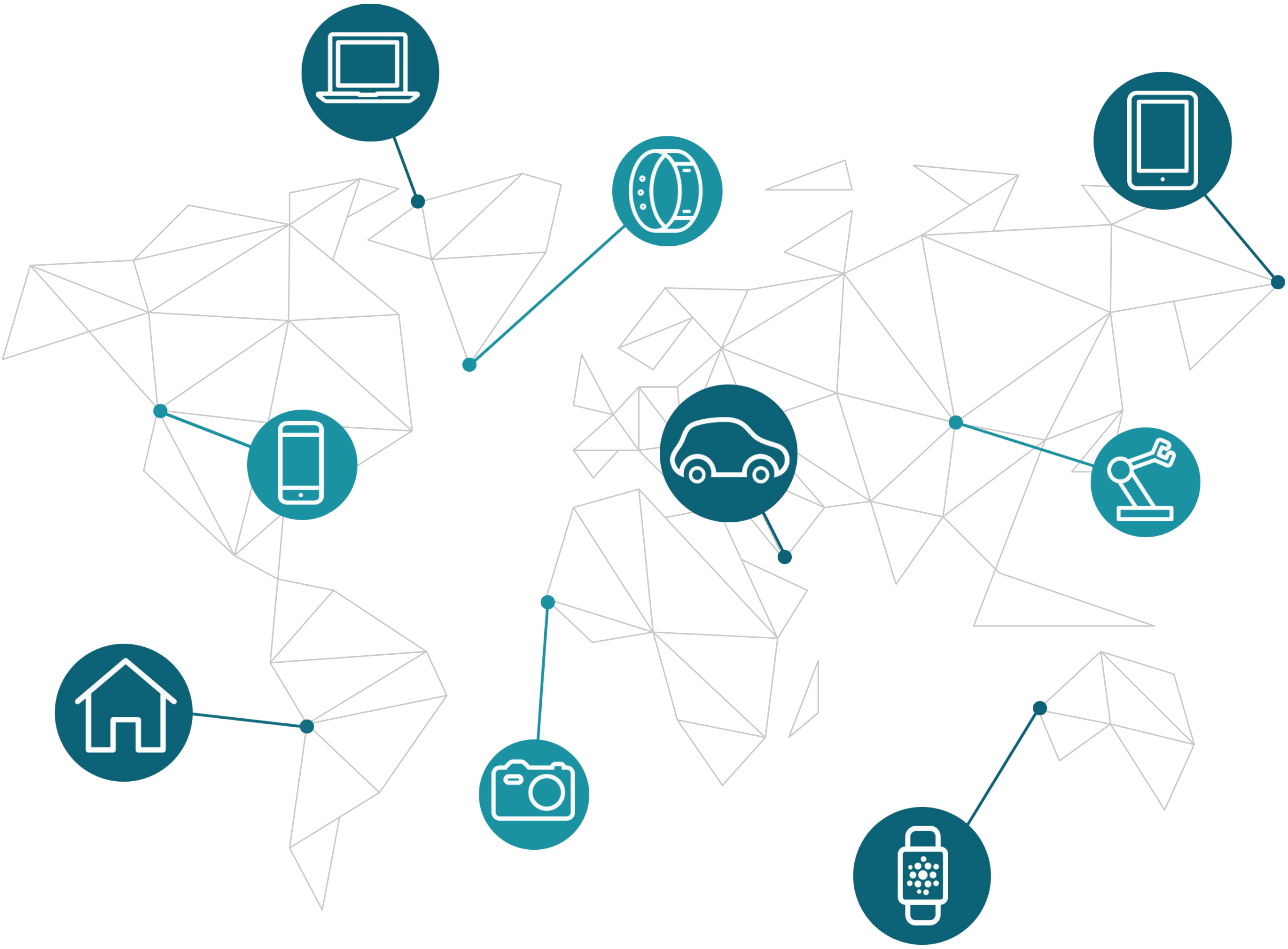
A white paper by Transatel

DATA SECURITY FOR MOBILE EMPLOYEES



What are the risks associated with public Wi-Fi?

What are the solutions offered by cellular connectivity?

2017

EXECUTIVE SUMMARY

Employees tend to use Wi-Fi, especially while traveling abroad, to access their company's Information Systems. Not only is this inconvenient for the workforce, but it places the company at risk.

Companies are still widely indifferent to the risks weighing on their corporate data assets. And many are not yet aware of the solutions available for secure data transmission, namely the ones offered with cellular connectivity. Global cellular solutions, such as Transatel's SIM 901, are not as costly as one might imagine.

This white paper explores reliable and cost-effective options to protect corporate data assets in the modern, open workplace, where a large proportion of the workforce is on the go.

Cellular connectivity is the secure option, as it leverages the intrinsic security benefits of cellular networks—a private and controlled, trusted network environment paired with the hardware-based security provided by the SIM card.

SECURE CONNECTION
via cellular networks

+

STRONG AUTHENTICATION
to access the company's Information Systems

=

SECURING THE MOBILE WORKFORCE

THE MOBILE WORPLACE'S SECURITY CHALLENGES

In 2017, the mobile workforce already accounts for nearly 40% of the global workforce, and is bound to continue to increase year on year[1]. Ensuring corporate data security in this context has therefore become a mainstream concern, though the dangers—expressed in terms of 'risk'—are not easy to convey to decision makers.

[1] Strategy Analytics, 09 Nov, 2016: the global mobile workforce is set to increase to 1.87 Bn. people in 2022, accounting for 42.5% of the global workforce. Continued globalization will drive the growth of mobile workers in all regions.

WHAT RISKS ARE WE TALKING ABOUT?

Three years ago, Maurits Martijn, a Dutch journalist at De Correspondent, entered a café in Amsterdam with Wouter Slotboom, an ethical hacker. Within minutes, Slotboom had set up his gear, consisting of a laptop and a small black device. He connected to the coffeeshop's Wi-Fi. Soon enough, his laptop started to display what other people in the café were doing on their devices: what games they were playing, what apps they had installed, Google searches, passwords, email accounts and more. Slotboom's small device (under 80 €) could fool a phone into connecting to his own Wi-Fi network, giving him control over the entire traffic coming and going from any device[2].

Yet, probably because the demonstration was conducted by a professional hacker, awareness didn't take place as expected. In January 2015, however, to put the dangers of open networks into perspective, a virtual private network (VPN) provider recruited a child to attack a public network[3]. The seven-year-old watched an online video tutorial before being asked to hack into a Wi-Fi hotspot. Betsy Davies from Dulwich in South London hacked a willing participant's laptop while they were connected to an open Wi-Fi network. It took her under 11 minutes to infiltrate the network by setting up a rogue access point. This example did go viral, and ensured quite a bit of publicity for the security offered by VPNs.

In this paper, we aim to prove, however, that VPNs are far from sufficient to ensure true data protection for mobile workers.

MOBILE INITIATIVES FOR EMPLOYEES HAVE BECOME CRITICAL PRIORITIES

An important proportion of any company's workforce today is dispersed in the field and dependent on available public Wi-Fi—in hotels, airports, public areas, etc—or their smartphone to connect to the company's IT infrastructure. Moreover, mobile applications are increasingly introduced by companies for employees' day-to-day operations, since they help with cost cutting and with improving employee productivity and efficiency. However, because employees connect over many networks often controlled by third parties, corporate data security is a paramount concern.

[2] *https://thecorrespondent.com/1101/what-we-give-away-when-we-log-on-to-a-public-wi-fi-network/31040493-53737dba*

[3] *http://www.dailymail.co.uk/sciencetech/article-2919762/Hacking-Wi-Fi-s-child-s-play-Seven-year-old-shows-easy-break-public-network-11-minutes.html#ixzz4f4tk6BOO*

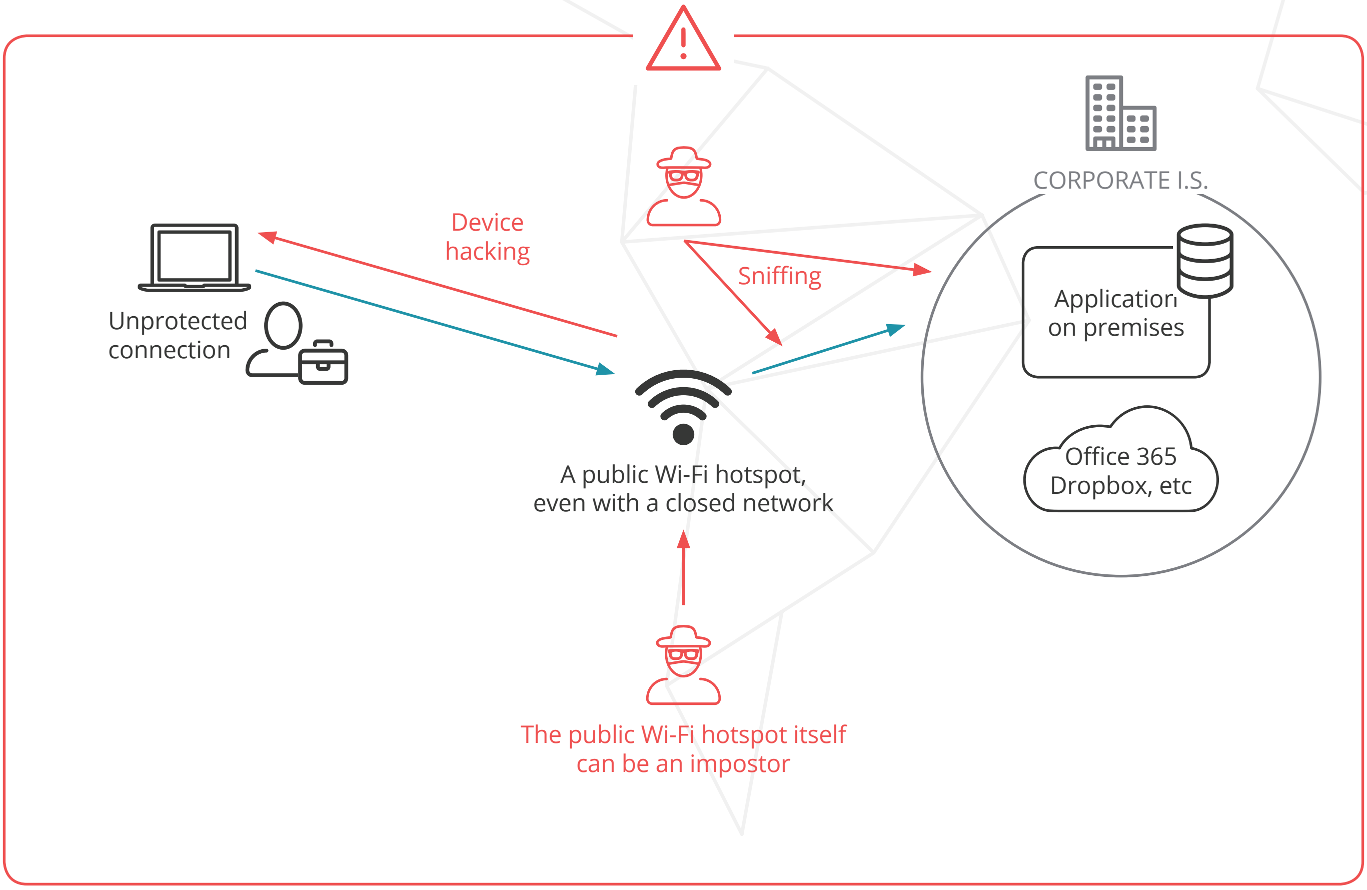
A NECESSARY BALANCE: PROTECTING DATA ASSETS VS. INCREASING EMPLOYEE PRODUCTIVITY

Best practices in terms of IT security often focus on employee behavior, since the human factor is hardest to control. As a result, to achieve a fool-proof system, processes introduce multiple and regularly renewed levels of identification, firewalls, shielded work environments etc, and impose a strict regimen in many day-to-day tasks.

Security in a mobile deployment is a difficult trade-off between protecting corporate data assets and ensuring that security measures don't impede on worker productivity. An appropriate security policy must satisfy the needs of three categories of employees:

- Managers who want their teams to reach the highest level of productivity while in the field
- Mobile workers who want remote access to be immediate and seamless
- IT professionals whose responsibility it is to ensure corporate information and assets are secure

THE DANGERS OF PUBLIC WI-FI



TO ENSURE DATA SECURITY, A VPN IS NOT ENOUGH!

Even of your employees connect to the VPN via a public Wi-Fi, hackers can still perform attacks.

The most common techniques are the following:

- **Snooping/sniffing**

The hacker tricks a network into passing all the data through his/her computer before sending to the user of a Wi-Fi network. The hacker is thereby able to listen passively without the user's knowledge. Cybercriminals use software kits and devices to assist them with eavesdropping on Wi-Fi signals.

- **The man-in-the-middle attack**

The hacker intercepts data by pretending to be a reputable access point to the internet, such as a hotel's Wi-Fi access point. The victim's device unknowingly connects to the wrong destination system, i.e. the hacker's machine.

- **DNS cache poisoning**

A method of attack whereby 'updated' data is used to enable the hacker to divert the traffic to the hacker's destination of choice.

- **Malware distribution**

Thanks to software vulnerabilities, hackers can slip malware onto a victim's device entirely unnoticed. Hackers exploit a weakness or a security hole found in an operating system or a software program and target this vulnerability to inject the malware in the victim's device.

- **The brute-force attack**

The hacker simply tries to break the victim's passwords by repeatedly trying to log in with different credentials, a method that can take hours, days or months depending on the complexity of the password.

RELYING ON THE INTRINSIC SECURITY BENEFITS OF CELLULAR NETWORKS

The use of open, public Wi-Fi networks presents a security threat for any organization's data. Quite the opposite, cellular mobile networks are controlled, managed, private, and benefit from built-in security features to protect data flows and enable strong authentication of a company's employees.

Industry standard encryption via a single VPN tunnel keeps data secure as it traverses multiple networks. However, as shown in the previous section, corporate communications are at risk even if they are conducted via a VPN, if the access to this VPN takes place via an open, public, or unencrypted network.

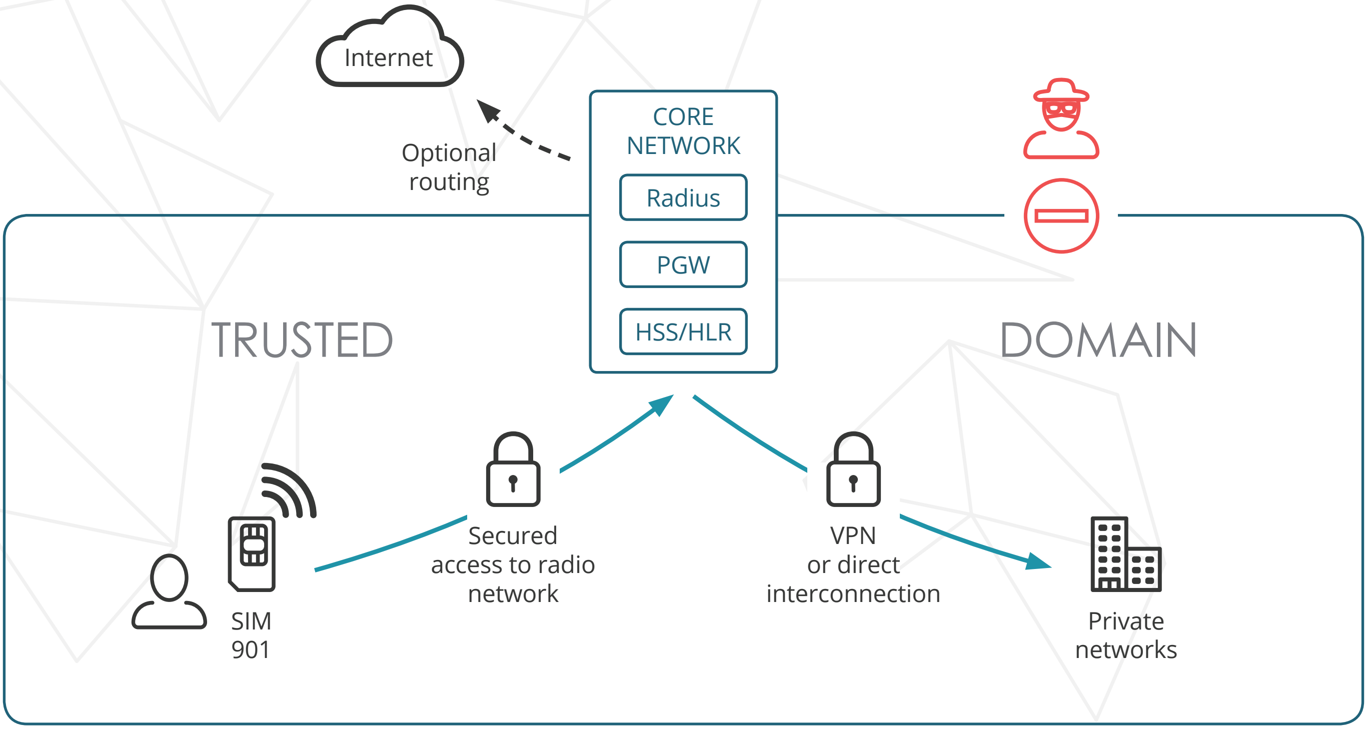
CELLULAR NETWORKS ENABLE END-TO-END CONTROL OF DATA TRANSMISSION

One can truly consider communications are safe if they are conducted within a 'sphere of trust', composed of different elements resulting in a multi-layered security system.

By design, cellular networks offer security because:

- Access to networks is controlled via mutual authentication
- Data transmission is encrypted
- The operator guarantees closed user groups
- All communications can be screened by company security policies
- Companies can monitor IP addressing, routing, and high availability mechanisms

CELLULAR NETWORKS ENABLE MOBILE WORKERS TO REMAIN WITHIN A TRUSTED DOMAIN



LEVERAGING THE STRENGTHS OF THE SIM CARD

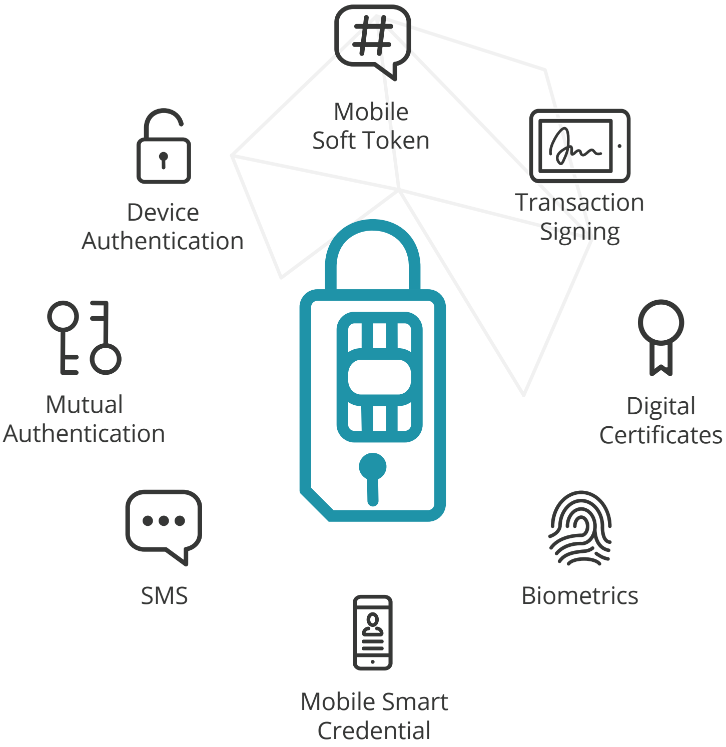
THE SIM IS A 'SMART CARD' TO BE USED AS A SECURE ELEMENT

A SIM card is a physical element that cannot be tampered with or duplicated. It offers a security domain with an isolated, private, and dedicated container, and is designed for secure storage and computation. Moreover, it offers a secure, dedicated communication channel allowing the remote management of its content.

A SIM-BASED VAULT OFFERS MANY ADVANTAGES FOR CORPORATE SECURITY POLICIES

A SIM card offers the possibility to safely store and compute passwords and biometric credentials, bank account information, certificates and keys, software licenses and network settings. These capabilities in turn enable some of the fundamental requirements of a security policy, such as:

- Authentication—whether that of the device or of the user, to enable mutual authentication, VPN authentication, etc
- Signature—whether for a transaction, a document, a firmware, etc
- Encryption—for a financial transaction, a file transfer, an SMS, an email, etc



SECURING EMPLOYEE IDENTIFICATION WITH STRONG AUTHENTICATION

Between September and December 2016, Yahoo shocked the world by revealing that at least 1 billion user accounts had been breached[4]. The violation is believed to be the largest theft of personal data from a major technology company ever. Nonetheless, many organizations still protect their data with simple login/password procedures, either within cloud applications (such as Office 365, GSuite, Dropbox...) or on premises (for a VPN access, web portals, databases...).

Passwords have reached their limits. Humans have little patience and memory, so to alleviate the process, most individuals use the same passwords for almost every platform and interaction. This explains why systems that rely exclusively on a password scheme offer weak protection against systems intrusions.

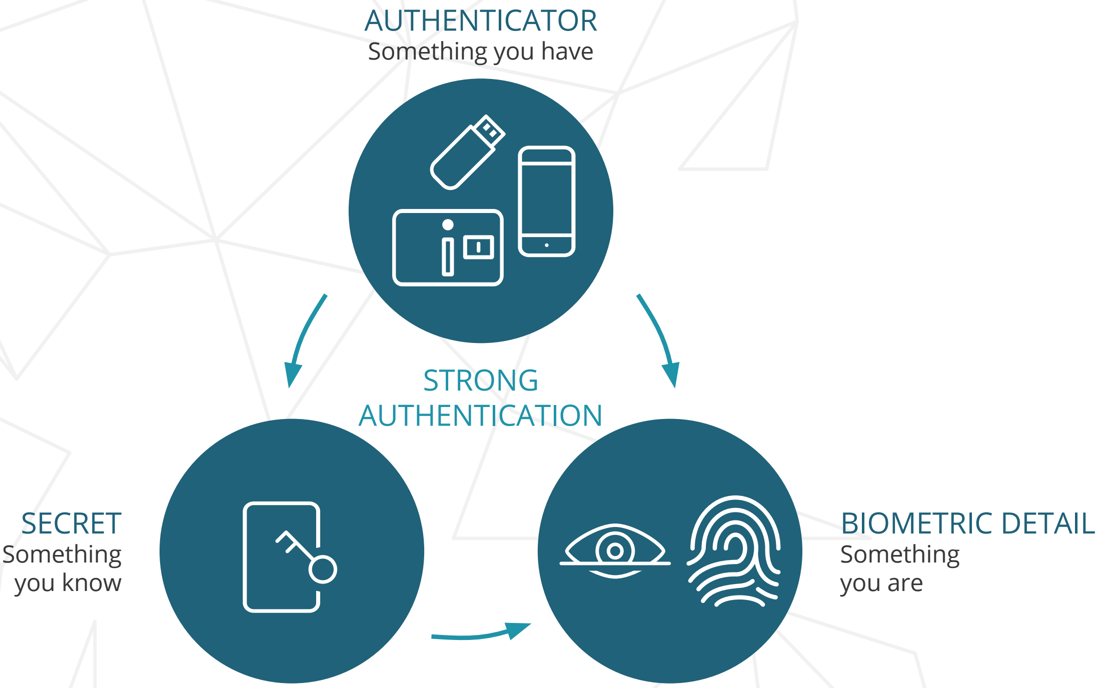
Security systems enforced with passwords can be easily violated with the previously mentioned hacking techniques such as social engineering, phishing, brute force attacks, shoulder surfing, keystroke logging, eavesdropping, and dictionary attacks. The need for stronger methods of authentication has arisen, to allow for trustworthy transactions. In the case of a company policy, transactions can be financial, of course, but may also merely concern any individual logging into the company's information systems.

[4] *https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached*

WHAT IS 'STRONG AUTHENTICATION'?

It is a measure by which the authentication procedure relies on the concatenation of at least two authentication factors. Only the combination of these factors can ensure robust and consistent authentication. These elements are known to be:

- Something only the authorized user knows (PIN, login, a secret phrase...)
- Something only the authorized user has (a magnetized card, an RFID, a USB key, a PDA, a SIM card, a smartphone ...)
- Something only the authorized user is, i.e. a person with identifiable criteria, such as digital or retinal prints, the structure of a hand, facial structure, or any other biometric detail



THE 'ONE-TIME PASSWORD'

The One-Time Password, or OTP, is the most widely used second factor of authentication. The first layer of authentication remains the personal password. But the user must also enter an OTP, received for example via an SMS on the user's device.

The idea here is that the OTP is only accessible to the user in question. Which is—in theory—supposed to guarantee that a third party cannot take advantage of an access to the user's login credentials.

WHAT IS A ONE-TIME PASSWORD OR OTP?

As its name implies, this password is valid only for one session or transaction. OTPs offer protection against hacking techniques based on repetition and the use of memorized passwords. However, as these passwords cannot be remembered by humans, complementary technology is necessary to produce them and use them.

EXISTING OTP TECHNOLOGIES

OTPs are generated thanks to tokens that can be hardware-based or software-based.

The hardware-based token ensures a high level of trust, but there's an obligation to always carry it on oneself, and it comes at an extra cost to acquire and manage.

The software token does not rely on a specific material, and can be integrated into the smartphone, with fewer risks of loss or forgetfulness. Arguments against the software token include the synchronized key. OTPs obtained via a smartphone app are based on the temporary synchronization of the device and a shared key. If this key is compromised, a cybercriminal can clone the authentication application with a victim's parameters. From a general standpoint, any software solution is unsecured[5].

Token	Benefits	Threats
Hardware	• Secure against replay attacks • Prevents against phishing	• The user needs to carry the device everywhere • There is a risk that it may get stolen or lost
Software *(mobile)*	• Users simply need to carry their cell phones • No additional device required	• Still vulnerable to active attacks

[5] In How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication, Radesh Krishnan Konoth, Victor van der Veen and Herbert Bos, 2016

ARE SMS THE BEST SOLUTION FOR THE DELIVERY OF OTPs?

Among software tokens, OTPs sent via SMS are superior, as they're entirely random and therefore unpredictable—they're not related to a timely action or a shared secret. They're also the most user friendly.

The user receives an OTP directly on their cell phone to validate a transaction. The best-known example of this technology is 3D Secure. Arguments for the OTP received via SMS are that there's no need to download a third-party application. Also, if anyone tries to authenticate his/herself on your account, the OTP's SMS serves as a warning.

HIJACKING SMS IS ELEMENTARY!

The main argument against the reception of OTPs via SMS is that they can be hijacked through a vulnerability in the SS7 (Signalling System 7), a set of protocols allowing global phone networks to exchange information. For this reason, the NIST, a non-regulatory agency of the United States Department of Commerce, has downgraded SMS with regards to security[5].

The increasing use of SMS for the transfer of OTPs to users is problematic, because messages are not encrypted. Even beginner hijackers can find software and services enabling them to intercept text messages[7]. All they need from there on is the cell phone number of their victims. Once the system is in place, they can intercept SMS and transfer them to other cell phones to use them for authentication.

[6] In Digital Authentication Guideline, National Institute of Standards and Technology (NIST), 2016

[7] In How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication, Radesh Krishnan Konoth, Victor van der Veen and Herbert Bos, 2016

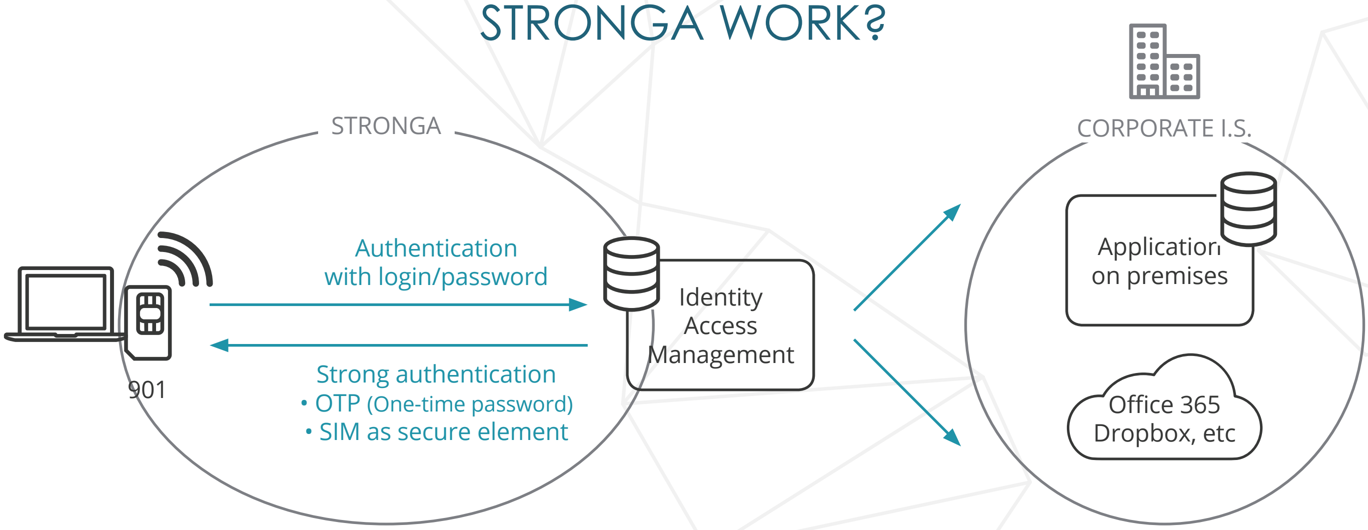
SIM 901's 'STRONGA': STRONG AUTHENTICATION TO PROTECT CORPORATE DATA ASSETS

Up until today, companies looking for a two-factor authentication method were faced with an impossible choice. On the one hand, using SMS OTP or software tokens with a tolerable level of security, but still far from air-tight. On the other hand, using hardware tokens, with the highest level of security, but expensive and inconvenient for the end user.

Transatel now offers the ideal secure authenticator for any company using devices with cellular connectivity. SIM 901's StrongA offers hardware-based security. It's always available to the user, since it can be placed in a PC, tablet, dual-SIM smartphone or smart hotspot. Also, it's associated with a local PIN.

It allows for strong authentication of the user and a high assurance level of eIDAS, the new EU regulation for electronic signatures.

HOW DOES SIM 901'S STRONGA WORK?



WHAT IS SIM 901's STRONGA?

It's a method for strong authentication composed of two elements:

- The SIM 901 SIM card, including the StrongA authenticator application. This application is natively compatible with any SIM toolkit-compliant device, including any iOS/Android device (smartphone or tablet).
- Transatel's StrongA API gateway, to be integrated as an alternate second factor authenticator within an Identity Management System /SSO (Single Sign On).

COMPANIES, STAY WITHIN THE SAFE ZONE!

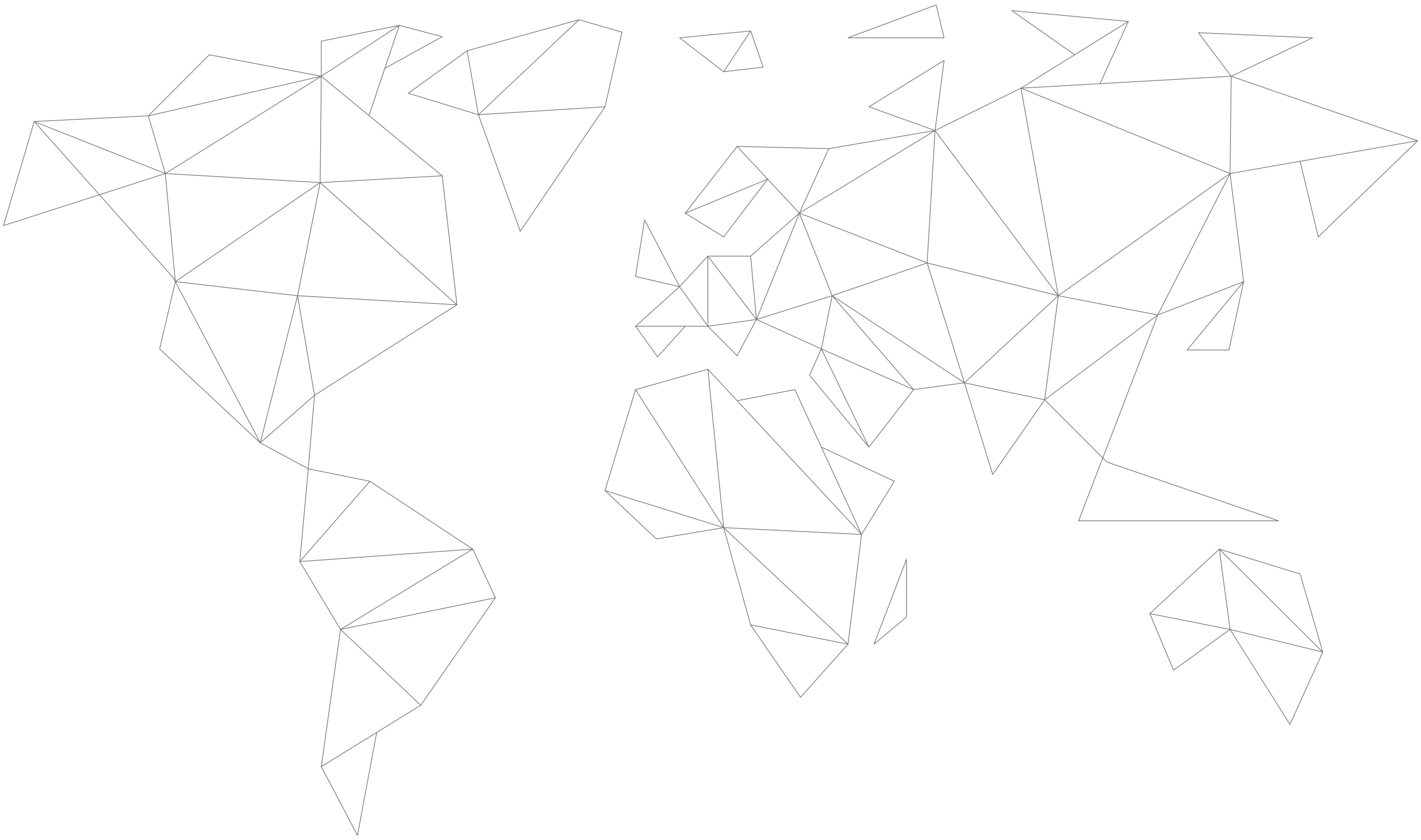
40% of a company's workforce on average is on-the-go. Therefore, employees must be able to connect to the company's information systems at all times. Here is the new challenge IT decision makers face, in a context of growing systems complexity and vulnerability.

The most widely recommended solution to protect the data flow, VPNs, can't fully protect the data while the employee's device is connecting to the internet. Thanks to cellular technologies, you can create a private network connecting the SIM card directly to the company's information systems without ever using the public internet. This allows mobile workers to evolve in an environment that is fully controlled and protected.

Using the private cellular network offered with Transatel's SIM 901, any company benefits from end-to-end security for its employees' communications.
Additionally, via StrongA, SIM 901 enforces employee strong authentication with minimal impact on the workflow.

SIM 901 is available for employees traveling to more than 100 destinations.

The global private cellular network offered with Transatel's SIM 901, combined with employee strong authentication, ensures end-to-end protection for corporate data assets.



CONTACT US

info.901@transatel.com
www.transatel-sim901.com