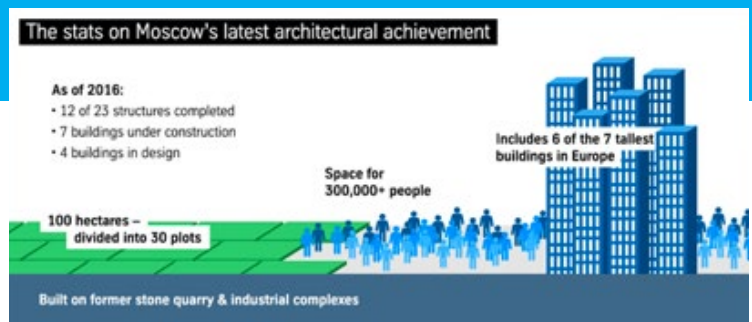FEIG
ELECTRONIC

SKYSCRAPERS IN MOSCOW STREAMLINE PARKING ACCESS WITH SECURE UCODE DNA RFID TAGS

FEIG
ELECTRONIC

Established in 1992 and still under development, Moscow International Business Center, also known as Moscow City, is the revitalization and transformation of an industrial riverfront into a new, modern, vibrant and upscale business and residential district. A mix of residential, hotel, office, retail and entertainment facilities, it is located approximately four kilometers west of Red Square along the Moskva River. Twelve of the twenty-three planned facilities have already been completed. Seven are currently under construction and four are in the design stage. Six skyscrapers soar to a height of 300 meters or more. Europe's tallest building, rising more than 100 stories to 373.7 meters, Federation Tower is located here; a must-

see point of interest for visitors to admire the beauty of Moscow from the observation decks.

Upwards of 300,000 people live, work, and visit here on any given day. Responding to the growth and popularity of the area, new highways and interchanges have been built to connect the complex to Moscow's major thoroughfares. Two metro rail lines with three station stops also serve this area and a pedestrian bridge over the Moskva River connects to the urban center.

The stats on Moscow's latest architectural achievement

As of 2016:
- 12 of 23 structures completed
- 7 buildings under construction
- 4 buildings in design

Includes 6 of the 7 tallest buildings in Europe

Space for 300,000+ people

100 hectares – divided into 30 plots

Built on former stone quarry & industrial complexes

Moscow City

Visually obvious is the stylish, appealing modern architecture, while hidden from view are the embedded smart technologies that transparently provide convenience and security to the commercial businesses, government ministries, residents, and visitors of the district. One of these technologies is RFID, a wireless, contactless identification technology used to authorize vehicle entry into areas reserved for private residential use or corporate tenants, and made

available for temporary, fee-based visitor parking.

The primary function of any access control system is to prevent unauthorized entry, limiting access to only those authorized to enter. Around the world, secure corporate and government facilities, private member-only clubs, exclusive residential communities, valet and fee-based public parking areas rely on physical barriers to restrict entry. Much thought is given to

the design, installation, systems and software that operate these barriers. Yet ironically, the majority of controlled access installations use the most basic, insecure, and often compromised or easily hacked methods to grant access.

Moscow City chose long-range UHF RFID, recognizing the shortfalls inherent in every other automatic identification technique used to authenticate a user in access control systems. It is understood

> Underscoring NXP's innovation and leadership in developing advanced RAIN RFID technologies, our UCODE DNA was chosen to be incorporated into Feig's and ISBC's implementation of the contactless identification system for vehicles entering the prestigious Moscow City," said Mahdi Mekic, marketing director for RAIN RFID with NXP Semiconductors. "This exciting project represents yet another successful deployment of NXP's contactless portfolio, and showcases our continued ability to meet the high security requirements of highly demanding applications without compromising user convenience.

NXP

that keypad PINs are often innocently shared with friends and guests in residential communities. It is generally known that unsecured radio transmitter signals can be sniffed, decoded, and retransmitted. Optical identification technologies that read license plates or barcode tags placed on the window of authorized vehicles can be simply photographed as they exit a facility, then inexpensively reproduced to obtain subsequent access. None are truly secure, each can be easily defeated, and all are inferior to the security and performance of RFID.

However, MIBC not only selected long-range, passive UHF RFID to implement in its controlled parking areas, it also chose to implement UCODE DNA, the highest form of secure RFID technology.

UCODE DNA is based on International Standards. It uses the GS1, UHF RFID, Generation 2 Version 2 air protocol and ISO/IEC 29167-10 for proof of origin based on AES (Advanced Encryption Standard). In addition to all the UHF RFID GEN2 features, such as Serialized TID, EPC memory, Kill tag commands and Access Password, UCODE DNA adds Privacy Protection, BlockPermalock and two, 128bit AES keys plus an AES digital core for crypto authentication along with a Trust Provisioning service available through NXP.

UCODE DNA is considered the only identification technology to match the physical protection of a barrier with the cybersecurity necessary to truly protect entrances from unauthorized access. The long-range capability of UHF RFID also provides user convenience in terms of speed. Vehicles do not have to come to a complete stop. The authentication takes place in milliseconds as the vehicle approaches and the barrier quickly opens to allow passage. Drivers are not required to stop and open a window to present a credential to a card reader. The data capture is immediate, reliable, and transparent.

ISC.LRU1002 UHF LONG RANGE READER

The most significant advantage of UCODE DNA for access control applications is its cryptographic authentication. The tag and reader must mutually authenticate to one another before data is wirelessly transmitted. Because of this mutual authentication, the protocol and data exchange only occurs between authorized equipment. The UCODE DNA tag remains silent to queries issued by a reader that fails the secure channel algorithm. One cannot hack that which cannot be seen. On top of this, the data exchange is unique with each transaction. Even if a bad actor were to sniff the protocol, the transmission is only good for that single exchange of information; thereby making an attempt at retransmission not only ineffective but also easily detectable. This is the same technique that is used in the most sensitive and secure data communication networks.

Each RFID tag is unique; incorporating a factory-programmed Transponder Identifier (TID) placed in a Read-Only Memory (ROM) partition that cannot be modified. The tag includes a separate memory partition for data storage. This read/write memory area is flexible in its use. It may be freely written to, modified, password-protected, and temporarily or permanently locked based on user preference.

" "UCODE DNA is considered the only identification technology to match the physical protection of a barrier with the cybersecurity necessary to truly protect entrances from unauthorized access", said Manuel Haertlé, senior product manager for FEIG ELECTRONIC. "Also well known as a contactless payment technology company, FEIG transfers a lot of security know-how from its payment terminals which are fully certified according to the latest versions of various high-class security standards into their RFID system. For example, FEIG vehicle access control RFID readers incorporate secure key storage elements and can support methods for secure key injection." "

As a wireless technology, RFID also allows the greatest flexibility for tag placement. It can be placed within the vehicle as a windshield sticker that permanently deactivates upon removal. It can be discretely placed inside the headlamp, hung from a rearview mirror, or placed on the dashboard as a visible, temporary pass.

In addition to the freedom of tag placement, a UCODE DNA tag allows the most flexible choice as to how it is deployed while also having the ability to be easily changed as future demands as new requirements present themselves. For example, the initial MIBC deployment utilized a password feature before the system was advanced to using full cryptographic encryption.

Not every RFID reader is capable of key handling or has a secure, tamper protected element to safely store encryption keys and detect fraudulent attempts to access the system. Further, not all manufacturers have the capability to securely provision encryption keys into the readers. FEIG ELECTRONIC, a manufacturer of RFID readers, payment terminals, sensors, and controls was found to be the exception. FEIG RFID readers incorporate secure key storage elements, a function brought into their RFID reading equipment from their Contactless Payment Division. Further, FEIG's Weilburg, Germany manufacturing facility is the only certified and audited secure facility that offers long-range RFID technology that is able to securely provision authentication keys into its devices.

Partnering with ISBC and deploying FEIG ELECTRONIC RFID solutions, Moscow International Business Center is delivering security and control access to its city center today and as it grows into a city of tomorrow.

"The most significant advantage of UCODE DNA for access control applications is its cryptographic authentication. The tag and the reader must go through an authentication procedure before the reader will accept the data from the tag, which is wirelessly transmitted, as trustworthy", said Andrey Krasovskiy, director of the RFID department at ISBC Group. "Because of this authentication requirement, only authorized equipment can be used to handle the secure protocol and the data exchange with the UCODE DNA based tag. The readers which do not possess the required cryptographic secrets query the tag practically in vain, because the tag's response cannot be interpreted or understood. On top of this, the data exchange in the authentication procedure is unique with each transaction. So even if a malicious actor were to sniff the communication, the transmission is only good for that single exchange, making the tag untraceable and most importantly protecting the tags unique identity from cloning. This kind of authentication technique is also used in the most sensitive and secure data communication networks."

FEIG
ELECTRONIC

VEHICLE ACCESS CONTROL

› Gated Communities
› Parking Access
› Controlled Perimeters
› Corporate Facilities

Main Plant and Headquarters in Germany

FEIG ELECTRONIC GmbH
Lange Strasse 4
35781 Weilburg, Germany
Phone: +49 6471 31090
Email: info@feig.de
www.feig.de

Headquarters in the USA

FEIG ELECTRONICS INC.
2220 Northmont Parkway, Suite 250
GA, 30096 Duluth, USA
Phone: +1 770 491 8060
Email: info@feig-electronics.com
www.feig-electronics.com

FEIG ELECTRONIC is a privately held manufacturing company with more than 50 years of experience and is diversified across many markets and applications including authentication, payment, ticketing and access to accurately and securely identify people, vehicles and assets. FEIG is a global supplier of RFID readers and antennas for all standard operating frequencies: LF (125kHz), HF (13.56MHz) and UHF (860-960 MHz).

FEIG
ELECTRONIC