

Our mission is to help every person and every organization have secure access to the information they want in communication networks through an easy and secure identity authentication process. To find out more about the revolutionary potential of swIDch for you and your business, get in touch today. We look forward to speaking with you.

The logo for swIDch, with 'sw' and 'ch' in white and 'id' in yellow.

## Get in touch

**Email:** [info@swidch.com](mailto:info@swidch.com)

swIDch Ltd, Office 163, 1st Floor,  
3 More London Riverside,  
London, SE1 2RE

**[www.swidch.com](http://www.swidch.com)**

Discover the power of

The logo for swIDch, with 'sw' and 'ch' in white and 'id' in yellow.

*"We create authentication technology for every digital identity in daily life, business, even in the off-the-network environment."*

**More secure and accurate authentication & identification**



# Easier, more secure authentication in daily life and business

swIDch is an authentication technology startup.

We are committed to bringing secure authentication to every digital identity even in the off-the-network environment.

Since its establishment in December 2018, swIDch has been recognized for its breakthrough technology and rapid growth through various Accelerator programmes and global awards organised by global organisations as well as the UK. Initially launched through GEP from UK government's Department for International Trade (DIT) and LORCA from UK government's Department for Culture, Media and Sport (DCMS), swIDch has experienced remarkable growth. OTAC (One-Time Authentication Code) technology developed by swIDch has already been provided to over 50 clients and is developing business models with organisations in a variety of industries.

## Our Vision

We are driven by one vision: to utilise our authentication technology, OTAC to become the "oxygen" in the IT environment over the world. swIDch's disruptive technology enables secure authentication for everyone, from any device, and from anywhere, while giving people full control of their digital identity.

Our mission is to help every person and every organization have secure access to the information they want in communication networks through an easy and secure identity authentication process.

Our authentication technology guarantees trustworthy access anywhere in the world, regardless of network connection. We prove that authentication is not a difficult technology, but a secure transport that leads to the desired information.

## Part of something bigger...

SSenStone is the parent company of swIDch, proving its technological prowess and growth potential by taking first place with the best score in the "Baby Unicorn 200 project" of the Ministry of SMEs and Startups, Republic of Korea. Consisting of cybersecurity experts with over 10 years of experience, SSenStone continues to research and develop technologies that provide safer and more convenient identification and authentication between humans and devices or devices and devices in a rapidly changing ICT environment. For further information, please visit the official website of SSenStone: [www.ssenstone.com/eng/](http://www.ssenstone.com/eng/)

**SSenStone**  
Simple & Sensible Stone

*Our vision is to utilise our authentication technology, OTAC to become the "oxygen" in the IT environment the world over.*





# The problem

## What we face

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?

### Risk of static information

Card numbers, ID, password, and PINs which we use every day are great examples of static information used as authentication credentials. As the world becomes more connected, using static information for authentication carries with it a huge vulnerability allowing cyber crimes such as identity theft, card-not-present fraud, and hijacking to take place.

### Complex authentication process

OTP, which is widely used for secure identity authentication, cannot perform user authentication alone, so an initial authentication step (usually ID and password) is required. Since you must go through more than one authentication step, this adds to the complexity for users.

### Network connection distress

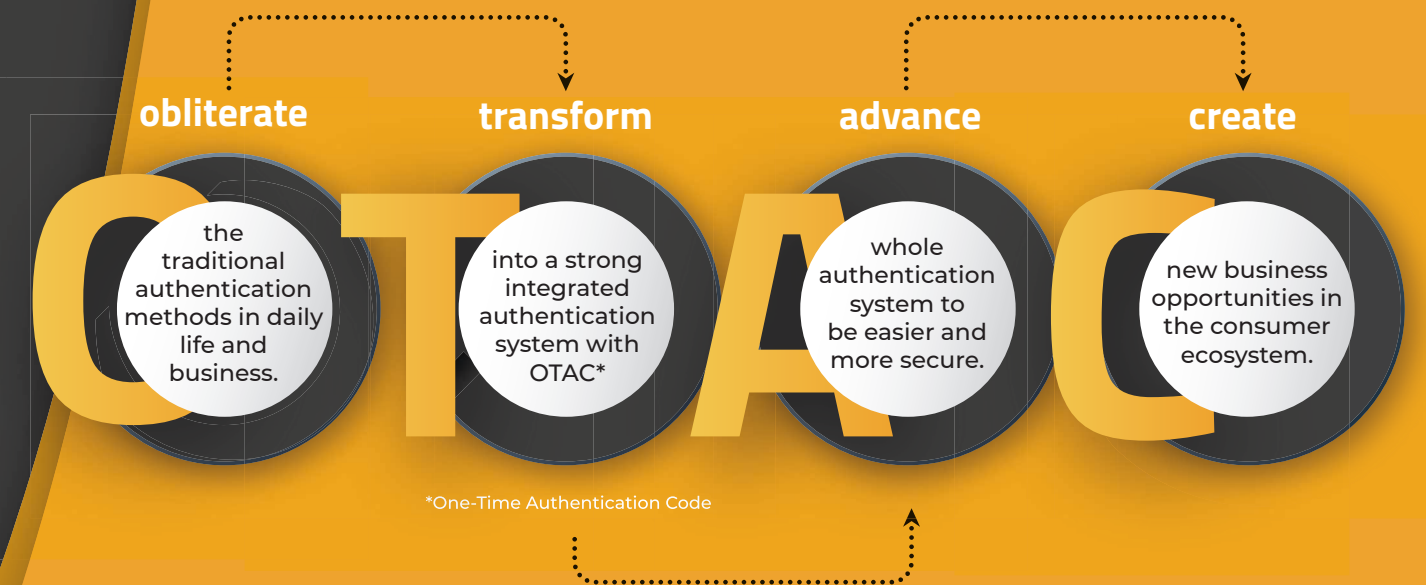
In locations with poor network, it is very difficult to force the use of a communication network to authenticate. The token method is used in numerous authentication environments and has become one of the most common ways of performing secure authentication. This is limited due to the reliance of connectivity between a user, a server and a TSP. It also only operates in an environment controlled by a central server.



# Our solution

## Enter One Time Authentication Code, OTAC.

A new paradigm for user authentication and device authentication.



## What we offer

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. It generates a single dynamic code that both identifies and authenticates the user at the same time and can do so without a network connection. And because it's a single-use, time-based code that's unique to the user, it can't be used by someone else or used again.



### Strong security

Passwordless Multi-factor Authentication.

No identity theft and CNP (Card-not-present) frauds by completely eliminating the attack surface.



### Scalability and flexibility seamless Integration

Use of API/SDK to bring simple and frictionless integration for IT admins.



### Unlimited scalability & flexibility

The lightness of OTAC enables applications in multiple industries and not limited to devices.



### Incredible cost saving

No need to build heavy token infrastructure. Save costs associated with network traffic, maintenance, and fraud compensation.

# Solutions & Use Cases

swIDch's OTAC technology enhances the power of the most advanced identification and access management methods providing a hyper secure single step solution across multiple industries.



## Payment

OTAC technology can generate dynamic virtual card details without a network connection, thereby adding an extra layer of security to the payment process. This patented technology is a CNP (card not present) security solution that replaces static card information with dynamic details, which gives users full control over their security and finance.

- Biometric Display Card
- Virtual Numberless Cards
- Corporate Cards



## IoT

OTAC is a unidirectional authentication technology that allows devices to simply authenticate your user/object with a dynamic code. Enable your users to locally generate OTAC and deliver it over various channels such as voice, keypad, Bluetooth, etc. Algorithm size under 4KB fits into any device chips for enhanced security.

- OTAC generated from user's device, locally.
- Read code out loud to authenticate
- Codes transmitted via Ultrasonic wave
- Drones: security, safety & regulation



## Connected Car

Current digital key solutions require network connectivity when it comes to car sharing to receive and activate the key. Issues arise when the vehicle is located in a basement or rural area where network connectivity is weak.

OTAC allows drivers to access a vehicle in a networkless environment.

No matter where the driver or car is located, there are no obstacles for drivers activating the digital key and sharing it with an authorized person.

- Digital keys generated from user's device, locally.
- Digital keys can be generated offline
- Share with 3rd party users. E.g. Family, Corporate, Rental etc.



## M2M

Enterprises are moving towards microservice environments implemented with end-to-end trust. However, authentication flows can be cumbersome and involve many round-trips, with an irreducible time cost for each; authorisation services can become overwhelmed as each microservice relies on them for access control.

OTAC allows secure authentication of a user in a single ended flow, greatly reducing the number of round trips.

- Improve M2M communication
- Role authorization
- Digital transformation enabler



## Enterprise

Forget passwords and OTPs. Users can securely access services and networks with OTAC code alone. OTAC guarantees hassle free log-in that works even in an off-the-network environment. With OTAC, access your company applications anywhere and anytime. Remote working is no longer a problem.

- Secure and simple authentication
- Seamless UX for employees
- Safe, reliable access management



## ICAM

By assigning users with specific roles and ensuring they have the right level of access to corporate resources and networks, swIDch provides strong security, improved user experience, and comfort for IT admin and users for mobile and remote working environments.

- Protect and secure data and people
- Access and authority
- Easy integration to IAM solutions



## Military

In the midst of battle, it is very difficult to identify your friendlies or targets. Current solution to the problem is to identify friendlies from their devices using static information, which can be hacked and used by the enemy. OTAC can completely eliminate this risk by generating dynamic codes locally without a network. Wherever a soldier is located, their device will send a dynamic code which hackers cannot steal so that their own force can identify securely.

- OTAC for IFF (Identification Friend or Foe)
- Removes hijacking threat
- No threat from cloning or spoofing attacks

**Even in a critical digital environment, the OTAC algorithm benefits businesses by increasing efficiency, reducing costs, and improving user experience (UX) whilst providing the highest level of cyber security.**



# The problem

## What we face

As many organisations start implementing and adopting technology to enable digital transformation, the number of websites and services that require personal information have increased exponentially. However, security in regards to personal information is far from sufficient. Most users still prefer using the same ID and password in traditional ID and password input systems. Once this personal information is leaked, it can be used as a master key login to access multiple websites and services.

### Password leak

Leakage of personal information can be obtained by hackers with ease, resulting in irreparable damage to individuals and service providers across multiple industries.

### Password reuse

Users are using the same password for multiple online accounts leaving them vulnerable to account theft and further incidents.

### Reset password

To create a secure password, users adopt difficult passwords which can be easily forgotten. The users' repetitive and unproductive approach to password creation often results in significant opportunity costs.

**Easier, faster, and more secure authentication for all business and everyday needs!**



# swIDch Auth SDK

## All-in-one User Authentication Security SDK

swIDch Auth SDK provides diverse authentication solutions such as FIDO certified international standard biometric authentication, convenient mobile device authentication mOTP, and the world's first one-way dynamic authentication OTAC login.



FIDO



mOTP



OTAC Login

### FIDO

swIDch Auth SDK provides groundbreaking FIDO-based authentication security functions that overcome the vulnerability of ID and password methods. From user biometrics (e.g., fingerprints, facial recognition, etc.), integrative authentication with PIN and pattern input, convenient PC logins with QR codes to electronic signatures, you can expect a secure environment of the highest standard.

Biometrics / PIN / Private Verification / Electronic Signature / Pattern / PC Login (QR Login)

### mOTP

swIDch Auth SDK provides easy-to-use mobile OTP functions for situations that require more powerful authentication security. Unlike standard OTP, mOTP can generate one-time passwords without physical security cards by using a smartphone app. Thus, you can build a very powerful identity verification system.

mOTP Generation·Authentication / PIN linkage / Transaction mOTP

### OTAC Login

swIDch Auth SDK provides login functions based on our self-developed, powerful authentication security technology, OTAC (One-Time Authentication Code). OTAC provides the most secure authentication security because it is impossible to reuse, never duplicates or overlaps with others, and generates real-time dynamically changing verification methods without connecting to a server.



# Looking to the future

## Innovation enabler

### Innovation, Experience, Creation

Our long-term commitment to innovation provides our customers with unprecedented experiences. We want our customers to deploy authentication technology not only to sell products or services, but to develop entirely new products and services.

## Borderless Business

### Worldwide channel

We are not limited to a specific country or continent, but serve as a secure access channel to all products and services around the world. Whether it's a technologically advanced country or a country with insufficient infrastructure, our technology will be present in all products and services that require authentication

## Game changer

### Human-to-Human, Human-to-Object, Communication

If electricity has become the catalyst for human night-time activities, our technology will revolutionize fraud-free human-to-human, human-to-object, and object-to-object communication. Our technology advances a new era where people, free from the threat of fraud, can embrace new challenges and explore new opportunities.

# Why swIDch?

## An award-winning game changer



## Our company at a glance

