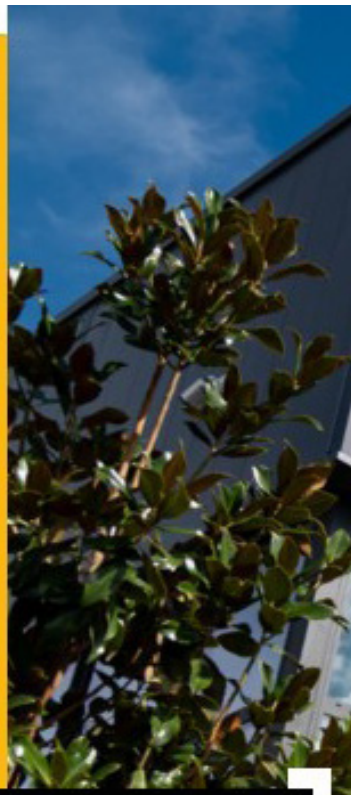
KNOWLEDGE PARTNER

ENSURING HIGH SECURITY AND FRICTIONLESS USER EXPERIENCES

Vincent Dupart, CEO, STid assesses the variety of threats that users are facing and how this is impacting security needs and requirements



The access control market is taking a decisive turn towards a contactless and frictionless user experience. Today, more than ever, security and access control systems need to be flawless.

As a matter of fact, the IT infrastructures of both large and small organisations are increasingly subject to attacks. And, these attacks occur both in physical and digital realities. For example, an ill-intentioned person, with physical access to the corporate server room or even just a workstation connected to the network, can often easily gain access to critical IT systems.

If this happens, the consequences can be disastrous and the complete infrastructure may be taken hostage or made inaccessible, thus impacting all business processes and endangering the continuity of the organisation. The loss or theft of sensitive or confidential data may also have serious financial implications or result in damage to the reputation of the company.

Securing the corporate IT infrastructure and systems should not only be about information security, however; the physical security of IT facilities and also any physical access points to the network should be an integral part of your security planning and policies.

High security? Yes, but what else?

STid has managed to combine two seemingly paradoxical requirements in access control solutions: ensuring a level of physical security that protects against cyber-threats while offering a seamless user experience by removing traditional identification technology constraints.

We design and manufacture contactless identification systems and solutions for physical security, logical access control and automatic vehicle identification. For STid, high security is not a vogue concept: our solutions were designed, developed and produced with this in mind.

Optimising the user experience should of course not imply compromising security. Our main strength is our capacity to offer comprehensive and uniform end-to-end security. End-to-

"The physical security of IT facilities and also any physical access points to the network should be an integral part of your security planning and policies."

ARTICLE

ENSURING HIGH SECURITY AND FRICTIONLESS USER EXPERIENCES

ISJ - Issue 39

May 2022

end security principles are applied to communication between the card and the reader (with MIFARE DESFire EV2/EV3 technologies) and also between the reader and the controller/LPU with systems capable of supporting OSDP™ and SSCP® (Secure & Smart Communication Protocol) protocols.

Security departments have become aware of the importance of selecting and deploying trusted technologies that offer certified and interoperable security. The SSCP protocol, certified by French Cyber Security Authority (ANSSI), is synonymous with freedom, interoperability and responsiveness to threats.

Indeed, STid is a firm believer in the concept of open technologies. We help organisations to depend less on proprietary technology and remain in full control of all components in their security chain. Our customers are not locked into a solution or tied down by proprietary technologies. This approach benefits both our customers and partners.

When technology makes the everyday life of people easier

Users are more likely to adopt simple and effective systems. At STid, we develop solutions to make the everyday life of people easier while safeguarding effective data protection.

STid readers and solutions are compatible with all access control systems currently available. The modular setup of STid's unique readers futureproofs the infrastructure of end users and it allows partners to offer enhanced levels of security to their clients, even when their secured estates grow or when their requirements change.

The two ranges of STid Architect and STid SPECTRE nano readers are both multi-technology and capable to read both physical and virtual credentials through the compatibility with STid Mobile ID®, our solution to allow the use and management of virtual access control cards.

Take a look, for example, at the Architect RFID, NFC and Bluetooth® reader with built-in QR code module.

ARTICLE

ENSURING HIGH SECURITY AND FRICTIONLESS USER EXPERIENCES

ISJ - Issue 39 May 2022

Access control systems that support the use of QR codes to identify people offer a cost-effective and reliable solution for visitor management within an office or other facility.

QR Codes can be generated by existing systems/software and used in a paper format or they can be transferred to the smartphone (by email, virtual cards, etc.). Numerous deployments have proven that QR codes are an effective and relatively secure way to offer temporary access privileges to visitors, contractors, drivers and suppliers. A new opportunity to identify and trace the whereabouts of these temporary guests throughout the public zones of your secured facilities!

Offering a virtual access card management solution without recurring fees

STid Mobile ID is a perfect example of a technology that makes the everyday life of people easier. STid Mobile ID is an innovative virtual card management solution. The smartphone, our valuable personal device, becomes the access control key, resulting in improved operational effectiveness, flexibility and instinctiveness.

With STid Mobile ID, users can carry their virtual access cards on their smartphone using a free app whilst also benefiting from experiencing being identified in various ways, without any compromise on usability or security. Six different instinctive modes of identification and user interaction are supported.

The STid Mobile ID platform also consists of an easy-to-use and powerful administrative portal, which puts our clients back in control of security management. You can deploy hundreds of cards in one mouse-click! The system can be deployed as a cloud-based solution (hosted by STid) or it can be installed on-premises by the customers that require it.

But, above all, STid Mobile ID is based on a unique business model that sets this solution apart from any other virtual card management solutions. The use of STid Mobile ID virtual badges does not require any subscription. Customers only pay a fee when virtual cards are issued. Moreover, when virtual cards are revoked, we allow our customer to re-issue these virtual cards to other users, without any additional cost. Virtual cards can be re-used without limitation.

That is why the total cost of ownership of STid Mobile ID virtual cards is much lower than that of any other security identifier, whether in physical or virtual form. Once obtained, a STid Mobile ID virtual card can be used as long as you want, without hidden fees. You pay for it once and it remains your property. There are no recurring costs and virtual cards cannot be lost or broken. In addition, STid also makes sure there is not any

ARTICLE

ENSURING HIGH SECURITY AND FRICTIONLESS USER EXPERIENCES

ISJ - Issue 39

May 2022

compromise on the quality of service or the level of security.

STid Mobile ID badges are also now used for much more than access control. We have collaborated with many customers and partners who have integrated STid Mobile ID into their access control, identity management, smart building, printing, leisure and event subscription solutions. The ecosystem has expanded so much that the solution is considered the unofficial standard for virtual cards.

Combining vehicle and driver identification

One of the priorities for companies that manage a fleet of vehicles is to ensure that only registered vehicles with authorised drivers can access a parking lot. Whether it is to avoid the occupancy of limited parking space by unauthorised vehicles, malicious acts (theft, damage) or the abandoning of vehicles – parking access control is essential to securing a building. Contactless technologies offer new possibilities to streamline parking access and protect corporate assets.

Security managers often have to combine two challenges in their policies: Securing access to car parks while ensuring a smooth traffic flow. Addressing both these challenges is essential because statistics show that seven out of ten employees use their car to get to work; this fact emphasises the importance of providing new solutions to simplify user mobility and secure parking access.

Contactless technologies offer new possibilities to make accessing the car park more instinctive and secure. How? By deploying technologies that enable the automatic identification of a vehicle and/or its driver. Ultimately, vehicle access control should be equally instinctive as the secure identification of people.

STid offers a full range of passive UHF readers and battery-less tags which are maintenance-free with an unlimited lifespan. These readers and tags support the identification of vehicles and/or their drivers without the need to roll down a window or get out of the car.

In addition to our successful SPECTRE reader for UHF tags, we are now launching the SPECTRE nano; its ultra-compact size, robustness and technological innovations offer new perspectives for vehicle access control. SPECTRE nano combines Bluetooth and UHF technologies for dual identification. The system supports single lane vehicle access (up to 6m) for employee cars and visitors can access with a badge or even their smartphone because of the integration of the STid Mobile ID ecosystem.

When we talk about the identification of vehicles and of people, we should not focus exclusively on technology. To deploy a successful installation, we first need to understand the processes, identify the added value of technologies that we consider using and calculate the return on investment of the optional scenarios.

If we really analyse the needs and requirements properly and if we are able to work closely together with the teams involved in the project, we will be able to implement an identification solution with greater freedom of movement and high security levels.

VEHICLE IDENTIFICATION: SUCCESSFUL DEPLOYMENT AT MONTCLAIR STATE UNIVERSITY, US

Montclair State University (MSU), a suburban campus located 12 miles from New York City, has upgraded its vehicle access control system with STid's identification solutions.

MSU needed to upgrade its old access control system. The University decided to address the main gate entrance first. Delays when entering through this gate can cause undesirable ripple effects, like professors and students being late for class, meetings and other activities. Flawless security combined with a frictionless user experience was required and expected – the essence of STid's knowhow.

This project involved approximately 200 tags to be mounted on vehicles and a number of readers at the main campus gate. When an authorised driver approaches the car park entrance, the vehicle is automatically detected and identified.

A high security UHF tag – a TeleTag – is fitted onto the driver's windscreen; the fully passive TeleTag has a virtually unlimited lifespan with invariable performance levels and offers a high level of security, a rapid return on investment and requires no further maintenance once installed.

ARTICLE

ENSURING HIGH SECURITY AND FRICTIONLESS USER EXPERIENCES

ISJ - Issue 39 May 2022