Kings are able to protect their possessions

by **Mário Púš**, CEO, Patrol Slovakia, s. r. o.

The adoption of efficient contactless technologies is growing and will be used by everybody in the future. People have started using contactless payment cards, smart cards, biometric identity cards, and passports that use RFID (Radio Frequency Identification) technology at a frequency of 13.56 MHz.

A typical user of contactless technology is not aware of the risk of possible theft. These technologies usually have lower rates of security which makes casual or accurate directional data retrieval and subsequent misuse straightforward. Criminals now possess equipment with sensitive antennas and sophisticated software that can read RFID cards and NFC (Near Field Communication) from a distance much greater than four centimeters (indicated in the specification of commonly used equipment). However, this information is overlooked or ignored by the average person, as if it did not concern them. But the fact is that anyone who has a phone with NFC can download an app which can read data from credit or debit cards stored in your wallet.

RFID Technology works on a relatively simple principle. A RFID card, sticker or other passive device sends its identification data when it is close to a sensor. Uses include attendance systems, immobilizers for cars, chipped animals, etc. Contactless card systems at a frequency of 13.56 MHz typically have a range of up to one meter. This is determined by the type of chip and reader antenna. A passive RFID device can be read at a distance of eight meters under optimal conditions.

NFC technology allows two electronic devices to communicate if they are very close to each other, for example, a credit card with a terminal or a mobile phone and an ATM, etc. Devices can exchange information or data in both directions. This technology uses the 13.56 MHz frequency band. The transfer is undertaken using inductive coupling, so it only works when the devices are in close proximity, within their mutual magnetic field. Transfer rates of 100 to 500 kbit/s allow small files to be transferred quickly. Communication takes place in only one direction at a time. This makes NFC terminals safer, as they only communicate with one client device at a time.

Thieves, hackers and cyber-criminals are already using electronic devices such as sophisticated RFID readers with antenna, RFID devices used in retail stores and mobile phones with NFC that can read sensitive data from cards in seconds. This data can then be sold on the black market, used to steal money from an account or make online purchases, for car rental, fraudulent contracts, and other criminal activities.

Most everyday users are unaware of the risk of unauthorized reading and possible falsification of data. Some technologies secure information using stored access keys or different encryption technologies. However, there have already been cases where inadequate physical security of the access keys has bypassed this security. There are also many different applications available for smartphones; you need only go to an app store and search for "credit card reader".

It is also possible to make a mistake when paying. When a customer has more than one card, which are kept together, a payment terminal receives payment from the first contactless card which responds to the transmitted signal. This means that if you use two different smart contactless cards, which are both in the same wallet, payment could be made from the wrong card. This could also happen when the other card or wallet is too close to the payment terminal you are using.

Given the current rate of technological progress, it is very likely, and predicted by banks and government agencies, that all cards and passports will be contactless in the near future. Therefore, the risk of not only financial but also identity data theft – personal data, PIN, address, credit details, etc. and their possible abuse will increase enormously.

The PS Shield card was developed to protect against this kind of data theft. It is a product for the future that offers continuous protection of contactless cards and biometric passports (introduced to the market by Patrol Slovakia, s.r.o – hence the name PS Card). It is easy to use, inserting the shield card next to a contactless cards blocks unwanted data reading. According to the manufacturer, it provides protection by shielding 98% of transmissions. In practice, this means it protects up to three contactless cards simultaneously. The card uses a shield with taffeta fabric, which has very good conductivity, so it absorbs and reflects high-frequency signals. The card can be used in wallets to block possible RFID transmissions of contactless payment cards in your wallet. The card was developed by a British security firm and is patented in many countries. Patrol Slovakia already offers PS Shield cards to entrepreneurs and businesses under the new EU regulation 25/05/2018 related to GDPR.