
DevAddr	at+cfgex 1015	4	Yes	End device address – Identifies the device within the current network

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 *smart*BASIC program can be loaded before or after setting the keys.

```
ati 0

10    0     RM186
00
at+cfgex 1013 "deb1dad2fad3bad4fab5fed6abbadbba"
00
at+cfgex 1014 "deb1dad2fad3bad4fab5fed6abbadbba"
00
at+cfgex 1015 "550df170"
00
atz
00
```

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.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0600

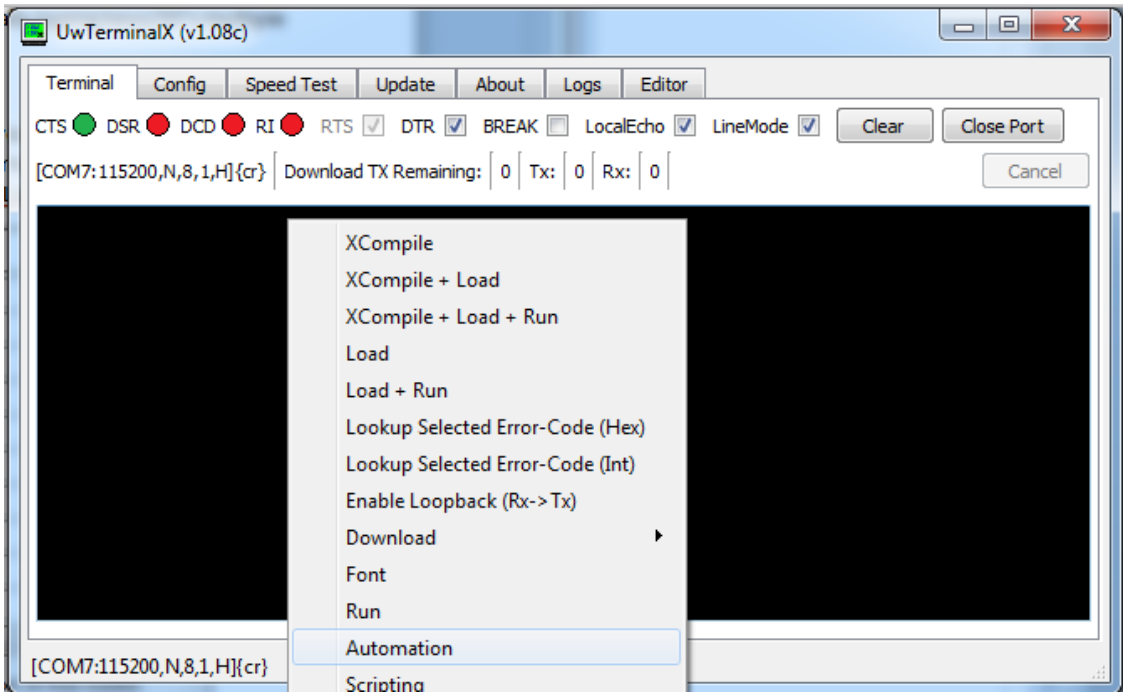

Figure 3 Accessing the Automation feature

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).

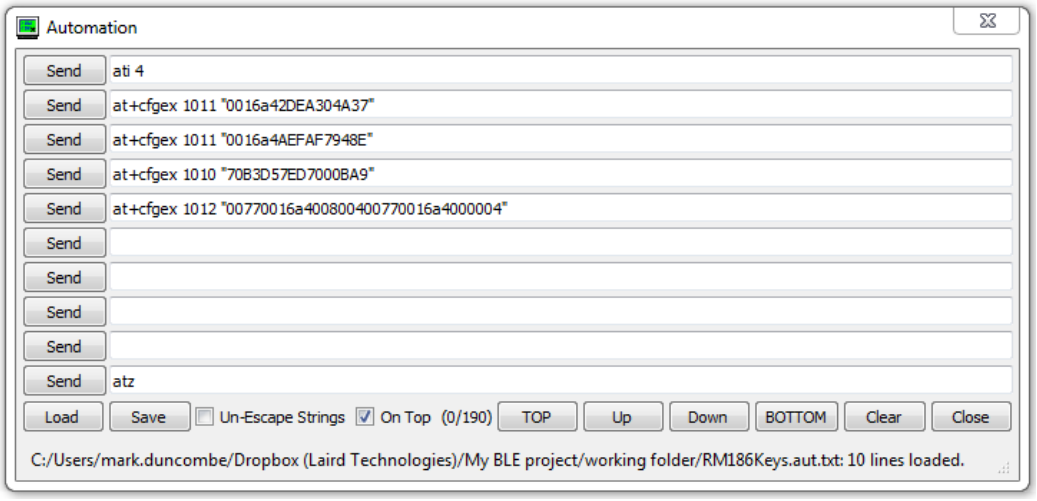

Figure 4 Automation screen example

- **At&f 1** can be used to clear the file system, deleting any loaded *smart*BASIC programs without deleting any stored keys.
- **At&f 256** can be used to delete any stored keys without deleting any loading *smart*BASIC programs.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0600

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 they EUI and key used in the following screenshot with your own.

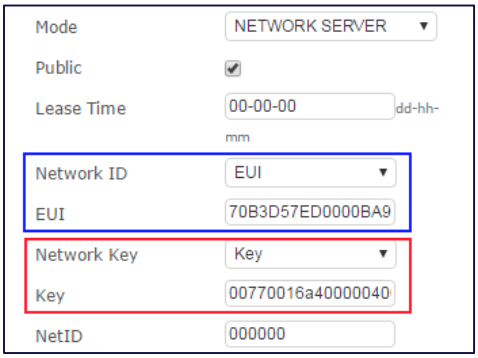

Figure 5: Multitech Conduit LoRa configuration example

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
```

```
Using username "admin".
Using keyboard-interactive authentication.
Password:
Last login: Fri Dec  2 12:13:13 2016 from 192.168.0.109
admin@mtcdt:~# nc -u localhost 6677
node add aabbccdd 1122334455667788 11223344556677cc deb1dad2fad3bad4fab5fed6abbadbba deb1dad2fad3bad4fab5fed6abbadbba
node list
Net Addr     Dev EUI                 Class  Joined               Seq Num       Up      Down       1st       2nd  Dropped
aa:bb:cc:dd  11-22-33-44-55-66-77-cc  A      2016-12-02T12:14:34Z        0        0         0         0         0        0
```

Figure 6: Multitech Conduit Netcat example

REFERENCES

The following additional references are available:

- Interfacing with LoRoWAN – RM186
  http://cdn.lairdtech.com/home/brandworld/files/Interfacing%20with%20LoRaWAN%20-%20RM186.pdf
- Interfacing with LoRoWAN – RM191
  http://cdn.lairdtech.com/home/brandworld/files/Interfacing%20with%20LoRaWAN%20-%20RM191.pdf
- Connecting to a Multitech Conduit Gateway
  http://cdn.lairdtech.com/home/brandworld/files/Connecting%20to%20a%20Multitech%20Conduit%20Gateway%20-%20RM1xx%20Series.pdf
- Conduit AEP: LoRa Use with Third-Party Devices
  http://www.multitech.net/developer/software/lora/conduit-aep-lora-communication/aep-lora-use-third-party-devices/
- UWTerminalX
  https://github.com/LairdCP/UwTerminalX/releases

REVISION HISTORY

Version	Date	Notes	Approver
1.0	19 Dec 2016	Initial Release	Mark Duncombe

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0600