



# OTAC ACCESS MANAGEMENT



swidch




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

# ACCESS Management

swiDch's One-Time Authentication Code (OTAC) is a technology that can be applied to technical and physical security control, offering a safer and more efficient user authentication process for privacy protection and access control.

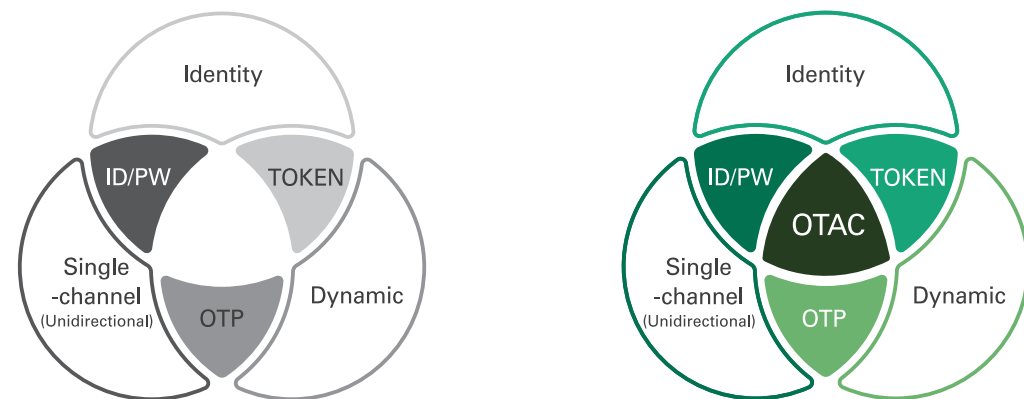
## Challenges

The business environment is changing rapidly, causing many companies to modify their work environment and procedures. With remote work and the use of personal mobile devices as access cards, obtaining and sharing information has become easier than ever. At the same time, however, the open network environment opens up businesses to significant risks in privacy protection.

RF cards at risk of loss, theft, and duplication	ID/PW theft because of weak remote work / network separation environment	Information centralized to smartphones
 <p>A total of 90% of the access control market is dominated by RF cards that communicate on frequency. However, because of the risk of duplication and loss, its security is questionable. The card's security needs to be bolstered to avoid duplication or usage when lost or stolen. Recently, the replacement of smartphones with a simple mobile ID (App) is also gaining attention.</p>	 <p>Because of the COVID-19 crisis, remote workers became susceptible to the negative effects of social engineering methods. In particular, 91.5% of related cyber threats are from email phishing. A separate security control means access to the internal network of the company is the most important aspect of remote work. The use of a VPN to provide end-to-end encryption is recommended. However, using a VPN without a secondary authentication can expose the authentication to theft.</p>	 <p>Personal ID and payments are now all available on smartphones. As a result, people rely more and more on their mobile device. If a person is unable to use a smartphone to access facilities such as public offices, military bases, power plants, etc. that have a commanding security environment, which prevents photography, transmission of information, etc., other IDs and tools for access control will be required.</p>

## Why OTAC?

swiDch's OTAC technology provides the strengths of the three most used authentication systems, namely, ID/PW, authentication codes generating RSA hardware and software, and Tokenization. With all their functions combined, it provides an even more efficient and effective authentication process.



### Limits of the existing authentication methods

- Fixed identification values are vulnerable to exposure/leak.
- The OTP code alone cannot authenticate the user.
- Only operates in the two-way communication connection state between user and server (pull and push)

### One-way unique randomized authentication code

- Dynamic authentication code without any duplicate within a group
- Generates dynamic authentication code in a noncommunication device
- Tokenization available through one-way communication (reduced server load)

## Solutions

swiDch's OTAC provides control to users in mobile and remote work environments or grants a certain level of authority to access corporate resources and networks. It also offers more efficient control by providing a safe and simple authentication process when physical access to a certain space is required. OTAC can be provided both as software and hardware to upgrade individual or corporate access management.

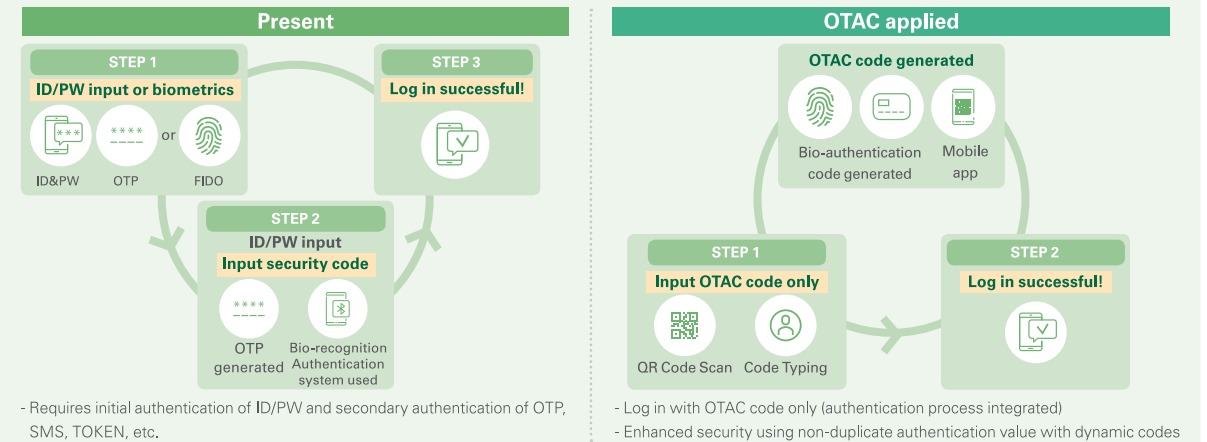
### OTAC Access Management Product

 <p><b>Fingerprint OTAC card</b></p> <ul style="list-style-type: none"> <li>- Using <b>energy-harvesting technology</b> (No Battery)</li> <li>- <b>User authentication</b> through fingerprint recognition</li> <li>- <b>OTAC code or QR code</b> generation (for access control)</li> <li>- Can utilize <b>non-network environment</b></li> <li>- Card <b>display</b> screen option selection available</li> <li>- System log in and gate/door access control <b>all available</b></li> </ul>	 <p><b>OTAC Mobile App</b></p> <ul style="list-style-type: none"> <li>- OTAC log in code generation through <b>card tapping, bio-authentication</b> on mobile device, etc.</li> <li>- Using fingerprint recognition or ID card</li> <li>- Using mobile-generated code or QR code</li> <li>- Can utilize <b>non-network environment</b></li> <li>- Additional function can be linked (App functions)</li> <li>- System log in and gate/door access control <b>all available</b></li> </ul>
---	--

### OTAC Access Management Service

#### Web/App LOGIN

A user's ID and password are a typical fixed-value authentication method, and even the most complex passwords can easily be hacked. Multi-factor authentication (MFA), PIN and password, biometrics, etc. have been proposed to address this issue, but a simpler and more efficient authentication technology is required as the number of complex access environments and processes continue to rise. OTAC logs its users using mobile app-based biometrics, and its security is bolstered by single-use dynamic codes that never recur.



#### Physical access control

The security hole of radio-frequency identification (RFID) cards is as a result of using static key values. If stolen, all other cards can become exposed. Access control cards using OTAC, on the other hand, generate dynamic codes in regular intervals through a mobile app, allowing safer access control by copying these in a near-field communication (NFC) card. Dynamic codes used in authentication are only available for a certain period, preventing their misuse when duplicated or lost.

