WISeKey's Security to Enable New Telehealth Applications

The ongoing Coronavirus disease (COVID-19) is a new illustration of how remote patient monitoring can change the efficiency and economics of modern healthcare systems. Protected Health Information is at the heart of telehealth concerns.

Geneva, Switzerland – March 6, 2020: WISeKey International Holding Ltd. ("WISeKey") (SIX: WIHN, NASDAQ: WKEY), a leading global cybersecurity and IoT company, announced today that it is partnering with global technology organizations to provide an extensive set of security bricks to bring cybersecurity into the area of modern telemedicine. Additional information about these partnerships will be announced at a later date.

In 2017, Foley Telemedicine and Digital Health Survey reported that in just three years the telehealth situation dramatically changed from 87 percent respondents not expecting their patients to use telemedicine to 75 percent having already implemented, or planning to implement, telemedicine services. This surging demand has multiple explanations. For personal convenience, health cost reduction or in case of contagious situation, patients are increasingly encouraged/advised to stay home. Remote patient monitoring (RPM) capabilities are instrumental in keeping Health Delivery Organizations (HDO) in touch with their patients.

As emphasized in the May 2019 National Cybersecurity Center of Excellence (NCCoE – part of the US National Institute of Standards and Technology [NIST]) and The MITRE Corporation description of a new project about Securing Telehealth Remote Patient Monitoring Ecosystem, cybersecurity concerns exist about having RPM equipment out of HDO secure environment. Both the US Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the more recent EU General Data Protection Regulation (GDPR) enforce the protection of private data by defining clear legal responsibilities, including in the telemedicine area.

"Over the last several years, WISeKey has been investing an average of more than 18% of its annual revenue to create a unique cybersecurity proposal from chip to cloud and therefore extend its recognized expertise in digital security to new boundaries," indicated Carlos Moreira, WISeKey's Founder and CEO. "New telehealth applications bring significant relief to patients. However, threats coming from possible cyberattacks exist that are not only about data privacy as this could be illustrated by the example of remotely controlled infusion pumps."

WISeKey has combined a complete set of technologies to guarantee health data integrity and confidentiality, whenever they are at rest or in transit from patients' home to HDO, following this possible RPM infrastructure:

- A secure element is added to the RPM device to protect the data at source and encrypt & digitally sign them over a Bluetooth Low Energy (BLE) connection to a local communication gateway. This secure element is either a certified WISeKey's **VaultIC407** added to the device microprocessor, or

a secure enclave of this microprocessor based on **WISeKey's proven security Intellectual Properties (IPs)**.

- Patients' drugs containers and other sensitive consumables are equipped with **NanoSealRT**, the WISeKey's NFC solution to provide any object with a communication channel for authentication, tracking or interactivity purpose.
- A local gateway connects all medical devices at home to the HDO server through a 5G network. Similarly to connected devices, the gateway contains a **VaultIC407** or **WISeKey's security IPs** to protect the local BLE network of medical devices and guarantee the health data integrity and confidentiality until the HDO server.
- WISeKey's **VaultiTrust** service for secure data generation and injection into secure elements is at the heart of this infrastructure. It provides any object with a strong digital identity.
- On the HDO server, patient's medical data are still managed under a consistent security scheme with **WISeKey's Public Key Infrastructure (PKI) based on the OISTE Foundation Root-Of-Trust**. **WISeKey's blockchain technology** is used whenever a secured distributed ledger must assure the ubiquitous availability of the data.

Want to know more about WISeKey's Security for Telehealth Applications? Please visit our website: https://www.wisekey.com/solutions/connected-security/.

About WISeKey

WISeKey (NASDAQ: WKEY; SIX Swiss Exchange: WIHN) is a leading global cybersecurity company currently deploying large scale digital identity ecosystems for people and objects using Blockchain, AI and IoT respecting the Human as the Fulcrum of the Internet. WISeKey microprocessors secure the pervasive computing shaping today's Internet of Everything. WISeKey IoT has an install base of over 1.5 billion microchips in virtually all IoT sectors (connected cars, smart cities, drones, agricultural sensors, anti-counterfeiting, smart lighting, servers, computers, mobile phones, crypto tokens etc.). WISeKey is uniquely positioned to be at the edge of IoT as our semiconductors produce a huge amount of Big Data that, when analyzed with Artificial Intelligence (AI), can help industrial applications to predict the failure of their equipment before it happens.

Our technology is Trusted by the OISTE/WISeKey's Swiss based cryptographic Root of Trust ("RoT") provides secure authentication and identification, in both physical and virtual environments, for the Internet of Things, Blockchain and Artificial Intelligence. The WISeKey RoT serves as a common trust anchor to ensure the integrity of online transactions among objects and between objects and people. For more information, visit www.wisekey.com.

Press and investor contacts:

WISeKey International Holding Ltd
Company Contact: Carlos Moreira
Chairman & CEO

WISeKey Investor Relations (US)
Contact: Lena Cati
The Equity Group Inc.

Tel: +41 22 594 3000
info@wisekey.com

Tel: +1 212 836-9611
lcati@equityny.com

Disclaimer:

This communication expressly or implicitly contains certain forward-looking statements concerning WISeKey International Holding Ltd and its business. Such statements involve certain known and unknown risks, uncertainties and other factors, which could cause the actual results, financial condition, performance or achievements of WISeKey International Holding Ltd to be materially different from any future results, performance or achievements expressed or implied by such forward-looking statements. WISeKey International Holding Ltd is providing this communication as of this date and does not undertake to update any forward-looking statements contained herein as a result of new information, future events or otherwise.

This press release does not constitute an offer to sell, or a solicitation of an offer to buy, any securities, and it does not constitute an offering prospectus within the meaning of article 652a or article 1156 of the Swiss Code of Obligations or a listing prospectus within the meaning of the listing rules of the SIX Swiss Exchange. Investors must rely on their own evaluation of WISeKey and its securities, including the merits and risks involved. Nothing contained herein is, or shall be relied on as, a promise or representation as to the future performance of WISeKey.