



OTAC



One-Time Authentication Code

swidch

swIDch is willing to be your Authentication Security Lab
We provide the highest quality authentication security service.
Enquire now.

OTAC

One-way Dynamic Unique Identification Authentication Code

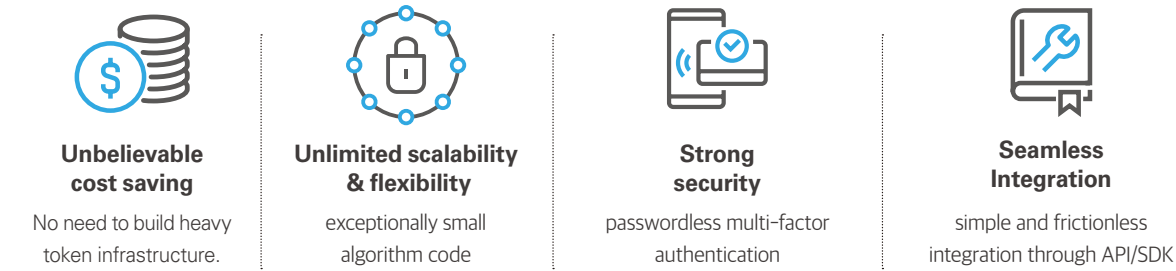
Challenges

A cyber-attack takes place somewhere around the world once every 39 seconds. As a result, there were 8 billion pieces of sensitive personal information being leaked to the market in 2019. These all cost the global economy a staggering \$2.9M every minute in 2020. But WHY does this happen?

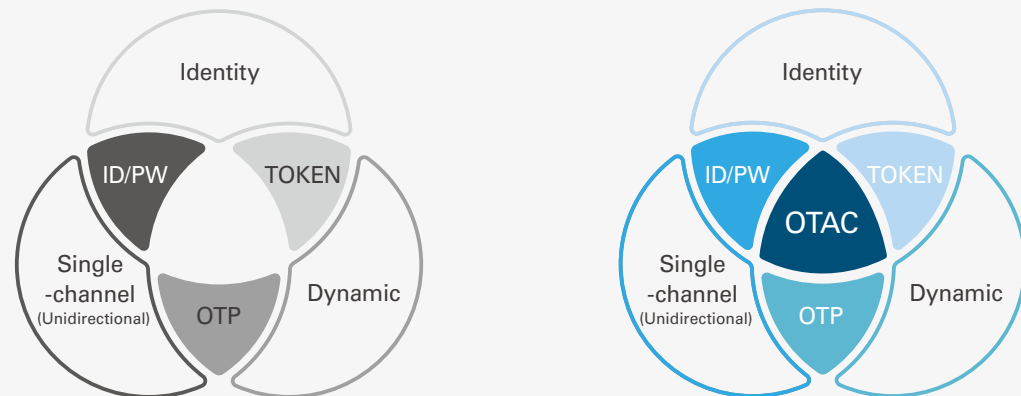


Solutions

Based on the world's first one-way dynamic authentication technology, swIDch's OTAC technology combines advantages of the three most common authentication systems – user ID/passwords, RSA hardware software for generating authentication codes, and tokenisation. This provides a solution that is more efficient and more effective than any of these elements individually.



OTAC's Concept: a new paradigm of identification and authentication between users and devices



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

Why OTAC?

Proposing a new paradigm of identification and authentication between users and devices, OTAC transcends the limitations of existing authentication technology and provides a whole new authentication experience. Even in an environment with no network connection, we can supply single-use, non-reusable, dynamic codes that can identify and authenticate between users and devices.

| Technology | Overcoming breach of information and illegal reuse issues | User Identification by code only | Single channel network environment (additional network communication not required) | Chances of duplication with other users 0% |
|------------------|---|----------------------------------|--|--|
| OTAC | ✓ | ✓ | ✓ | ✓ |
| ID & Password | X | ✓ | ✓ | ✓ |
| OTP | ✓ | X | ✓ | X |
| SMS | ✓ | X | X | X |
| ARS | ✓ | X | X | X |
| Token | ✓ | ✓ | X | X |
| FIDO(Biometrics) | △ | ✓ | X | ✓ |

Use Case

swIDch's OTAC provides one-way, dynamic user-user, device-device, and user-device identification and authentication in an algorithm as a service (AaaS), supporting the development of innovative products and services embedded with robust authentication security.

Payment



OTAC technology provides a security solution to eliminate card-not-present (CNP) fraud by generating and verifying dynamic card numbers. These numbers are made without a network connection and do not duplicate with other users.

ICAM & Enterprise



OTAC technology guarantees convenient and secure internal network access when working remotely. Smartphone or employee cards that are unconnected to the internal network can generate dynamic OTAC verification codes. Employees can then input these codes to gain access. With OTAC technology, there is no longer any need to manage frequent PW changes

Connected Car



Unlike existing digital keys limited by the vehicle's network restrictions, OTAC technology improves the user experience by allowing control of the vehicle with one-way dynamic codes sent from a smartphone, regardless of network connection status.

IoT



Applying OTAC to the communication protocols of network-connected devices and remote modules ensures authentication processes perform more securely and accurately.

M2M



Meeting the needs of the Industry 4.0 era, OTAC technology strengthens authentication security between devices and provides an authentication environment unrestricted by shadow zones and communication delays.

Military Defense



OTAC technology enables defense systems to identify friendly aircrafts, vehicles, and troops both accurately and safely.