TTA Standard

정보통신단체표준(국문표준)

TTAx.xx-xx.xxxx 제정일: 2018년 xx월 xx일

# 드론 기반 서비스를 위한 보안 능력

# Security Capabilities for Drone-based Services

한국정보통신기술협회
Telecommunications Technology Association

**표준초안 검토 위원회** 응용보안 및 평가인증 프로젝트그룹(PG504)

**표준안 심의 위원회** 정보보호기술위원회(TC5)

| | 성명 | 소 속 | 직위 | 위원회 및 직위 | 표준번호 |
|---|---|---|---|---|---|
| **표준(과제) 제안** | 강유성 | 한국전자통신연구원 | 책임연구원 | PG504 위원 | |
| **표준 초안 작성자** | 강유성 | 한국전자통신연구원 | 책임연구원 | PG504 위원 | |
| | 김주한 | 한국전자통신연구원 | 책임연구원 | | |
| | 김건우 | 한국전자통신연구원 | 책임연구원 | | |
| | 김태성 | 한국전자통신연구원 | 책임연구원 | | |
| | 이승광 | 한국전자통신연구원 | 선임연구원 | | |
| **사무국 담당** | 김재웅 | TTA | 단장 | | |
| | 문서연 | TTA | 전임 | | |



본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.

본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2018.12

# 서 문

## 1 표준의 목적

이 표준의 목적은 드론 기반 서비스 프레임워크를 구성하는 구성요소 사이의 데이터 보호를 위한 보안 메시지 흐름과 관련된 보안 능력을 정의하는 것이다.

## 2 주요 내용 요약

이 표준에서는 드론 기반 서비스에서 드론을 중심으로 한 데이터 통신 환경을 고려하여 데이터 기밀성, 구성요소간 인증, 통신정보 부인방지, 메시지 무결성 등의 보안 서비스를 제공하는 보안 메시지 흐름과 관련된 보안 능력을 정의한다. 특히 보안 메시지 흐름을 구체적으로 정의하며, 이 표준에서 정의한 보안 메시지 흐름은 보안 프로토콜로 구현되는 토대가 된다.

## 3 인용 표준과의 비교

### 3.1 인용 표준과의 관련성

해당사항 없음

### 3.2 인용 표준과 본 표준의 비교표

해당사항 없음

# Preface

## 1 Purpose

The standard defines security capabilities related to security message flow in order to protect communication data among service components consisting of drone-based services.

## 2 Summary

The security capabilities defined in this standard provides security services such as data confidentiality, mutual authentication, non-repudiation, and message integrity for drone-based services. In particular, this standard explains the security message flow among service components in detail. The security message flow becomes the basis of the security protocol for drone-based services.

## 3 Relationship to Reference Standards

Not applicable

# 목 차

# 드론 기반 서비스를 위한 보안 능력
# (Security Capabilities for Drone-based Services)

## 1 적용 범위

이 표준이 다루는 범위는 드론 기반 서비스 프레임워크 구성요소에 기반한 서비스 제공 시 드론과 구성요소 사이의 통신 메시지 흐름 및 보안 동작과 관련된 보안 능력(Security Capabilities)이다. 이 표준에서 정의한 보안 메시지 흐름과 관련된 보안 능력은 보안 프로콜로 실현될 수 있으며, 드론과 구성요소 간 메시지 무결성, 메시지 인증, 부인 방지 등의 보안 서비스를 제공할 수 있다.

드론 기반 서비스 프레임워크를 구성하는 구성요소 중 서비스 요청자, 서비스 제공기관 및 지상 제어 장치 간 보안 채널 구성은 이 표준에서 고려하지 않는다. 즉 서비스 요청자, 서비스 제공기관 및 지상 제어 장치에서의 키 생성, 키 분배 및 보안 파라미터 관리와 관련된 구현 방법은 이 표준에서 고려하지 않는다.

이 표준은 드론 기반 서비스 환경에 대한 안전성과 신뢰성을 향상시켜 드론 기반 서비스 시장 활성화에 적용될 수 있다.

## 2 인용 표준

해당사항 없음

## 3 용어 정의

### 3.1 드론 (Drone)

조종사가 탑승하지 않고 무선전파 유도에 의해 비행 및 조종이 가능한 비행기나 헬리콥터 모양의 항공기
주) 국내 항공법에서는 연료를 제외한 자체 중량이 150kg 이하인 것은 ‘무인비행장치’로, 150kg을 초과하는 것은 ‘무인항공기’로 규정함

### 3.2 디지털 택배함 (Digital Strongbox)

물품이 배달되는 지점에 위치한 통신장치
주) 무인 배달서비스에서는 디지털 택배함이 무인 배달장치와 통신하여 배달 완료 여부를 확인함

### 3.3 무인 감시서비스 (Unmanned surveillance service)
사람이 직접 현장에 가지 않고 특정 지역 또는 특정 사건에 대해 무인이동체를 통해 수집한 정보를 이용하는 감시 서비스
주) 예를 들면 감시정찰용 드론을 통해 영상 정보 또는 센싱 정보를 수집하여 감시하는 서비스임.

### 3.4 무인 배달서비스 (Unmanned delivery service)
배달물품을 사람이 직접 전달하지 않고 무인이동체를 통해 전달하는 배달서비스
주) 예를 들면 배달용 드론이 책 또는 의약품 등을 배달하는 서비스임

### 3.5 무인 배달장치 (Unmanned delivery device)
사람이 직접 탑승하지 않고 원격으로 제어되거나 또는 사전 프로그래밍된 정보에 따라 배달지점을 찾아가서 물품을 배달하는 장치
주) 최초에 출발한 지점으로 되돌아오는 기능을 포함하기도 함. 본 표준의 드론이 대표적인 무인 배달장치 중 하나임.

### 3.6 무인이동체 (Unmanned Vehicle)
사람이 탑승하지 않는 이동수단
주) 드론, 자율주행차, 무인잠수정 등 사람이 타지 않고 원격제어 또는 미리 입력된 명령에 따라 임무를 수행함

### 3.7 지상 제어 장치 (GCS, Ground Control System)
드론과 통신하여 임무를 부여하고 제어하는 장치
주) 드론의 출발/도착 및 배달 과정에서도 통신이 가능함

**[출처(3.1~3.7)]** TTAK.KO-12.0317 (2017), 드론 기반 서비스를 위한 보안 요구사항

### 3.8 보안 능력 (Security Capabilities) **[출처]** 한국정보통신기술협회 정보통신용어사전
정보의 침해로부터 시스템을 보호하기 위해 사용되는 각종 대책 및 솔루션
주) 이 표준에서는 드론 기반 서비스를 위한 보안 프로토콜로 구현될 수 있는 보안 메시지 흐름을 포함함

### 3.9 화이트박스 암호 (White-Box Cryptography)
공격자가 암호 연산과정 및 암호키가 저장된 메모리에 접근 가능한 높은 공격력을 가지고 있는 경우에도 암호키 누출을 방지할 수 있는 키 은닉 암호

## 4 약어

GCS Ground Control System
IP Information Provider
SC Service Client
SP Service Provider

## 5 드론 기반 서비스를 위한 보안 능력

### 5.1 드론 기반 서비스

드론 기반 서비스는 드론을 이용하여 제공할 수 있는 다양한 서비스를 모두 포함한다. 대표적인 서비스는 드론 기반 무인 감시서비스와 드론 기반 무인 배달서비스가 있다.

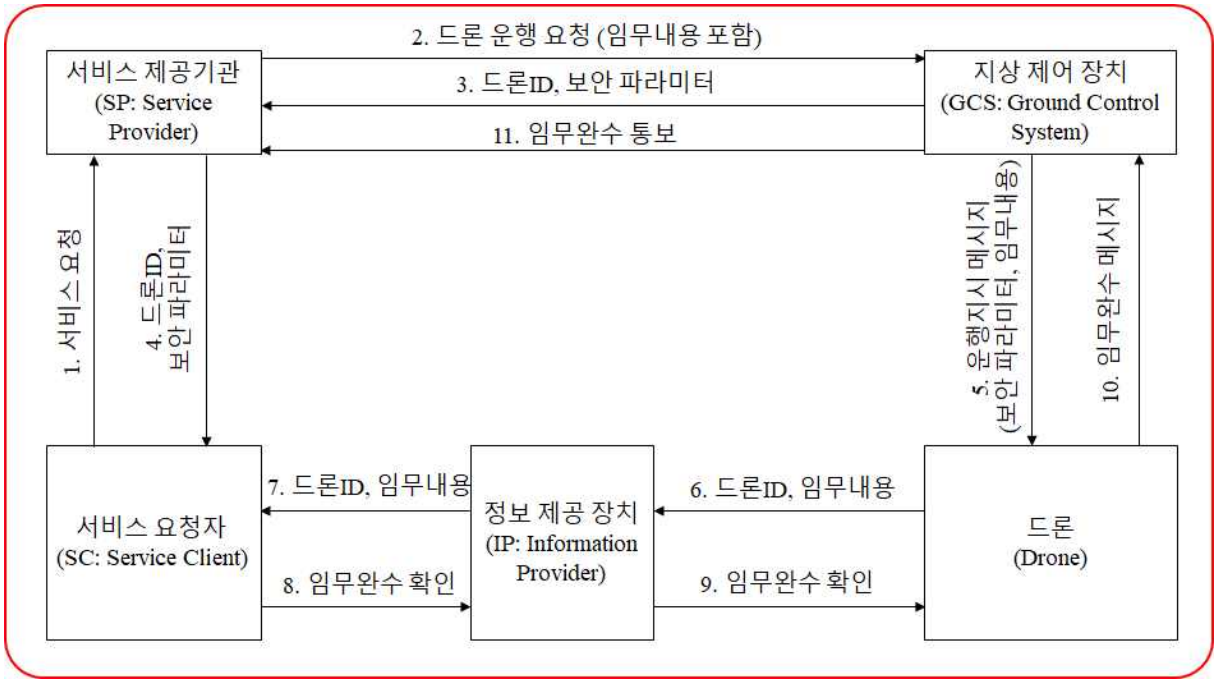
드론 기반 무인 감시서비스는 사람이 직접 현장에 가지 않고 특정 지역 또는 특정 사건에 대해 감시정찰용 드론을 통해 영상 정보 또는 센싱 정보를 수집하여 감시하는 서비스이고, 드론 기반 무인 배달서비스는 배달물품(예를 들어, 책 또는 긴급의약품 등)을 사람이 직접 전달하지 않고 배달용 드론을 통해 전달하는 서비스이다. 이 외에도 드론이 통신 중계기 역할을 하여 통신영역을 확장하는 드론 기반 통신중계 서비스도 가능하다.

이 표준은 대표적인 서비스인 무인 감시서비스와 무인 배달서비스에서의 임무완수를 위한 메시지 흐름과 관련된 보안 능력을 대상으로 한다.

### 5.2 구성요소 및 메시지 흐름

다음에 보이는 (그림 5-1)은 이 표준에서 정의하는 드론 기반 서비스 제공을 위한 구성요소들 사이의 메시지 흐름도이다. 이 표준에서 고려하는 드론 기반 서비스를 위한 시스템 구성요소는 TTAK.KO-12.0317 (2017) “드론 기반 서비스를 위한 보안 요구사항”에 정의되어 있으며, 이 표준에서는 이를 준수한다. 그러나 이 표준에서는 TTAK.KO-12.0317 (2017) “드론 기반 서비스를 위한 보안 요구사항”에서 정의한 시스템 구성요소 중 구역 관리 장치는 고려하지 않는다. 따라서 (그림 5-1)과 같이 5개의 구성요소에서의 11개의 메시지 흐름을 정의한다.

이 표준에서는 서비스 요청자와 서비스 제공기관 사이의 통신, 서비스 제공기관과 지상 제어 장치 사이의 통신, 지상 제어 장치와 드론 사이의 통신 및 서비스 요청자와 정보 제공 장치 사이의 통신은 안전한 채널이 형성되어 있다고 가정한다. 메시지 흐름 및 각 메시지 보호를 위한 보안 기능은 다음과 같으며, 여기서 정의되는 단계별 일련번호는 (그림 5-1)의 일련번호와 동일하다.




(그림 5-1) 드론 기반 서비스 메시지 흐름도

1) 서비스 요청자는 서비스 제공기관에게 서비스를 요청하는 메시지를 보낸다. 예를 들면, 드론 기반 무인 배달서비스의 경우는 물품 값을 결제하고 물품 배송을 요청하는 개인 고객의 메시지이고, 드론 기반 무인 감시서비스의 경우는 특정 지역 또는 특정 사건의 영상 정보나 센싱 정보를 요청하는 감시자(지방자치단체, 경찰, 소방당국, 경비업체 등)의 메시지이다.
2) 서비스 제공기관은 지상 제어 장치에게 드론 운행을 요청하는 메시지를 보낸다. 이 메시지는 임무내용 및 기타 필요한 정보를 포함한다. 예를 들면, 드론 기반 무인 배달 서비스의 경우는 배송지 주소, 물품 정보 등을 포함할 수 있고, 드론 기반 무인 감시 서비스의 경우는 감시대상 지역 등을 지정할 수 있다.
3) 지상 제어 장치는 서비스 제공기관에게 임무를 수행할 드론에 대한 정보와 보안 파라미터를 회신한다. 드론 기반 서비스 종류에 상관없이 동일한 메시지가 전달된다.
4) 서비스 제공기관은 서비스 요청자에게 단계 3)에서 수신한 정보를 전달한다. 서비스 요청자는 수신된 정보를 사용하여 보안 기능을 수행한다.
5) 지상 제어 장치는 드론에게 운행지시 메시지를 보낸다. 이 메시지에는 임무내용, 보안 파라미터 및 기타 필요한 정보 등이 포함된다. 임무내용과 기타 필요한 정보 등은 드론이 직접 복호화하여 판단할 수도 있고 또는 서비스 요청자만 복호화할 수 있도록 암호화하여 전달할 수도 있다.
6) 드론은 비행 중에 만나는 정보 제공 장치에게 드론 자신의 아이디, 임무내용 및 기타 필요한 정보를 전달한다. 정보 제공 장치는 드론 기반 무인 배달서비스의 경우 드론이 운반해 온 물품을 받았다는 확인을 해 주는 장치로 서비스 요청자의 관리하에 있는 디지털 택배함에 해당하고, 드론 기반 무인 감시서비스에서는 감시대상 영역에서

센싱 정보를 보내거나 무인감시 서비스 상황을 확인시켜 주는 장치에 해당한다.

7) 정보 제공 장치는 서비스 요청자에게 단계 6)에서 수신한 정보를 전달한다. 서비스 요청자는 단계 4)에서 수신한 정보와 보안 파라미터를 사용하여 임무수행 중인 드론을 확인하고 보안 기능을 수행한다. 이 단계에서 서비스 요청자는 드론을 이용한 서비스가 정상적으로 제공되었는지 판단할 수 있다.
8) 서비스 요청자는 정보 제공 장치에게 드론 기반 서비스 제공 성공/실패 메시지를 전달한다.
9) 정보 제공 장치는 드론에게 단계 8)에서 수신한 메시지를 전달한다.
10) 드론은 최초 운행을 지시했던 지상 제어 장치로 돌아와서 지상 제어 장치에게 단계 9)에서 수신한 메시지을 전달한다.
11) 지상 제어 장치는 서비스 제공 성공/실패 여부를 확인하고 서비스 제공기관에게 임무완수 여부를 통보한다. 서비스 제공기관이 서비스 요청자로부터 최초 서비스 요청을 수신하여 서비스 개시 후에 최종적으로 지상 제어 장치로부터 서비스 제공이 완료되었음을 수신하는 것으로 드론 기반 서비스의 시작과 끝이 된다.

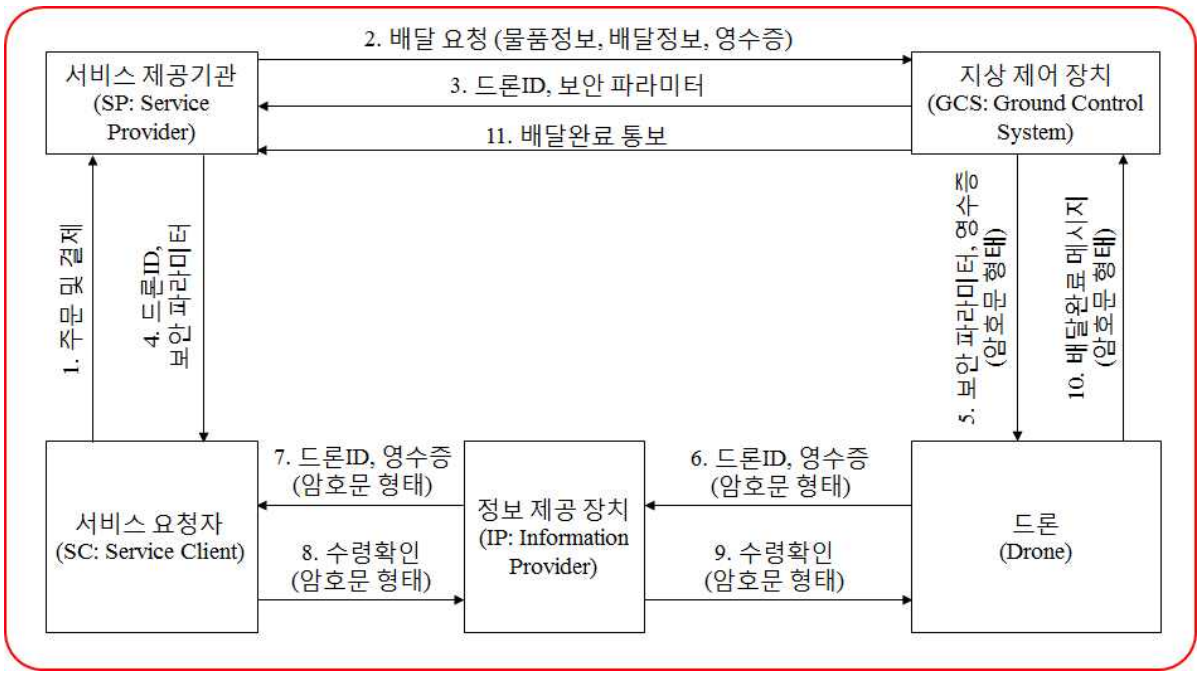
# 부 록 Ⅰ

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

# 드론 기반 서비스를 위한 보안 능력의 보안 프로토콜 적용 예

## Ⅰ.1 드론 기반 무인 배달서비스용 보안 프로토콜

드론 기반 무인 배달서비스용 보안 프로토콜의 주요 목적은 공격자의 불법 포획을 통해 노출될 수 있는 드론과 디지털 택배함에 저장된 보안키를 보호하는 것이다. 이 부록에서는 서비스 요청자와 서비스 제공기관 사이의 통신, 서비스 제공기관과 지상 제어 장치 사이의 통신, 지상 제어 장치와 드론 사이의 통신 및 서비스 요청자와 정보 제공 장치 사이의 통신은 안전한 채널이 형성되어 있다고 가정한다.




(그림 Ⅰ.1-1) 드론 기반 무인 배달서비스 메시지 흐름도

위에 보이는 (그림 Ⅰ.1-1)은 (그림 5-1)에서 정의한 드론 기반 서비스를 위한 일반적인 메시지 흐름을 드론 기반 무인 배달서비스에 적용한 것이다. 무인 배달서비스에서 각 구성요소는 다음과 같은 기능을 담당한다.

- 서비스 요청자 : 서비스 요청자는 물품을 주문하고 배달서비스를 요청하는 고객(Customer)이다. 물품 주문은 컴퓨터 또는 스마트폰을 이용한 인터넷 주문이며, 디지털 택배함을 통해 물품을 수령한 후에 수령확인 메시지를 보내는 역할을 한다.
- 서비스 제공기관 : 서비스 제공기관은 서비스 요청자의 배달서비스 요청에 따라 배달서비스를 제공하는 물품 판매자(Seller)이다. 배달 요청 정보를 지상 제어 장치에게 전

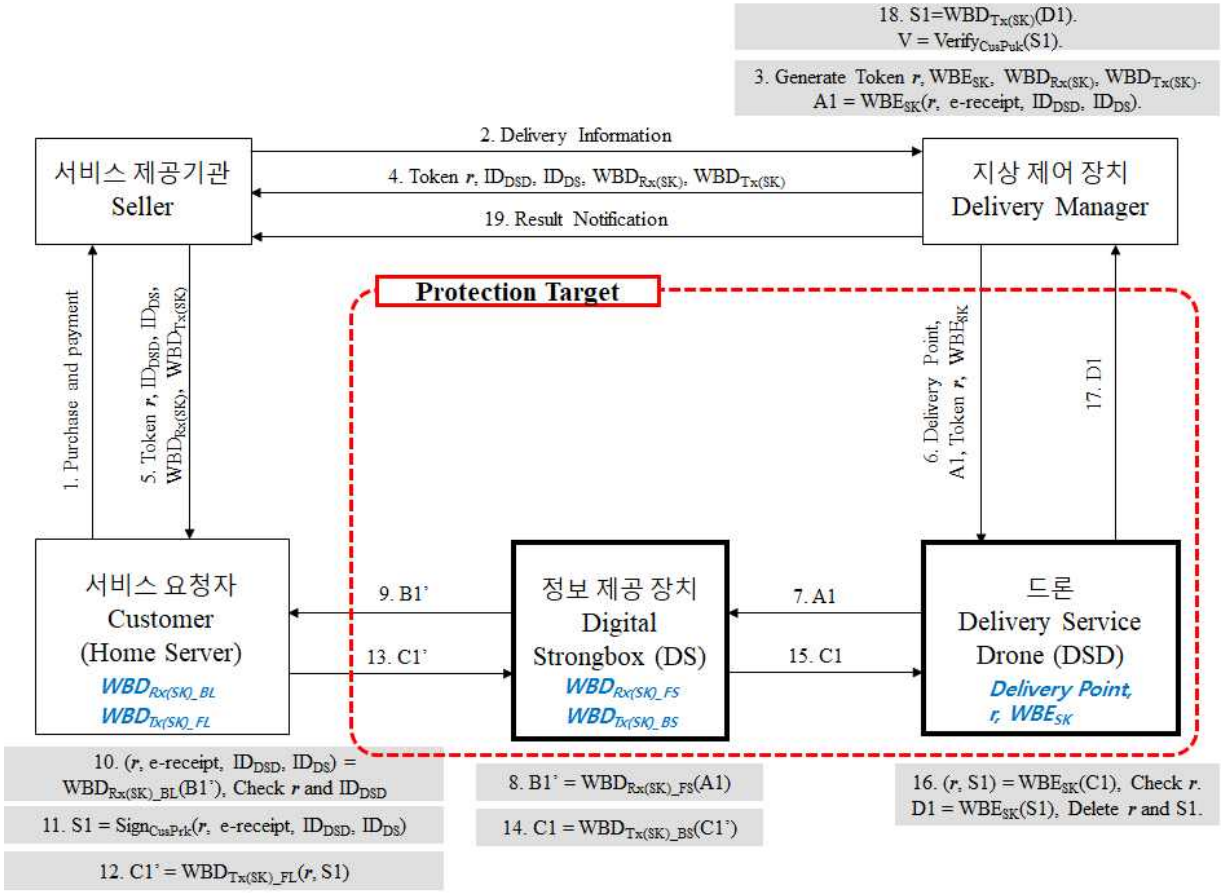
달하며, 최종적으로 지상 제어 장치로부터 배달완료 통보를 수신하는 역할을 한다.

- 지상 제어 장치 : 지상 제어 장치는 드론 운영자로서 드론을 이용한 배달서비스를 관리하는 배달 관리자(Delivery Manager)이다. 배달서비스를 수행하는 드론을 관리하는 주체로서, 서비스 제공기관의 물품 배달부서 또는 배달 전문 대행업체가 보유한 장비이다.
- 드론 : 드론은 배달 임무를 수행하는 배달서비스 드론(Delivery Service Drone)이다. 지상 제어 장치의 명령에 따라 물품을 배달 목적지까지 운반하는 역할을 한다.
- 정보 제공 장치 : 정보 제공 장치는 배달 목적지에 위치하여 드론으로부터 물품을 받는 디지털 택배함(Digital Strongbox)이다. 서비스 요청자가 관리하는 장치이며, 드론으로부터 물품을 수신하고 드론에게 수령확인 메시지를 응답하는 역할을 한다.

다음에 보이는 (그림 I.1-2)는 드론 기반 무인 배달서비스 보안 프로토콜 동작 수행 시 필요한 보안 파라미터의 흐름과 기능을 보다 구체화하여 정의한 것이다. 그리고 다음에 보이는 <표 I.1-1>은 (그림 I.1-2)의 보안 프로토콜에서 사용되는 파라미터를 정의한 것으로 I-2절의 보안 프로토콜 설명에서 참조되는 파라미터이다.

<표 I.1-1> 보안 프로토콜 파라미터

| 기호 | 설명 |
|---|---|
| r | 지상 제어 장치가 생성하는 랜덤 토큰 |
| $ID_{DSD}$ | 드론(Delivery Service Drone) ID |
| $ID_{DS}$ | 정보 제공 장치(Digital Strongbox) ID |
| e-receipt | 서비스 요청자(Customer)에 의해 확인(서명)되어야 하는 전자영수증 |
| $WBE_{SK}$ | 암호키(Secret Key)로부터 유도된 화이트박스 암호화 모듈 |
| $WBE_{SK}(M)$ | 화이트박스 암호화 모듈($WBE_{SK}$)로 메시지(M)를 변화시키는 암호화 연산 동작 |
| $WBD_{Rx(SK)}$ | 정보 제공 장치가 드론으로부터 메시지를 수신할 때 사용하는 암호키(Secret Key)로부터 유도된 화이트박스 복호화 모듈 |
| $WBD_{Tx(SK)}$ | 정보 제공 장치가 드론에게 메시지를 송신할 때 사용하는 암호키(Secret Key)로부터 유도된 화이트박스 복호화 모듈 |
| $WBD_{Rx(SK)\_FS}(M)$ | 화이트박스 복호화 모듈($WBD_{Rx(SK)}$)의 앞쪽 작은 영역($WBD_{Rx(SK)\_FS}$)으로 메시지(M)를 변화시키는 복호화 연산 동작 |
| $WBD_{Rx(SK)\_BL}(M)$ | 화이트박스 복호화 모듈($WBD_{Rx(SK)}$)의 뒤쪽 큰 영역($WBD_{Rx(SK)\_BL}$)으로 메시지(M)를 변화시키는 복호화 연산 동작 |
| $WBD_{Tx(SK)\_FL}(M)$ | 화이트박스 복호화 모듈($WBD_{Tx(SK)}$)의 앞쪽 큰 영역($WBD_{Tx(SK)\_FL}$)으로 메시지(M)를 변화시키는 복호화 연산 동작 |
| $WBD_{Tx(SK)\_BS}(M)$ | 화이트박스 복호화 모듈($WBD_{Tx(SK)}$)의 뒤쪽 작은 영역($WBD_{Tx(SK)\_BS}$)으로 메시지(M)를 변화시키는 복호화 연산 동작 |
| $Sign_{CusPrk}(M)$ | 서비스 요청자 비밀키(private key)로 메시지(M)에 서명하는 연산 동작 |
| $Verify_{CusPuk}(M)$ | 서비스 요청자 공개키(public key)로 메시지(M) 서명을 검증하는 연산 동작 |




(그림 I.1-2) 드론 기반 무인 배달서비스용 보안 프로토콜 동작과 기능

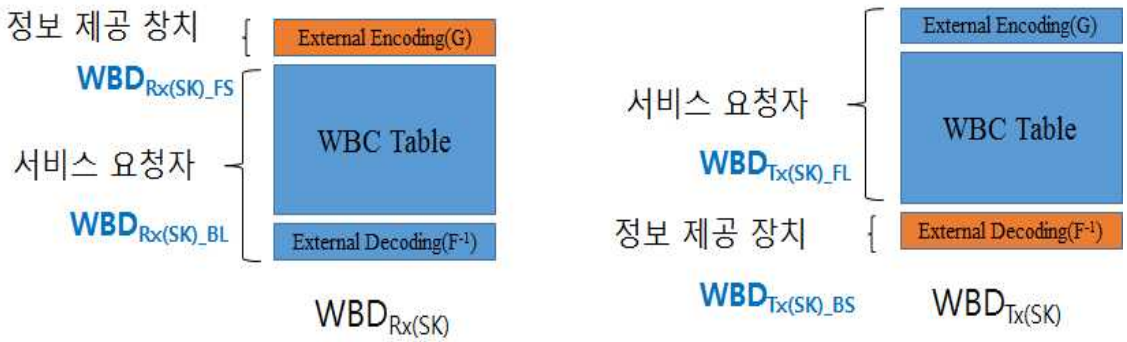
## I.2 보안 프로토콜 동작순서

보안 프로토콜의 동작 순서는 다음과 같으며, 사용된 파라미터는 I.1절의 <표 I.1-1>을 참조한다. 여기서 설명되는 단계별 설명의 일련번호는 (그림 I.1-2)의 일련번호와 동일하다.

1) 서비스 요청자가 물품을 구입하고 배달서비스를 요청한다.
2) 서비스 제공기관은 지상 제어 장치에게 배달정보(예를 들면, 고객 주소, 제품 모델명, 전자영수증 e-receipt 등)을 전달한다.
3) 지상 제어 장치는 토큰 r, $WBE_{SK}$, $WBD_{Rx(SK)}$, 그리고 $WBD_{Tx(SK)}$를 생성한다.[1] 그런 다음, (r, e-receipt, $ID_{DSD}$, $ID_{DS}$)를 $WBE_{SK}$로 암호화하여 암호문 A1을 생성한다. 즉 A1 = $WBE_{SK}$(r, e-receipt, $ID_{DSD}$, $ID_{DS}$) 이다.
4) 지상 제어 장치는 서비스 제공기관에게 (r, $ID_{DSD}$, $ID_{DS}$, $WBD_{Rx(SK)}$, $WBD_{Tx(SK)}$)을 보낸다.

1) 여기서는 WBC-AES128 알고리즘을 디폴트 암호 알고리즘으로 고려한다. 그러나 지상 제어 장치를 포함한 드론 기반 배달서비스 시스템을 운영하는 서비스 사업자는 자체적인 화이트박스 암호 알고리즘을 선정하여 운영할 수 있다.

5) 서비스 제공기관은 서비스 요청자에게 (r, $ID_{DSD}$, $ID_{DS}$, $WBD_{Rx(SK)}$, $WBD_{Tx(SK)}$)을 전달한다.
6) 지상 제어 장치는 드론에게 배달 지점 정보 및 (r, $WBE_{SK}$, A1)을 보낸다.
7) 드론이 배달 목적지로 날아간다. 이때 드론의 비행동안 드론이 저장하고 있는 정보는 배달 지점 정보와 (r, $WBE_{SK}$, A1)이다. 배달 지점에 도착한 드론은 정보 제공 장치(예를 들면, 디지털 택배함)에게 암호문 A1을 보낸다.
8) 정보 제공 장치는 수신된 암호문 A1에 $WBD_{Rx(SK)_FS}$를 적용하여 부분적 복호화된 메시지 B1'을 생성한다. 이를 위해서는 단계 5) 직후에 서비스 요청자와 정보 제공 장치가 다음에 보이는 (그림 I.2-1)과 같이 WBC 복호화 테이블을 서로 나누어 가지고 있어야 한다. 정보 제공 장치가 드론으로부터 수신한 암호문을 복호화하기 위한 WBC 테이블 중 정보 제공 장치가 가지고 있는 복호화 모듈은 $WBD_{Rx(SK)_FS}$이고, 드론에게 보낼 암호문을 암호화하는데 사용할 WBC 테이블 중 정보 제공 장치가 가지고 있는 모듈은 $WBD_{Tx(SK)_BS}$이다. 이에 상응하여 드론으로부터 수신한 암호문을 복호화하기 위한 WBC 테이블 중 서비스 요청자가 가지고 있는 복호화 모듈은 $WBD_{Rx(SK)_BL}$이고, 드론에게 보낼 암호문을 암호화하는데 사용할 WBC 테이블 중 서비스 요청자가 가지고 있는 모듈은 $WBD_{Tx(SK)_FL}$이다. 이렇게 설계된 이유는, WBC 테이블은 순차적으로 적용되어야 하므로 정보 제공 장치보다 서비스 요청자가 항상 더 큰 테이블을 다루게 함으로써 정보 제공 장치가 메모리 사용량이나 연산 속도 부담을 줄이기 위함이다.




(그림 I.2-1) 화이트박스 암호 복호화 테이블의 구분

9) 정보 제공 장치는 부분적 복호화 메시지 B1'을 서비스 요청자에게 보낸다.
10) 서비스 요청자는 부분적 복호화 메시지 B1'에 $WBD_{Rx(SK)_BL}$을 적용하여 (r, e-receipt, $ID_{DSD}$, $ID_{DS}$)을 복원한 후, 복원된 r 및 $ID_{DSD}$를 단계 5)에서 수신한 r과 $ID_{DSD}$와 비교한다. 비교 결과, 일치하지 않는 경우 서비스 요청자는 오류 메시지를 응답하고 모든 절차를 종료한다.
11) 서비스 요청자는 자신의 개인키를 이용하여 복원된 메시지 (r, e-receipt, $ID_{DSD}$, $ID_{DS}$)를 서명하여 서명문 S1을 생성한다.
12) 서비스 요청자는 (r, S1)에 $WBD_{Tx(SK)_FL}$을 적용하여 부분적 암호문 C1'을 생성한다.
13) 서비스 요청자는 부분적 암호문 C1'을 정보 제공 장치에게 보낸다.
14) 정보 제공 장치는 $WBD_{Tx(SK)_BS}$를 적용하여 드론에게 보낼 암호문 C1을 생성한다.

15) 정보 제공 장치는 암호문 C1을 드론에게 보낸다.
16) 드론은 $WBE_{SK}$를 이용하여 암호문 C1을 복호화하여 (r, S1)을 복원한 후, 복원된 r과 드론에 저장되어 있는 r을 비교한다. 비교 결과, 일치하지 않는 경우 드론은 오류 메시지를 응답하고 모든 절차를 종료한 후 지상 제어 장치로 복귀하고, 일치하는 경우 드론은 서명문 S1에 $WBE_{SK}$을 적용하여 암호문 D1을 생성하고 곧바로 r과 S1을 삭제한다. 따라서 드론이 지상 제어 장치에게 복귀하는 동안에는 암호문 D1만 저장하고 있는 상황이 된다.
17) 드론이 지상 제어 장치에게 도착하면 드론은 지상 제어 장치에게 암호문 D1을 보낸다.
18) 지상 제어 장치는 $WBD_{Tx(SK)}$을 이용하여 암호문 D1으로부터 서명문 S1을 복원한 후, 서비스 요청자의 공개키를 이용하여 서명문 S1을 검증한다.
19) 최종적으로, 지상 제어 장치는 서비스 제공기관에게 검증 결과를 전달한다.

# 부 록 II-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

## 지식재산권 확약서 정보

해당 사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

# 부 록 II-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

# 시험인증 관련 사항

## II-2.1 시험인증 대상 여부

해당 사항 없음

## II-2.2 시험표준 제정 현황

해당 사항 없음

# 부 록 II-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

# 본 표준의 연계(family) 표준

## II-3.1 TTAK.KO-12.0317 (2017), 드론 기반 서비스를 위한 보안 요구사항

드론 기반 서비스를 위한 구성요소 및 역할을 정의하고 있으며, 각 구성요소가 가져야 하는 일반적 보안 요구사항과 각 구성요소 간 인터페이스에서의 보안 요구사항을 정의한 표준임.

## II-3.2 연계 표준 관계

이 표준(드론 기반 서비스를 위한 보안 능력)은 TTAK.KO-12.0317 “드론 기반 서비스를 위한 보안 요구사항”에서 정의된 시스템 구성요소 및 보안 요구사항을 고려하여 드론 기반 서비스에서의 드론 내부 키 은닉, 구성요소 간 통신 데이터 보호, 인증 등을 제공할 수 있는 보안 메시지 흐름과 관련된 보안 능력을 정의한 표준임. 이 표준에서 정의한 보안 메시지 흐름과 관련된 보안 능력은 보안 프로콜로 실현되어 보안 서비스를 제공할 수 있음.

# 부 록 II-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

# 참고 문헌

[1] Seung-Hyun Seo, Jongho Won, Elisa Bertino, Yousung Kang, Dooho Choi "A Security Framework for a Drone Delivery Service", DroNet 2016 - 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use, held with ACM Mobisys'16

# 부 록 II-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

## 영문표준 해설서

해당 사항 없음

# 부 록 II-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

## 표준의 이력

| 판수 | 채택일 | 표준번호 | 내용 | 담당 위원회 |
|---|---|---|---|---|
| 제1판 | 2018.12. | 제정<br>TTAx.xx-xx.xxxx | 드론 기반 서비스를 위한<br>보안 능력 | PG504 |