

## **Kudelski launches IoT security for automotive and industrial based on STMicroelectronics connectivity and MCU technologies**

- The Kudelski IoT Security Platform Client is integrated with the ST4SIM-200M, an industrial-grade eSIM solution, and the STM32 MCU series
- The solution enables a wide range of security use cases for applications running on STM32 MCUs, including authentication, zero-touch on-boarding to multiple cloud platforms and token-based feature activation
- It is specifically adapted to the high-performance, high-security requirements of automotive and industrial IoT applications

**Cheseaux-sur-Lausanne, Switzerland, and Phoenix (AZ), USA, March 10<sup>th</sup>, 2020** – The Kudelski Group (SIX: KUD.S), the world leader in digital security, today announced the availability of its Kudelski IoT Security Platform integrated with ST4SIM eSIM solutions from STM Microelectronics. The integration creates a robust foundation for connected MCUs, such as STM32-based products, that is specifically adapted to the high functionality and security requirements for the industrial equipment and automotive manufacturer markets.

Gartner says 5.8 billion enterprise and automotive IoT devices will be in use next year<sup>1</sup>, with connected industry and cars being two of the key drivers for this 18% year-over-year growth. These devices provide critical data that creates cost savings for enterprises, and they enable innovative new features for automobile owners. Yet many equipment manufacturers still don't secure their devices by design, leaving their end customers with an unacceptable amount of risk to manage.

To enable new features and manage cyber-risks, Kudelski is integrating its Root of Trust application into ST's ST4SIM-200M industrial-grade eSIM solution, providing a robust foundation for the execution of any security use case. Combined with Kudelski's Security Client Library running on the STM32 MCU, IoT solution creators have access to a rich set of APIs that enable key security features like zero-touch provisioning, end-to-end data encryption, secure FOTA, remote attestation, secure storage and processing and device and command authentication.

"Companies building IoT devices need a strong, sustainable, end-to-end security strategy in order to protect their revenues and reputation, but integrating and using that security has to be simple," said Patrick Hauert, Vice President of IoT Security at Kudelski Group. "By working with ST to embed our technology at the core of their products, we are providing that simplicity and reduction of risk. We are also allowing manufacturers to securely enable new device features while preventing fraud, protecting the user experience from cyberattacks and giving the ability to use security as a competitive advantage."

"The Kudelski IoT Security Platform integrating our ST4SIM industrial-grade eSIM technology, together with the STM32 MCU, is well-designed and adapted to answer the increasing security requirements of industrial and automotive connected devices. It offers the first solution able to provide very high-end security features in combination with SIM connectivity." said Laurent Degauque, Marketing Director, Secure Microcontroller Division, STMicroelectronics.

---

<sup>1</sup> <https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io>

The Kudelski IoT Security Platform provides end-to-end protection from silicon to cloud for IoT devices, thereby securely and sustainably enabling new business models and operational efficiencies. It provides device security, data security, access management and active security to safeguard the entire product lifecycle. The Platform has already been adopted by communication service providers and consumer electronics, medical, asset tracking and industrial IoT partners and clients.

To watch a video demonstration of the ST/Kudelski solution, please click [here](#).

### **About the Kudelski Group**

The Kudelski Group (SIX: KUD.S) is a world leader in digital security and a provider of end-to-end convergent media solutions, including services and applications requiring access control and rights management to secure the revenue in digital television, internet, mobile and interactive applications. The Group also offers cybersecurity solutions and services focused on helping companies assess risks and vulnerabilities and protect their data and systems. It also supplies integrated solutions to manage access control of people and vehicles to sites and events. The Kudelski Group is headquartered in Cheseaux-sur-Lausanne, Switzerland and Phoenix (AZ), USA. For more information, please visit [www.nagra.com](http://www.nagra.com).

### **Media contacts**

Christopher Schouten  
Kudelski Group – IoT Security  
Head of Marketing  
+1 (480) 819-5781  
[christopher.schouten@nagra.com](mailto:christopher.schouten@nagra.com)

Cédric Alber  
Kudelski Group – Corporate Communications  
Director Media Relations  
+41 79 647 61 71  
+1 (415) 962-5005  
[cedric.alber@nagra.com](mailto:cedric.alber@nagra.com)