令和三年十二月一日制定（国官参次122号）

部长办公室参赞（下一代航空移动性）远

程ID设备和应用程序应具备的要求

1.目的

航空法（昭和27年第231号法律。以下简称“法”。）根据第131-7条的航空法实施规则（昭和27年交通部令第56号。以下简称“规则”。）根据第236-6条第1款第2项的规定，被登记的无人驾驶航空器必须具备远程ID，远程ID是用于远程识别无人驾驶航空器登记符号的功能，如果不激活，不得供航空使用。

本要求根据规则第236-6条第2项规定，关于在无人驾驶航空器上安装用于显示登记符号的远程ID功能的义务，规定制造商在开发和制造无人驾驶航空器安装的远程ID功能或外部远程ID设备（以下简称“RID设备等”），以及用于输入登记符号和其他必要信息的应用程序（以下简称“应用程序”）时应遵循的具体要求。

2.对象

适用于规则第二百三十六条第二项所列的RID设备等和应用。

3.配置要求

本要件构成如下。

（附带）远程ID技术标准

（附件1）远程ID设备接口规范

（附件2）制造商应用程序应用程序接口规格书（附件3）自我验证结果/型式信息等通知书

（附件4）远程ID公钥应用验证码通知申请表

附则（令和三年国官参次128号）

该要求自令和四年六月二十日起施行。

（附加）

一卜ID技术规格书，

关于这件事的问题和咨询只以电子邮件或书面形式接受。

国土交通省航空局下一代航空移动规划室

邮编100-8918东京都千代田区霞关21-3

hqt-jcab.remoteid@mlit.go.jp

1.常规

本远程ID技术标准（以下简称“技术标准”）。）根据航空法第131-7条第1款和航空法实施条例第236-6条第1款第2项的规定，配备远程ID的无人驾驶航空器和远程ID设备（以下简称“RID设备等”）。）的开发和制造过程中，规定制造商应遵循的标准。对象范围如图1所示。

RID设备等的制造商必须使用由国土交通省航空局开发和管理的无人驾驶航空器登记系统（以下简称“登记系统”）。）通知的注册符号和RID加密所需的加密密钥信息，由国土交通省航空局开发和管理的智能手机应用程序（以下简称“国家应用程序”）。）或登录系统
RID设备制造商开发和管理的应用程序（以下简称“制造商应用程序”）。）进行写入，需要按照技术规格书开发和制造RID设备等。

本文档涵盖的范围

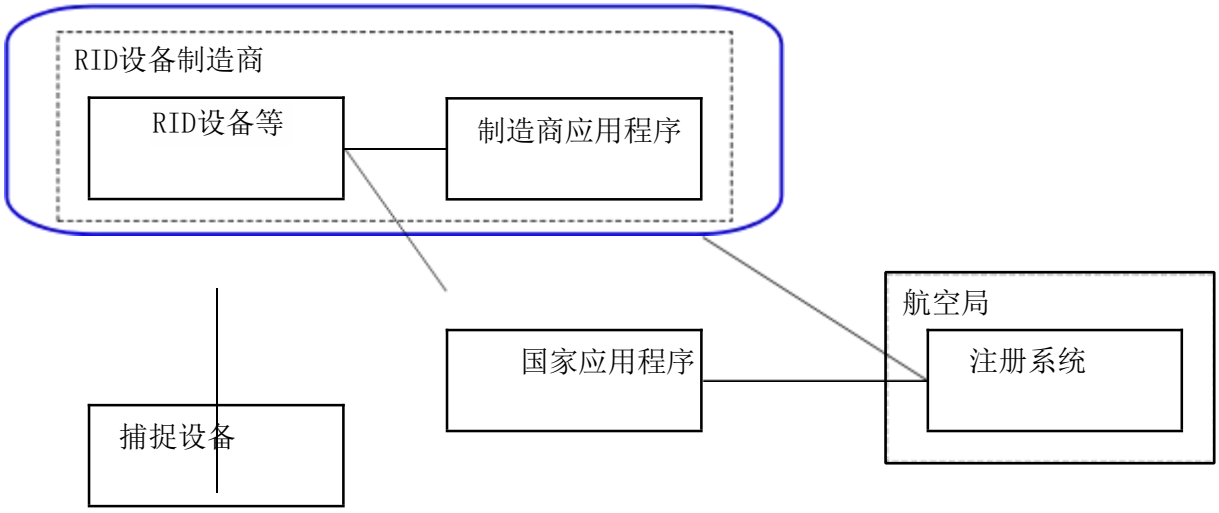

图1覆盖范围

2.RID设备等性能要求

（1）远程ID信号（以下称为“RID信号”。），蓝牙5.x蓝牙LE Long Range（以下称为“蓝牙5.x”。），Wi-Fi Neighbor Awareness Networking（以下简称“Wi-Fi Aware”）。）或Wi-Fi Beacon的直接广播方法（具有接收功能的终端直接接收从RID设备等发送的RID信号的通信方法）。

（2）根据“3.RID信号的数据格式”，RID信号应至少包括以下信息。

①根据航空法第131-6条第3款规定接到通知的登记符号；

②制造商规定的生产编号

③无人驾驶航空器位置、速度信息和时刻信息

④认证信息

（3）RID信号的发射周期应在①~④中每秒至少发出一次，并在无人驾驶航空器飞行时持续自动发射。另外，关于位置、时刻等动态信息，必须在获取信息后1秒以内发送信息。

（4）RID信号发射无线电波的等效各向同性辐射功率（EIRP）应满足。应当注意，在理想的环境下，希望能够从水平距离为300米或更远的地点接收RID信号。

·蓝牙5.x+5dBm或更高

·Wi-Fi Aware或Wi-Fi Beacon+11dBm或更高

然而，EIRP应以无线电法技术标准的值为上限（详见无线电法无线电设备规则第49-20条）。

（5）在理想环境下，位置信息的精度应大于或等于GNSS单独定位的精度（期望在±30米以内）。

（6）在无人驾驶航空器飞行过程中，RID信号的发射不能因驾驶员等操作而停止。

3.RID信号的数据格式和通信方式

RID信号被称为ASTM International F3411-19“远程ID和跟踪标准规范”（以下简称“ASTM标准”）。）的5.性能要求（注释）。在ASTM标准中，被认为是Mandatory的项目是必需项目，必须包含在RID信号中，而被认为是可选项目是任意项目，不必须包含在RID信号中。

（注）Wi-Fi Beacon不包括在ASTM标准中，但ASTM标准将进行修订

如果有，将允许以符合修订后的ASTM标准的方式发送，但下列项目应遵循以下要求。

（1）对于基本ID消息（Basic ID Message），必须发送以下双方。

·根据航空法第131-6条第3款规定收到通知的登记符号。前头后加上“JA.”的形式发出信息。UAS ID类型必须为2。（例如：JA.JU12345ABCDE）

·制造商规定的生产编号。UAS ID类型必须为1。

（2）对于认证消息（Authentication Message），必须作为必填项发送。Auth Type为3，Page Count为0，Length为17，Timestamp为32位时间戳，从2019-01-01T00：00:00 Z开始的秒数（时区为UTC）。Authentication Message Header设为0，根据下面生成的消息认证码为认证数据（Authentication Data）。（表1）

A）以Basic ID消息之后的数据为对象。验证Message需要包含Authentication Data的值用0填充的数据，在任意发送Self-ID Message，System Message以及Operator Message的情况下，需要包含这些数据。数据大小为25的倍数。

B）通过AES-128bit-CCM（Counter with Cipher block chaining Message authentication code，Counter with Cipher block chaining Message authentication code，Counter）加密对A）验证的数据进行消息传递

进行合并身份验证并生成消息验证码（12 bytes）（注释）要做的事。

（注意）验证数据不需要包含同时生成的密文（数据大小与A相同）。

用于C）B）消息认证的公共密钥（16bytes）必须由4.（2）写入RID设备等，且Nonce（12bytes）必须由以下从左到右指示。

（a）由4.（2）写入RID设备等（6字节）

（甲）位置/速度消息的时间戳（2位）

（U）“验证消息”（Authentication Message）的时间戳（4字节）

（3）为了满足（1）和（2），根据图2，RID信号必须作为一个消息包（Message Pack）一起发送。

（4）当通过蓝牙5.x发送RID信号时，ASTM标准5.4.7.1中的“If implementing this specification using Bluetooth 5 Long Range，Legacy（ADV_NONCONN_IND）advertisements must（BB50010）be sent，as described in 5.4.6，for backwards compatibility with less capable receivers.”不适用。

4.RID设备等的制造要求

（1）RID设备等必须经过基于无线电法的技术标准符合证明等。

（2）向RID设备等写入登记符号信息和生成认证消息的消息认证码所需的加密密钥信息（公共密钥和随机数生成所需的值）。

①国家应用程序的方法（RID设备等需要符合附件1“远程ID设备接口规范”）

②制造商应用程序方法（制造商应用程序必须符合附件2“制造商应用程序应用程序接口规范”）

（3）由（2）写入的加密密钥信息必须保存在RID设备等中，并采取措施防止窃取，篡改或其他第三方攻击。

（4）制造商规定的生产编号应由RID设备制造商在生产时预先输入，然后销售。此外，生产编号为

根据ANSI/CTA-2063-A进行编号。

（5）RID设备等的设计应允许无人驾驶航空器驾驶员在飞行前检查中确认RID设备等正在运行。此外，在无人驾驶航空器飞行过程中，希望设计使驾驶员能够把握RID设备等正在工作时的意图，以及由于故障等导致RID设备等不工作时的意图，即使在无人驾驶航空器飞行过程中也能把握该意图。

5.对RID设备制造商的要求等

（1）RID设备等制造商完成了RID设备等或制造商应用程序的开发

时，应将该设备的制造商名称和型号名称（如为制造商应用程序，则为应用程序名称）连同自己确认和验证该设备或制造商应用程序符合技术标准的文件，按附件3向航空局备案。

（2）航空局收到上述第（1）款通知后，应以适当方式公布RID设备的制造商名称和型号名称等。

（3）RID设备等的制造商在收到第（1）项的通知后，可以在RID设备等上注明其为已向航空局通知的RID设备等，并进行销售。

（4）RID设备等的制造商不得销售根据技术标准文件开发和制造的RID设备等，除非第（1）项的通知被接受。此外，不得销售不符合技术规格的RID设备等。

表1验证消息详细信息

奥夫塞特 Byte	长度（Bytes）	数据项	详细
1	1	验证类型 页码	bits[7..0][0000][0000] 验证类型：：bits[7..4] 默认消息集签名（Message Set Signature，3）页码： bits[3..0]
2	1	页数	bits[7..0][0000][0000] 保留：bits[7..4] 总页数：bits[3..0] 缺省值必须为0
3	1	长度（Bytes）	合并所有验证页上的所有验证数据的总数据 长度 默认值为17
4	4	时间戳	00:00:00：00 01/01/20从19开始的32位Unix时间戳（要还原为标准Unix时间戳，请将1546300800设置为 00:00:00 01/01/19添加到70标准）
8	1	验证数据头	0：AES-128bit-CCM 1-255：保留 缺省值必须为0
9	12	身份验证数据	根据3.（2）生成的认证数据
21	4	保留	

消息包								
消息类型（4位）Bits[7 4]	协议 Version（4位）Bits[3 0]	消息大小（1字节）	没有Msgs in Pack（N）	基本ID Msg（类型0x0）（ID类型=1，UA序列号）	基本ID Msg（类型0x0）（ID类型=2，UA注册ID）	定位/向量Msg（类型0x1）	身份验证Msg（类型0x2）（第0页）	…
0xF	0x0-0xF	0x19（25）	<1 Byte>	<25 Bytes>	<25 Bytes>	<25 Bytes>	<25 Bytes>	…

图2消息包

（附件1）

远程ID设备接口规范

1.常规

（1）本规范适用于《远程ID技术标准5.RID设备等的制造要求》中所述的由国土交通省航空局开发和管理的智能手机应用程序（以下简称“智能手机应用程序”）。），具有远程ID的无人飞行器和远程ID设备（以下简称“RID设备等”）。）中定义了RID设备等在写入生成注册符号信息和认证消息的认证数据所需的加密密钥信息（公用密钥和初始化向量）时应具备的接口规范。

（2）RID设备的制造商应在申请书（附件4）中填写必要事项，并以电子邮件方式向下列申请窗口提交。

航空管理局在完成申请信息确认后，通知申请人开发和制造RID设备等所需的电子签名公钥和应用验证码等。

如需变更公钥和应用验证码等，应由航空局通知RID设备制造商变更原因及变更后的公钥和应用验证码等其他必要信息。

【申请窗口】

国土交通省航空局下一代航空移动规划室

电子邮件：hqt-jcab.remoteid@mlit.go.jp

2.智能手机应用程序与RID设备等通信要求

（1）RID设备等和智能手机应用是蓝牙4.x规定的低能源通信模式（以下称为“BLE”。）中，使用1M PHY的物理层进行通信。

（2）RID设备等是BLE规范中规定的通用访问配置文件（以下简称“通用访问配置文件”）

叫做“GAP”。）中规定的Peripheral的作用运作，在连接时向周围发送advertising数据包，告知RID机器等的存在。

（3）智能手机应用程序作为GAP中规定的Central的作用运行，发现从RID机器等发出的advertising数据包，并给予连接许可。

（4）根据LE Secure Connections（使用Just Works）将已确认连接的RID设备等与智能手机应用进行配对，并在配对之后以加密的状态进行通信。

（5）已确认连接的RID设备等是BLE规范中规定的一般属性配置文件（以下称为“GATT”）。）中规定的服务器，并提供访问RID设备等保持的属性信息的服务。RID设备等必须提供的服务的定义等在“4.RID设备等的服务配置”中规定。

（6）连接确认的智能手机应用程序作为GATT中规定的Client进行操作，通过与RID机器等之间的一系列手续（顺序），实现向RID机器等写入登记符号信息等。关于在RID设备等和智能手机应用程序之间写入信息的顺序，在“5.写入RID设备等的顺序”中规定。

（7）字符串或ID和二进制数据，从左到右，从最高字节(MSB)到最低字节(LSB)，除了根据数字的大小表示大小等以外，从最高字节(MSB)到最低字节(LSB)

的顺序读取的网络字节顺序发送和接收。以数字大小表示的数字等被视为“little endian”（在本规范的下文中称为“LE”），其中LSB位于左侧，MSB位于右侧，如16位或32位整数（纬度，经度，海拔高度，时间戳等）。

3. 对RID设备等的要求

在RID设备中实现以下要求等。

（1）RID设备等具有在写入本规范中规定的注册信息等的模式和发送远程ID技术标准中规定的远程ID信号的模式之间切换的功能。

（2）在与智能手机应用程序配对时，能够通过生产编号确定目标RID设备等。

（3）在国土交通省根据第1.（2）通知的公钥和应用认证码等需要变更时，应通过固件更新等方式应对变更。

4. RID设备等的服务配置

RID设备等应根据关贸总协定的规定，提供表1所示的服务。如表1所示，该服务提供三种类型：RID Auth（访问与应用程序认证相关的属性），RID Command（访问与RID设备等的命令指令相关的属性）和RID Response（访问与RID设备等的命令指令响应相关的属性）。

表1 RID设备等服务配置

分类	种类	UUID	Permission	Value	值大小（字节）
服务声明	声明	0x2800	读取	-表2：远程ID服务UUID	16
Characteristic 1	声明	0x2803	读取	Prop=Write	1
	Value	-表2：Remote ID Auth UUID	加密 写入	（应用程序验证码）	32
	Description	0x2901	读取	RID Auth	_
Characteristic 2	声明	0x2803	读取	Prop=Write	1
	Value	-表2：远程ID命令UUID	加密 写入	-表3：命令的框架格式	176
	Description	0x2901	读取	RID命令	_
Characteristic 3	声明	0x2803	读取	Prop=Notify	1
	Value	-表2：Remote ID Response UUID	_	-表4：响应的帧格式	176
	CCCD	0x2902	加密 读写	bit0 0=Notification disabled 1=Notification enabled	2
	Description	0x2901	读取	RID响应	_

表2 RID设备等服务的UUID列表

种类	大小	UUID
远程ID服务UUID	128位	f9ed6165-faa8-4f2d-8b82-dc67d3444b0f

远程ID Auth UUID	128位	aacf388f-0e69-4802-8067-3508b1b50c3a
远程ID Command UUID	128位	2d67083e-5291-4dfa-a357-8ae4317413f5
远程ID响应UUID	128位	d98c42d8-3013-462 e-8d35-2b5b61eea94d

5.写入RID设备等时的序列

当对RID设备等执行写入登记符号信息等的处理时，按照以下所示的序列调用处理。

（1）与RID设备等的连接处理

①操作RID设备等，切换到可以与智能手机应用程序连接的模式，开始广告。

②智能手机应用程序扫描Service UUID，发现发送Remote ID Service UUID的RID设备等。进而将CompleteLocalName-制造编号作为过滤条件，发现相应的RID机器。

③在智能手机与发现的RID设备等进行配对。

④配对后，按照GATT规定的结构开始通信。

⑤从智能手机应用程序向RID机器等的RID Auth字符进行写入。在这种情况下，如果写入的值与国土交通省事先在第1.（2）中通知的RID设备的应用程序验证码不同，则断开连接

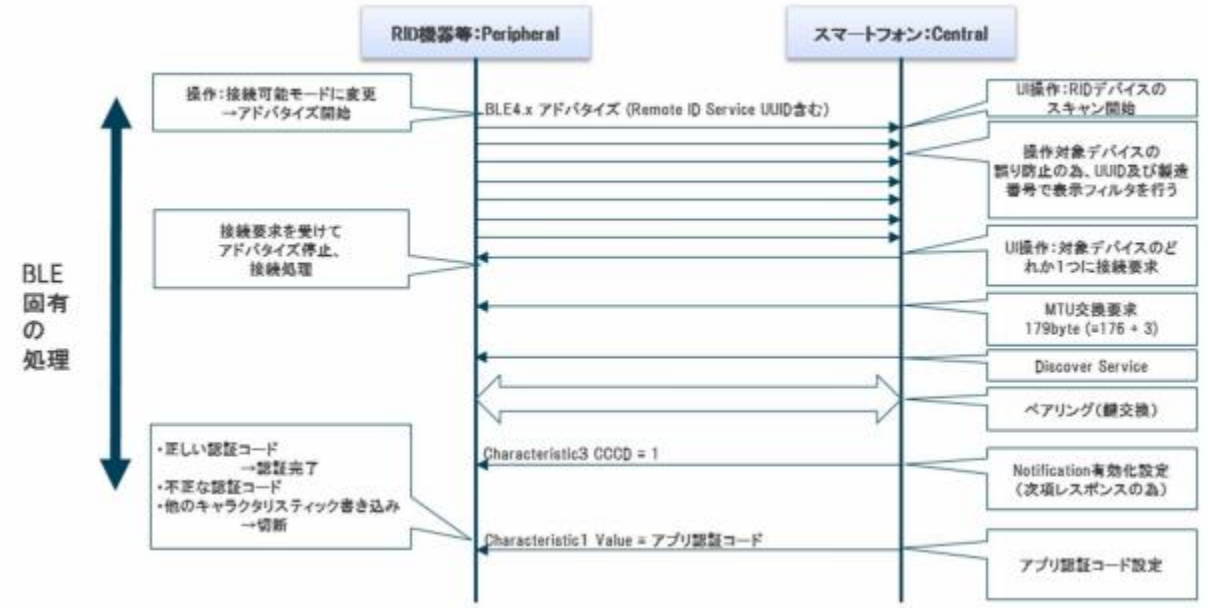

图1到RID设备等的连接处理序列

（2）命令处理（正常系统）

与RID设备等的连接成功结束，RID设备等与智能手机应用程序

以间的通信成立为前提，按照以下所示的顺序呼出处理。

①从智能手机应用程序向RID机器等的RID命令字符进行命令写入。

②写入成功后，RID机器等根据指令内容实施处理。

③RID机器等将处理结果写入RID响应特性，并通知智能手机应用程序。

图2命令处理（正常系统）序列

（3）处理命令（处理错误时）

在指令处理的中途发生异常时，按照以下所示的顺序中断处理。

①从智能手机应用程序向RID机器等的RID命令字符进行命令写入。

②写入成功后，RID机器等根据指令内容实施处理。

③处理结果为错误时，将错误内容写入RID Response字符集，通知智能手机应用程序。

④显示错误内容，并与RID设备等进行断开。

图3命令处理序列（处理错误）

错误代码中，命令自变量的错误返回0x01，除此以外的内部错误返回0x02，关于错误结果的记述内容，在172bytes的范围内返回在RID机器等内部确认的错误现象的跟踪。

（4）响应错误时的命令处理

当指令处理结果的响应出现异常时，判断为通信路径中发生异常的可能性较高，按照以下所示的顺序中断处理。

①从智能手机应用程序向RID机器等的RID命令字符进行命令写入。

②写入成功后，RID机器等根据指令内容实施处理。

③RID机器等将处理结果写入响应特性，并通知智能手机应用程序。

④当响应校验和异常时，显示错误并与RID设备等断开。

图4响应错误时的命令处理序列

（5）命令处理（通信错误）

在指令处理的途中，检测出BLE的通信错误时，进行一定次数的重试，在反复重试处理仍未完成的情况下，按照以下所示的顺序使处理中断。

①从智能手机应用程序向RID机器等的RID命令字符进行命令写入。

②如果因通信错误而失败，则尝试一定次数的重试。

③如果重试中没有成功，则显示错误内容，与RID机器等实施切断。

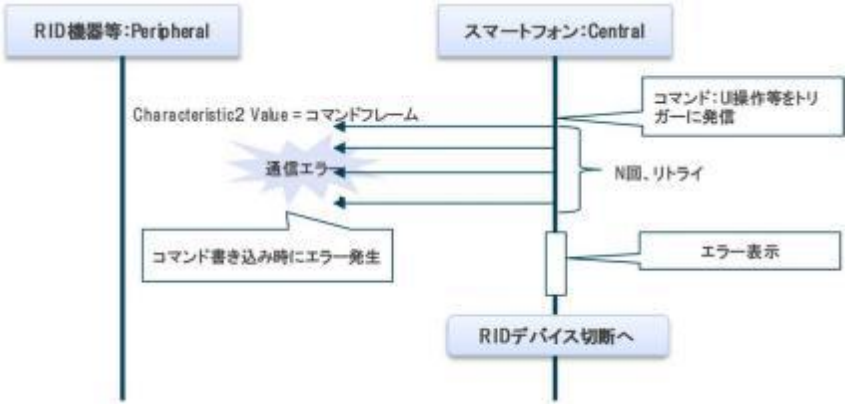

图5命令处理序列（通信错误）

（6）命令处理（超时）

在指令处理的过程中，当检测到由于某种原因没有返回响应的状态时，判断为通信路径或RID机器等发生故障的可能性较高，按照以下所示的顺序中断处理。

①从智能手机应用程序向RID机器等的RID命令字符进行命令写入。

②如果写入完成，但在一定时间内没有响应，则显示错误内容，并与RID设备等进行断开。

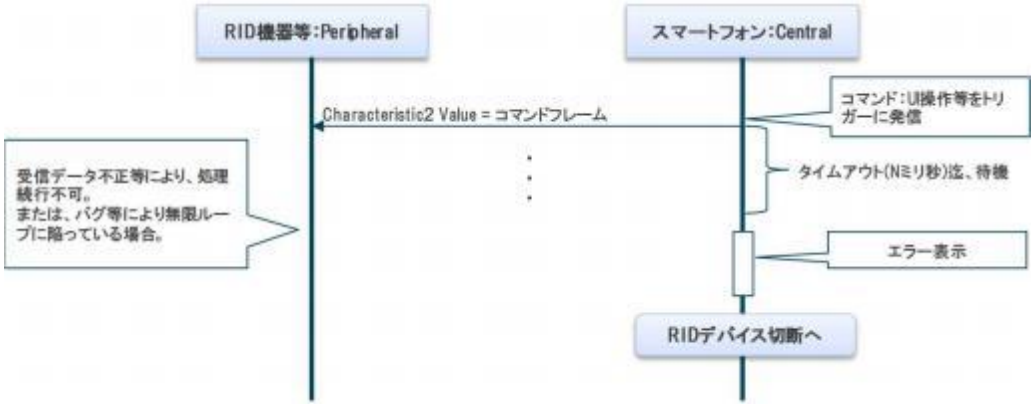

图6命令处理（超时）序列

（7）与RID设备等的断开处理

当需要与RID机器等之间的切断时，按照以下所示的顺序中断处理。

①从智能手机应用程序向RID设备等发出断开处理指令。

②接受切断指示，切断连接。

③根据需要，操作RID设备等，切换到可以发送远程ID信号的模式。

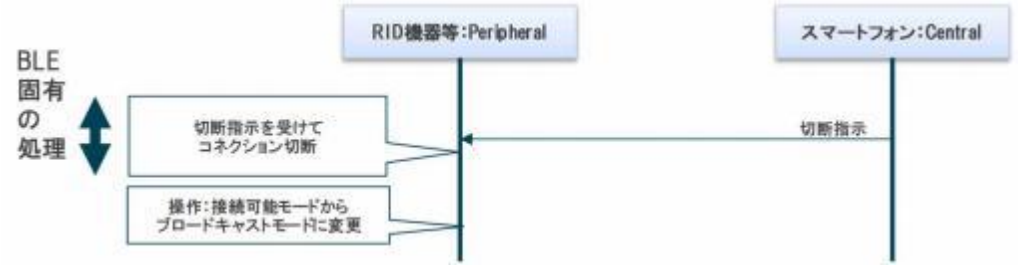

图7与RID设备等的断开处理序列

6.与RID设备等通信的帧格式

在RID设备等和智能手机应用程序之间，如表1 RID设备等的服务结构中所述，通过在Remote ID Command UUID/Remote ID Response UUID所示的属性值的176byte的帧中读写值来进行通信。以下是命令/响应的各个帧格式。

（1）命令的帧格式

表3表示命令的框架格式。

表3命令的框架格式

offset	大小（bytes）	Endian	数据	备注
0	1	_	序列号	每次发出命令时递增
1	1	_	Command ID	0x01 RID写入 0x02 RID查询
2	1	_	保留	_
3	172	（下文）	（每个命令的数据）	→7.记载在每个命令的数据定义中
175	1	_	校验求和	Offset 0-174之间的山姆

（2）响应的帧格式

表4表示响应的帧格式。

表4响应的帧格式

offset	大小（bytes）	Endian	数据	备注
0	1	_	序列号	存储在命令帧中的序列号
1	1	_	Command ID	命令帧中存储的Command ID
2	1	_	状态	成功（Success）：0x00 命令参数错误：0x01，其他内部错误：0x02
3	172	（下文）	（每个响应的数据）	→7.记载在每个命令的数据定义中
175	1	_	校验求和	Offset 0-174之间的山姆

7.每个命令的数据定义

（1）RID写入命令

①命令数据的定义

RID写入指令的指令数据定义如表5所示。

另外，删除远程ID信息时，将制造号码以外的信息作为0x00发送。

表5 RID写入命令的命令数据定义

offset	大小（bytes）	Endian	数据	说明	备注
0	1	_	密钥类型	用于生成认证码的密钥类型	0x00：未注册 0x01：指示AESCCM的密钥（128位） 其他未定义（如果将来添加验证方法，则添加值） 在服务器端生成
1	1	_	UA类型	机体种类 从服务器端获取	远程ID技术标准：基本ID消息的UA类型
2	15	_	注册符号	在国家发行的登记符号的开头加上“JA.” 从服务器端获取	远程ID技术标准文档：基本ID消息的UAS ID，ID类型=2
17	20	_	生产编号	RID设备的生产编号等 （如果与出厂设置中的制造编号不匹配，则会导致写入错误） 从服务器端获取	远程ID技术标准文档：基本ID消息的UAS ID，ID类型=1 如果生产编号少于20位，则后面填0x00
37	4	LE	开始	注册有效期起始日	从2019/1/1 00:00:00开始的秒数 （远程ID技术标准书：认证消息页0：与时间戳相同的计算方法）在服务器端生成
41	4	LE	Expire	注册有效期届满日期	
45	32	_	密钥信息	密钥信息	与密钥类型相对应的密钥信息 AECCCM的情况下，开头16字节是密钥信息，后面6字节是nonce信息，后面的10byte是0x00填充的值。 在服务器端生成
77	23	_	保留	_	全部填0x00。
100	72	_	签名信息	从Offset 0-99中的数据生成的数字签名	散列算法包括SHA-256、 在服务器侧，通过使用P-256曲线的ECDSA生成的电子签名 DER编码的二进制数据 如果小于72byte，则后面填充0x00

②确认写入结果

最好是将使用国土交通省事先通知的公共密钥对签名信息进行解密的结果与使用SHA-256算法从命令数据中除去签名信息的部分数据中获取的散列值进行对照，以验证数据的真实性。

③响应数据的定义

如果操作成功，则所有响应数据都返回0x00。

错误时，返回172byte范围内的错误内容。

（2）RID查询命令

①命令数据的定义

全部装0x00交给。

②响应数据的定义

如果处理成功完成，则返回表6 RID查询命令的响应数据定义中所示的响应数据。

表6 RID查询命令响应数据定义

offset	大小（bytes）	Endian	数据	说明	备注
0	1	_	密钥类型	密钥类型	0x00：未注册 0x01：指示AESCCM的密钥（128位） 其他未定义（如果将来添加验证方法，则添加值）
1	1	_	UA类型	机体种类	远程ID技术标准：基本ID消息的UA类型
2	15	_	注册符号	在国家发行的登记符号的开头加上“JA.”	远程ID技术标准文档：基本ID消息的UAS ID，ID类型=2
17	20	_	生产编号	制造商发布的RID设备的生产编号等	远程ID技术标准文档：基本ID消息的UAS ID，ID类型=1如果生产编号短于20位，则后面填0x00
37	4	LE	开始	注册有效期起始日	从2019/1/1 00:00:00开始的秒数 （远程ID技术标准：认证消息第0页：与时间戳相同的数据格式）
41	4	LE	Expire	注册有效期届满日期	
45	127	_	保留		ALL 0x00

错误时，返回172byte范围内的错误内容。

（附件2）

制造商应用程序应用程序接口规范

1.常规

（1）本规范适用于《远程ID技术标准5.RID设备等制造要求》中所述的由国土交通省航空局开发和管理的无人驾驶航空器登记系统（以下简称“登记系统”）。）连接的远程ID设备（以下称为“RID设备等”。）制造商开发和管理的应用程序（以下简称“制造商应用程序”）。）必须具备的要求，从登记系统获取向RID设备等写入登记符号等时所需的信息，以及规定将登记符号等的写入结果存储到登记系统时所需的接口规范。

（2）制造商应用程序制造商应在申请书（附件4）中填写必要事项，并通过电子邮件提交给以下申请窗口。

航空管理局完成申请信息确认后，通知申请人开发制造厂商APP所需的电子签名公钥和APP验证码等。

如需变更公钥和应用验证码等，应由航空局通知厂商应用制造商变更原因及变更后的公钥和应用验证码等其他必要信息。

【申请窗口】

国土交通省航空局下一代航空移动规划室

电子邮件：hqt-jcab.remoteid@mlit.go.jp

2.厂商APP与注册系统通讯要求

（1）厂商应用程序和登录系统通过因特网，通过https协议进行加密通信。

（2）厂商应用与注册系统连接时，在注册系统提供的认证基础上，通过注册系统的用户ID/PW进行用户认证。另外，认证方式使用Open ID Connect。

（3）登录系统提供的API以REST形式使用Web API，以OpenAPI形式记述并公开规格。

3.对厂商APP的要求

（1）注册符号和认证信息只能由用户或其应用程序访问，不得由第三方访问。对于Android，不要在/sdcard区域放置注册符号和认证信息。

（2）在国土交通省根据第1.（2）通知的公钥和应用认证码等需要变更时，通过固件更新等方式应对变更。

4.远程ID信息注册的顺序

制造商应用程序从注册系统获取注册符号信息和密码密钥信息，将该信息写入RID机器等，将写入结果存储在注册系统中的一系列处理流程如图1所示。

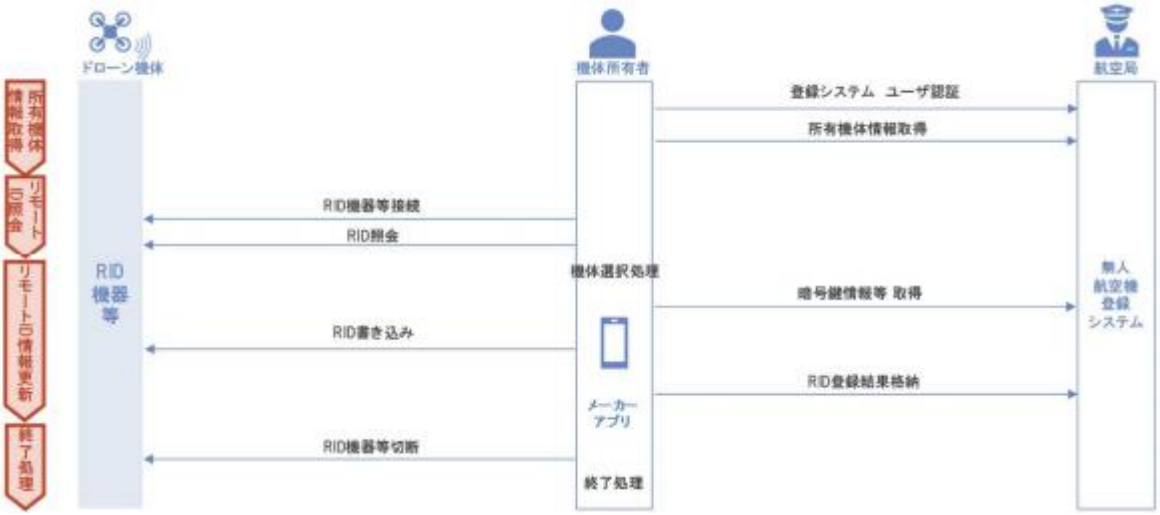

图1远程身份信息注册序列

（1）获取所有机体信息

连接登记系统，获取所拥有的无人驾驶航空器的信息一览表。

①注册系统用户认证

使用注册系统的认证基础提供的认证功能进行用户认证。基于在此取得的访问权限，实施与以下登录系统的访问。

②获取所有机体信息

获取用户拥有的机身信息（机身注册符号，制造商，型号，生产编号，RID设备的生产编号等）。

（2）远程身份信息查询

连接到进行写入的RID机器等，查询写入前的远程ID信息。

①RID设备等连接

连接制造商应用程序和RID设备等。

②RID信息查询

查询写入RID设备等的登记符号和RID设备等的生产编号等。

（3）远程ID信息更新

将登录系统上的机体信息与连接到制造商应用程序的RID设备等相结合，进行远程ID信息的更新。

①注册机体选择

从现在开始进行更新的登录系统上的机体和RID机器等的1：1选择处理。在选择时，使用RID设备等的制造编号进行对接，以防止将登记符号信息写入错误的RID设备等。

②获取密码密钥信息等

从注册系统获取密码密钥信息等。仅当需要向RID设备写入时，才获取加密密钥信息等。

③RID写入

更新RID设备的登记符号信息等。

④RID写入结果存储

向RID设备等写入登记符号信息等的结果存储在登记系统中。

（4）终止处理

注册完成后，实施终止处理。另外，由于错误等一连串的处理手续中途结束的情况下，也要执行本处理。

①切断RID设备等

根据需要，断开与RID设备等的连接，并执行RID设备等恢复到未连接状态的处理。

②终止处理

执行删除处理，以确保加密密钥信息不留在制造商应用程序的内部。

5.与注册系统定义厂商应用界面

制造商应用程序和注册系统使用以下所示的应用程序接口来写入注册符号信息等。

（1）整体序列

制造商应用程序和登录系统在登录系统提供的认证基础上，实施基于Open ID Connect的认证处理，使用由此得到的访问令牌，根据被认证的用户的权限发出各种API的请求。整体的顺序如图2所示。

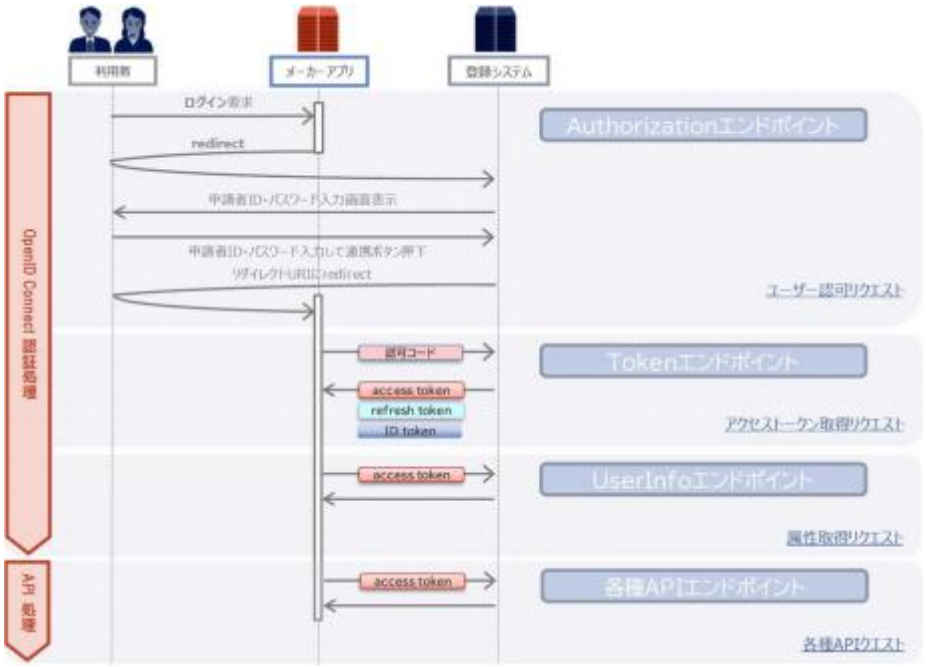

图2整体序列

（2）用户验证

用户认证使用注册系统提供的认证基础。

认证处理遵循开放ID连接，并应用用于防止同一设备中的认证信息泄漏的扩展（RFC7636：Proof Key for Code Exchange by OAuth Public Clients）。

①认证处理的顺序

认证处理的序列如图3所示。

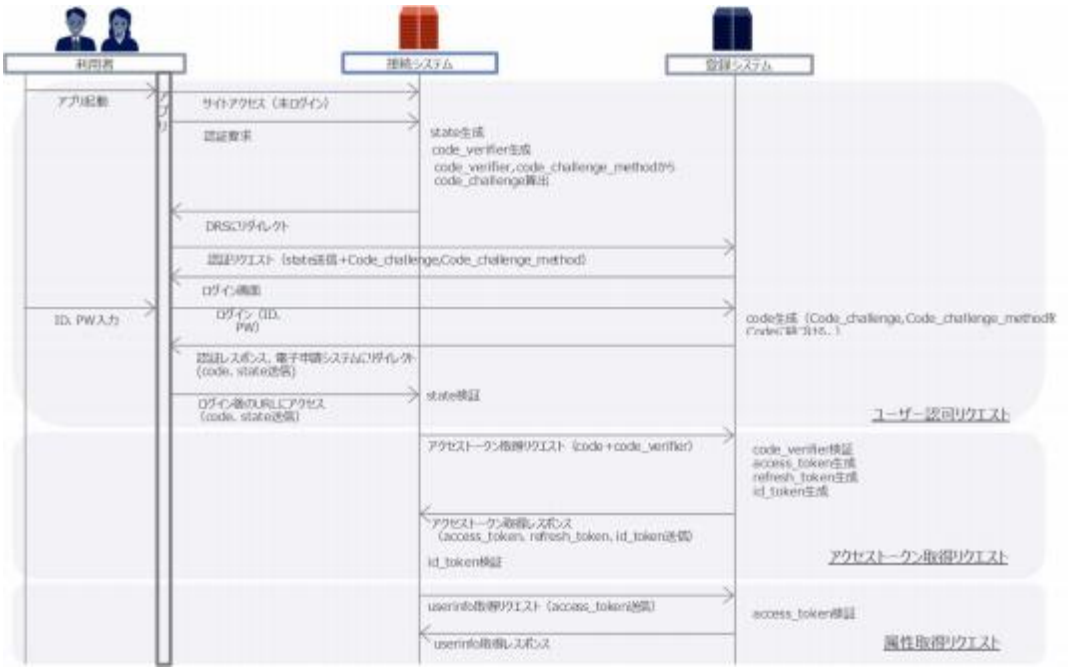

图3开放ID连接验证序列（PKCE扩展）

②关于认证的请求处理

认证请求处理（用户授权，访问令牌获取和用户属性获取处理）是根据Open ID Connect的规范执行的。

运用环境中的请求URL等依据登录系统的规格。

（3）为写入注册符号信息等提供的API

为写入登录记号信息等提供的API如表1所示。

表1为写入注册符号信息等提供的API

API名称	种类	API路径	内容
获取所有机体信息列表	GET	/rid/aircrafts	获取用户拥有的机身信息的列表。 根据取得的机体信息确认RID写入所需的机体诸元。
获取所有机体信息	GET	/rid/aircrafts/{registration_code}	将登记符号作为键获取用户拥有的机体信息。
加密密钥信息获取	GET	/rid/remoteid	获取生成认证消息的认证数据所需的加密密钥信息。（可以使用参数重新创建加密密钥）
远程ID写入结果存储	开机自检	/rid/remoteid	向RID设备等写入的结果存储在登记系统中

今后，当发生不向后兼容的API变更时，作为版本管理，在文字“v”上附加编号，将“v2”，“v3”……插入API路径。本规范作为“v1”省略。

例如：所有机体信息一览表获取API为“/rid/v2/aircrafts”

①请求

每个API的请求参数描述在单独的API定义中。

在请求每个API时，（2）将通过用户认证获得的访问令牌附加到授权：Bearer标头，以便通过用户权限进行限制。

另外，运用环境中的请求URL等依据登录系统的规格。

②响应

如果请求成功，则返回单独API定义中所述的响应。登录系统内发生错误时，返回表2所示的响应代码和表3所示的以下响应主体。

表2错误响应代码

HTTP状态	意义	内容
400	请求参数错误	处理失败（参数错误）
500	API中的系统错误	意外的系统错误

表3错误响应主体

项目名称	参数名称	数据类型	必需	内容
错误代码	errorCode	字符串	○	错误代码
错误	errorMessage	字符串	○	错误的详细说明

（4）所有权机体信息一览表获取API的定义

获取申请人拥有的无人机机体信息一览表。

①无请求参数

②响应体

所有机体信息一览获取API的请求成功时的响应主体的定义如表4所示。

表4所有机体信息列表获取API成功时的响应主体

项目名称	参数名称	数据类型	必需	内容
机体信息		排列	○	机身信息的排列 0到N个
注册符号	registration_code	字符串	○	国家颁发的注册符号
制造分类	manufacturing_category	字符串	○	下列值之一 1：制造商的机体/改造后的机体 2：自制的机体
制造商日语	manufacturer_jpn	字符串	○	无人驾驶飞机制造商名称（日语）
型式日语	model_jpn	字符串	○	无人驾驶飞机型号名称
制造商英语	manufacturer_eng	字符串	○	无人驾驶飞机制造商名称（英语）
型式英语	model_eng	字符串	○	无人驾驶航空器类型名称（英文）
生产编号	manufacturing_number	字符串	○	无人驾驶飞机的制造编号
改造有无	remodeling_type	字符串		1：有改造 2：没有改造
类型	aircraft_type	字符串	○	下列值之一 1：飞机 二：旋翼机（直升机） 3：旋翼飞机（多旋翼） 4：旋转翼飞机（其他） 5：滑翔机 6：飞艇
RID是否存在	rid_type	字符串	○	有RID的机体 0：无 1：有（内置） 2：有（外置）
RID外部设备制造商日语	rid_manufacturer_jpn	字符串		RID外部设备制造商的名称（日语）。 内置RID时，与无人机制造商相同
RID外部设备类型日语	rid_model_jpn	字符串		RID外部设备的型号名称（日语）。 内置RID时，与无人飞行器型号相同
RID外部设备制造商英语	rid_manufacturer_eng	字符串		RID外部设备制造商的名称（英文）。 内置RID时，与无人机制造商相同
RID外部设备类型英语	rid_model_eng	字符串		RID外部设备的型号名称（英文）。 内置RID时，与无人飞行器型号相同
RID外部设备的生产编号	rid_manufacturing_number	字符串		RID外部设备的生产编号。 内置RID的情况下，与无人飞机的制造编号相同
修改时间	modified_date	字符串	○	更新时间(UTC) 初始注册时返回空字符串 格式为YYYY-MM-DDThh：mm：ssZ。
写入标志	write_status	字符串	○	向RID设备写入登记符号信息的状态等。 0：未写入 1：已写入

（5）所有权机体信息获取API的定义

以登记符号为关键，获取申请人拥有的1架无人机机体信息。

①无请求参数

②响应体

所有机体信息一览获取API的请求成功时的响应主体的定义如表5所示。

表5所有权机体信息获取API成功时的响应主体

项目名称	参数名称	数据类型	必需	内容
注册符号	registration_code	字符串	○	国家颁发的注册符号
制造分类	manufacturing_category	字符串	○	下列值之一 1：制造商的机体/改造后的机体 2：自制的机体
制造商日语	manufacturer_jpn	字符串	○	无人驾驶飞机制造商名称（日语）
型式日语	model_jpn	字符串	○	无人驾驶飞机型号名称
制造商英语	manufacturer_eng	字符串	○	无人驾驶飞机制造商名称（英语）
型式英语	model_eng	字符串	○	无人驾驶航空器类型名称（英文）
生产编号	manufacturing_number	字符串	○	无人驾驶飞机的制造编号
改造有无	remodeling_type	字符串		1：有改造 2：没有改造
类型	aircraft_type	字符串	○	下列值之一 1：飞机 二：旋翼机（直升机） 3：旋翼飞机（多旋翼） 4：旋转翼飞机（其他） 5：滑翔机 6：飞艇
RID是否存在	rid_type	字符串	○	有RID的机体 0：无 1：有（内置） 2：有（外置）
RID外部设备制造商日语	rid_manufacturer_jpn	字符串		RID外部设备制造商的名称（日语）。 内置RID时，与无人机制造商相同
RID外部设备类型日语	rid_model_jpn	字符串		RID外部设备的型号名称（日语）。 内置RID时，与无人飞行器型号相同
RID外部设备制造商英语	rid_manufacturer_eng	字符串		RID外部设备制造商的名称（英文）。 内置RID时，与无人机制造商相同
RID外部设备类型英语	rid_model_eng	字符串		RID外部设备的型号名称（英文）。 内置RID时，与无人飞行器型号相同
RID外部设备的生产编号	rid_manufacturing_number	字符串		RID外部设备的生产编号。 内置RID的情况下，与无人飞机的制造编号相同
修改时间	modified_date	字符串	○	更新时间(UTC) 初始注册时返回空字符串 格式为YYYY-MM-DDThh：mm：ssZ。
写入标志	write_status	字符串	○	向RID设备写入登记符号信息的状态等。 0：未写入 1：已写入

（6）加密密钥信息获取API的定义

以向RID机器等写入时的数据块的形式返回由登记符号确定的机体的有效密码密钥等信息。 此外，由于不在多个无人驾驶航空器中写入同一外接模块，因此接收密码密钥信息获取API请求，在无人机登记系统中以该外接RID设备等的制造编号为密钥，检查是否存在已向所有所有者、机体写入写入标记的机体，如果已有同一模块写入的机体，则无法获取数据块。 （返回空字符。）

①请求参数

加密密钥信息等获取API的请求参数的定义如表6所示。

表6获取密码密钥信息API的请求参数

项目名称	参数名称	数据类型	必需	内容
注册符号	registration_code	字符串	○	选定机身的注册符号
加密密钥重新创建标志	key_remake	字符串	○	指定重新创建加密密钥的参数 0：没有重新创建加密密钥 1：有密码密钥再作成

在RID机器等中初次写入时，由于不需要加密密钥的再制作，因此请求参数的加密密钥再制作标志指定为0。第2次以后的写入时，从安全性的观点出发，加密密钥的再制作是必须的，通过参数1指定进行请求。第一次、第二次以后的判断是根据所有者信息获取API、所有者信息一览获取API的响应项目即更新日期和时间的有无来进行判断。

②响应体

加密密钥信息等获取API的请求成功时的响应主体的定义如表7所示。

表7加密密钥信息获取API成功时的响应主体

项目名称	参数名称	数据类型	必需	内容
注册符号	registration_code	字符串	○	国家颁发的注册符号
写入数据块	数据	字符串	○	写入RID设备的信息（二进制）的base64编码。数据的定义如表8所示。
写入标志	write_status	字符串	○	向RID设备写入登记符号信息的状态等。 0：未写入 1：已写入
修改时间	modified_date	字符串	○	更新时间(UTC) 初始注册时返回空字符串 格式为YYYY-MM-DDThh：mm：ssZ。
发信方式	broadcast_method	字符串	○	远程ID信号的发送方式。下列任一项 0：未配置传出方式 1：RID技术规格书中记载的BLE5.0的发送方式 2：RID技术标准书中记载的Wi-Fi Aware的发送方式3：RID技术标准书中记载的Wi-Fi Beacon的发送方式

通过用Base64形式解码写入数据块，可以得到具有以下构造的二进制数据。

注意，此处获取的数据的结构如“（附件1）远程ID设备接口规范表5 RID写入命令的命令数据定义”中所述

由于与数据相同，因此可以直接写入RID机器等。　　数据的定义如表8所示。 字节顺序为“little endian”的项目在Endian列中记作“LE”。

表8写入数据块定义

offset	大小（bytes）	数据	Endian	说明	备注
0	1	密钥类型	_	用于生成认证码的密钥类型	0x00：未注册 0x01：表示AES-CCM的密钥（128位） 其他未定义（在将来添加验证方法时添加值）在服务器端生成
1	1	UA类型	_	机体种类 从服务器端获取	远程ID技术标准：基本ID消息的UA类型
2	15	注册符号	_	在国家发行的注册符号的开头添加“JA.”从服务器端获取	远程ID技术标准文档：基本ID消息的UAS ID，ID类型=2
17	20	生产编号	_	RID设备的生产编号等 （如果与出厂设置中的制造编号不匹配，则会导致写入错误） 从服务器端获取	远程ID技术标准文档：基本ID消息的UAS ID，ID类型=1 如果生产编号少于20位，则后面填0x00
37	4	开始	LE	注册有效期起始日	从2019/1/1 00:00:00开始的秒数 （远程ID技术标准书：认证消息页0：与时间戳相同的计算方法） 在服务器端生成
41	4	Expire	LE	注册有效期届满日期	
45	32	密钥信息	_	密钥信息	与密钥类型相对应的密钥信息 AEC-CCM的情况下，开头16字节是密钥信息，后面6字节是nonce信息，后面的10byte是0x00填充的值。 在服务器端生成
77	23	保留	_	_	全部填0x00。
100	72	签名信息	_	从Offset 0-99中的数据生成的数字签名	散列算法包括SHA-256、 在服务器侧，对使用P-256曲线的ECDSA生成的电子签名进行DER编码的二进制数据 如果小于72byte，则后面填充0x00

如表8所示，在写入数据块内，收纳了从登录系统取得的信息和其签名信息。 当接收到响应时，将使用国土，基础设施，基础

（7）远程ID注册结果存储API的定义

远程ID信息注册完成后，注册结果存储在注册系统中。

①请求主体

远程ID登录结果存储API的请求主体的定义如表9所示。

表9远程ID注册结果存储API请求主体

项目名称	参数名称	数据类型	必需	内容
注册符号	registration_code	字符串	○	选定机身的注册符号
写入标志	write_status	字符串	○	向RID设备写入登记符号信息的状态等。 0：未写入 1：已写入

②响应体

远程ID登录结果存储API的请求成功时的响应主体的定义如表10所示。

表10远程ID注册结果存储API成功时的响应主体

项目名称	参数名称	数据类型	必需	内容
注册符号	registration_code	字符串	○	国家颁发的注册符号
写入标志	write_status	字符串	○	向RID设备写入登记符号信息的状态等。 0：未写入 1：已写入
修改时间	modified_date	字符串	○	更新时间(UTC) 格式为YYYY-MM-DDThh：mm：ssZ。
发信方式	broadcast_method	字符串	○	远程ID信息的发送方式。下列任一项 0：未配置传出方式 1：RID技术规格书中记载的BLE5.0的发送方式 2：RID技术标准书中记载的Wi-Fi Aware的发送方式3：RID技术标准书中记载的Wi-Fi Beacon的发送方式

6.OpenAPI

```
openapi：3.0.0
info：
  title：RemoteID
  版本：“1.0”
  描述：-
    用于向无人机写入远程身份信息的API
  连接：
    名称：国土交通省
  license：
    名称：MLIT
标记：
  -name：所有者
paths：
  /rid/aircrafts：
    get：
      摘要：获取所有机身信息列表
      标记：
        -所有者
      参数：[]
      响应：
        ’200’：
          描述：确定
          内容：
            appl ication/json：
              schema：
                类型：array
                items：
                  $ref：‘#/components/schemas/Aircraft’
        ’400’：
          描述：Bad Request
        ’500’：
          描述：内部服务器错误
      operationId：get-r id-aircrafts
      描述：-
        获取用户拥有的机身信息的列表。

  /rid/aircrafts/{registration_code}：
    get：
      摘要：获取所有权信息
      标记：
        -所有者
      参数：
        -name：registration_code
          description：注册符号
          in：path
          required：true
          schema：
            $ref：‘#/components/schemas/Registration_Code’
      响应：
        ’200’：
          描述：确定
          内容：
            appl ication/json：
              schema：

                $ref：‘#/components/schemas/Aircraft’
```

```
      '400':
        描述：Bad Request
      '500':
        描述：内部服务器错误
    operationId：get-rid-aircrafts-by-registratyion_code
    描述：-
      以登记符号为键获取用户拥有的机身信息。
/rid/remoteid：
  get：
    summary：获取加密密钥信息
    标记：
      -所有者
    参数：
    -name：registration_code
      description：注册符号
      schema：
        $ref：‘#/components/schemas/Registration_Code’
      in：query
      required：true
    -name：key_remake
      描述：重新创建加密密钥标志
      schema：
        $ref：‘#/components/schemas/Key_Remake’
      in：query
      required：true
    响应：
      '200':
        描述：确定
        内容：
          appl ication/json：
             schema：
              类型：对象
              属性：
                registration_code：
                  $ref：‘#/components/schemas/Registration_Code’
                数据块：
                  格式：字节
                  类型：str ing
                  description：写入RID设备的base64编码信息wr ite_status：
                  $ref：‘#/components/schemas/Wr ite_Status’
                modified_date：
                  格式：日期时间
                  类型：str ing
                  说明：更新日期
                broadcast_method：
                  $ref：‘#/components/schemas/Broadcast_Method’
      '400':
        描述：Bad Request
      '500':
        描述：内部服务器错误
    operationId：get-r id-remoteid
    description：获取生成验证消息的验证数据所需的加密密钥信息。 post：
    summary：远程ID注册结果存储
    标记：
      -所有者
    参数：[]
    requestBody：
      内容：
```

```
          appl ication/json:
            schema:
              类型：对象
              属性：
                  registration_code:
                    $ref: ‘#/components/schemas/Registration_Code’

                  wr ite_status:
                    $ref: ‘#/components/schemas/Wr ite_Status’

        说明：RemoteID写入结果
      响应：
        ’200’:
          描述：确定
          内容：
            appl ication/json:
              schema:
                类型：对象
                属性：
                  registration_code:
                    $ref: ‘#/components/schemas/Registration_Code’
                  wr ite_status:
                    $ref: ‘#/components/schemas/Wr ite_Status’
                  modified_date:
                    格式：日期时间
                    类型：str ing
                    说明：更新日期
                  broadcast_method:
                    $ref: ‘#/components/schemas/Broadcast_Method’
        ’400’:
          描述：Bad Request
        ’500’:
          描述：内部服务器错误
      operationId:
      description：将写入RID设备的结果存储在注册系统中
components:
  schemas:
    注册表名代码：
      类型：str ing
      minLength：12
      最大长度：12
      描述：注册符号
    Wr ite_Status:
      枚举：
      - "0"
      - "1"
      类型：str ing
      描述：-
        RID写入状态
         “0”-未写入
         “1”-已写入
    Broadcast_Method:
      枚举：
      - "0"
      - "1"
      - "2"
      - "3"
      类型：str ing
      描述：-
        发信方式
```

“0”-未配置发送方式
“1”-RID技术标准中描述的BLE5.x传输方法
“2”-RID技术标准中的Wi-Fi Aware呼叫方法
“3”-RID技术标准中的Wi-Fi Beacon呼叫方法
制造类别：
枚举：
- "1"
- "2"
类型：str ing
描述：-
制造分类
“1”-制造商的机身/改装的机身
“2”--我自己造的飞机
Manufactur ing_Number：
类型：str ing
最大长度：20
说明：制造编号
Remodel ing_Type：
枚举：
- "1"
- "2"
类型：str ing
描述：-
改造有无
有一个改造
“2”-没有改造
Aircraft_Type：
枚举：
- "1"
- "2"
- "3"
- "4"
- "5"
- "6"
类型：str ing
描述：-
类型
一架飞机
“2”-旋翼机（直升机）
“3”-旋翼飞机（多旋翼）
“4”-旋翼机（其他）
五号滑翔机
六号飞艇
Rid_Type：
枚举：
- "1"
- "2"
- "3"
类型：str ing
描述：-
RID是否存在
“0”-无
“1”-有（内置）
“有2”（外置）
Key_Remake：
枚举：
- "1"
- "2"
类型：str ing
描述：-

```
      指定重新创建加密密钥的参数
      “1”-没有加密密钥重新创建
      “2”-加密密钥已重新创建
  Aircraft:
    类型：对象
    描述：-
      机体信息
      从注册系统规格中摘录标识机体的信息
    属性：
      registration_code:
        $ref: ‘#/components/schemas/Registration_Code’
      manufacturing_category:
        $ref: ‘#/components/schemas/Manufacturing_Category’
      manufacturer_cn:
        类型：str ing
        说明：制造商日语
      model_cn:
        类型：str ing
        description：类型日语
      manufacturer_eng:
        类型：str ing
        说明：制造商英语
      model_eng:
        类型：str ing
        description：型式英语
      manufactur ing_number:
        $ref: ‘#/components/schemas/Manufactur ing_Number’
      remodel ing_type:
        $ref: ‘#/components/schemas/Remodel ing_Type’
      aircraft_type:
        $ref: ‘#/components/schemas/Aircraft_Type’
      rid_type:
        $ref: ‘#/components/schemas/Rid_Type’
      rid_manufacturer_cn:
        类型：str ing
        说明：RID外部设备制造商日语
      rid_model_cn:
        类型：str ing
        描述：RID外部设备类型日语
      rid_manufacturer_eng:
        类型：str ing
        说明：RID外部设备制造商英语
      rid_model_eng:
        类型：str ing
        描述：RID外部设备类型
      r id_manufactur ing_number:
        $ref: ‘#/components/schemas/Manufactur ing_Number’
      modified_date:
        格式：日期时间
        类型：str ing
        说明：更新日期
      wr ite_status:
        $ref: ‘#/components/schemas/Wr ite_Status’
    required:
      -registration_code
      -manufacturing_category
      -manufacturer
      -模型
      -manufactur ing_number
      -aircraft_type
```

```
        -rid_type
        -wr ite_status
```

7.与注册系统进行认证的请求和响应一览表

以下记载与注册系统认证的详细信息。

（1）认证请求处理

认证请求处理（用户授权，访问令牌获取和用户属性获取处理）是根据Open ID Connect的规范执行的。

有关认证的要求如表11所示。

表11认证请求

请求名称	种类	请求路径	内容
用户授权	GET	/auth/realms/drs/protocol/openid-connect/auth	判断用户的认证状态和授权状态，将其重定向到适当的页面，并返回授权代码。
访问令牌检索	开机自检	/auth/realms/drs/protocol/openid-connect/token	获取访问令牌和刷新令牌（用于更新访问令牌）。
属性检索	GET	/auth/realms/drs/protocol/openid-connect/userinfo	获取用户属性信息。

每个请求的标头和参数在单独的请求定义中描述。

（2）定义用户授权请求

判断用户的认证状态和授权状态，将其重定向到适当的页面，并返回授权代码。

①请求参数

认证请求的请求参数如表12所示。

表12验证请求的请求参数

项目名称	参数名称	数据类型	必需	内容
响应类型	response_type	字符串	○	code固定
客户机ID	client_id	字符串	○	为每个制造商应用程序预先定义的[客户端ID]
重定向URI	redirect_uri	字符串	○	为每个制造商应用程序预先定义[重定向到登录成功等的URL]
范围	scope	字符串	○	openid offline_access固定
状态	状态	字符串	○	用于维护请求和相应回调之间的状态的参数
代码挑战	code_challenge	字符串	○	使用SHA256散列（加密）访问令牌获取请求时指定的参数“code_verifier”的字符串，并将其编码为Base64URL格式
代码挑战方法	code_challenge_method	字符串	○	S256固定
显示语言	ui_locales	字符串	-	下列值之一。 ja en 如果未指定，则根据Accept-Language请求头切换日语/英语显示。

②响应（正常）

请求成功时，转移到输入登录ID和密码的画面。

当用户执行登录操作时，重定向到“为每个制造商应用程序预先定义的[登录成功时重定向URL]”。 登录成功时的重定向查询参数如表13所示。

表13成功登录时的重定向查询参数

项目名称	参数名称	数据类型	必需	内容
认可代码	代码	字符串	O	认可代码
会话状态	session_state	字符串	O	会话状态
状态	状态	字符串	O	检查请求时保存的值是否与回调时的值相匹配。如果不匹配，则不执行访问令牌获取请求，因为可能是CSRF。

③响应（错误时）

错误发生时，转移到系统错误画面。

将某些错误重定向到“每个制造商应用程序预先定义的[URL重定向到登录成功时等]”。 登录错误时的重定向查询参数如表14所示。

表14登录错误时的重定向查询参数

项目名称	参数名称	数据类型	必需	内容
错误代码	错误	字符串	O	错误代码
错误内容	error_description	字符串	O	错误的详细说明
状态	状态	字符串	O	检查请求时保存的值是否与回调时的值相匹配。不一致时有CSRF的可能性。

登录系统在系统维护中时，以JSON形式返回表15所示的响应主体和表16所示的错误响应。

表15系统维护响应主体

项目名称	参数名称	数据类型	必需	内容
错误代码	errorCode	字符串	O	错误代码
错误	errorMessage	字符串	O	错误的详细说明

表16系统维护期间的错误响应

HTTP 状态	错误代码	错误	说明
503	E5030001	无	注册系统维护期间调用API

（3）访问令牌获取请求的定义

返回访问令牌和刷新令牌（用于更新访问令牌）。

①请求头

存取令牌获取请求的请求头如表17所示。

表17访问令牌获取请求的请求头

项目名称	标头名称	数据类型	必需	内容
内容类型	内容类型	字符串	O	application/x-www-form-urlencoded；charset=UTF-8“固定

②请求参数

存取令牌获取请求的请求参数如表18所示。

表18访问令牌获取请求的请求参数

项目名称	参数名称	数据类型	必需	内容
赠款类别	grant_type	字符串	O	authorization_code固定
认可代码	代码	字符串	O	用户授权请求返回的授权代码
重定向URI	redirect_uri	字符串	O	为每个制造商应用程序预先定义[重定向到登录成功等的URL]
客户机ID	client_id	字符串	O	为每个制造商应用程序预先定义的[客户端ID]
代码验证器	code_verifier	字符串	O	由43到128个字符组成的随机字符串，包括“A-Z”、“a-z”、“0-9”、“-”、“.”、“_”和“~”。

③响应体（正常时）

存取令牌获取请求正常时的响应主体如表19所示。

表19获取访问令牌请求的正常响应主体

项目名称	参数名称	数据类型	必需	内容
存取令牌	access_token	字符串	O	发出userinfo请求或API时所需的token
过期时间	expires_in	数值	O	access_token的有效时间（秒）
刷新令牌过期	refresh_expires_in	数值	O	refresh_token的有效时间（以秒为单位）
刷新令牌	refresh_token	字符串	O	更新access_token所需的token
令牌类型	token_type	字符串	O	bearer固定
ID令牌	id_token	字符串	O	ID标记（JWT（JSON Web Token））
不稳定政策	不相关策略	数值	O	用于验证访问令牌有效性的值
会话状态	session_state	字符串	O	会话状态
范围	scope	字符串	O	openid profile offline_access rid固定

④响应体（错误时）

存取令牌获取请求错误时的响应代码如表20所示。

表20访问令牌获取请求的错误响应主体

项目名称	参数名称	数据类型	必需	内容
错误代码	错误	字符串	O	错误代码
错误内容	error_description	字符串	O	错误的详细说明

存取令牌获取请求的代表性错误代码如表21所示。

表21访问令牌获取请求的典型错误代码

HTTP状态	错误代码	说明
400	unauthorized_client	参数“client_id”无效
400	invalid_request	参数“grant_type”无效
400	invalid_grant	授权代码无效、过期或无效，参数“redirect_uri”无效

（4）获取属性获取请求的定义用

户属性信息。

①请求头

属性获取请求的请求标题如表22所示。

表22属性获取请求的请求头

项目名称	标头名称	数据类型	必需	内容
授权	授权	字符串	O	Bearer[access_token从访问令牌获取请求中获取]

②无请求参数。

③响应体（正常时）

属性获取请求正常时的响应主体如表23所示。

表23属性获取请求的正常响应主体

项目名称	参数名称	数据类型	必需	内容
帐户管理号	sub	字符串	O	帐户管理号（返回内部ID）
用户名	preferred_username	字符串	O	用户名

④响应体（错误时）

属性获取请求错误时的响应主体如表24所示。

表24属性获取请求的错误响应主体

项目名称	参数名称	数据类型	必需	内容
错误代码	错误	字符串	O	错误代码
错误内容	error_description	字符串	O	错误的详细说明

属性获取请求的代表性错误代码如表25所示。

表25属性获取请求的典型错误代码

HTTP状态	错误代码	说明
400	invalid_request	无访问令牌
401	invalid_token	访问令牌错误、过期、无效
403	干扰信号	访问权限不足

8.API中出现错误时的响应列表

以下详细描述了在为写入注册符号信息等提供的API中发生错误时返回的错误响应。

（1）每个API通用的错误响应

各API中共同发生的错误及其响应的详细情况如下所示。

①访问令牌验证错误时

当发生访问令牌验证错误时，返回表26所示的响应主体。

表26访问令牌验证错误时的响应主体

项目名称	参数名称	数据类型	必需	内容
错误	消息	字符串	_	错误内容

访问令牌验证错误发生时的错误响应如表27所示。

表27访问令牌验证错误时的错误响应

HTTP状态	错误	说明
401	Unauthorized	无访问令牌
403	Forbidden	访问令牌验证NG
500	内部服务器错误	访问令牌验证失败（异常终止）

②处理逻辑错误时

当处理逻辑发生错误时，返回表28所示的响应代码和表29所示的响应主体。各API共同发生的错误代码如表30所示。在单独的API定义中描述了在每个API中单独出现的错误代码。

表28处理逻辑错误响应代码

HTTP状态	意义	内容
400	请求参数错误	处理失败（参数错误）
500	API中的系统错误	意外的系统错误

表29处理逻辑错误响应主体

项目名称	参数名称	数据类型	必需	内容
错误代码	errorCode	字符串	○	错误代码
错误	errorMessage	字符串	○	错误的详细说明

表30处理逻辑错误时的API常见错误代码

HTTP状态	错误代码	错误	说明
400	E4000001	A system error has occurred.发生系统错误。	参数错误（json透视错误）
500	E5000002	A system error has occurred.发生系统错误。	API处理内部的系统错误（如DB连接错误）

③注册系统维护时

注册系统处于系统维护中时，返回表31所示的响应主体和表32所示的错误响应。

表31系统维护响应主体

项目名称	参数名称	数据类型	必需	内容
错误代码	errorCode	字符串	○	错误代码
错误	errorMessage	字符串	○	错误的详细说明

表32系统维护期间的错误响应

HTTP状态	错误代码	错误	说明
503	E5030001	无	注册系统维护期间调用API

（2）每个API的错误响应

各API中个别发生的错误及其响应的详细情况如下所示。

①所有机体信息一览表获取API

在所有机体信息一览获取API的处理逻辑中发生的API个别错误代码如表33所示。

表33所有机身信息列表获取API中的单个错误代码

HTTP状态	错误代码	错误	说明
400	E4000101	A system error has occurred.发生系统错误。	无法从访问令牌获取用户ID

②自有机体信息获取API

在所有机体信息获取API的处理逻辑中发生的API个别错误代码如表34所示。

表34所有机身信息列表获取API中的单个错误代码

HTTP状态	错误代码	错误	说明
400	E4000201	A system error has occurred.发生系统错误。	无法从访问令牌获取用户ID
400	E4000202	A system error has occurred.发生系统错误。	参数检查错误（必填符号，12位）

③获取加密密钥信息等API

加密密钥信息等获取API的处理逻辑中发生的API个别错误代码如表35所示。

表35获取加密密钥信息API的单个错误代码

HTTP状态	错误代码	错误	说明
400	E4000301	A system error has occurred.发生系统错误。	无法从访问令牌获取用户ID
400	E4000302	A system error has occurred.发生系统错误。	参数检查错误（必填符号，12位）
400	E4000303	A system error has occurred.发生系统错误。	参数检查错误（加密密钥重新创建标志（必需，值域））
500	E5000301	A system error has occurred.发生系统错误。	对没有申请权限的机体调用API
500	E5000302	A system error has occurred.发生系统错误。	对未注册RID的机体调用API

④远程ID注册结果存储API

远程ID登录结果存储API的处理逻辑中发生的API个别错误代码如表36所示。

表36远程ID注册结果存储API中的单个错误代码

HTTP 状态	错误代码	错误	说明
400	E4000401	A system error has occurred.发生系统错误。	无法从访问令牌获取用户ID
400	E4000402	A system error has occurred.发生系统错误。	参数检查错误（必填符号，12位）
400	E4000403	A system error has occurred.发生系统错误。	参数检查错误（写入标志（必需，值域））
500	E5000401	A system error has occurred.发生系统错误。	对没有申请权限的机体调用API
500	E5000402	A system error has occurred.发生系统错误。	对未注册RID的机体调用API
500	E5000403	A system error has occurred.发生系统错误。	多个机体对同一RID机器等进行RID写入时

9.验证认证请求的注意事项

（1）state验证

state的验证如下实施。如表37所示。

表37 state验证方法

否	验证方法
1	在用户授权响应中获取的state值必须与在请求中发送的值相同。

（2）ID令牌验证

id_token是JSON Web Token JSON Web Token(JWT)格式，以“.”（句点）分隔，分为标题部分、有效载荷部分和签名部分。nonce包括在有效载荷部分中。

标题部、有效载荷部用Base64编码，设定如表38所示的值。

※记载了id_token验证中使用的主要内容。实际上还包含其他值。

表38用于验证ID令牌的关键参数

分类	参数名称	验证方法
标题部分	alg	用于对id_token签名的散列算法。
有效载荷部分	iss	id_token的发布者。 “https：//［注册系统的成为FQDN]/auth/realms/drs’。
	aud	id_token的接收人。 设置RP的client_id。
	exp	id_token的到期时间。 UNIX时间（自UTC 1970/1/1 00:00:00以来的秒数）。
	iat	id_token的到期时间。 UNIX时间（自UTC 1970/1/1 00:00:00以来的秒数）。
	auth_time	验证用户的时间。 UNIX时间（自UTC 1970/1/1 00:00:00以来的秒数）。

ID令牌的验证是如表39所示的执行。

表39如何验证ID令牌

否	验证方法
1	验证iss（id_token的发布者）的值是否与https：//[注册系统的FQDN]/auth/realms/drs匹配。
2	验证aud（id_token收件人）的值是否与在验证请求中发送的client_id相匹配。
3	验证exp（id_token到期时间）是否晚于当前时间。
4	验证iat（id_token发布时间）是否早于当前时间且不太旧。 ※允许多老的id_token，由RP方判断。
5	确保auth_time（用户验证的时间）早于当前时间，但不太早。 ※允许多长时间的老用户的认证时刻，由RP方来判断。

（附件3）

年月日

自我检验结果，型式情报等申请书，

国土交通省航空局部长官房参赞（下一代航空移动）先生

通过对远程ID设备的自我验证，我们确认其符合远程ID技术标准，现将其报告如下。

通知人（公司名称）：
代表职务和姓名：
联系人职务和姓名：
地址：
电话：
电子邮件地址：

制造商名称	
类型名称	
内部/外部区别	☐内置型（与无人驾驶飞机一体） ☐外置（独立于无人驾驶航空器）
通信方式	☐蓝牙5.x长范围 ☐Wi-Fi感知（加权感知） ☐Wi-Fi Beacon
尺寸（总长度x总宽度x总高度）	
重量	
外观照片	

1.如果开发制造了厂商APP，应在型号名称栏中填写该名称。尺寸、重量和外观照片不需要。

2.内置型的，型号、尺寸、重量应填写无人驾驶航空器的；

3.提交并附经验证符合远程ID技术标准的文件；

（附件4

）年月日

远程身份公钥应用验证码通知申请表

国土交通省航空局部长官房参赞（下一代航空移动）先生

在确认远程ID技术标准后，我们申请通知电子签名公钥和应用验证码，以开发和制造远程ID设备和制造商应用程序。

通知人（公司名称）：
代表职务和姓名：
联系人职务和姓名：
地址：
电话：
电子邮件地址：

开发制造的东西	□远程ID设备等 □内置型（与无人驾驶飞机一体） □外置（独立于无人驾驶航空器） □厂商应用程序
远程ID设备等的通信方法	□蓝牙5.x长范围 □Wi-Fi感知（加权感知） □Wi-Fi Beacon
预计开发时间	岁月
预计开发完成时间	岁月
（对于制造商应用程序，请提供以下OpenIDConnect信息※ ）	
登录后重定向URL	
访问源IP地址	

※对于制造商应用程序的制造者，在与登录系统连接时的OpenID Connect认证中，将必要的客户端ID一并通知。