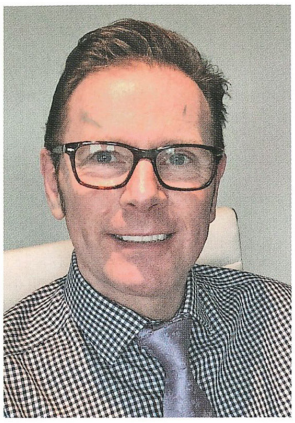
Spotlight feature on:

STid

An important milestone for access and security

Vincent Dupart



Gordon Mackay

STid's Architect Blue series, the world's most awarded access control readers, have been certified to meet the Security Industry Association (SIA) Open Supervised Device Protocol (OSDP) standard for access control and security.

STid's readers also support the European SSCP standard. In this interview Vincent Dupart, STid's CEO and Gordon Mackay, UK & Ireland Sales Director discuss STid's growth and the key importance of OSDP and SSCP certification.

Why is it important to be certified against the Security Industry Association (SIA) OSDP standard?

Gordon Mackay: STid's Architect readers have supported the OSDP standard for several years. With our current growth in all strategic business areas, particularly in the United States, it was important that our readers were tested and verified to meet the SIA OSDP communications and interoperability standard for access control security. OSDP certification for our Architect Blue range is an important milestone for us to be able to continue offering industry leading, high-security access control solutions. Having the readers verified was also crucial because clients requested it and we always evolve with the needs and requirements of our customer! STid has the widest range of OSDP verified readers on the market today!

STid registered record growth. Can you tell us more?

Vincent Dupart: After an exceptional year 2021, we are now entering a new stage in our strategic development. Being a European leader in contactless identification technologies already, STid is now planning to structure its corporate activities around a growth plan that is aimed at further international expansion. The challenges that our teams have undertook during the most delicate moments of the health crisis, show our ability to convert difficulties into opportunities. We made the strategic decision to position our supply chain in France to minimise supply times significantly and to ensure business continuity for our partners.

How do you explain this great international success of STid?

Gordon Mackay: One of STid's major strengths is our ability to respond simultaneously to two, seemingly contradictory, market demands: on one hand, security departments demand that access control applications meet the highest security levels and on the other hand, corporate security managers are expecting that employees are more willing to comply with new security policies when access control systems can be used instinctively. This significant investment in user-centric innovation, without compromising security, has resulted in the fact that many clients currently are in favour of STid's bespoke solutions. Importantly, we promote open technology. We guarantee organisations independence and autonomous management of their security. This freedom is vital for STid: our customers are not locked into a solution or tied down by proprietary technologies. This bold positioning entices and retains our customer-base.

End-to-end security

Another STid strength: our capacity to offer uniformed end-to-end security. We ensure impeccable end-to-end security between the card and the reader (with MIFARE DESFire EV2/EV3 technologies), and between the reader and the controller/LPU with systems capable of supporting OSDP and SSCP protocols.

Could you explain the specifics of SSCP Protocol?

Vincent Dupart: Powered by the SPAC European Alliance, the SSCP Protocol guarantees end-to-end security between physical and logical access control equipment. It allows integrity and confidentiality by the encryption of sensitive data. SSCP is the only certified protocol in France for the security industry. SSCP Protocol is based on certified security and transparent technology which delivers total customer independence and autonomy to their security management. The SSCP Protocol is agnostic of the interface: It can therefore secure much broader domains than access control, in particular for smart buildings or for demanding and sensitive industries. Based on European technologies, the SSCP protocol supports our aim for autonomy in terms of security. These key characteristics make SSCP the preferred industry standard for security departments. The current political situation in the world bears witness to the importance of fighting for an independent and independent Europe. The SSCP Protocol is a widely embraced because it is based on trusted and proven technology. Technology that is certified to provide interoperability. In turn, interoperability provides the customer with real and tangible freedom.

Open technology

Our success is direct result of our commitment to promote open technology. With STid, customers are not locked into a solution or tied down by proprietary technologies. As a result, customers now have full control of their security portfolio.

Press_05_2022_Professional_Secuirity_ARTICLE