Secure UHF Access Control Deployed in Moscow

Government and private-sector employees both use a secure parking area at Russia’s Moscow International Business Center (MIBC), one of the world’s largest business district projects, commonly known as Moscow-City. This year, the operator of that parking area deployed a UHF RFID system that provides secure entry to authorized vehicles at a greater distance, and thus more efficiently than close-proximity technologies.

The UHF system comes with security features intended to prevent the hacking of data. The solution was provided by technology company ISBC, using FEIG Electronic’s LRU 1002 RFID readers and a built-in NXP UCODE DNA chip that leverages an untraceable command. The parking operator has asked to remain unnamed.

The MIBC, a commercial development first conceived in 1992, is still under development. Initially, it was a riverfront industrial zone and a rock quarry populated by closed
factories and abandoned buildings. Now, following revitalization, between 250,000 and 300,000 people work and/or live in the area, which features skyscrapers for offices, residences, stores and entertainment venues. Construction for the tallest skyscraper, known as One Tower, began this year; once it’s finished, the structure will stand 403.5 meters (1,324 feet) in height, making it one of the tallest buildings in Europe.

Recently, the parking area operator sought a way to not only boost the efficiency of its automated access system, but also provide the tightest security possible, according to Roman Podprugin, the head of ISBC Group’s RFID sales department. The site had used a MIFARE system at its entry gates in the past, requiring drivers to carry a card that was then scanned as they entered. This meant they would have to open their window, insert the card into the machine or place it against a reader and wait for the responding approval and opening of the barrier.

Another technology it had trialed was based on camera images of license places, but clear images could not be guaranteed if snow or mud obscured the plate. Therefore, the company began working with ISBC to create a secure but faster solution using longer-range technology. One requirement for such a system, Podprugin says, was that “UHF equipment must support secure data transfer technology,” which was possible with FEIG readers using tags embedded with UCODE DNA chips featuring AES 128-bit encryption.

The benefit of UHF transmissions is that the long range enables gate readers to authenticate a driver before a vehicle comes to a complete stop; however, that long range also allows the potential for hacking from a nearby reader device. Using the UCODE DNA chip in untraceable mode ensures that the transponder in the card will not respond to an unauthorized reader, essentially making the transponder immune to a hacker’s attack, explains Mike Hrabina, FEIG’s global product
manager.

Each tag comes with a UCODE DNA Gen2V2 chip, as well as a unique ID number and an encryption key that requires a reader with a matching key. “If a hacker’s going to attempt to make an attack,” Hrabina says, “the first thing they have to do is find the tag, but with this implementation the tag doesn’t talk unless it’s interrogated by an authorized reader with a matching encryption key.” The reader sends an encrypted challenge that the tag must decrypt and send back to the reader. If the tag is unable to decrypt the challenge it remains silent, thus providing another level of security since no key can be used twice.

Not long ago, Hrabina says, systems integrators had to choose between having a long read range or data protection provided by cryptography. As a result, he says, “Whenever security became the primary purpose of the system, integrators were limited to using a short-range reader.” That changed with the Gen2V2 protocol for UHF technology, which enabled untraceable commands. To employ this feature, FEIG has built an encryption key into each reader, and that key is stored in a protected area on the device’s secure element (SE).

The company already has experience with similar highly secure applications, Hrabina notes, since it provides readers for payment terminals. The encryption key in the SE is protected from any tampering; if a reader detects a tamper effort, it will automatically destroy the key. FEIG’s injection of keys into the reader is a secure process as well, Hrabina explains. Numerous individuals audit the process to ensure it is carried out properly. When placed in the untraceable mode, the UCODE DNA chip will only respond with encrypted data to the appropriate readers.

Not all who utilize the parking lot are utilizing the new UHF system, Podprugin notes. Those who are using UHF must first
acquire a tag, which can be affixed to their vehicle’s windshield. Thus far, approximately 2,000 tags have been provided for this purpose. Some gates are equipped with FEIG readers. Although Podprugin declines to specify the number of readers deployed onsite, he says the reader and barriers totaled more than 20 pieces.

The unique ID encoded on each tag is linked in the software to a specific individual authorized to access the parking lot. As he or she approaches the gate, the gate reader captures a transmission from that tag. “The label data is transferred to the software,” Podprugin says, which determines if the individual is authorized or prohibited to enter. If the driver is authorized, the software will issue a prompt to the gate to open the barrier.

ISBC’s solution captures tag reads and forwards that information to the operator’s software, which can then accomplish other functions, such as maintaining statistics regarding entrance and exit traffic related to the date and time each vehicle came and went, as well as at which specific control point this occurred. Additionally, Podprugin says, the parking company can adjust the tags’ read range by changing the power setting of the RFID module in the FEIG reader.