N32WB031系列芯片配对与绑定的安全配置V1.0

简介

本文档介绍 N32WB031系列 32 位 蓝牙芯片（以下简称 N32WB031）配对与绑定的安全配置操作说明,包括配对绑定基础知识、结合SDK讲解相关配置代码。本文档目的在于让使用者能够快速熟悉芯片的配对绑定操作流程，以减少开发前期的准备时间，降低开发难度和出现错误操作的概率，最终达到快速开发量产的目的。

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

一、基本概念 ---- 1
- 配对 ---- 1
- 绑定 ---- 1

二、 配对绑定流程 ---- 2

2.1 配对信息交换 ---- **2**
- 配对请求包 ---- 2
- 配对响应包 ---- 5

2.2 链路认证 ---- **6**

2.3 密钥分配 ---- **7**
- 临时密钥 ---- 7
- 短期密钥 ---- 7

2.4 配对绑定设置 ---- **8**
- Just Work 方式 ---- 9
- PassKey 方式 ---- 9
- 绑定配置 ---- 10

注意事项 ---- 11

历史版本 ---- 12

声明 ---- 13

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

一、基本概念

对于低功耗蓝牙来说，配对和绑定是两个不同的概念。简单讲，配对是蓝牙主从加密特性的交换，并创建临时密钥。绑定则是在配对之后交换和保存长期密钥，用于以后的连接。为了保证低功耗蓝牙的绝大多数安全特征，蓝牙设备必须完成配对和分配用于加密、保障隐私的密钥。因此为了了解安全机制是如何工作的，关键在于理解配对和密钥分配的工作原理。

- 配对

配对是加密结构的交换，包括 IO 能力、是否需要中间人保护。客户端（Client）发起交换，一旦主从设备执行了交换，加密机制就会确定并生效。比如服务器端（Server）在 IO 能力上仅支持 NoInput/NoOutput，那么双方就会采用“Just Works”的连接方式。配对完成后，一个临时的密钥就已经被生产和交换，连接已经被加密，但是仅使用一个临时的加密密钥。这个加密连接过程中，长期密钥已经产生和交换。长期密钥类似一个数字签名。具体交换哪些密钥、密钥长短还要取决于配对双方设备支持的加密结构。配对是为了在连接基础上加密（通信数据经过加密为密文），提高蓝牙链路传输的安全性。

- 绑定

绑定是真正意味着在加密结构交换和连接加密，双方的长期密钥交换完成，双方已经存储并将在下一次连接的时候使用该密钥。密钥可以通过绑定程序交换。绑定是配对发起时的一个可选配置。把配对信息记录（存储到flash）下来，下一次不用配对自动进入加密的连接；所以没有在绑定列表里的设备不影响连接，只是每次需要输入配对密码。

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

二、 配对绑定流程

配对涉及两个设备的身份认证，链路加密以及随后的密钥分配，身份解析等。如果配对时设置了绑定，分配的密钥用户可以存储在flash中，这样两个设备在第二次重连时的安全启动会更快，而不需要像第一次一样需要再启动整个配对过程。

配对有三个阶段：

第一阶段：配对信息交换（主要就是两边设备的IO能力，设置绑定标志，链路是否需要MITM保护，设置绑定分配哪些密钥等信息）。

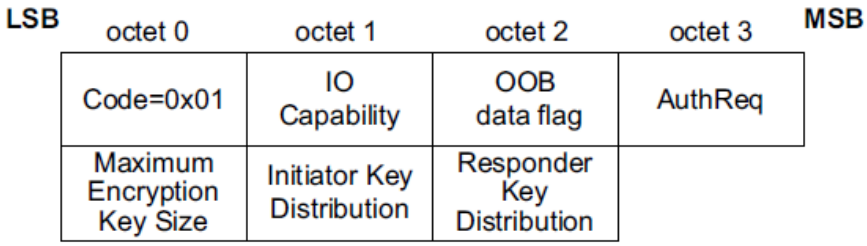
第二阶段：链路认证（输入密码的过程就是认证的一种方式）。

第三阶段：密钥分配。

2.1 配对信息交换

配对的第一个阶段涉及配对信息交换，用于确认设备的配对方式，以及确定在最后的阶段将会分配哪些密钥。两台设备间配对信息的交换是通过配对请求和配对响应数据包实现的。

- 配对请求包



配对请求包是从机向主机提交的配对请求信息，下面对这个配对请求包数据结构进行说明：

第0字节：

Code代码字段，当code = 0x01的时候，表示为配对请求包；

当code = 0x00时候，表示为配对响应包；

第1字节： IO Capability字段，表示IO能力，表示两端设备的输入输出能力，协议栈定义IO能力如下：

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

Value	Description
0x00	DisplayOnly
0x01	DisplayYesNo
0x02	KeyboardOnly
0x03	NoInputNoOutput
0x04	KeyboardDisplay
0x05-0xFF	Reserved for future use

在代码中，gap.h的文件中，对该IO能力定义如下：

```
/// IO Capability Values
enum gap_io_cap
{
    /// Display Only
    GAP_IO_CAP_DISPLAY_ONLY = 0x00,
    /// Display Yes No
    GAP_IO_CAP_DISPLAY_YES_NO,
    /// Keyboard Only
    GAP_IO_CAP_KB_ONLY,
    /// No Input No Output
    GAP_IO_CAP_NO_INPUT_NO_OUTPUT,
    /// Keyboard Display
    GAP_IO_CAP_KB_DISPLAY,
    GAP_IO_CAP_LAST
};
```

第2字节：

OOB DF(OOB Data Flag),即Out of Band的缩写，采用外部通信方法交换一些配对过程中使用的信息。OOB媒体可能是任何一种能够传输相应信息的其他无线通信标准，如NFC或二维码。

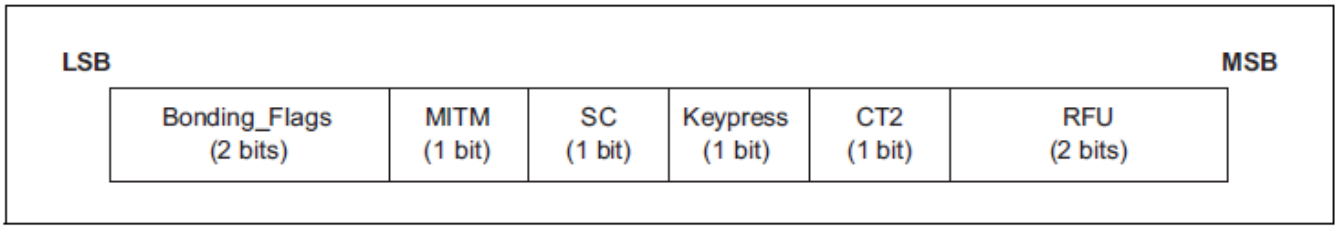
Value	Description
0x00	OOB Authentication data not present
0x01	OOB Authentication data from remote device present
0x02-0xFF	Reserved for future use

0x00：身份验证数据不存在；
0x01：来自远程设备的身份验证
0x02 – 0Xff：预留给以后使用

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

第3字节：

AuthReq授权请求，这个授权请求里可以展开，8位数据如下表所示：



Bonding Flags:绑定标志位，2个bit位：

01绑定中（Bonding）表示绑定是配对发生之后的长期密钥交换，并将这些密钥存储起来以供日后使用——即在设备间创建永久的安全连接。配对机制是绑定的前提。

00表示没有绑定。

10和11：保留未来使用。

Bonding_Flags b_1b_0	Bonding Type
00	No Bonding
01	Bonding
10	Reserved for future use
11	Reserved for future use

MITM:1个bit位，是中间人的意思。1：表示设备需要MITM保护。如果需要输入密码，那么就置为1。

SC:1个bit位，Enable LE Secure Connection pairing(LESC)。设置为1，请求低功耗安全连接配对；0：采用低功耗传统连接。因此这一标识是决定第二阶段配对方法的一项指标。

Keypress：1个bit位，表示使能启用键盘按键通知。

CT2：是一个bit位标志，在传输时将被设置为1.支持h7功能，之歌功能是经典蓝牙模式下使用的，低功耗蓝牙可以关注，默认配置即可。

RFU:2个bit位，Reserved for future use简写，保留部分。

第4字节：

Maximum Encryption Key Size，最大加密密钥规模，用于定义设备能够支持的最大的密钥长度，最大密钥规模范围为7–16字节。

第5字节：

Initiator Key Distribution/Generation：发起者密钥分配。设置发起配对者的密钥分配机制。

第6字节：

Responder Key Distribution/Generation：响应者密钥分配。设置响应者的密钥分配机制。

密钥的5种分配机制如下：

- 临时密钥（TK）
- 短期密钥（STK）

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

- 长期密钥（LTK）(包含EDIV和Rand的值)
- 身份解析密钥（IRK）
- 连接签名解析密钥（CSRK）

说明：临时密钥（TK）和短期密钥（STK）是在密钥配对过程中必须产生的两个验证密钥，而第三步验证可以通过短期密钥(STK)根据这里选择的分配机制产生诸如：长期密钥（LTK）、身份解析密钥（IRK）、连接签名解析密钥（CSRK）、从LTK中导出链接密钥（LTKlink）等加密机制。

- 配对响应包

配对响应包格式与配对请求包基本一样，不再赘述；

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

2.2 链路认证

通过配对请求和配对响应信息所携带的消息，主从设备之间可以通过对比来确定合适的配对算法，下表是根据主从设备两者的输入和输出能力来确定的使用算法：

配对请求 / 配对响应	只有显示屏	只有键盘	显示屏+选择 YES 和 No	显示屏+键盘	无键盘与显示屏
只有显示屏	正常连接	输入密码	正常连接	输入密码	正常连接
只有键盘	输入密码	输入密码	输入密码	输入密码	正常连接
显示屏+选择 YES 和 No	正常连接	输入密码	正常连接	输入密码	正常连接
显示屏+键盘	输入密码	输入密码	输入密码	输入密码	正常连接
无键盘与显示屏	正常连接	正常连接	正常连接	正常连接	正常连接

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

2.3 密钥分配

一旦 STK 加密配对过程完成后，设备将会分配所需的密钥机制，以下的密钥可以分配：LTK、IRK、CSR 等。如果没有设置，默认是使用长期密钥 LTK 机制，一般 LTK 是存储在设备的安全数据库中的一个随机数，但是蓝牙设备往往资源有限，一般难以维护一个安全数据库。为了解决这个问题，从设备向主设备分配两个值：EDIV 和 RAND。这两个值存储在主设备上，当从设备重新连接的时候再发回给对方。这时候，从设备通过 LTK 加密连接。

- 临时密钥

配对过程中，首先需要用到临时密钥（TK）。临时密钥通过认证的时候选择的配对算法生成，主要用以计算后面的短期密钥。临时密钥有以下几种：

Just work，这种模式是当有限的客户界面，用户不方便输入验证密钥时，用来连接低功耗蓝牙设备的。该模式下 TK 的值设为 0，因此该方式并没有执行认证。建立在这种方式之上的分配密钥很容易受到中间人的攻击。

Passkey entry，这种模式是当用户的设备界面支持数值显示或者输入按键时使用。当使用这个方式时，TK 的值设置为两个设备的数字输入值，取值范围是 0~999999，因此，入侵者只能有很小的概率猜对当前连接使用的值，几率只有百万分之一。因此这种方式生成密钥认为是一种有限的防止攻击的可认证密钥。

Out of band，这种模式是主从设备通过蓝牙外的另一种技术获取认证信息。比如通过芯片自带的 NFC 在两个设备之间输入一个值，作为认证的 TK 值。

一旦临时密钥 TK 的值确定后，则会使用该 TK 值、已知的配对值、配对请求和响应请求、主从设备产生的随机数这几个参数，来计算一个确定值。这时，主从设备就开始叫唤随机数和确定值，主从双方开始检查确定值是否匹配随机数和所有其他共享信息。如果确定值不匹配，说明配对过程不正常，设备将发送配对设备信息终止配对。如果确认匹配，说明主从设备具有相同的配对请求和配对响应参数、相同的地址信息、相同的 TK 值和正常的随机数。如果一切都确认无误，则认证中交互的随机数将用于计算 STK。

- 短期密钥

当两个设备首次配对时，需要使用短期密钥STK。STK由三个部分信息计算来：临时密钥TK和两个随机数。这两个随机数是主从设备发送配对请求时提供的。

临时密钥的公式如下：

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

$$STK = E_{TK}(S_{rand} \mid M_{rand})$$

公式中，E_{TK} 是通过 AES 对 TK 加密的密文，S_{rand} 和 M_{rand} 为两个随机数。

2.4 配对绑定设置

静态密钥连接，是在配置过程中使用进入Passkey entry方式。通过键盘输入的方式输入临时密钥TK。下面通过SDK中的实际配置代码进行讲解（以ble-> rdtss SDK为例）。

安全配置：

```
#define SEC_PARAM_IO_CAPABILITIES       GAP_IO_CAP_NO_INPUT_NO_OUTPUT       /**I/O 能力 */
#define SEC_PARAM_OOB                   0       /**< Out Of Band data not available. */
#define SEC_PARAM_KEY_SIZE              16      /**< Minimum encryption key size. 7 to 16 */
#define SEC_PARAM_BOND                  1       /**< Perform bonding. */
#define SEC_PARAM_MITM                  1       /**< Man In The Middle protection not required. */
#define SEC_PARAM_LESC                  0       /**< LE Secure Connections not enabled. */
#define SEC_PARAM_KEYPRESS              0       /**< Keypress notifications not enabled. */
#define SEC_PARAM_IKEY      GAP_KDIST_NONE  /**< Initiator Key Distribution. (@enum gap_kdist)*/
#define SEC_PARAM_RKEY      GAP_KDIST_ENCKEY  /**< Responder Key Distribution. (@enum gap_kdist) */
#define SEC_PARAM_SEC_MODE_LEVEL    GAP_NO_SEC    /**< Device security requirements (minimum
security level). (@enum see gap_sec_req) */
```


国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

- Just Work 方式

1、 首先程序中需要调用加密初始化：

```
void app_ble_init(void)
{
    struct ns_stack_cfg_t app_handler;
    app_handler.ble_msg_handler  = app_ble_msg_handler;
    app_handler.user_msg_handler = app_user_msg_handler;
    //initialization ble stack
    ns_ble_stack_init(&app_handler);

    app_ble_gap_params_init();
    app_ble_sec_init();
    app_ble_adv_init();
    app_ble_prf_init();
    //start adv
    ns_ble_adv_start();
}
```

2、 IO能力配置为GPA_IO_CAP_NO_INPUT_NO_OUTPUT
3、 以SDK中透传例程为例，首先烧录程序，然后打开手机设置中蓝牙，开始扫描；
4、 点击要连接的设备，设备名称见宏定义“CUSTOM_DEVICE_NAME”；
5、 手机会弹窗配对提示窗口，点击配对按钮即可完成配对；

- PassKey 方式

1、修改IO能力为GAP_IO_CAP_DISPLAY_ONLY
2、手机设置中蓝牙进行扫描，稍作等待；

点击要连接的设备，手机会出输入配对密码的弹窗，默认密码是 123456；

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

```
void app_ble_sec_init(void)
{
    struct ns_sec_init_t sec_init;

    sec_init.rand_pin_enable = false;
    sec_init.pin_code = 123456;

    sec_init.pairing_feat.auth      = ( SEC_PARAM_BOND | (SEC_P
    sec_init.pairing_feat.iocap     = SEC_PARAM_IO_CAPABILITIES
    sec_init.pairing_feat.key_size  = SEC_PARAM_KEY_SIZE;
    sec_init.pairing_feat.oob       = SEC_PARAM_OOB;
    sec_init.pairing_feat.ikey_dist = SEC_PARAM_IKEY;
    sec_init.pairing_feat.rkey_dist = SEC_PARAM_RKEY;
    sec_init.pairing_feat.sec_req   = SEC_PARAM_SEC_MODE_LEVEL;

    sec_init.bond_enable            = BOND_STORE_ENABLE;
    sec_init.bond_db_addr           = BOND_DATA_BASE_ADDR;
    sec_init.bond_max_peer          = MAX_BOND_PEER;
    sec_init.bond_sync_delay        = 2000;

    sec_init.ns_sec_msg_handler     = NULL;

    ns_sec_init(&sec_init);
}
```

3、点击配对按钮即可。

- 绑定配置

```
//bond conifg
#define MAX_BOND_PEER                   5
#define BOND_STORE_ENABLE               0
#define BOND_DATA_BASE_ADDR             0x01020000
```

1、 app_user_config.h 文件中有几个绑定相关的宏定义开关；

2、MAX_BOND_PEER 表示最大绑定设备信息的数量；BOND_STORE_ENABLE 用来控制是否存储绑定信息；BOND_DATA_BASE_ADDR 是存储绑定信息的 flash 空间起始地址；

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

注意事项

暂无。

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

历史版本

版本	日期	备注
V0.5	2022.05.05	新建文档

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

声明

国民技术股份有限公司（以下简称国民技术）保有在不事先通知而修改这份文档的权利。国民技术认为提供的信息是准确可信的。尽管这样，国民技术对文档中可能出现的错误不承担任何责任。在购买前请联系国民技术获取该器件说明的最新版本。对于使用该器件引起的专利纠纷及第三方侵权国民技术不承担任何责任。另外，国民技术的产品不建议应用于生命相关的设备和系统，在使用该器件中因为设备或系统运转失灵而导致的损失国民技术不承担任何责任。国民技术对本手册拥有版权等知识产权，受法律保护。未经国民技术许可，任何单位及个人不得以任何方式或理由对本手册进行使用、复制、修改、抄录、传播等。

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057