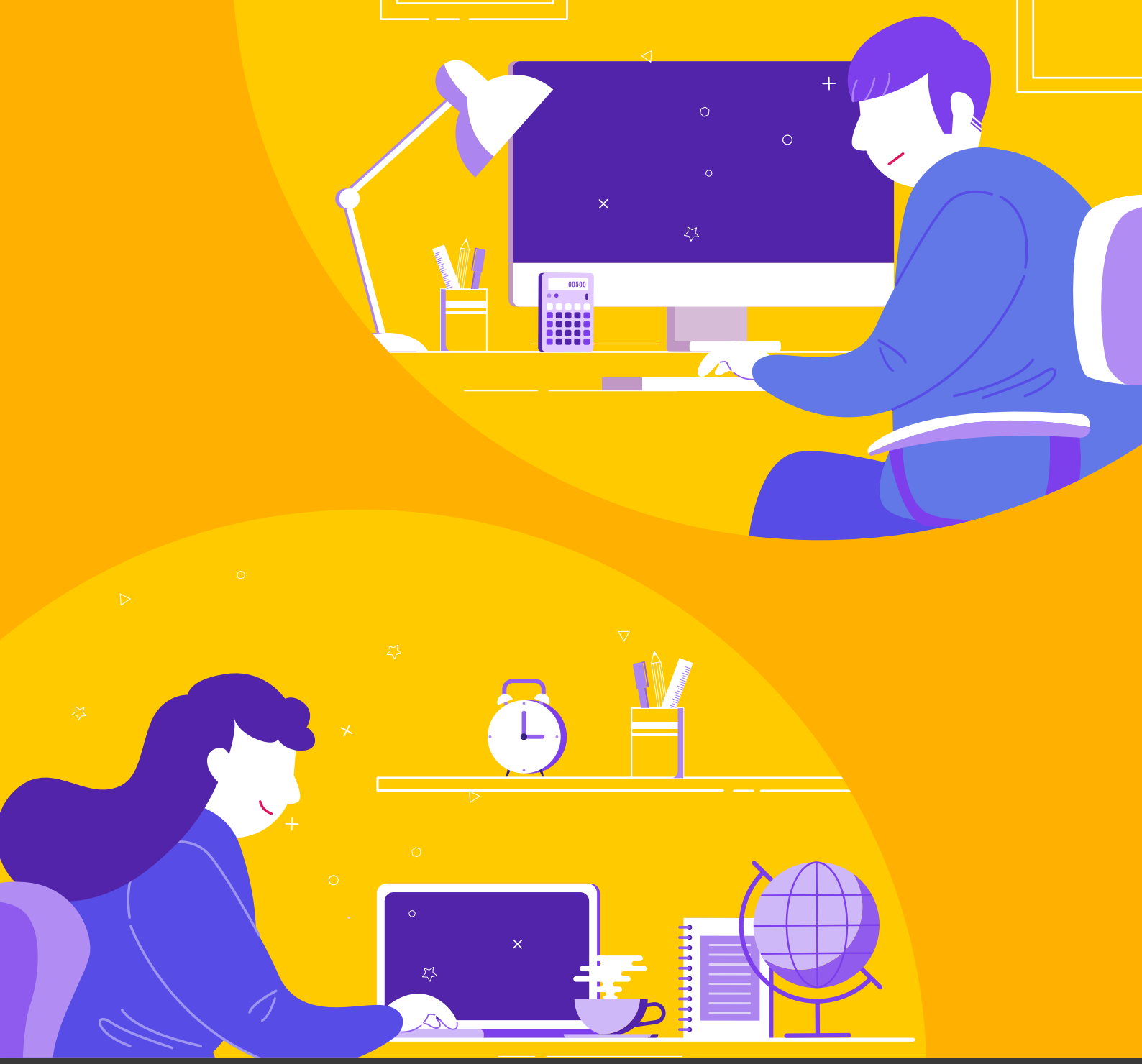

Switch to swIDch:

Easier, more secure access management with one-time authentication

swidch

Introduction

To keep hackers away from their sensitive data and systems, businesses typically try to manage access by operating in a closed network environment. However, as a growing number of people work from home or use mobile devices from remote locations, more of them are accessing their workplace systems via an open network, potentially putting business security at risk.

Another issue with today's authentication methods is that they rely heavily on traditional authentication technologies such as ID/passwords, one-time passwords (OTPs), tokens and SMS messages. All of these increase operational costs for businesses.

One recent survey of cybersecurity professionals found that 89 per cent agree that identity and access management is very or extremely important for risk management and security. Yet 55 per cent acknowledge their organisations are only somewhat effective at best.

Because everything in this world is connected to a network, here's a question to consider: Is this the right way – and the safest way – to handle authentication? Security-sensitive organisations clearly need better approaches. Some businesses are exploring alternative solutions, using things like artificial intelligence (AI) and big data to strengthen existing authentication technologies.

But there is a solution available now that solves many problems associated with current methods of identity and access management. It's called one-time authentication code (OTAC) technology.

In the pages that follow, we'll explore today's identity and access management challenges in more detail. And we'll show why OTAC technology is the best choice for any organisation.

> **"One recent survey of cybersecurity professionals found that 89 per cent agree that identity and access management is very or extremely important for risk management and security.**

Overview of access management

Evolving needs and demands
As more and more enterprises transform how they work to enable truly digital business, they will need identity and access management systems fit for purpose. A major obstacle to achieving that is identity systems built for an earlier era. These often lack the security, efficiency and flexibility required today.

But updating those systems can be difficult and costly – not an ideal option for businesses watching their bottom lines more closely than ever.

Organisations are also facing the need to manage access for millions of employees who are, increasingly, working from home. This requires accommodating a wide range of device types, operating systems and network connections of varying speeds, reliability and security.

Key challenges for administrators and users
Many organisations developed their identity and access management systems over time. This often resulted in numerous incompatible systems that users must access with multiple usernames and passwords. This is not only inefficient but also difficult for IT administrators to manage when they must provision or deprovision accounts or reset passwords. It becomes even more complicated when people add new technologies without IT's approval or awareness (known as shadow IT).

Depending on its existing identity and access management systems, an organisation can face different challenges:

- User IDs and passwords might be effective, but they are difficult to remember and easy to steal.
- OTP (RSA key-based) authentication using hardware or software to generate authentication codes might offer improved security over passwords, but it can't identify users with the codes alone – whoever has the hardware or software has access.
- Dynamic tokens are effective but require an active network connection – which is not always available – as well as two network channels.

> "Organisations are also facing the need to manage access for millions of employees who are, increasingly, working from home.

swIDch's OTAC technology

What it is and what it does

Organisations can choose from a wide range of identity and access management solutions but these usually come with drawbacks. Some require costly and complex infrastructure investments. Others are difficult to use or don't scale easily. And many don't work without a network connection, which limits when and where they can be used – and also means hacking is more of a risk.

But one approach eliminates all of these and other concerns: swIDch's OTAC technology. This patented, algorithm-based approach identifies, verifies and authenticates users quickly and efficiently, without the need for new infrastructure or two-way connectivity.

swIDch's OTAC technology combines elements of the three most common authentication systems – user ID/passwords, RSA hardware/software for generating authentication codes, and tokenisation. This provides a solution that's 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 a second time.

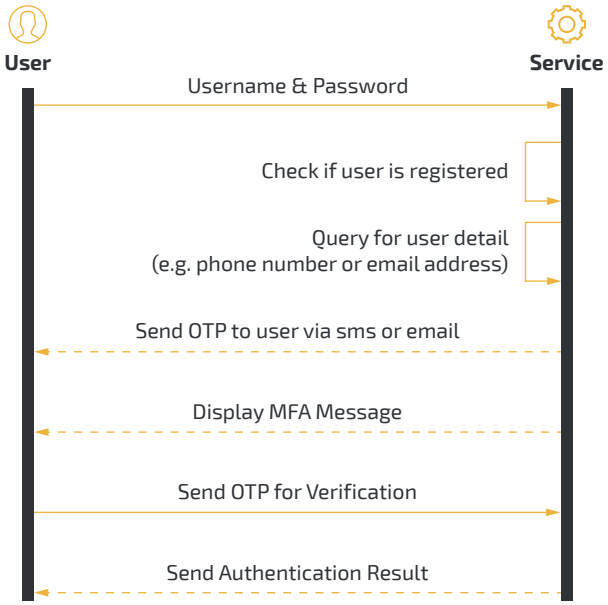

Figure 1: Current ID/password method to generate one-time password

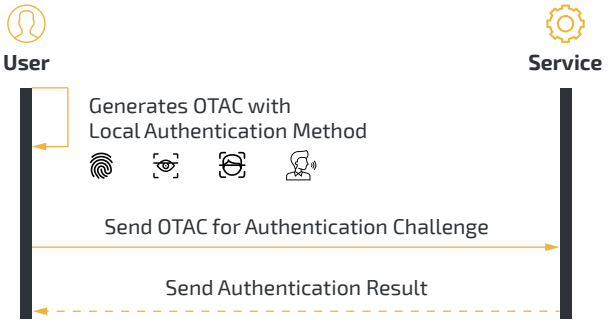

Figure 2: One-time authentication code (OTAC) method

How it works

To access a system using OTAC, authorised users can use their mobile device and – for an extra layer of security – something like an employee ID or bank card enabled with swIDch's technology. By launching the swIDch app, or the client's own app integrated with swIDch technology, and then touching the ID or bank card to the mobile device, users can generate a one-time alphanumeric or QR code. In effect, the user's device acts like a token server, generating a one-time code for access without the need to connect to a network. Identification and authorisation are then both enabled when users type or scan their code into the system they want to access.

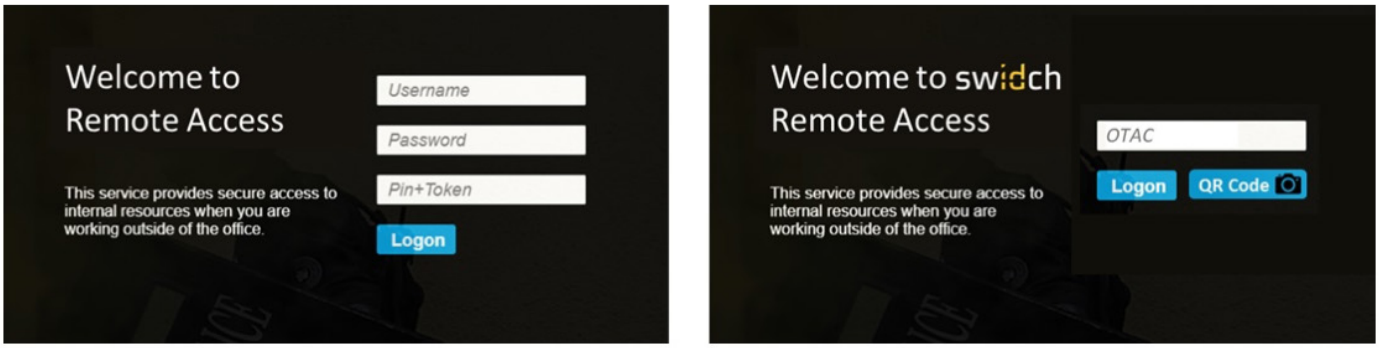

Figure 3: Traditional company intranet access (L) and company intranet using swIDch (R)

Why it's better

swIDch's technology eliminates the disadvantages of other common identification and authentication methods.

Because it works without user IDs or passwords, people no longer have to remember long, complicated strings of letters, numbers and symbols, change them regularly or risk having someone else steal and misuse that information.

Organisations using OTAC are also assured that access is available only to properly identified and authorised users, rather than to someone who might obtain a legitimate RSA key by illegitimate means. And everyone who is authorised to access critical systems can do so whether or not an active mobile network connection is available. This helps to both reduce network traffic and enable secure, reliable access management no matter the limitations of local connectivity.

> "swIDch's technology eliminates the disadvantages of other common identification and authentication methods.

Benefits of OTAC for security-minded organisations using access management

swIDch's one-time authentication technology offers many benefits. It's easily implemented without costly or time-consuming improvements to existing infrastructure. It reduces network traffic loads and related expenses. And with no need for mobile networks or two-way communication, there's less risk of hacking from threats such as man-in-the-middle attacks.

Because the technology is based on application programming interfaces (APIs), it integrates seamlessly into modern mobile and cloud architectures. That's a plus for usability, especially considering many larger organisations must manage privileged access for hundreds of employees, each of whom might have multiple passwords and accounts.

OTAC technology also offers flexibility and works with a range of devices and applications. As algorithmic software, OTAC is compatible with – and can be applied to – any operating system or application used in today's IT systems. And because the software is extremely small and lightweight at just 4KB, it's easily used with any wearable devices, such as smart watches, smart cards and smart bands, whether or not those normally rely on network connections. Because swIDch's technology is so lightweight, it can also be used for authentication between chips: for example, in mobile SIM cards for an extra layer of security, as well as in Internet of Things (IoT) devices.

Beyond its effectiveness in managing access to secure systems and locations, OTAC can provide a way to validate government agency IDs or to verify identities and authenticate users on payment platforms, intelligent speakers, IoT devices, drone applications and more. This makes the technology highly customisable to your organisation's unique needs.

> **"Because the technology is based on application programming interfaces (APIs), it integrates seamlessly into modern mobile and cloud architectures.**

Conclusion

Security is non-negotiable, even as device numbers proliferate and more people work remotely. It's critical that organisations ensure access only to those who are properly authorised. A variety of technologies can do this, but many are easily misused or prone to security failures, as shown in Table 1. This puts organisations at risk.

Authentication Technologies

	ID and Password	OTP	SMS	ARS	FIDO (Biometric)	Tokenisation	OTAC
Free from the risk of identity information theft	×	○	△	○	○	○	○
The ability to authenticate on its own	○	×	×	×	○	○	○
Free from the risk of variable in a networked environment	○	○	×	×	×	×	○

Table 1. Comparison of risks in various authentication technologies

swIDch's authentication technology provides a better and simpler way to manage access securely, efficiently and cost effectively. It delivers benefits that other multi-factor authentication technologies can't offer on their own, as shown in Table 2. Moreover, OTAC can be used with a range of technologies and applications and is easy to deploy with no change to existing infrastructure.

2 Factor Authentications

	ID and Passwords			FIDO (Biometric)**	Tokenisation**	OTAC**
	combined with OTP	combined with SMS	combined with ARS			
Security	High	High	High	High	High	High
Flexibility	Low	Low	Low	High	High	High
Risk from using same authentication info across number of platforms*	High	High	High	Low	Low	Low
Network Reliance	None	High	High	High	High	None
Cost	None/Low	High	High	Variable	Variable	Low

* E.g. use of same ID & Passwords across number of other platforms

**Multi-factor authentication is a combination of what you know (e.g. passwords), what you have (e.g. devices, smartphones), and what you are (e.g. fingerprints). FIDO, Tokenisation & OTAC operates on top of 'what you have', therefore, it is a multi-factor authentication

Table 2. Comparison of benefits delivered by various multi-factor authentication technologies

The benefits to organisational users are clear: more secure and reliable access management, greater flexibility, and reduced network and infrastructure requirements. Individual users also benefit through a technology that is easy to learn and easy to use, employing already familiar devices and applications.

To learn more about swIDch's one-time authentication code (OTAC) technology, or to get started implementing OTAC in your organisation

Contact us today on:
hello@swidch.com