ACCESS CONTROL 2020

TRENDS & TECHNOLOGY

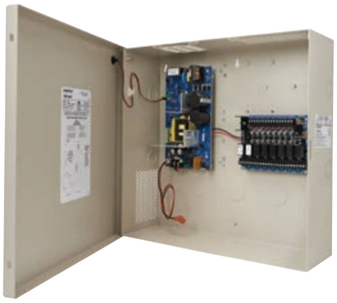
Supplement to Locksmith Ledger International, Security Business, Security Technology Executive

www.LocksmithLedger.com, www.SecurityInfoWatch.com

Access Control's New Normal

July/August 2020

ENDEAVOR BUSINESS MEDIA



YOU NEED
the Power Supply.

YOU NEED
the Electric Strike.

YOU NEED
the Stocking Door
Hardware Expert.

Everything you need to get the job done.

From our unmatched in-stock inventory of premium brands, to the unparalleled knowledge and experience of our technical sales team, we deliver the door hardware products and expertise you need.

SECURITY LOCK DISTRIBUTORS

SECLOCK.COM | 800-847-5625

ASSA ABLOY

ASSA ABLOY ELECTRONIC SECURITY HARDWARE
HES | Securitron

Request information: www.SecurityInfoWatch.com/10215009

TRINE
ACCESS TECHNOLOGY

4200CC-10B-32D

THE ONE BOX SOLUTION

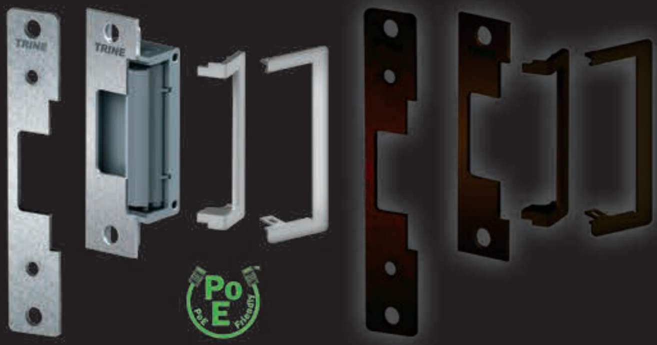
FOR CYLINDRICAL LOCKS & DEADLATCHES

- Two Finishes - One Box - NO Competition
- Door Sag – Tallest Latch – NO Problem
- Worth It – Compare Us – NO Match

Best Store Front Solution

4200CC7-10B-32D

Two 6-7/8" faceplates added
for deadlock conversions



SEE THESE STRIKES AND MORE @ TRINEONLINE.COM

Request information: www.SecurityInfoWatch.com/10215438

ACCESS CONTROL 2020
TRENDS & TECHNOLOGY

Advertisers' Index

Advertiser Name	Page	WebSite URL
Alarm Lock Systems, Inc.	S7	www.securityinfowatch.com/10212743
Altronix Corporation	S11	www.securityinfowatch.com/10212790
Banner Solutions	S33	www.securityinfowatch.com/12071932
Camden Door Controls	S29	www.securityinfowatch.com/10213140
Continental Access	S40	www.securityinfowatch.com/10213301
DKS DoorKing Systems	S39	www.securityinfowatch.com/10213482
dormakaba Group	S17	www.securityinfowatch.com/12304402
HID Global Corporation	S5	www.securityinfowatch.com/10213866
Marks USA	S13	www.securityinfowatch.com/10214311
ProDataKey	S31	www.securityinfowatch.com/12407119
SALTO Systems, Inc	S23	www.securityinfowatch.com/10225529
Security Lock Distributors	S2	www.securityinfowatch.com/10215009
Southern Lock & Supply Co.	S27	www.securityinfowatch.com/10215166
Speco Technologies	S20-S21	www.securityinfowatch.com/10215180
TownSteel, Inc.	S6	www.securityinfowatch.com/12361123
Trine Access	S3	www.securityinfowatch.com/10215438
UHS Hardware	S35	www.securityinfowatch.com/21143796
Viking Electronics	S37	www.securityinfowatch.com/10556843

ACCESS CONTROL 2020
TRENDS & TECHNOLOGY

PUBLISHED BY
ENDEAVOR BUSINESS MEDIA

1233 Janesville Ave
Fort Atkinson WI 53538
920-563-6388; 800-547-7377
Access Control – Trends & Technology 2020 is a supplement to *Locksmith Ledger, Security Business* and *Security Technology Executive* magazines.

EDITORIAL
Editorial director | Steve Lasky
Editor, *Locksmith Ledger* | Gale Johnson
Editor, *Security Business* | Paul Rothman
Editor, *Security Technology Executive* | Steve Lasky
Editor, SecurityInfoWatch.com | Joel Griffin

SALES
Group Publisher | Nancy Levenson-Brokamp
(847) 454-2702
nancy@securityinfowatch.com
Northeast US & East Canada
SB, STE, SecurityInfoWatch | Janice Welch
(224) 324-8508
janice@securityinfowatch.com
Midwest
Locksmith Ledger, SB, STE,
SecurityInfoWatch | Brian Lowy
(847) 454-2724
brlowy@endeavorb2b.com
Western US & Western Canada
***SB, STE,* SecurityInfoWatch** | Bobbie Ferraro
310-800-5252
bobbie@securityinfowatch.com
Display/classified | Kristy Dziukala
(920) 568-8324
kdziukala@endeavorb2b.com

PRODUCTION
Production Manager | Jane Pothlanski
jpothlanski@endeavorb2b.com
Audience Development Manager | Courtney Wethal
cwethal@endeavorb2b.com
Art Director | Bruce Zedler
bzedler@endeavorb2b.com

ENDEAVOR BUSINESS MEDIA, LLC
Chief Executive Officer | Chris Ferrell
Chief Revenue Officer/CMO | June Griffin
Chief Financial Officer | William Nurthen
Chief Operations Officer | Patrick Raines
Chief Technology Officer | Eric Kammerzelt
Chief Administrative and Legal Officer | Tracy Kane
EVP Key Accounts | Scott Bieda
EVP/Group Publisher | Lester Craft
EVP Special Projects | Kristine Russell

Subscription Customer Service
Toll-Free 877-382-9187; Local 847-559-7598
Circ.SecDealer@omeda.com

Article Reprints • Brett Petillo
Wright's Media 877-652-5295, ext. 118
bpetillo@wrightsmedia.com

HELLO SIGNO

The Signature Line of Readers from HID Global

Meet Signo at hidglobal.com/**signo**

HID

Powering **Trusted Identities**

Request information: www.SecurityInfoWatch.com/10213866

In Crisis Technology Mode

By Steve Lasky

It is not like we haven't dealt with a problematic virus prior to the COVID-19 specter appeared. Earlier this century it was the SARS outbreak that was predicted to explode across the globe in biblical proportions, but thankfully it failed to reach an epic scale. And just a decade ago the world stared down the outbreak of H1N1 that proved less of a threat than most experts expected. However, even the most jaded crisis manager and security professional couldn't have predicted the swiftness and voracity of the current pandemic and how it has dwarfed any previous global viral experience governments, businesses and organizations have ever encountered.

Undoubtedly, beyond the mounting death count and economic devastation, the most insidious aspect of this coronavirus pandemic has been an almost total alteration of daily life. From the way we interact with people, shop for our groceries, comfort our loved ones in hospitals or nursing homes to sending our children to school, everything has changed.

As school administrations contemplate how – or if – they will be able to open their schools come this fall, the one constant is it won't be business as usual. According to William Plante, a Senior Principal with ADT Commercial's Enterprise Security Risk Group, no planning he'd ever seen could adequately prepare the U.S. student population and workforce for what has been wrought by COVID-19.

"Much of the new workplace and classroom norm is a direct result of almost on-the-fly planning to mitigate virus exposure and to simultaneously support remote-based productivity and learning in this new reality. We're still in the midst of COVID-19, and the impacts on the workplace and campuses will create a new normal, even when we have an immunized population and a rigorous testing program available. We may have the perfect storm of three colliding phenomena that will forever impact the campus environment and security strategies," says Plante, citing the transformational design changes being created for campus spaces, the more streamlined security technology that accounts for user experience, and what he calls the COVID-19 maelstrom.

For Guy Grace, who serves as the Director of Security and Emergency Planning for Littleton Public Schools outside of Denver, it is all about adapting to the new normal.

"It is so important for schools right now to be working with other stakeholders. These stakeholders are designated school personnel with decision-making authority (with the collaboration of registered school nurses) should work with the local health department to coordinate steps for the upcoming school year. However, when we put in measures the end goal is always safety. The best safety is when it is holistically applied. Does it empower the students to learn, the teachers to teach and the community who has their love ones in the school to function the best that it can," explains Grace.

The bottom line is that the relationship between technology and its users will never be the same as it relates to the security industry. The crisis has created a new normal. ■

Easier Wireless Access Locking, *Your Style, Your Way*

- **Class-leading wireless access locks for every application** - *Lowest-maintenance, longest battery life, keyless access, multi-credentials, matching models inside & out*
- **Cost-saving, easily networked - No Panels, No PIMs** - Choose Networx® Ethernet, WiFi &/or POE Gateways & Extenders, each controlling over 60 locks
- **Wireless keyless access solutions for all doors,** from mortise, to narrow stile, to exit devices. Cylindricals simply retrofit standard locksets in about an hour.
- **Global or Local Management & Lockdown -** Networked to save staff labor from door-to-door operations & provide emergency solutions, via lock, keyfob or server, including Enterprise Integration in realtime, with top platforms, Continental, Lenel®, Software House®
- **ArchiTech Networx: Same proven Trilogy® electronics, but designer minimalist look, customizable** with hundreds of architectural finishes & Grade 1 Lock styles and various colors/shapes of multi-tech ID reader + Smart Mobile iLock® App
- **New! Security Manager App option, makes any smart phone a Virtual Enterprise Workstation;** control doors, users, threat levels, etc. (w/CA4K)

MORE AFFORDABLE
Lowest labor & equipment costs without sacrificing top conventional access features

CENTRALLY MANAGED
Auto-Schedule program updates, queries, or free access by time, by door & more

GLOBAL LOCKDOWN
or unlock in seconds from the server or any lock

EASY INSTALL
Replaces any door lock, on any door type, neatly, quickly

EASY NETWORK
No wires to run to doors. Uses customers' existing network or Ethernet & multi-lock (63 locks/gateway) gateways & opt'l repeaters

USERS
Supports thousands of PIN, ID or iLock App users. Easily local/remotely

networx
by ALARM LOCK

From the Makers of #1 Trilogy Locks

1.800.ALA.LOCK • www.alarmlock.com

Trilogy, Networx, ArchiTech, iLock, Continental & CA4K™ are trademarks of Alarm Lock, a Division of Napco. Other marks remain intellectual property of their respective cos.

Request information: www.SecurityInfoWatch.com/10212743

For Solid Access Control, Security Begins with

Enhanced card security is characterized by advanced technologies like biometrics, Bluetooth and mobile apps

By Jeffrey E. Barnhart

With the ease of set-up, use and management, card-based access control systems are the most secure way to give access to the right person at the right time.

Courtesy of BigStock.com – Copyright: StanciuC

Trust

Access control is an essential part of commercial security systems—keeping buildings, designated areas and sensitive information secure and safe by controlling entry or restricting access. With the wave or swipe of a card, authorized individuals can gain entry to an entire facility or secured zone through an entry point like a door, turnstile or gate. In an era of growing security concerns, governments, corporations and property managers must elevate the importance of a trusted identity while balancing the demand for convenient and efficient access.

The two primary types of access control are physical and logical. While physical access control limits access to buildings, rooms and spaces within a building, logical access control allows authorized and authenticated personnel access to resources, systems, directories, networks and files. Combining physical and logical access control delivers a higher level of security, granting companies the ability to limit and monitor access to sensitive data and physical locations.

Access cards are tied to a person's identity through a physical access control (PAC) system, which involves a two-step process that links a card to a person after the card has been printed. Some card personalization software systems can also connect to and update the PAC system after the card has been personalized. "Access control begins with a trusted identity, which validates the person who is entitled to the benefits associated with a credential," said Sebastian Tormos, Entrust Datacard's director of vertical marketing, who is an International Card Manufacturers Association (ICMA) member. First, a system identifies an individual. Then, his or her credentials are authenticated via a badge, smart card, password, mobile device, or biometric (i.e. fingerprint, facial recognition or iris pattern). Following authentication, access is granted.

Uncover Security Vulnerabilities with a Risk Assessment

Although digital technologies are transforming how identity is authenticated around the globe, a risk assessment and an application audit comprise the backbone of the security framework and are the first steps in determining vulnerabilities and which type of access control technology is needed. The goal of a risk assessment is to gain an understanding of the existing system and environment and then use the data to allocate mitigation resources to the areas that will significantly lower the enterprise's risk profile. When done well, the risk assessment will identify high impact areas, allowing the integrator and user to prioritize mitigation to vulnerable areas.

"Risk assessments are critical for end-user enterprises," said Kevin Freiburger, director of identity programs at Valid, who is an ICMA member. "They are often overlooked or are not allocated the proper resources by companies, which can lead to security vulnerabilities. It is recommended that end-user companies engage integrators from the industry to ensure a comprehensive risk assessment and audit of security applications." Not every integrator is equivalent in terms of experience and expertise, so the integrator of choice should itself be considered a potential risk. Therefore, it is important to lower the risk by performing due diligence and research on various companies and products within the industry. It is essential for companies to carefully vet vendors to ensure that they have all of the compliance credentials in building and deploying software and protective systems. "An experienced integrator is a valuable partner and a critical link throughout the risk assessment and audit," Freiburger added. "Having confidence in the integrator's ability to analyze assets, threats, and vulnerabilities to mitigate risk by deploying the proper solutions and technology to minimize security risks is paramount."

Recently, there have been several large-scale data breaches and that is what is driving security, giving information technology directors much of the power in purchasing decisions. "However, it isn't just about data breaches," Freiburger said. "It is about privacy issues and how the data will be used." Risks and vulnerabilities will arise; therefore, an organization must have a solid information security framework, which will enable a business to pivot and address new risks and vulnerabilities over time.

Technological advancements like the deployment of wireless technology, are enhancing access control.

Choose the 'Right' Card Technology

The top two factors in card technology choice for most businesses are budget and security. As companies realize the potential impact of a security breach, they are proactively taking measures to ensure employees and residents have access to applicable buildings, zones and entrances at the right time.

Technological advancements like the deployment of wireless technology, are enhancing access control.

"One type of card is not best for a specific application," Freiburger said. "There's choices and tradeoffs, especially with different types of cards, reader technologies and software vendors."

There are two categories of access control cards—nonsecure and secure—and both provide ways to monitor who is accessing resources or entering or exiting a building. A proximity (prox) card is the most common type of access card for commercial and residential buildings; however, it offers little security.

Typically, the size of a credit card, an access card usually lasts five to 10 years before it has to be replaced. However, many factors affect the durability and lifespan of the card, such as the type of card substrate and personalization techniques used, how the card is stored and if the card is resistant to chemicals, abrasion, moisture and ultraviolet light.

Although the three types of access control cards—proximity, magnetic stripe and smart—may look the same, the technologies driving them to vary significantly.

Prox cards, which use an older technology resulting in a low-security card, can be made of several different materials, as well as forms—cards, tags, or fobs—but they all work in the same way: by being held in close proximity to a card reader. The low-frequency 125kHz credential has an embedded antenna, which when in close proximity, such as a few inches to two feet—sends a signal from the card to the controller that grants or denies access.

Magnetic stripe cards work by swiping a magnetic stripe through a card reader like a credit card. They are one of the oldest forms of access cards and offer minimal security because they can be copied very easily. Magnetic stripe cards typically work as a single application card and are primarily used in low-security settings like for guest entry to a hotel room or for casino playing cards. Many companies are moving away from magnetic stripe cards and replacing them with prox cards.

The most recent advancement in the access control card market segment—smart cards—was developed with the goal of being hard to duplicate. Smart cards are more reliable than magnetic stripe and prox cards, and with an increasing demand for security solutions, growth is significant. The three types of smart cards—SEOS, MIFARE DESFire EV2, iCLASS SE—offer the most security, operating at 13.56Mhz (compared to a prox card that operates at 125kHz). Smart cards contain an embedded integrated circuit and are capable of writing data, as well as reading it, which allows the cards to store more information than traditional prox cards. Smart cards can also provide personal identification, authentication, data storage, application processing and can be combined with other card technologies for increased security.

Previously, smart cards were used primarily by the U.S. Department of Defense for logical access management and in higher education settings for student identification cards, but now there is widespread adoption in the electronic benefits transfer, health care and financial markets. "Smart cards are the best fit for commercial and residential building access because they provide greater security with an encrypted credential that must be decrypted by a reader," said Martin Hoff, Entrust Datacard's product marketing manager of hardware, who is an ICMA member. "It's much easier to spoof proximity and magnetic stripe cards." Although prox cards aren't as flexible as smart cards and don't offer multifunctionality like the ability to load payment purses and applications onto the card—a prox card does allow the user to be contactless.

"There's definitely an uptick in prox card use," Freiburger said. "We are seeing more interoperability, which does make a prox card more viable. For example, they can be used in multiple systems for logical and physical access control systems."

TROVE
MADE IN THE U.S.A.

Security is a top concern for both private and public entities; many industries are transitioning to smart cards. "Smart cards are the most secure type of access card and are used most often in government, health care and financial sectors, while proximity cards are commonly used in higher education and enterprise," Hoff added.

Control Access: From Keys to Cards

With the ease of set-up, use, and management, card-based access control systems are the most secure way to give access to the right person at the right time. Surprisingly, 20 years into this century, some businesses are still using traditional locks and keys for access. Although there is little need to use keys in today's interconnected world, keys still make sense in some use cases.

Keys may be the right choice if a company has a completely offline system or is located in a very remote area. In that instance, it may be difficult or expensive to implement a card-based access control system, especially if there is no internet connectivity. To be secure, an access control system needs to be updated, maintained and monitored and depending on the connectivity of a building or a system a physical key could make perfect sense. However, it is time-consuming and tedious to change locks and replace keys if they are lost, stolen, or misplaced. If an access card is lost, stolen or permissions need to be amended, an integrated card management system allows the administrator to easily turn off a card and then notify the other integrated systems to turn off physical access control as well as logical access.

"Access cards are encoded with a unique decimal number, which is linked to a user's record," said Howard Albrow, HID Global's NPI product line manager of PACS credentials, who is also an ICMA member. "Typically, an access control card does not contain any personally identifiable information, but through the system, it can link to a data record that may hold personally identifiable information."

Today, most buildings are using an integrated access control system.

> Card-based access control systems are the most secure way to give access to the right person at the right time.

Access Control Trends to Watch

Though access cards still play a powerful role in the access control market, some companies are turning toward smartphone Bluetooth-enabled and Near-field Communication (NFC) technology. Both are wireless technologies that give individuals frictionless access. The introduction of mobile credentials has the potential to revolutionize the access control industry, eliminating the need to carry and swipe a card. Instead, a phone's technology can be used to authenticate identity and grant entry. "There has been a tremendous uptick in the popularity of mobile credentials," said Albrow. "A mobile credential can be used via a smartphone to interact with an access control reader in the place of a physical card, which is more convenient, allows greater flexibility, improves privacy and can also lower the maintenance costs of credential management for end-users." However, when it comes to a trusted identity, physical cards will continue to play a valued role in securely granting or restricting access—especially in the health care and government sectors. The combination of a physical card with digital identity is powerful and provides multi-layered security. "There's definite growth in mobile," Freiburger added. "When it is used properly with an application for access control, security is incredible. Issuers want to meet their customers where they are and that is typically on a phone or on a cloud service."

Another major advancement in access control is the propagation of biometrics, a category of authentication that relies on unique biological characteristics to verify a user's identity.

Biometric identification is the only mode of authentication that can unequivocally validate a person's identity. It is on the rise with retinal eye scanners, fingerprint readers and facial recognition scanners becoming more common. In some cases, multiple methods of biometric identification are combined with the use of a card (or used in place of a card) for even greater security. Unlike prox cards, smart cards, or keys, biometric security cannot be transferred. A person must be physically present to gain physical or logical access. "The adoption of biometrics will be a continuum," Freiburger said. "Looking ahead to the next five or 10 years, growth will likely accelerate as the prices come down and biometric systems can be inexpensively deployed and upgraded." ■

About the author:

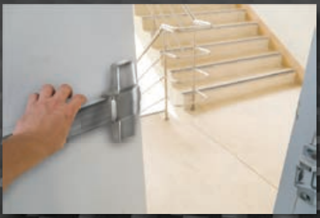
***Jeffrey E. Barnhart** is the founder and executive director of the International Card Manufacturers Association (ICMA). He can be reached at jbarnhart@icma.com*

Save up to 40% with Marks USA Exit Devices

Same Top Grade 1 Performance, For Life

M9900 Exit Devices, *Grade 1, also new Hurricane-Certified M9900H*

M8800 Narrow Stile Exit Devices *Grade 1 heavy-duty panic hardware for single & double doors*



Tough Enough for Any Application, But Easy on the Budget

- Money-saving, long-life exit solutions - Ideal for any Grade 1 Panic & Fire-listed hardware requirement, i.e., schools, hospitals, government & office buildings
- Marks USA Exit Devices now in Narrow-Stile, Standard &/or Hurricane-Certified Models – ***Compare to VD99 or 33A Series, Save up to 40%***
- Reliable control of all types of single & double-doors
- Easy installation & retrofits all popular preps
- Ultra-durable, heavy gauge extrusion; smooth case and low-profile minimizes catch hazards
- Panic Protector End Caps™ prevent breaking with flush mitered-steel design
- ANSI 156.3 (2001), Grade 1, 3-Hour fire rated dead latch bolts
- Marks Lifetime Mechanical Warranty

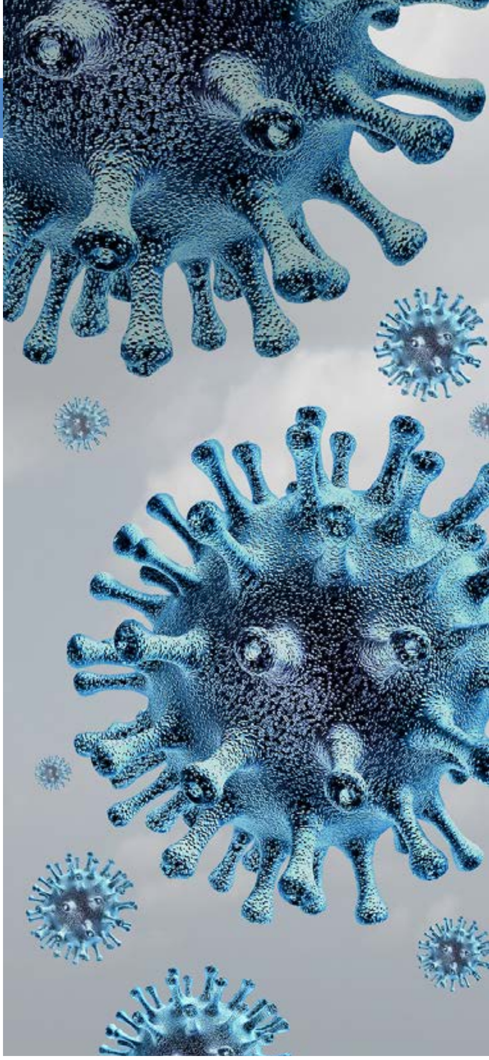
MARKSUSA

Contact your local Marks Sales Rep or Distributor today

1-800-645-9445 • salesinfo@marksusa.com • www.marksusa.com

LIFETIME WARRANTY MARKSUSA

Request information: www.SecurityInfoWatch.com/10214311



With a New School Year Comes a New Normal

Strategic safety and security protocols will mandate how schools implement security systems

By Steve Lasky

As school districts around the United States plan for the upcoming fall sessions, there is little doubt that it will not be business as usual. With some medical experts predicting the possibility of a major spike in the coronavirus around the country, especially in regions which opened with little regard for testing or following established CDC pandemic protocols, the potential for delayed or launches or staggered schedules looms as a reality.

That being said, most agree that there will be a school year whether it is shared with the brick and mortar facility and a version of on-line classes. Either way, the security strategies and the technologies used inside the school buildings figure to see some changes. From more intense monitoring of staff and student comings and goings, temperature scans and tracking to revamped approaches to access control and door hardware, the 2020 fall school year will certainly be unlike others before it.

In conjunction with dormakaba, one of the top three companies for access control and security solutions in the global market, and two of the industry's top security practitioners, the print and digital platforms of SecurityInfoWatch.com Security Group present a roundtable discussion of the "new normal" that might characterize the impending school year for K-12 students and staff and how administrators can work with vendors and integrators to keep the spread of COVID-19 at bay and maintain the safety of all concerned.

The two roundtable participants who joined Editorial Director Steve Lasky include Guy M. Grace and Jonathan Jones.

Grace has worked in the security field for 35 years. He currently serves as the Director of Security and Emergency Planning for Littleton Public Schools, a suburb of Denver, Colorado. He also serves as the Chairman of the Partner Alliance for Safer Schools (http://passk12.org/). Grace has been providing district security services and leadership to Littleton Public Schools (LPS) for 31 years. He is a recipient of many national and security industry awards and recognitions to include the Association of School Business Officials International Pinnacle award, Security Magazines Most Influential People in Security, The 2014 American Red Cross Century of Heroes award, the Security Industry Association (SIA) Insightful Practitioner Award, the NSCA 2019 Volunteer of the Year Award and the 2019 NCS4 Professional of the year award. Grace is a regular speaker at school safety trade conferences and a regular security media commentator for various trade magazines and media. Jones is the President of JL Jones Group. JL Jones Group is a manufacturer's representative agency located in the Rocky Mountain region providing support in Colorado, Utah, Wyoming, New Mexico, Idaho, and Montana. The JL Jones professional team is unique to the industry in that the firm takes a holistic approach with their construction projects with team members calling on distributors, contractors, wholesalers, integrators, end-users, and architectural design firms. The company represents

As school districts around the United States plan for the upcoming fall sessions, there is little doubt that it will not be business as usual.

Courtesy of BigStock.com – Copyright: digitalista

several prominent security and door hardware brands. Jones has 12 years of industry experience in various management and sales roles.

Steve Lasky – Given the current environment faced by security professionals as a result of the ongoing coronavirus threat, discuss some of the major access control trends that are either currently on the market or close to market that will address the "new normal" of electronic access control and/or door hardware devices.

Guy Grace – In a time of crisis we are reminded how important the Layers of Security and the Safety Security components are for schools. Leadership and coordination at the district level are integral to the successful development and adoption of school safety processes, plans, technologies and procedures and for ensuring these measures are updated for consistency with evolving best practices. Most school safety measures have district-wide components or responsibilities. It is critical for districts to understand the fundamental link between readiness for day-to-day emergencies and disaster preparedness.

School districts that are well prepared for individual emergencies involving students or staff members are more likely to be prepared for complex events like a community disaster we are dealing with now. Prevention, Mitigation, Response and Recovery should all be considered in all aspects of an emergency response plan. To me, a security system is one of the core tools we need to have a place for the all-hazard emergency responses in schools. District-wide physical security standards must be robust in a pandemic. The physical security standards of our district facilities must be strong during a pandemic. All facets of the systems must be kept up and running during the emergency. Criminal activity to facilities often increases when schools are unoccupied.

I believe that a major access control measure for the future is the deployment of Unified Security Systems by school districts. Unified Security and Life Safety Systems take safety and security components such as policies and procedures, people (roles and training), architectural, communication, access control, video surveillance and detection and alarms to deliver enhanced interoperability and ease of use. Unified Security and Life Safety Systems can overcome concerns with the integration of technology such as differences in functionality between different systems within the connected environment in which they reside in. A good Unified Security and Life Safety System will provide consistent functionality for all of the security components. A properly implemented Unified Security and Life Safety System will help with integrations of new components and allow a district to continue to evolve and expand and deal with many situations to include COVID-19.

Jonathan Jones – The need for touchless access points is driving a major shift to touchless readers and credentials. Readers that require a wave of the hand to open a door and credentials located on a personal phone. Both options have become more and more affordable and user friendly in the last few years. The current environment seems to finally be pushing these applications to the market at a much faster pace. From a mechanical door hardware perspective, it is all about copper-based materials and antimicrobial coatings that help minimize the transfer of germs.

Lasky – ***Because of the already tight budget situations almost every K-12 school districts find themselves, how can vendors and integrators work with end-user clients to create a strategic access control roadmap that integrates with other solutions, is proactive in its approach and can provide a cost-effective solution?***

Grace – I believe the budgets are even going to get tighter. When we look at the financial impact on our great country that has arisen with COVID 19 I am very worried. Typically, school districts often spend about one percent of their total operating budget on physical security and typically include manpower. Schools now will have to mitigate for COVID-19, and it is not going to be simple or inexpensive. The funding that was going to be utilized for other security measures likely may be diverted. However, school communities are going to have to realize that the other hazards that schools deal with every day that we put in place components to deal with are still going to be there when the buildings are occupied.

Guy Grace *currently serves as the Director of Security and Emergency Planning for Littleton Public Schools.*

It is my belief that security staff like myself should always work closely with our integrators and manufacturers. A properly implemented Unified Security and Life Safety System is something that is developed through strong partnerships between the district, integrators and the manufacturers. These partnerships certainly have helped me to deal with the challenges of finances and funding over the years.

Jones – As schools shift their budgets to products that keep their buildings clean, I think it is a matter of educating the districts on the options and cost-effective ways security can help accomplish this. A few of the current cost-effective trends we are seeing are foot pulls on restrooms, touchless readers where auto operators are used, copper adhesives on everything from exit devices to levers, and Healthy Hardware from companies like Trimco.

Lasky – ***From a practical standpoint, how do you see security playing a major role this fall as schools bring back staff and students, realizing that things like social-distancing, possible temperature-sensor applications, and more network infrastructure capacity figure to transform the traditional school experience from an open to a more closed environment?***

Grace – As for my experience security and emergency preparedness has a major role now and for the upcoming school years. When I read the question one of the most important measures a good security program can do is NOT make the school look like a fortress or a place that promotes fear by its measures that are designed to mitigate threats. It is so important for schools right now to be working with other stakeholders. These stakeholders have designated school personnel with decision-making authority (with the collaboration of registered school nurses) should work with the local health department to coordinate steps for the upcoming school year. However, when we put in measures the end goal is always safety. The best safety is when it is holistically applied. Does it empower the students to learn, the teachers to teach, and the community who has their love ones in the school to function the best that it can.

Jones – The openings in a school are one of the highest touchpoints in the building from the entry doors, to the classroom, to the gym, or cafeteria. Limiting the transfer of germs in these openings will be critical in the coming school year. Foot pulls, arm pulls, touchless readers, Bluetooth credentials, antimicrobial hardware, and copper-based products the security industry offers all help to limit the transfer of germs. These products have all been on the market for many years and you've seen the predominately used in the healthcare industry. Now with the current environment, we are in you're seeing them move into the education vertical.

Jonathan Jones *is the President of JL Jones Group, a manufacturer's representative agency.*

Lasky – ***As we move into the future, what course do you see access control technology taking as clients migrate to contact-less and more mobile technology applications?***

Grace – I believe the Unified Security and Life Safety Systems are the future of K-12 security. These systems can overcome concerns with the integration of technology such as differences in functionality between different systems within the connected environment in which they reside in. A good Unified Security and Life Safety System will provide consistent functionality for all of the security components. A properly implemented Unified Security and Life Safety System will help with integrations of new components and allow a district to continue to evolve and expand.

Jones – Access control has always played a large part in our education vertical by keeping students and faculty safe and secure. Now, with the market moving towards cleanliness and the security industry being at the cusp of that wave I think the industry will be looked to provide even more support than we previously did. The manufacturers who can innovate at high levels to bring touchless focused products to market at the fastest pace will ultimately dictate which way the technology goes and lead us to a cleaner future. ■

Touchless Access Solutions

Good for Hygiene. Good for You.

Low energy swing door operators

Touchless switches

Reduce the spread of germs in your facility.

Touchless door activation can make the difference when it comes to a clean, hygienic facility. Touchless access is crucial in high contact public places such as healthcare facilities, restaurants, schools, offices and restrooms. dormakaba offers many solutions to fit your needs for touchless access including touchless switches and low energy swing door operators. With touchless access, abuse-related replacement expenses are greatly reduced. Minimizing high frequency touchpoints contributes to healthier facilities (health, safety and security).

dormakaba.us/Touchless-LL

dormakaba

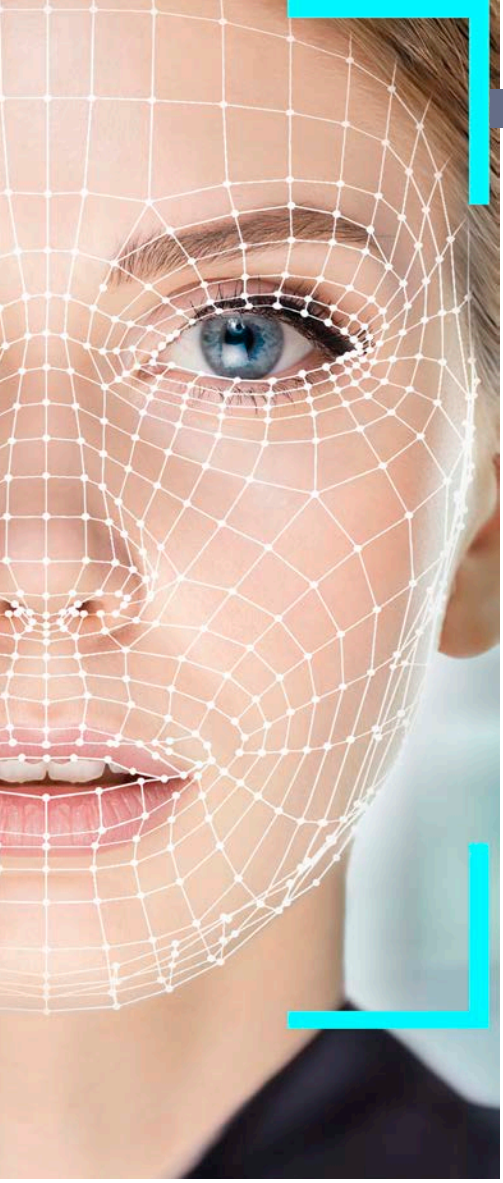
Request information: www.SecurityInfoWatch.com/12304402

The Role of Biometrics in a Post COVID-19 World

Experts say touchless modalities will likely grow while fingerprint, other touch-based solutions will see their use decline

By Joel Griffin

As lockdowns across the nation begin to lift and people start to return to some semblance of their routine daily lives in the wake of the coronavirus pandemic, nearly everyone agrees that the so-called "new normal" will look much different for businesses of all shapes and sizes. Security technology will also undoubtedly figure prominently among the solutions leveraged by organizations as they look to mitigate the spread of COVID-19.



Biometrics like facial recognition are integrating themselves into the fabric of a new approach to post-COVID-19 access control.

Courtesy of iStock / Getty Images Plus -- guvendemir

While thermal imaging and contact tracing technologies have garnered much of the attention in the early days of what has been a gradual reopening of the economy in some states, these solutions are but one part of what portends to be a fundamental shift in how companies think about and use security systems. Access control, which has always been the first and foremost consideration in any security environment, is also going to be significantly impacted by the lasting effects of the pandemic. This includes biometric entry devices, the adoption of which could be simultaneously helped and harmed over coronavirus concerns.

"There is a realization that things may not return to what they used to be and we may be in for designing and defining a new norm," says Shiraz Kapadia, CEO and President of Invixium, a maker of multi-modal biometric access control solutions.

However, according to Kapadia, the original drivers behind the adoption of biometrics, which was to replace traditional access control methodologies in favor of something (faces, fingerprints, etc.) that cannot be forgotten or stolen remain the same and will continue to advance their use in a wide variety of industries. "That aspect of biometrics is not going to change and, if anything, may even fast track adoption," he says.

Even before the pandemic, Mohammed Murad, Vice President of Global Sales and Business Development at Iris ID, a provider of iris recognition solutions, says that much of the market was already clamoring for contactless biometrics and that this will only serve to further increase that demand.

"We feel very strongly that under the circumstances now and previously, in the majority of cases, customers do want something that is non-contact, accurate and frictionless," Murad says, adding the contactless biometrics are going to play a crucial role in future access control applications.

John Calzaretta, President and Chief Revenue Officer of Sentry Enterprises, maker of the SentryCard which integrates fingerprint verification into a smart card for both physical and logical access, believes the adoption rate of biometrics in the enterprise market – many which already have experience with or have explored biometric solutions – are going to move more quickly to adopt touchless access products in the wake of COVID-19.

"I feel like the enterprise clients we're engaged with are moving five times faster now. Where before a non-communal biometric was intriguing to them, now they feel it is a must-have," he says.

While the SentryCard wasn't initially designed with hygiene in mind, Calzaretta says that it solves the problem of the communal biometric touchpoints in businesses as the only person who touches the biometric on the card is the user when they want to access a door or workstation.

"I don't think COVID per se impacted biometric adoption, I think it is just smarter security and was already recognized, but now post-COVID, it is how do you achieve those biometric goals without putting the health and safety of your employees at risk," he adds.

Vince Gaydarzhiev, Founder and CEO of Alcatraz, whose solution leverages a combination to facial recognition and artificial intelligence (AI) for access control, says that products that require physical touch are going to be phased out by many organizations moving forward and will likely not even be specified for most projects. "The importance of biometrics, especially those that don't require any (physical) interaction will be key in the future," he says.

Until recently, Gaydarzhiev says that the capabilities of touchless biometrics simply could not meet the requirements of many organizations but that has changed as the technology has progressed.

"The technology up until now just wasn't there. The experience was not there," he adds. "If you're talking about facial recognition or even a couple of other technologies on the biometrics side, it was either expensive or it took a while to process and you needed a lot of servers and infrastructure on the backend to support it. COVID-19 will put this more into perspective where cost is not going to be the main concern anymore, but it will be all about functionality and how to create a (safer) environment no matter the cost."

Will Fingerprint, Other Biometrics Still Have a Part to Play?

Although contactless biometrics will likely be the preferred modality for access control and other use cases in the future, Murad said that other technologies, such as fingerprint, vein pattern recognition and other solutions

speco technologies®
Giving You More.

MULTI-FACTOR AUTHENTICATION with Speco Technologies' NEW O2TML

2MP Temperature Reading Panel with Face and Mask Recognition

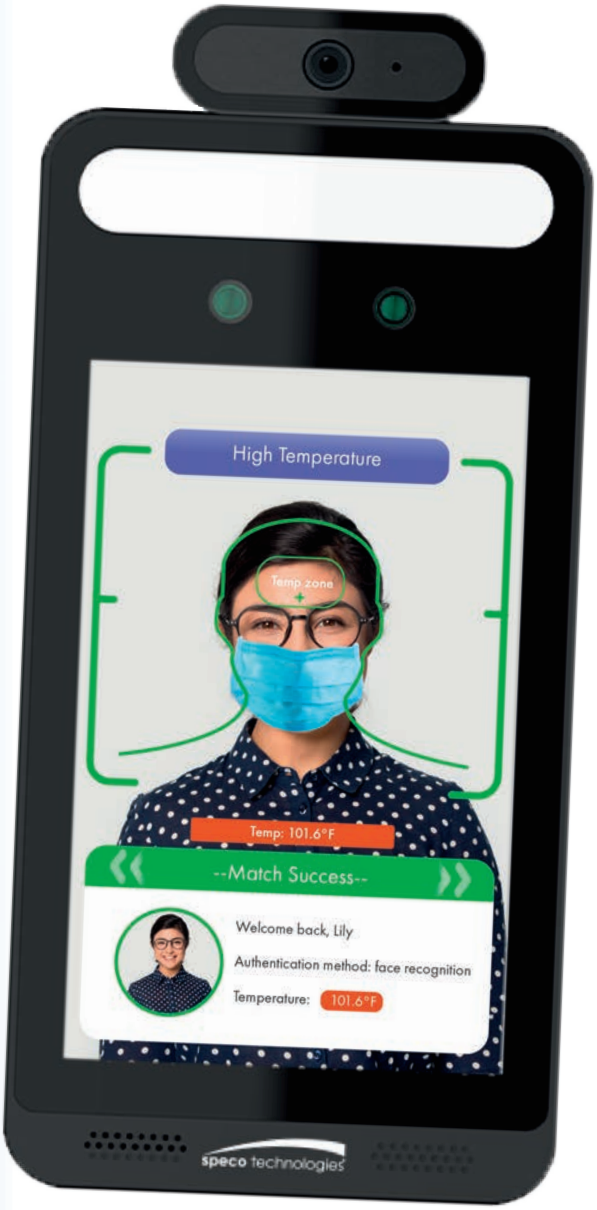
CHOOSE THE BEST ALERTS FOR YOUR BUSINESS!

☑ **Mask Detection**

☑ **Facial Recognition**

☑ **Elevated Temperature**

*This device is not intended for use in the diagnosis of any disease or other conditions or in the cure, mitigation, treatment, or prevention of any disease



O2TML

2MP Temperature Reading Panel with Face and Mask Recognition

- 8-inch LCD screen
- Supports IR high-accuracy body temperature measurement
- Can recognize faces with masks
- Triggers voice alarm when abnormal temperature or mask-less face is detected
- Deep learning algorithm with high face recognition accuracy rate
- Supports remote live view and two-way talk
- Requires 12V 1A power supply (sold separately)
- Wall mount is included

Optional Accessories:
(sold seperately)

TMLDSK
Desktop Mount

TMLPMT
Pole Mount

TMLFLR
Floor Mount

PSW5
Power Supply

Scan to **watch video**!

Visit us at specotech.com to learn more!

1-800-645-5516

FOLLOW US AT
SpecoTechnologies

that rely on physical contact with a reader won't go completely away, at least not immediately.

"We believe all biometrics have a role to play, but it depends on the application you're using it for," he explains. "For example, if you're providing access control to a building, moving forward you would likely consider having the least amount of contact with a particular device, so you would lean towards a contactless biometric, which is face and iris."

Many people may still be comfortable using fingerprint technologies on their phones or locks for their home, but Kapadia believes it will "take a beating" in the enterprise market.

"Post-COVID, we are definitely going to see a dramatic shift in the negative direction (for fingerprint biometrics) because people are going to be quite hesitant to touch things that other people have touched," he explains, adding that touchless biometrics, such as facial and iris recognition, will likely become much more popular. "Touchless modalities will see a dramatic spike and I can corroborate because we've seen a spike for our own touchless biometric products."

And while there may be less demand for things like fingerprint readers across parts of North America and Europe following the pandemic, these solutions will likely remain in use in certain regions due to the lower costs they provide to end-users, according to Kapadia. "I would say that the adoption or the speed at which fingerprint was getting adopted will slow down globally," he says. "Is fingerprint going to go extinct? I don't think so."

Merging Credentials with Biometrics

Despite advancements in biometrics and their growing adoption, Murad says that the requirement for credentials in organizations will remain a security staple for some time.

"We have been merging tokens, such as smart cards or prox cards, for a long time and we're starting to see an interest in mobile credentials where you can have a credential – rather than carry a physical card – on your mobile device," he adds. "The requirements for credentials are there and will be there because organizations want to create distributed databases. If you're talking about an enterprise that has locations all over the world, there are some issues with GDPR and other (legislation) where they may not want to have the biometric data cross borders without the person's knowledge so they will create a token with the biometrics stored on the token and they will able to use that token when they get to the facility."

Prior to the onset of the pandemic, Calzaretta says one of the issues he heard from security integrators and end-users was that they already had a variety of biometric solutions in place, be it fingerprint, facial recognition, iris or otherwise, that were not unified in any way.

"That aside, one of the big challenges is that with the use of biometrics, they were storing their employees' biometric templates in a database or in the cloud. With GDPR in Europe and now the CCPA in California, storing employee biometrics is a no-no and comes with significant fines and compliance issues," explains Calzaretta.

Gaydarzhiev agrees that organizations will be looking to deploy more unified solutions in the future, which will undoubtedly be aided by the resulting fallout from the coronavirus outbreak.

"The post-COVID-19 era will significantly increase that traction. In the next couple of years, not only between the two to three waves of COVID but after that companies will be looking to unify technologies and platforms," he says.

> "There is a realization that things may not return to what they used to be and we may be in for designing and defining a new norm."
>
> **— Shiraz Kapadia, CEO and President of Invixium.**

Solution Integrations

One of the biggest trends within many organizations and public facilities in the wake of COVID-19 has been the use of thermal imaging for fever detection. Many biometric firms are also now looking at ways to integrate these cameras into their solutions to create a comprehensive offering for access control and coronavirus mitigation.

Murad says that Iris Id is exploring ways to integrate thermal cameras into their product portfolio as well as it seems unlikely that these types of requests from end-users will be going away anytime soon.

"We feel this demand is not just temporary, but an ongoing request so we are looking at what we can do to incorporate those sorts of features," he says. "They are asking for thermal cameras; they are asking for some audit trail reports…. and they are also requesting integration with other solutions, such as enterprise resource management applications."

Invixium recently announced that its IXM TITAN device will now be available with a new Enhancement Kit that will equip the reader with a thermal infrared camera capable of providing fever detection of people with up to +/- 0.5°C accuracy. In addition, the company said that it will also be offering a face recognition algorithm upgrade for the reader to enable identification of individuals wearing masks and veils. ■

SALTO

The role of access control in the modern era of converged infrastructure is set to become one of the most challenging discussions in the security industry for the next decade.

Courtesy of BigStock.com -- Copyright: iqoncept

A New World of Technology Convergence

Set for Access Control Industry

The new paradigm of access control is leading to a need for a clear definition of identity-driven access management **By Pierre Bourgeix**

The role of access control in the modern era of converged infrastructure is set to become one of the most challenging discussions in the security industry for the next decade. The new realities presented by the Covid-19 pandemic has further highlighted the requirement for frictionless and contactless entry. Security leadership now faces a greater burden of ensuring public health and the need to contend with the precipice of exponential changes that may result in an overhaul of their current and likely soon-to-be-extinct access control technologies and processes.

For as long as we have challenged people at an entry, we have used access control. This will always be our first line of defense from a potential threat. However, in the last 50 years, as digital technology became a part of the entry process, we have seen access control become more relevant in business operations. Many traditional methods have been challenged by emerging solutions like facial recognition, contactless biometric and mobile credentials but thus far none have emerged as the clear paradigm-shifter.

The most substantial change in access control is that it no longer applies to simply a door. Convergence of systems across every area of our world has made it both difficult and challenging to segment and secure processes from the nation-state syndicates and bad actors. The consequences of events such as 911 and breaches of large corporations like Target have only amplified the need for more stringent converged access controls. Pre-pandemic, one of the growing concerns was privacy and how best to utilize an employee's biometric information without the burden and potential liability of storing that information in a database or server. Now organizations are faced with a must-be-addressed health-related view of access control. It would be hard to argue that existing "communal-touch" methods are no longer viable.

New Definitions of What is Access

This new paradigm within the already changing landscape of access control is leading to the need for a clear definition of identity-driven access management which is being driven by greater interconnectivity of systems in the IT, OT, PS, and IoT arena. Access control is now part of the entry into all things such as IT Information Technology, OT Operational Technology, PS Physical Security, IoT Internet of Things, and CoT Cellular of Things. This broad-brush now entails our understanding of all the domains of security since they are all interconnected and with that the birth of the new paradigm of access control management and its technology.

Access Control IT, OT, and Physical Security

- Access management has always been a rudimentary process driven by controlling people with processes to managing security and access to critical and non-critical infrastructure.
- Access granted or denied is a very one-dimensional concept since it relies primarily on a physical card, password, biometric reader, or using a two or three-part authentication process at the reader.
- Access control does not define identity it merely allows permission-based on access control management processes.
- Where does the validation of the person begin and end? And equally important, who controls the mechanism for validation?
- What are the role and implications of relying on a Bring-Your-Own-Device approach?

Access Control Information Technology

- Traditionally alphanumeric passwords
- Two-part encrypted password defined by biometric or question-based authentication
- Identity authentication methodology

Operational Technology Access Control

- Traditionally alphanumeric passwords
- Non-intelligent systems with one-dimension access control
- Open PLC programable logical controls and SCADA Supervisory control and data acquisition
- Unsecured communication systems

Physical Security Access Control

- Card-based access
- Two-part authentication with biometric
- Three-part with Iris, retinal scan, facial recognition or palm or finer recognition

Credentialing as access control has generated a multitude of solutions that are striving to define the permission based on a secured defined identity.

This path has led to establishing the six domains of identity recognition within the access control world:

1. Facial recognition in IT, OT, PS, IoT

2. Biometric authentication using retinal, and finger, temperature, heart, body movement, breathing, voice and palm print technology

3. Intelligent cards with biometric authentication on board

4. Intelligent entry systems using behavioral and voice technology tied to sensors

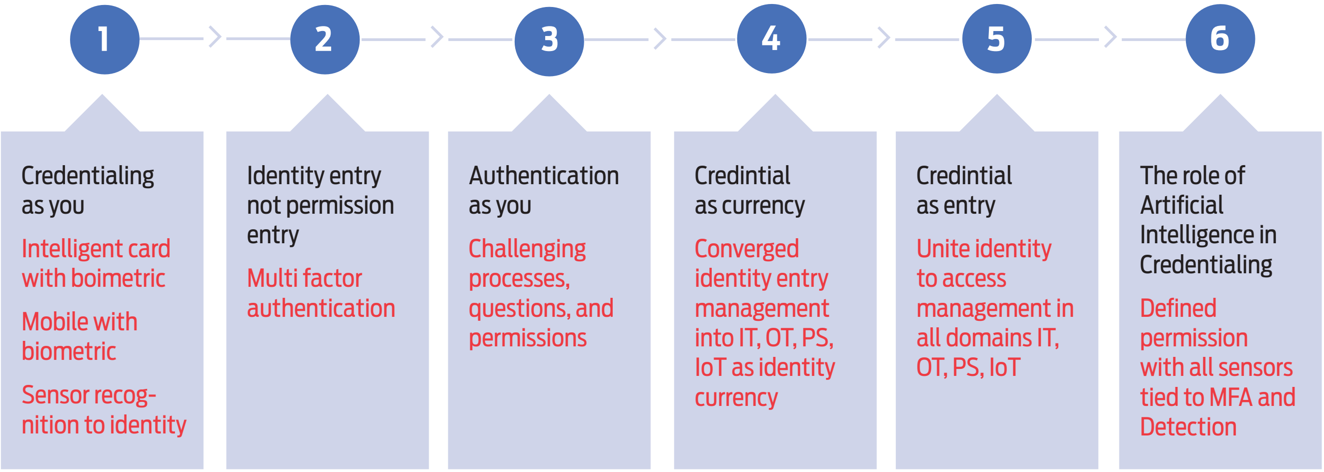
5. Visitor and Access management using defined permission with multi-factor authentication tied to challenging questions and behavioral tracking systems.

6. Products that recognize you AI, deep learning and machine learning and intelligent chip embedded biological chips, and sensor technology

New Norms for Access Control

The process of access control is changing and with that it is critical to understand that we must now establish a new norm which incorporates the aspects of identity recognition and acceptance as part of the overall promise of entry. We no longer can define access control as part of a siloed process, but rather a part of a new organic and multi-dimensional converged eco-system. These are the six steps that are tied to the 6 domains of identity recognition.

It is very clear that the process of identity-driven access control is moving to the edge and with this is the use of technology to make that happen. The inevitability of the use of a biometric



1

Credentialing as you

Intelligent card with boimetric

Mobile with biometric

Sensor recognition to identity

2

Identity entry not permission entry

Multi factor authentication

3

Authentication as you

Challenging processes, questions, and permissions

4

Credintial as currency

Converged identity entry management into IT, OT, PS, IoT as identity currency

5

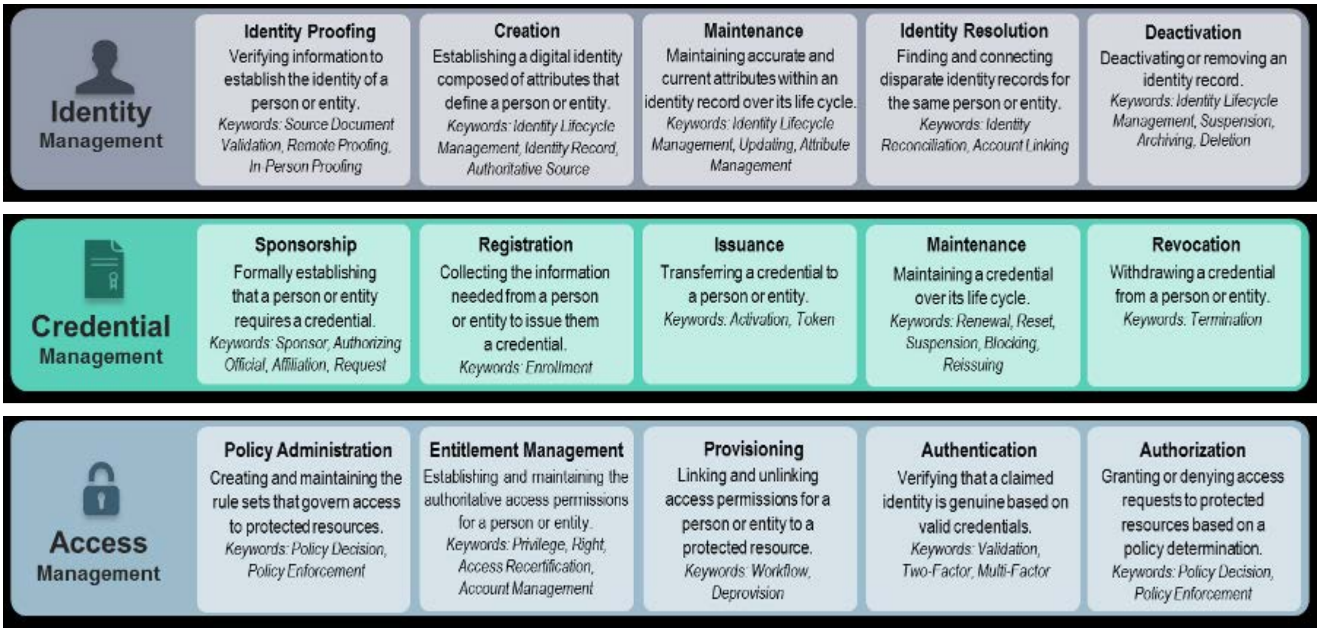
Credintial as entry

Unite identity to access management in all domains IT, OT, PS, IoT

6

The role of Artificial Intelligence in Credentialing

Defined permission with all sensors tied to MFA and Detection



Identity Management	**Identity Proofing** Verifying information to establish the identity of a person or entity. *Keywords: Source Document Validation, Remote Proofing, In Person Proofing*	**Creation** Establishing a digital identity composed of attributes that define a person or entity. *Keywords: Identify Lifecycle Management, Identity Record, Authoritative Source*	**Maintenance** Maintaining accurate and current attributes within an identity record over its life cycle. *Keywords: Identify Lifecycle Management, Updating, Attribute Management*	**Identity Resolution** Finding and connecting disparate identity records for the same person or entity. *Keywords: Identity Reconciliation, Account Linking*	**Deactivation** Deactivating or removing an identity record. *Keywords: Identity Lifecycle Management, Suspension, Archiving, Deletion*
Credential Management	**Sponsorship** Formally establishing that a person or entity requires a credential. *Keywords: Sponsor, Authorizing Official, Affiliation, Request*	**Registration** Collecting the information needed from a person or entity to issue them a credential. *Keywords: Enrollment*	**Issuance** Transferring a credential to a person or entity. *Keywords: Activation, Token*	**Maintenance** Maintaining a credential over its life cycle. *Keywords: Renewal, Reset, Suspension, Blocking, Reissuing*	**Revocation** Withdrawing a credential from a person or entity. *Keywords: Termination*
Access Management	**Policy Administration** Creating and maintaining the rule sets that govern access to protected resources. *Keywords: Policy Decision, Policy Enforcement*	**Entitlement Management** Establishing and maintaining the authoritative access permissions for a person or entity. *Keywords: Privilege, Right, Access Recertification, Account Management*	**Provisioning** Linking and unlinking access permissions for a person or entity to a protected resource. *Keywords: Workflow, Deprovision*	**Authentication** Verifying that a claimed identity is genuine based on valid credentials. *Keywords: Validation, Two-Factor, Multi-Factor*	**Authorization** Granting or denying access requests to protected resources based on a policy determination. *Keywords: Policy Decision, Policy Enforcement*

or mobile credential (ideally with the biometric enrollment managed by the enterprise and not the end-user) tied to a sensor that is connected to a door strike that communicates over cellular may be closer than you think.

Security requirements aside, a key factor in this transition will be the optimization of previously expended capital; avoiding the need to "rip and replace" infrastructure. Adding a camera in the mix and either Lidar or Optex you have the potential to define piggybacking and tailgating at every door. This process lends credence to the discussions surrounding the use of cloud access/identity at the edge. There is a growing sentiment by large organizations that with intelligent identity access processes they may be able to connect all the business domains, therefore, create a new operational identity to entry model which doesn't need the burden of infrastructure -- especially if they tie it to secured cellular solutions and bypass the LAN environment segmenting the entire operational environment including access and identity from the IT data transaction world.

With the movement to identity-driven access control, we need clear policies and procedures as well as governance to ensure there are protections to the individual and the entity. The guidance established by HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation), The California Privacy Act are a few of many ways that we must incorporate protections as we move into this world of Access, Identity, to Entry.

Now that we have understood that everything is changing, we must now define and understand how to manage this interconnected world driven by identity. The DHS created a process that will help our world stay on the rails and hopefully not get derailed using technology. The goal simply put was to define a process of determining entry in the Federal and now in the public domain. The goal is the understanding and the importance of multi-factor identity authorization in the process of access management.

- Identity Management,
- Credential Management
- Access Management
- Governance
- Federation

https://www.dhs.gov/sites/default/files/publications/896_ICAM_Acquisition-Guidance_060818-508.pdf

The future of Access control and Identity management in the world of IT, OT, PS, IoT

- IoT and IIoT identity-based access control
- OT Identity based access control
- PS Identity based frictionless access control
- IT Identity-based agent and access control
- COT (Cellular of Things) Secured communication tied to Identity and access control

The Future of Identity Tied to Access control

- Unified identity: The convergence of identity and building the unification of privacy.
- Access, Identity, to Entry in the converged technological world.
- Bridging data protection with identity management in the world of IoT
- The path forward: Aligning assessment, testing, and Integration with identity
- Identity per industry: leveraging the rule of compliance and regulation to harness entry thru identity

Inevitably, however, once we establish a conclusively defined identity tied to entry the rule of privacy must become imperative. The holder of the identity inevitably must be the individual, not the entity. The use of a defined biometric algorithm tied to the individual locked by a process using open consent is the holy grail of access control in the modern era.

Our world is faced with a burden of guilt in obfuscating our rights for the "global interconnected world". We as humans must control our right to be free of manipulation and misuse of our identity. Our world is quickly approaching awareness with the recent conversation of tying health to an identity card tends to drift into the realm of big brother, and with China in full surveillance mode, we are seeing the progenitor of what George Orwell called Oceania, the totalitarian state wherein the ruling party wields total power "for its own sake" over the inhabitants.

So, can we have identity and still retain privacy? I believe we can but it is going to take the use of Identity governance within the overall process of access management. The use of technology such as a thermal camera to determine the temperature in response to the need to control entry in the post-COVID-19 pandemic world is another area to be defined. The workplace may be in a paradigm shift of its own due to the justifiable fears of contracting Covid-19 as we see identity-driven access control becoming more important than ever.

However, with this there must be protections put in place to ensure the employee rights are secure defined. As we come to the realization that access control is no longer a one-dimensional issue and that all things are connected, then we also must define a new expectation that identity is the underlying key to the new equation and with that will grow the need to take a firm but equal stance in how that is interwoven with our interconnected world.

Protecting Identity Rights

As we move to protecting identity as part of the access, we must realize that there will be challenges. One of the greatest challenges is identity theft and the world of fraud and misappropriation.

The unification of Access, Identity, to Entry in the IT, OT, PS, and IoT world is a reality and with the use of biometrics across many industries such as banking, transportation, retail and critical infrastructure, we are relying on systems to work as well as be secure. While nothing is 100% foolproof, I have always stated that the 80-20% rule applies. As we strive to become more secure using identity, we also have to understand that the layers of protection will inevitably fall short and it is our choice to accept a world that is totally imperfect by the use of one-dimensional access management or know that the 80% will afford us a chance to protect ourselves our property and our future. ■

About the author:

__Pierre Bourgeix__ is the CTO and founder of ESI Convergent, a management consulting firm focused on helping companies assess and define the use of people, processes, and technology within the physical and cybersecurity arena. ESI Convergent was formed to not only help end-users but also manufacturers in defining the proper strategy to drive products successfully into the marketplace. As a thought leader in the Security Industry Pierre Bourgeix has helped companies successfully launch and position products and solutions globally. ESI Convergent can produce market analysis, product briefs, product specifications, Physical and cyber assessments, and advisory practice surrounding cyber and physical security convergence in the security and risk management arena.

QUICK ORDER PAD | CONTACT US
ACCOUNT
CART (0)
PRODUCTS | BRANDS | ABOUT
Search by Part # or Keyword
NRT 410-TPN-689 DOOR CLOSER
ADD TO RFQ

A variety of widely adopted access control and other trusted identity technologies will play a key role in facilitating these measures and best practices for safe re-openings.

Courtesy of BigStock.com

How to Use Trusted Identity Technologies to Safely Re-Open Workplaces

Proactive measures and best practices will help normalize organizational operations during the global pandemic **By Mark Robinton**

As communities and economies re-open, concerns around COVID-19 and other infectious diseases will be changing practically every way that people live, work, and conduct regular business for some time. There are many proactive measures and industry best practices that organizations should adopt to create and maintain a safe and secure workplace while ensuring business continuity.

A variety of widely adopted access control and other trusted identity technologies will play a key role in facilitating these measures and best practices for safe re-openings. These include location services solutions proven in workplace optimization applications and physical identity access and visitor management software, among others.

Physical Distancing and Contact Tracing

One of the biggest challenges is implementing contact tracing and physical distancing procedures as well as improving hygiene to ensure a safe workplace.

Real-time location services technology is playing a key role here, automating how organizations monitor people's proximity to others and measure localized density in real-time. It is also dramatically simplifying contract tracing by enabling detailed and automated record-keeping of where an employee has been in a building, with whom they have interacted, and if they have been complying with disinfecting requirements.

Organizations will first need a physical-distancing plan. This includes thinking about how to rework the office layout for the distance between workplace positions, and how to enforce these new arrangements in the office and as employees move about. How are the restrictions and guidelines related to employee's access to the workplace going to change as a result of social distancing? Also, if an organization wants to maintain 50 percent office density, for instance, how is this tracked against the metric?

Organizations need to audit contact tracing against the entrance and exit logs as part of compliance requirements.

Today's physical identity and access management systems can be integrated with a facility's physical access control system to make this happen. Inside the building, real-time location services technologies are being employed that use Bluetooth LE beacons to monitor people's proximity to others or to measure localized density in real-time. This technology simplifies contract tracing by enabling detailed and automated record-keeping of where an employee has been in a building and with whom they interacted. The same technology can be used to ensure compliance around the usage of hand sanitation stations, for example.

Organizations need to audit contact tracing against the entrance and exit logs as part of compliance requirements. This can be handled anonymously, or by enabling the identification of the contacts that the person has been near. Organizations can also categorize their suppliers based on how they operate: i.e., some may be denied entrance if they continue to send employees to tradeshows, regardless of whether the staff in question had been to a tradeshow or not. It may be that organization will bar access to outside contractors or employees not because of their individual behavior, but because of the blanket policies of the organization they represent. Non-compliance has been associated with fines, but now it could play a role in inter-organization access. An organization being

out of compliance with the right policies could limit where, what and how much other organizations will allow staff access.

Safely Re-entering Buildings

Once a physical distancing and contract tracing solution has been determined, the first step in safely returning to buildings is to ensure that they are physically in shape to re-open after weeks or months of being unoccupied. Building readiness must be addressed completely before considering welcoming anyone inside. Also, who is coming back in and when? There will likely be a phased return to work.

After these decisions are made, the next step is to consider what, if any, additional screenings may be required for staff and contractors. These screenings might be related to travel history, temperature checking, whether they have shown any infection symptoms and other information. Depending on their answers, visits or interactions at points like delivery bays may be refused. Or, an individual might be required to go through additional checks. Many organizations have made temperature checking mandatory, often multiple times a day. The use of trusted identity technology can play an important role in further automating this vetting process and providing the necessary links back to building systems.

Guests will also need to be considered. Today's visitor management systems give organizations a single source of real-time and historical insights into who is, or was, recently in the workplace. Since first impressions are made at the front desk or lobby, the visitor experience needs to be a positive one. At the same time, though, any emergency event requires that there be strict control over who is entering the workplace. This policy also needs to be clearly communicated to visitors. Doing this minimizes risk to visitors as well as the workforce.

In addition to delivering a high-quality visitor experience, the ideal visitor management system must enable organizations to meet regulatory compliance mandates and facilitate check-in at a self-service kiosk to minimize wait times. It should be capable of customizing the visitor experience to support specific security needs, such as accelerating and simplifying check-in or requiring additional security pre-checks. It also must automate compliance as it relates to visitor access rules with historical visit reports.

Organizations can strengthen security at the registration kiosk using a flexible, enterprise-grade visitor management system to add visitor sign-in steps. This has proven successful in the past when used to control the spread of infectious disease during an outbreak. They provide two particularly important capabilities that can be used by organizations to protect their workplace from the uncontrolled spread of an infectious disease: 1) enhance visitor registration policy with additional mandatory questions to help identify any visitors who may need other screenings, and 2) extend the visitor registration kiosk with a mandatory pop-up asking further questions during visitor check-in. A typical workflow for implementing additional check-in questions is here.

> Many organizations have made temperature checking mandatory, often multiple times a day.

Also important for controlling the spread of infection throughout a facility is the ability to understand who has visited the workplace – and when. This requires the ability to automatically maintain an auditable trail of activity, which can be done using an enterprise-grade visitor management system that makes it easy to retrieve historical visit reports. This provides a timeline of who was in the workplace, and when they were there. The latest solutions include a single dashboard that provides useful visitor insights, and historical reports with visitor details including location and contact information, all in compliance with General Data Protection Regulation (GDPR) and other privacy regulations.

Another valuable option is the use of contactless technologies to further enforce social distancing and mitigate risk factors for infection transmission including such common surfaces as faucets, doorknobs and coffee pot handles. There also has been a growing demand for technologies that deliver contactless user experiences to securely access the workplace. These include automatic doors, contactless cards and mobile-based access, as well as automated turnstiles. Another example is "touch-free" processes such as emergency onboarding of employees through secure issuance and administration of staff badges and access control credentials. Solutions are available that combine cloud-based ID card printing with cloud-based identity management to minimize the impact on overwhelmed credential issuance departments and drive a more secure work environment.

As communities and economies begin to re-open, taking steps to address all of these issues will make it easier for organizations to control access and implement the levels of physical distancing that will be required to meet the challenges of safely operating under the threat of COVID-19. The complexity and number of challenges will vary depending on location but, in the mid to long term and on a more global level, there are proactive measures and best practices that will help an organization's staff, contractors and visitors safely return to the workplace. ■

About the author:

Mark Robinton *is Vice President of IoT Services at HID Global, where his group handles Location Services, Condition Monitoring, and Trusted Tag Services.*

New opportunities for today's locksmiths are driven by advanced door and access control technologies.

Courtesy of Getty Images -- PeopleImages

New Technologies Drive Evolving Lock Market

As the market for digital security products and services grow traditional locksmith services face new options **By John Moa**

Mechanical locks and keys have remained remarkably unchanged for thousands of years [1]. The earliest known locking devices, from Mesopotamia and Egypt, employed a series of wooden pins not so different from standard pin tumbler locks. While this ancient design continues to play a ubiquitous role in physical security, successful security providers have long expanded their offerings beyond simple door hardware. As lock construction evolved, early locksmiths became talented metal workers, plying a trade that was often not confined to locks and keys. Similarly, today's locksmith industry encompasses a wide range of security services, from residential and commercial security system installation, repair, monitoring, and surveillance, to key cutting, resale, and more. Although the demand for locksmithing services continues—indeed, society continues to build more and more structures that must be secured—the latest technology has essentially rendered many traditional services obsolete. In other words, while the market for security products and services is growing, the need for traditional locksmith services is in decline.

Locksmith Market Faces Crossroad

Innovative technologies, specifically a tech-savvy customer base, are a driving force behind the shrinking locksmith market. Inexpensive and convenient "Do it Yourself" security solutions are widely available, both online and at big-box retailers, providing commercial and residential customers with easy access to off-the-shelf products. Gone are the

days when installing a decent security system at home required an advanced technical degree. The average consumer now needs little more than a free afternoon to achieve comprehensive home surveillance, complete with remote monitoring and electronic access control on their entryways. In the rare case where a commercially available system isn't designed with the plug-and-play simplicity we've all grown to expect, the internet is sure to save the day with a seemingly endless supply of instructional videos and DIY tips. Even services that once fell exclusively within the purview of the local locksmith—key cutting, rekeying, programming vehicle fobs—have been automated or outsourced, whether to an online provider or a kiosk in the mall.

Perhaps most critical, this market evolution is placing growing pressure on a locksmith community that's likely to see a dramatic decline in membership through the coming decade. It's certainly no secret that locksmithing hasn't attracted near the same interest from Millennials and Gen Z as it did with Boomers and Gen Xers; as the lion's share of the locksmith community nears retirement, they might find it difficult to pass the torch.

All of which begs the question, how does a locksmith stay afloat in a rapidly shifting industry with a dwindling need for conventional services?

The silver lining to this evolution in the consumer security market is that interest in home security is at an all-time high[2]. Moreover, the proliferation of off-the-shelf products means that home security systems are now accessible to everyone. These mass-market security products have fortunately played an important role in educating customers that may have previously assumed that a robust security system was too complex or expensive. In turn, the education of the residential market has inspired small businesses that once believed installing a security system meant also hiring an IT department. Ultimately, the waning interest in traditional locksmith services has given way to a rapidly growing market for *all things security*. On paper, this is encouraging news for locksmiths and security professionals; we have an ever-expanding market, educated, attentive customers, and a glut of innovative security products. Frankly, the challenge for most firms has simply been embracing the change.

Evolution Spurs Revolution

Thinking back to the first locking devices, some 6,000 years ago, it's hard to imagine mechanical locks and keys truly going the way of the dinosaurs. And while the basic lock and key are likely to remain a constant in the industry, so too will these more advanced security innovations. Smart locks, keyless security systems, Wi-Fi cameras, IoT peripherals, and other electronic devices ultimately give customers what they crave most: control. Or, at the very least, the illusion of control. One of the most enduring byproducts of our connected world is the average consumer's desire to micromanage every aspect of their lives, often from the palm of their hand. It's evident in the way Uber and Lyft revolutionized the transportation industry, or online booking disrupted travel agencies at the turn of the millennium. Even insurance companies now have smartphone applications that let you monitor and fine-tune your policy, if your heart so desires. For better or worse, today's security offerings are no different.

Residential users now expect administrative-level control and visibility over their doors and cameras, all from the comfort of their couch. Admittedly, it's a dramatic shift from the years when only businesses and the wealthiest of residences would invest this level of attention in their security. The locksmiths that have thrived in this market are following examples from other industries disrupted by the smartphone era; they have embraced innovative solutions while identifying opportunities to generate recurring revenue through services and support. And honestly, they've invested time in customer engagement, building relationships, and differentiating themselves from arm's length retailers. To this end, locksmiths must identify real-world problems, find appropriate, affordable solutions, and assemble a team willing to embrace the future of the security industry.

It's a given that big box and online retailers will continue capturing sales for plug-and-play surveillance and access control products. However, many of these outlets are lacking in the type of post-sale customer engagement that can drive repeat purchases and build *lasting* recurring revenue streams. By engaging with existing security product users, locksmiths can optimize upsells with end-users that are already educated and readily understand the value add for complimentary services and support.

> Innovative technologies, specifically a tech-savvy customer base, are a driving force behind the shrinking locksmith market.

An Educated Client is the Best Customer

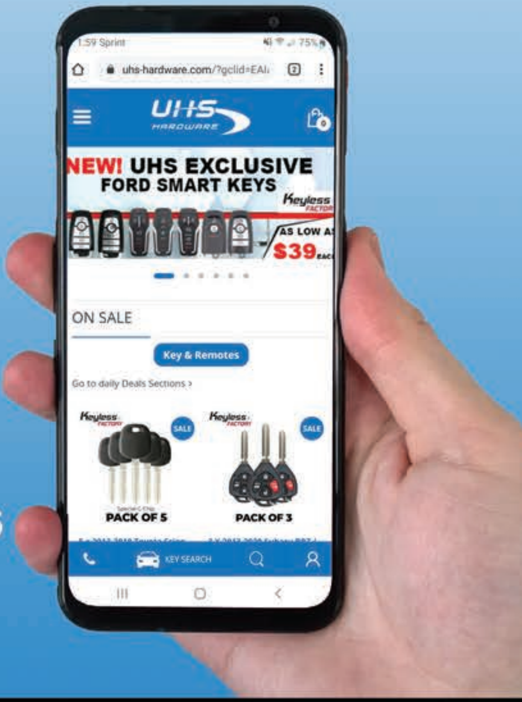
If nothing else, present-day shoppers are certainly more informed than previous generations. The typical end-user, armed with a smartphone and an endless supply of product review sites, may invest hours of research prior to purchasing. The importance of maintaining an online presence that's visible during this research phase can not be overstated. Beyond that, a locksmith's overall approach to security should feel comfortably familiar. First and foremost, locksmiths must be committed to listening.

Tune in to your local or online community to discover what customers are looking for. Repeated concerns indicate an opportunity to adopt technology to meet customer demand. Key control, rekeying, internal theft, community

UHS HARDWARE

ONE STOP SHOP FOR ALL YOUR LOCKSMITH NEEDS!

- KEYS & REMOTES
- LOCKS & CYLINDERS
- KEY PROGRAMMERS & KEY CUTTERS
- LOCKSMITH TOOLS
- ACCESS CONTROL
- EDUCATION



$ JOIN OUR REWARDS PROGRAM

FOLLOW US FOR EXCLUSIVE DEALS

SUBSCRIBE AND LEARN

www.uhs-hardware.com Tel: 1-800-878-6604 safety, and a variety of other anxieties are often voiced by individuals and businesses seeking assistance from a locksmith. Auditing security needs is a necessary protocol in growing business and ensuring future sustainability. It is essential for locksmiths to seek out solutions that solve the real-world problems customers are facing every day. If the solution isn't readily available, that doesn't mean it doesn't exist. Find it! If you aren't researching, I can assure you that your customer is; and they will happily take their business to a provider that has already identified a viable technology. The astute locksmith will find the solutions first, promote the benefits second, and let the inevitable consumer research bring clients through the door.

When looking to adopt new solutions, it is important for locksmiths to carefully consider their target market. There's a vast selection of products, each designed to meet the specific needs of everyone from residential customers to large commercial facilities. It's here that locksmiths can truly differentiate themselves from the big box retailers and online warehouses. By meticulously evaluating the needs and abilities of your clients, you can tailor a custom solution that addresses their security requirements without disrupting their daily operations. Success at this phase builds client trust, and trust is fundamental in securing the repeat purchases and recurring revenue commitments that support a sustainable business.

Find the RMR and the Right Partner

By and large, the security market hasn't escaped the plug-and-play mentality of computer peripherals. Most customers are seeking a security solution that is simple, both in installation and operation. Manufacturers have certainly taken note. New technologies, whether for residential or commercial access control, are designed, above all, for ease-of-use. More often than not, this means keyless systems, employing cellular devices connected via Bluetooth or Wi-Fi. There's no denying that these technologies have contributed to the shrinking need for traditional locksmith services. However, these new solutions not only satisfy overwhelming consumer demand, but they also provide lucrative opportunities to generate recurring revenue through subscription-based services and features.

What's more, these connected technologies often keep clients tethered close enough to foster post-sale engagement and build lasting relationships. As the market has been inundated with retailers and wholesalers competing solely on price, long-term customer relationships are critical in driving repeat purchases and optimizing upsells and complimentary services. For many traditional locksmiths, installation, and management of the latest innovative technology involve at least one technical capability that is beyond their comfort zone. In this case, it is imperative that locksmiths invest the resources to either improve their technical aptitude or consider a partnership that provides the necessary technical support.

Independent-minded locksmiths may understandably have reservations about partnering with another security provider. Under the right circumstances, however, it can provide tremendous value to both parties. Such an arrangement gives the locksmith the freedom to focus on revenue generation, namely, cultivating customer relationships and pursuing new opportunities. For instance, many security products are still brought to the market through specific channels. For locksmiths that lack an in-house technical team, it can be both cost and time prohibitive to adopt an innovative new product for customers.

When accounting for the necessary technical training, potential competition, and investment in demonstration products (typically requiring both hardware and software), the barriers to entry are high. And yet, customers will inevitably turn elsewhere for the right solution. In this case, forming a partnership with an established technology provider can help alleviate the growing pains associated with adopting a new product line, enabling the locksmith to capture business that would have otherwise fallen by the wayside. With properly aligned business objectives, a partnership should be mutually beneficial. Offloading resource-intensive support to a dedicated vendor allows for expanding customer reach while maintaining a manageable workload. Depending on the go-to-market channel for the product offering, the right partnership can also provide leverage in protecting deals and help maintain a loyal customer following within a targeted area.

If you are struggling to generate recurring revenue or need to identify new opportunities in your target market, consider partnering with a technology provider that supports you and your customers. ■

> The locksmiths that have thrived in this market are following examples from other industries disrupted by the smartphone era

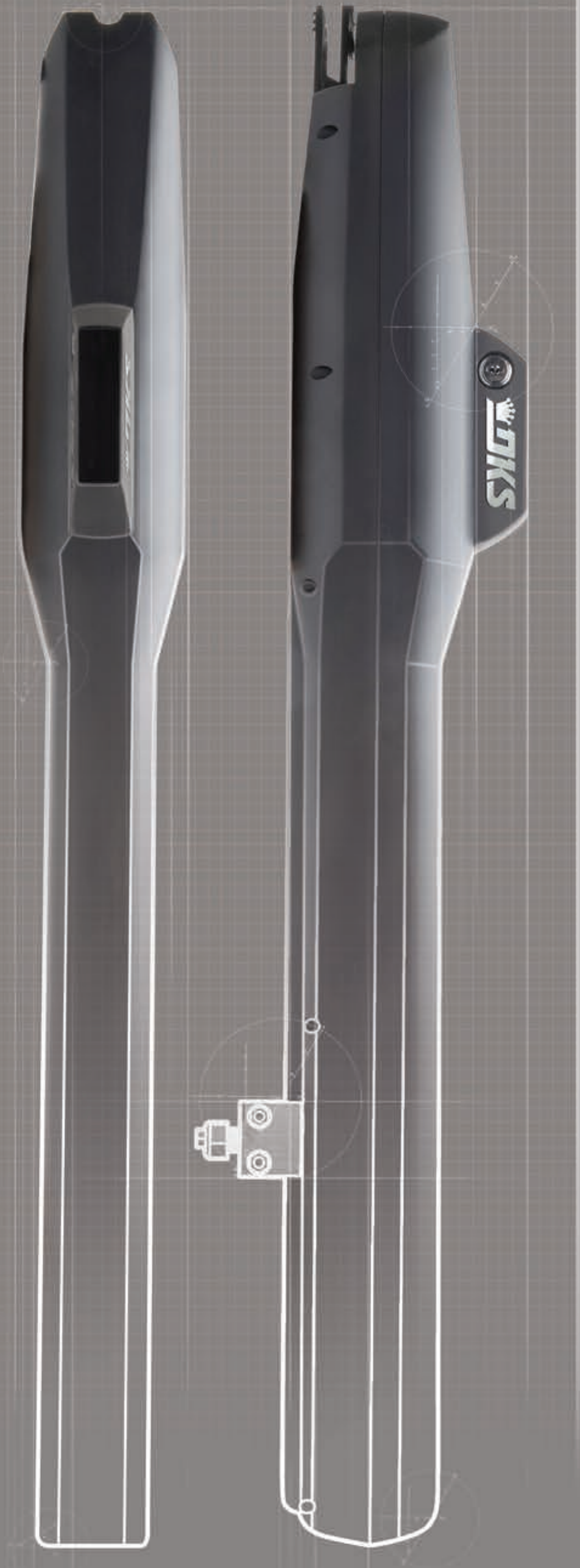
[1] Archaeologists have uncovered locking devices dating to 4,000B.C., in what was the ancient kingdom of Assyria, now modern-day Iraq.

[2] "Looking forward, the market value is projected to reach US$14.1 Billion by 2024, registering a CAGR of 19.7% during 2019-2024" (https://www.businesswire.com/news/home/20190709005374/en/North-America-Home-Security-System-Market-Expected)

About the author:

John Moa *is the Director of Sales at CyberLock Inc. which is located in Corvallis, OR. CyberLock Inc. is the global leader in smart-key, electronic-lock access control solutions. Learn more at www.cyberlock.com*

Welcome!
EZ HELP
LETTERS
NAMES
CALL / HANG-UP
VIKING
Call
Call
VIKING

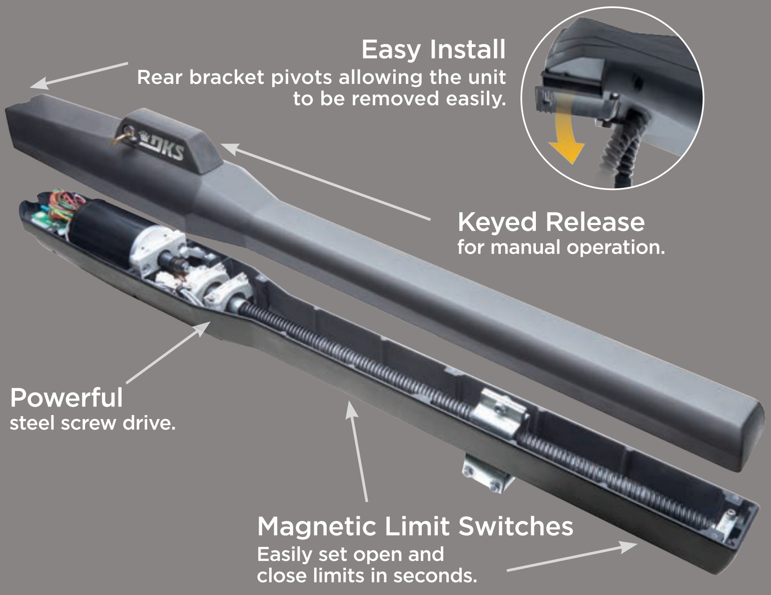


SWING GATE ACTUATOR

STRENGTH, STYLE, QUALITY- DESIGNED AND BUILT IN THE USA

The DKS 6006 Swing Gate Actuator offers convenience and reliability in a compact, aesthetic design. The powerful steel screw driven piston can move gates weighing up to 1600 lb.* Plus, there is no need to worry about hydraulic leaks, check valves or pumps.

The microprocessor-based electronic control board provides many advanced features not typically found in operators in this class, while the sleek and slim design means the gate is front and center.



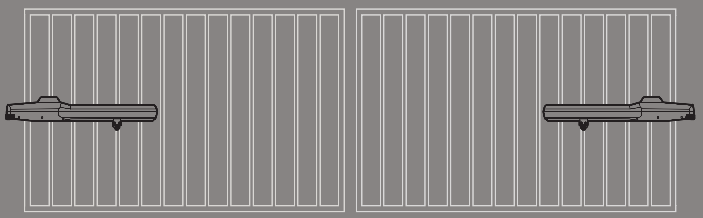
Easy Install
Rear bracket pivots allowing the unit to be removed easily.

Keyed Release
for manual operation.

Powerful
steel screw drive.

Magnetic Limit Switches
Easily set open and close limits in seconds.

Compact
Reversible design mounts right or left directly to the gate and pilaster, eliminating the need for concrete pads.



* 1600 lb, 8 ft max gate,
800 lb, 16 ft max gate, 600 lb, 18 ft max gate

MADE IN USA

Traffic Control | Access Control | Telephone Entry | Gate Operators

Member: AFA, DASMA, NAA, IDA, NOMMA, NPA, SIA, SSA, CANASA

DKS® DOORKING®

Visit the landing page to learn more:
Doorking.com/6006
800-673-3299 • info@doorking.com

Request information: www.SecurityInfoWatch.com/10213482

App: Virtual Enterprise Security Management Workstation in Your Pocket

Easy, Smart Management and Control of Doors, Lockdown, Threat Levels, Status, Control & Personnel

New! **CA4K® Access Manager App** adds another level of convenient intuitive mobile control to Continental Access' flagship CA4K Enterprise Integrated Access Control/Security/Video Management Software Platform, which also supports push notifications (or emails) in the event of an emergency, threat level escalation or lockdown events (shown). Built-in Mobile Credential - Ideal for schools, hospitals, multi-tenant & commercial buildings.

- **Supports any Smart Device** (smart phones, tablets); Available on iTunes® or Google Play®
- **Comprehensive Control of All Doors (1-32,000),** wireless PIN/Prox locks, readers, elevators & entryways
- **Activate & Control Global or APB Area-Specific Lock Down** or Unlock doors on anti-passback areas (APBs) on demand
- **Simplifies Security Management -** Add or disable credentials/badgeholders; change settings & schedules, threat levels, manage personnel privileges
- **Built-in Credential –** Provides logged access via a customizable list of approved entry-points without a physical credential
- **Cost-Saving Universal Functionality -** Brand Agnostic App use with any lock or reader brand on CA4K System
- **Integrators' *Shake-Swap* Control between multiple clients'** hosted or remotely managed enterprise systems – ideal complement to comprehensive CI Dealer Program

Continental
Access

Download on the App Store | GET IT ON Google Play

www.cicaccess.com | 1.800.645.9445
Continental Access, a Division of Napco Security Technologies, Inc.

CA4K, uniVerse™ and Trilogy Networx® are trademarks of Continental Access & or parent co. Napco Security Technologies Other marks remain intellectual property of their respective cos. Prelim data subject to change without prior notice.

Request information: www.SecurityInfoWatch.com/10213301