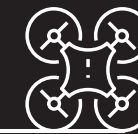




SSenStone

차세대 인증 보안 LAB, 센스톤  
최고의 인증 보안 서비스를 제공합니다. 지금 문의하세요.

# OTAC DRONE SOLUTIONS






# DRONE Solutions

Remoted Controlled Mobility

드론으로 인해 발생할 수 있는 다양한 위험을 해결하며, 드론의 보안 수준을 업그레이드할 수 있는 솔루션을 제공합니다.

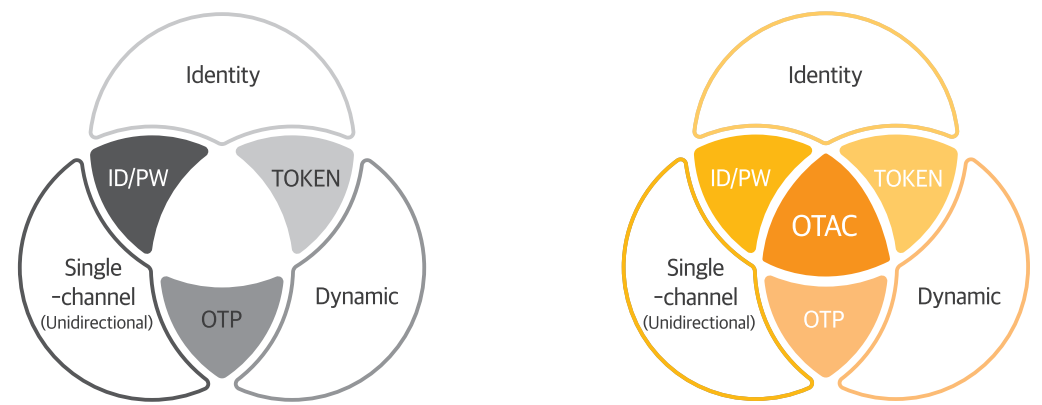
## Challenges

드론은 폭넓은 산업 분야로 확장되고 있으며, 나날이 성장 속도 또한 빨라지고 있습니다. 그러나 드론의 활용도가 높아짐에 따라 실시간 동영상 및 사진 촬영으로 인한 사생활 침해, 각종 충돌 및 폭발 등의 사고, 설계상의 보안 취약성으로 인한 다양한 해킹 위험 또한 높아지고 있습니다.

드론 보안 위협(하이재킹)	드론 식별 이슈	드론 관련 규제
 <p>하이재킹은 대표적인 드론 해킹의 방식으로 비행 중인 드론의 조종기능을 빼앗고 불법으로 납치하는 것입니다. 조종기와 드론 간의 통신은 대부분 암호화되어 있으나, 사용되는 코드 정보는 동일하여 하이재킹 공격 등에 타깃이 될 수 있습니다. 이러한 잠재적 위험을 방지하기 위해 드론 솔루션의 보안 및 제어 시스템을 강화해야 할 필요가 있습니다.</p>	 <p>드론은 다른 비행 비행 제트기에 비해 작고 빠르며 상대적으로 탐지가 어렵기 때문에 안전한 비행을 위해서는 유인 및 무인 항공기 여러 대가 비행할 때 각 항공기가 서로를 식별하고 통신하는 것이 필요합니다. 따라서, 드론 식별은 드론 탐지(비행 금지 구역에 침입한 드론 탐지), ID 식별(드론의 고유 정보를 통한 식별), 무력화(물리적인 방식을 통한 불법적인 드론 침입 무력화)에 활용될 수 있는 중요한 이슈입니다.</p>	 <p>드론 시장이 군정부용뿐만 아니라, 산업용과 소비자용 등 민간분야까지 폭발적으로 성장함에 따라 정부에서는 드론을 안전하고 유용하게 운영하는 방법에 대한 지침을 제공하기 시작했습니다. 국토교통부의 '드론 활용의 촉진 및 기반 조성에 관한 법률(드론법)'이나, 과기정통부에서 발표한 민간분야 '드론 사이버 보안 가이드' 등 드론 운영과 관련된 규제들을 준수하는 것은 필수적입니다.</p>

## Why OTAC?

센스톤의 OTAC 기술은 ID와 비밀번호, 인증코드 생성 RSA 하드웨어 및 소프트웨어, 토큰화(Tokenization) 등 가장 보편적으로 사용되는 3가지 인증 시스템의 장점들을 모두 제공합니다. 개별 시스템들이 제공하는 기능들이 모두 결합되어 있기 때문에 더욱 효율적이고 효과적인 인증 프로세스를 보장합니다.



기존 인증 방식의 한계	단방향 다이내믹 고유식별 인증 코드
<ul style="list-style-type: none"> <li>고정된 식별 값으로 유출·노출에 취약</li> <li>OTP코드 만으로는 사용자 인증 불가능</li> <li>사용자·서버간 양방향 통신 연결 상태에서만 구동(Pull&amp;Push)</li> </ul>	<ul style="list-style-type: none"> <li>동일 그룹내, 중복성 제로의 동적인증코드</li> <li>비통신 단말기에서 동적인증코드 생성</li> <li>단방향 통신만으로 Tokenization 가능(서버부하 감소)</li> </ul>

## Solutions

센스톤은 서버의 도움 없이 사용자나 드론이 생성한 다이내믹 코드를 간단히 인증 서버에 전달하는 것만으로 사용자 및 기기 식별을 지원합니다. 드론의 혁신적인 보안 업그레이드를 위해 드론 제조사 및 시스템 사업자에게 소프트웨어 및 하드웨어 형태로 OTAC 기술을 제공합니다.

