

# OTAC DRONE SOLUTIONS



swIDch is willing to be your Authentication Security Lab

We provide the highest quality authentication security service.

Enquire now.

Next Generation Authentication Security

# **DRONE Solutions**

Remoted Controlled Mobility

The Drone industry is rapidly developing and impacting our daily lives in numerous and innovative ways. However, with this innovation comes the potential negative impact of security breaches and exploitation from external rogue sources.



# **%** Challenges

As it stands, there are the 3 main challenges that the drone industry and/or drone market is facing today.

# Security: Hijacking



Drone communications with remote controllers are often encrypted, but the encrypted codes are often the same (i.e. static), which makes it a preferred and easy target for hijacking. In military drones, extra hardware, CMVP (Cryptographic Module Validation Program) is installed in drones to validate the security level in communications. Small commercial drones on the other hand often rely on the existing encrypted communication methods which are relatively easy to hijack.



Drones are small, fast, and relatively difficult to detect in comparison to a flying jet. When multiple aircrafts, both manned and unmanned, are flying, each device needs to identify and communicate with each other to guarantee safety and mission success. This is why there is need for an identification system for drones and its operators. The economic cost of an unidentified drone near an airport is 500.000 euros for every 30 mins an airport is stopped from operating.

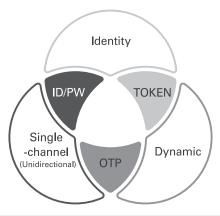
# **Regulation: Compliance**



Remote ID is a new regulation introduced by the FAA and it is the "ability of a drone in flight to provide identification and location information that can be received by other parties", such as law enforcement. To comply with this upcoming regulation, drone manufacturers are having to implement a solution to embed identification capabilities on drones in accordance with the standards given by the FAA. The drone pilots/operators must also register themselves with the FAA before they can legally fly the drones.

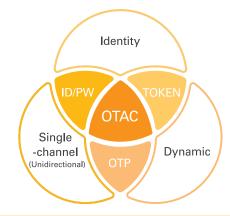
# Why OTAC?

swIDch's OTAC technology provides all the advantages of the three most commonly used authentication systems: ID and password, RSA hardware and software for generating authentication codes, and tokenisation. The functions provided by the individual systems are all combined in OTAC, ensuring a more efficient and effective authentication process.



# Limitations of Existing Authentication Methods

- Vulnerable to leakage/exposure by Static value
- User authentication is impossible with OTP only
- Communication required between User and server (Pull & Push)

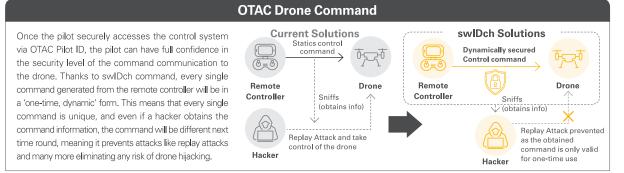


# One-way Unique Identification Authentication Code

- · No need to communicate with Server
- Real-Time changes every time for Secure authentication
- · Non-reusable One-Time Authentication

# Solutions

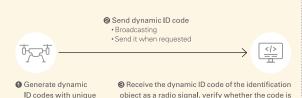
swIDch upgrades Drone solutions by preventing the use of static information and providing single-channeled dynamic codes to eliminate external threats. OTAC technology, which can be applied to both the software and hardware, maintains and enhances the robust security environment level required for Drone manufacturers and system operators.



## **OTAC Drone Authentication**

### OTAC IFF

Identification friend or foe (IFF) is an identification system designed for command and control. It sends an encrypted signal to determine whether it is a friend or a foe by the return signal, but commands can be stolen and misused. OTAC, a real-time dynamic ID code generated in the off-the-network environment, can identify friends whilst preventing theft and misuse of ID codes by the enemy.



generated in real time, and search for the unique

value of the identification object

### OTAC Authentication for CMVP

OTAC can be used to protect communication encryption modules that have received CMVP certification and to authenticate key value updates. It provides an improved security environment by using dynamic codes for the identification and verification process of the drone accessed to download the new keys.

 Verifying and identifying Drone using OTAC before updating cryptographic key Kev Verification





OTAC-based device authentication in case of encryption key leakage

# **OTAC Pilot Access Management**

# OTAC Pilot ID

values built-in the drone

OTAC ensures that licensed pilots are provided with the highest level of security when accessing drone remote systems. Pilots can use swIDch's mobile app or display card to authenticate themselves and securely access drone control systems.

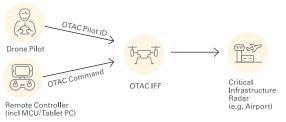


OTAC Pilot ID with a dynamic code, regardless of the cellular networks status of where the drone is used

<u>**Drone Controller**</u> can independently verify OTAC Pilot ID, which is a real-time dynamic code received in one dir

# OTAC Pilot ID&IFF

OTAC converts all commands among the pilot, the controller and the drone into a one-time dynamic code to enable safe communication. If there is a security issue with the pilot, controller, or drone, you can immediately re-evaluate the status of the drone and register it as an enemy drone and take actions.



# **OTAC Drone FDR**

FDR (Flight Data Recorder) is a black box for drones: it monitors and tracks any events during the drone flight and missions. The tracking device has a very weak specification on forgery and alteration of data which further leads to be used in wrong deeds. Controller OTAC FDR will be operated at the monitoring and tracking level on the system and will generate dynamic codes to hide the sensitive data as for enhancing the information security environment.

