



▶ EDITOR'S COMMENTS ... 1

▶ Who has the Keys 2

▶ Video Analytics changing the World.. 3

▶ How to choose a Digital Signature Solution 4

▶ Securing a Wireless Network

▶ Rise of Digital Certificates 4



○ ISSUE 5 | ○ VOLUME 1 | ○ September 2008

Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE.

Helping secure your world

The statement is often made that "we live in a digital world" and it certainly seems to be true. From simple things like cooking or baking food on stoves where all the controls are digital thru to the ubiquitous cell phone, digital technology is an all pervading facet of our lives. No where is this more true than in the security arena. Traditionally security has been viewed as an area of physical obstacles (walls, fences, locks etc) and men and while these are still key security concerns, increasingly it is digital technology that is used to secure our lives and conduct transactions. Even when traditional security measures are retained, such as physical keys, it is digital technology that is being used to better manage those security measures. Our first article, **Who has the keys**, in this issue of **SECURITY**

SOLUTIONS looks at exactly that topic, the management of physical keys.

Over the years it has come to be realized that in order for a security system to be truly effective, it must provide certain benefits. These benefits must cover:



Situational Awareness, Knowing what is happening at the site; Early Warning, Providing alerts and notification before serious problems occur; Controlling Access; Recording Activity; Responsiveness. The article, **How Video Analytics is changing the world of security**, introduces how the digital revolution is enabling video to provide these benefits.

Plain Email is clearly the preferred means of communication today but some communication must carry a signature. So how do you safeguard your signature and the document once you have digitized it. The article, **How to choose a digital signature solution**, shows you how.

Another method used for securely exchanging and securing documents is through the use of digital certificates. We look at this technology in the article, **The rise of digital certificates**.

Broadband internet access has sparked a surge in internet usage in the Caribbean. With that surge has come an increase in wireless networks at homes because they are so simple to set up. Wireless networks however have risks and we show you how to **Secure a wireless network**.

Brian Ramsey
Editor

Who Has the Keys?

By Mike McGovern · [July 2008](#)



Key management and control is a critical aspect of security

There is a mistaken belief among some that the use of traditional mechanical keys is becoming less important with the proliferation and evolution of sophisticated access control technology. The fact is, traditional mechanical keys are more common than ever, and today's security awareness dictates these keys be tracked, monitored and managed effectively. Casinos, convention centers, healthcare facilities, residential and commercial property management, educational institutions, government, transportation and delivery, auto dealerships and prisons are among the common users of good key management systems.

Key Control Networks

The concept of key management relates to keys secured in a locked or unlocked enclosure and each key is assigned a physical and logical location—or a hook in more primitive systems. Each key or key bundle may be assigned to someone whose security credentials permit the use of that key during that time period. Authority systems range from a guard identifying and issuing keys in basic systems to automated locking, release, tracking and timing in advanced systems. Returned keys are logged in—electronically or in writing—providing management with

a report of when and to whom the keys were issued and whether keys are available or remain out.

The first of three basic key control system methods is considered manual, or primitive. This means key possession is tracked and/or controlled by a sign-out sheet and the supervision of administrative and/or security personnel. This method is labor-intensive and susceptible to human error; there is no way of generating an automatic report when a key is not returned, for example.

In the second method, mechanical or electronic key controls involve a metal-to-metal contact identification. These technologies have been available for more than 20 years. Contact chips and similar systems rely upon electrical point-to-point contact points of the device attached to the key.

Keys are fundamentally mechanical devices subject to abuse and frequent exposure to dirt and moisture. These same mechanical devices are, for secure operations, dependent upon electrical contact points, which are subject to failure and high maintenance due to the normal wear and dirt acquisition of the contacts.

The final method is the newest form of key management. It is based on contactless RFID technology—similar to but more rugged than traditional proximity cards. An RFID tag is embedded into an indestructible key fob, docked into a round port in the key board. RFID technology is maintenance-free, and the contactless identification capability of the fob can be used for additional tasks related to access and control efficiency. RFID key fobs are not affected by dirt, moisture or wear. The first system of this type—proxSafe®—was introduced by Deister Electronics.

Item vs. Access Control

Key management may be seen as part of the broader category of item control, which is the cousin to access control. Item control is a natural step as people become more sophisticated in managing and controlling access to places, information and things. Today's technology provides means of identifying who is getting into a building, who is accessing its information technology and who is in

possession of its items or keys. Contactless RFID-based systems also are equally effective at managing safekeeping of small assets and laptops.

Smart key management, in fact, is essentially access control for assets. Such systems can be configured as standalone—in fact, about five years ago nearly all such systems were configured as stand-alone. These systems embed an access database and log locally, and run without centralized supervision. Data and changes are periodically updated and uploaded by system management.

Networking systems, often at multiple locations—from a short distance to halfway around the world—comprise a single overall key management and access system. Management is from a browser-accessible server, and the system resides on the local IT network with full Web access capability. A single database governs and records events and authority for all locations. Networked systems also must have a fallback—for all systems to operate effectively in stand-alone mode—in the event of a temporary failure of the network.

From a logical and administrative standpoint, a key or key bundle is really a kind of door object. The most advanced systems have open protocols that may be integrated into classic access control to take advantage of single databases, single management and the now far-reaching security needs of an organization.

Cost Benefits

Misplaced keys cost organizations in North America approximately \$35 billion annually in terms of inefficiency, shrinkage, liability and lock replacement costs. Consider the cost of replacing lost keys and cylinders, time spent while locating keys, and extra personnel to manage manual key systems, and you get an idea of just some of the costs that can be resolved by an effective system. Lack of effective key management also can result in lost sales revenues for properties such as assisted living and residential or commercial properties where an ineffective system would be seen as a detriment to security and value of the property. Automated electronic key management systems typically have a payback of less than 12

months when all risks and costs are analyzed.

Electronic access control has become a staple of the tools available to security directors within commercial and government areas to increase and manage security requirements within their arc of responsibility. Yet, relatively few of these same sophisticated executives have incorporated physical keys into a threat analysis. Great care is taken with access through doors to sensitive areas while some of the organization's highest-risk areas are accessible by physical keys loosely managed with a sign-out list.

Effective key management is an increasingly critical part of any comprehensive facility security plan. Electronic contactless RFID key management systems offer efficiency and security and are most cost-effective over time. As the most popular choice among users at many levels—facility management, security and IT—the RFID technology method of key management is destined to be the most obvious solution for a universal realm of future applications.

Increasing numbers of security directors and facility executives are assessing the risk posed by uncontrolled physical keys. This trend is changing toward much greater use of key management, in some cases in response to government mandates such as FIPS 201-1. As sophisticated access control systems integrate key control into the broader access control capability set, electronic key management is destined to achieve an equivalent ubiquitous presence.

About the author

Mike McGovern

Mike McGovern is the director of sales at Deister Electronics Inc.

Reprinted from

Security Products Magazine
July 2008

Amalgamated Security provides a GPS Tracking service with the most detailed maps of Trinidad

How Video Analytics is Changing the World of Security

By Doug Marman

Security professionals draw upon decades of training and experience when developing plans to protect sites and people. Systems they design can cover a wide range of requirements, from preventing accidental deaths in residential swimming pools, to catching thieves in retail stores, to defending high-risk facilities from attack or intrusion. However, the underlying principles for security and safety are basically the same in all applications:

- **Situational Awareness:** Knowing what is happening at the site, along with the expected activities and potential dangers.
- **Early Warning:** Providing alerts and notification before serious problems occur. The sooner you can identify potential breaches or risks, the stronger your protection will be.
- **Controlling Access:** Limiting those who are allowed to enter and when.
- **Recording Activity:** Capturing information to identify and prosecute offenders creates a significant deterrent against crime, and provides evidence for prosecuting criminals.
- **Responsiveness:** Preparation, training and tools to respond rapidly and appropriately when an alarm occurs.

It is rare to find a single technology that can improve every one of these five basic security functions at the same time. Video analytics are producing exactly such an impact. More importantly, systems that can extract information from video promise to bring us closer to how

ideal security systems should operate:

- Unobtrusive for those who live and work on the premises.
- Automated, so they require minimal human effort when everything is normal.
- Responsive to threats early enough to prevent problems before they occur.

Advancements in all these areas created by video analytics explain why this new technology might be the most significant breakthrough for safety and protection in the last forty years. Video Analytics promises to bring us closer to this ideal solution than any prior technology.



Advanced content analysis systems today already have the ability to:

- Automatically extract information from camera feeds and warn you when something might be going wrong. It is exactly like having your own digital guard.
- Alert people anywhere in the world, providing them video evidence of the detected event.
- Allow for live real-time remote viewing to track and stay in touch with what is happening.

Open up audio loudspeaker

communication with the site, so that intruders can be warned away immediately, before it is too late.

One remote guard using video analytics can now provide protection for 50 sites or more, making protection far more affordable than ever before. As importantly, all 500 - 1000 analytics managed cameras across those sites are continuously monitoring every scene, providing superior protection. Guard tour services, where guards physically walk through the premises on a cyclical basis, can see only a small percent of what is happening. This is no match for the lower cost and constant surveillance gained through video analytics.

Studies show that after 22 minutes, guards watching a video scene will miss up to 95% of all activity. The human brain is simply not designed for long periods of constant watching and waiting for something to happen. Video analytics, on the other hand, is tireless. It never blinks or is distracted.

The most advanced technologies get smarter the longer they study a scene. This is exactly what analytics do best.

For a more in-depth discussion of video analytics, please visit <http://www.videoiq.net/products/resources>

Doug Marman is CTO and VP Products at Video IQ Inc, a pioneer in the field video analytics and intelligent video surveillance.

Article Source:
http://EzineArticles.com/?expert=Doug_Marman

If you are interested in having First Aid Training or Defensive Driving Training for your staff, contact Amalgamated Security

How to Choose a Digital Signature Solution

By Olga Pulisman



There are 10 simple points to consider when choosing a Digital Signature Solution (standard electronic signature) for your organization. While not all are obvious, they are critical make-or-break factors for the smooth implementation, management and use of such a system, impacting on every aspect of your business processes. To ensure a low Total Cost of Ownership (TCO) and a speedy Return on Investment (ROI) from your Digital Signature solution, read on.

1. Seals Documents - This is the basic building block of a true digital signature solution. It guarantees the document is sealed from changes, whether incidental or the result of a late night hacking of your network.

Tip: Only digital signatures based on Public Key Infrastructure (PKI) technology can truly seal a document. Any other type of solution can be easily forged.

2. Multiple Application Support - Many digital signature solutions support only PDF and Word applications, which may be sufficient support for some. However, if your organization needs to digitally sign in additional programs such as Excel, AutoCAD, and web applications, this type of solution will fall short of your needs.

Tip: Make sure the applications you intend to sign in your organization are supported by the solution you choose.

3. Graphical Signatures - Of the standard applications that have

digital signature capacity, almost all lack graphical signature support. This is a major shortcoming. Graphical signatures ensure the signature is visually noticeable, and have a psychological impact: the signer is reassured they have signed the document and that it is legally compliant.

Tip: Occasionally, different graphical signatures are required (e.g., initials, full signature). Verify that your solution has this capability.

4. Multiple Signatures - Many digital signature solutions do not allow altering the document once a signature is applied. This is good in terms of sealing the document, but problematic if the technology also prevents additional users from adding their required signatures to the document.

Tip: If your company requires several people to digitally sign a document, ensure that your solution offers this feature.

5. Zero IT Management - Be aware that the time to deploy a system is typically lengthy and resource-intensive. IT staff can find themselves spending weeks every year managing the selected digital signature solution. Then again, the company may opt to employ an additional staff member to manage the task, or implement a help-desk just to ensure users can digitally sign their documents. Costs can skyrocket.

Tip: Ensure your solution is operational the moment it is deployed on your network, and that the "Zero-Management" requirement on your checklist is met.

6. Compliance - Each regulation has its own specific requirements pertaining to electronic documents. For example, the FDA 21 CFR Part 11 regulation for the Pharmaceutical market has numerous requisites that are not met by most digital signature solutions.

Tip: Review the regulations for your industry and make sure the solution covers all of those requirements.

7. Transportability (Worldwide Verifiable) - Do you want your customers or partners to be able to validate files you've signed electronically? This seemingly trivial task is not so trivial at all. Not every digital signature may be transportable outside of your organization. In fact, digital signature technology is not always embedded in your document.

Tip: Make sure your documents can be validated by external users without them having to install a 3rd-party application.

8. Seamless User Registration - Implementing your digital signature solution must be as simple as possible. Make sure that the moment the solution has been deployed, staff at your organization can start digitally signing documents without having to start a "wizard" to enroll or call on the IT department for support.

Tip: Make certain that your solution is capable of automatically and seamlessly updating user profiles from the company's user directory.

9. Simple-To-Use - Be sure to choose a system that is easy-to-use. You don't want staff to run a wizard application when they A) load the signature application onto their PC and then B) every other time they want to sign a document. IT staff involvement should be kept to a minimum.

Tip: It should take a single click to ensure your document is sealed and legally compliant.

10. Total Cost of Ownership - Not everyone considers TCO when purchasing a digital signature solution. But to ensure you don't pay too much in the long run, take the following costs into account: initial

product cost, deployment, help desk, digital certificates (which may be a recurring annual cost), and development of support for the application you're going to sign with.

Tip: Project your TCO three years into the future to reveal any hidden costs, such as renewal of annual certificates.

ARX (<http://www.arx.com>) is a worldwide provider of digital signatures (standard electronic signatures) for financial, commercial, legal, and government sectors. ARX offers a wide range of high-end, state-of-the-art products and services designed to simplify, seal, secure and accelerate digital transactions anytime, anywhere. The company specializes in designing and implementing quick-to-deploy and easy-to-use digital signature solutions.

If you're interested, there's some useful background (non-commercial) information about digital signatures at <http://www.arx.com/digital-signatures-faq.php>

Article Source:
http://EzineArticles.com/?expert=Olga_Pulisnik

Security is a requirement for sensitive information. Everyone, from CEOs of the largest companies to home users saving tax returns on their home computer, needs to protect sensitive information. Almost everyone has information, on occasion, that they email or store that needs to be protected. Sensitive information needs security that travels with it, wherever it goes.

One solution for protecting sensitive information is digital certificates with data-centric security. Put simply, data-centric security is security that always stays with your data, in transit and at rest. Unlike other security solutions that are focused on stopping attackers and protecting individual assets, data-centric security is about protecting the data itself.

Often when people hear the words "digital certificate" or "public and private key," they have come to expect yet another technical article on PKI (public key infrastructure). Digital certificates, in their simplest form, make authenticating and securing documents and emails extremely simple. Like many forms of technology, digital certificates were once expensive and reserved for large companies with multiple resources, but are now easy to use and available to the masses without requiring infrastructure. This makes implementing digital certificates practical for a variety of purposes -- you no longer need to be a big company with extensive IT resources to take advantage of digital certificates. Small businesses, and even consumers, can benefit greatly from digital certificates combined with data-centric security software. As stated earlier, almost everyone has the need to send or store something securely on occasion. The issue is making sure the software solution you choose is simple to use and works more like a utility than technical security software.

First, let's take a look at how a digital certificate works. A digital certificate is a general term for public and private keys that are digitally signed. When someone gets a key pair, it consists of a public and a private key. The public key is provided to anyone who wants to encrypt something for you. The private key, which only you have, is used to decrypt. A digital signature attaches an identity to the public key so you



Rise of the Digital Certificates

By Steve Laubenstein ·

May 2008

Accelerating access to critical information securely

Securely exchanging and storing documents and emails has become a necessity across multiple industries. An increasing number of businesses need to exchange data internally as well as with business partners and customers. The question is: How do you do exchange information easily, efficiently, *and* securely? How do you deploy a security solution that won't inhibit your business growth by keeping information from the people who need it?

know who it belongs to and is usually performed by a trusted party, such as your company or a certificate authority like Comodo® or Verisign®. This is done so if you receive a public key from a directory or another indirect source, you are assured it belongs to a particular person.

How do you get a public key so you can encrypt documents and emails for someone else? The two most common ways are for a person to email their public key to you, or for you or your security software to retrieve the public key from a directory. If you send an email out of Microsoft Outlook®, Outlook Express®, Vista Mail®, or others, there is an icon labeled, "digitally sign." If you click on the icon, it attaches your public key to the email. When the email is received, just add the person to your contacts where both their email address and public key will be saved. Using a person's public key, you can then encrypt emails and files for them. Public keys can also be found in a directory. Some security software packages can check directories for a public key for the intended recipient(s).

As one might suspect, it is very important to protect your private key. An important step in protecting your private key is to create a backup and store it in a safe place. This is very easy to do, but often overlooked. If you don't backup your private key and have your computer stolen or lost, or your private key becomes corrupt, you will not be able to open any of your encrypted files. (Some security software, like the Enterprise Edition of SecureZIP® from PKWARE®, offers a contingency key that allows companies to retrieve any files encrypted, regardless of what key or passphrase was used, for recovery and audit purposes.) Another important step is to lock your computer when you are not present so someone cannot export a copy of your private key. If they do export a copy, they then can open documents that were encrypted for you.

Why use digital certificates and data-centric security? Many users resist security products because they're often time consuming and difficult to use. Unfortunately, with data security becoming a necessity in today's technology-driven environment, being without it can leave you vulnerable.

Digital certificates and data-centric security, together, create an easy, efficient, and secure way of protecting sensitive documents and emails in transit or at rest. If the document is encrypted with a digital certificate, it can only be opened by your intended recipient, the one with the private key.

The Anachronism of Passwords

So why not just use a password instead of a digital certificate? The problem with passwords is they don't scale, are difficult to share with recipients, and are easy to forget. It is extremely difficult to use passwords when you are sending secure documents to multiple individuals. For example, how do you communicate the password to multiple recipients? Calling or emailing them with the password isn't very secure. In addition, passwords are easy to forget, requiring many people to write them down in locations where they might be discovered, ultimately resulting in sensitive data being compromised. Digital certificates eliminate the need to have to communicate or remember a password.

Digital certificates, used with data-centric security, are a good solution for ensuring your sensitive files and emails are protected. In today's technology-driven environment, data needs to be protected -- without it, the risks are just too high. It is important to secure sensitive emails and documents so they are not compromised if they fall into the wrong hands. It is also important to make sure your security isn't getting in the way of your business growth by stopping information from going where it should. With data-centric security, you can free your data to go wherever it needs to -- securely.

About the author

Steve Laubenstein

Steve Laubenstein has held executive positions with IT Security companies for over 20 years. Steve served as president of a consulting and marketing firm for ten years, helping networking and security companies bring their products to market. He has also held senior sales, marketing, and product management positions for a variety of IT security manufacturers including Symantec, Internet Security Systems, Aladdin, and PKWARE.

**Reprinted from
Security Products Magazine
May 2008**

Tips: Securing A Wireless Network

June 4, 2008

Increasingly, computer users interested in convenience and mobility are accessing the Internet wirelessly. Today, business travelers use wireless laptops to stay in touch with the home office; vacationers beam snapshots to friends while still on holiday; and shoppers place orders from the comfort of their couches. A wireless network can connect computers in different parts of your home or business without a tangle of cords and enable you to work on a laptop anywhere within the network's range.

Going wireless generally requires a broadband Internet connection into your home, called an "access point," like a cable or DSL line that runs into a modem. To set up the wireless network, you connect the access point to a wireless router that broadcasts a signal through the air, sometimes as far as several hundred feet. Any computer within range that's equipped with a wireless client card can pull the signal from the air and gain access to the Internet.

The downside of a wireless network is that, unless you take certain precautions, anyone with a wireless-ready computer can use your network. That means your neighbors, or even hackers lurking nearby, could "piggyback" on your network, or even access the information on your computer. And if an unauthorized person uses your network to commit a crime or send spam, the activity can be traced back to your account.

Fortunately, there are steps you can take to protect your wireless network and the computers on it. As no one step is a complete fix, taking all of the following steps will help you be more secure.

1. Use encryption. The most effective way to secure your wireless

network from intruders is to encrypt, or scramble, communications over the network. Most wireless routers, access points, and base stations have a built-in encryption mechanism. If your wireless router doesn't have an encryption feature, consider getting one that does.

Manufacturers often deliver wireless routers with the encryption feature turned off. You must turn it on. The directions that come with your wireless router should explain how to do that. If they don't, check the router manufacturer's website.

Two main types of encryption are available: Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP). Your computer, router, and other equipment must use the same encryption. WPA is stronger; use it if you have a choice. It should protect you against most hackers.



Some older routers use only WEP encryption, which is better than no encryption. It should protect your wireless network against accidental intrusions by neighbors or attacks by less-sophisticated hackers. If you use WEP encryption, set it to the highest security level available.

2. Use anti-virus and anti-spyware software, and a firewall. Computers on a wireless network need the same protections as any computer connected to the Internet. Install anti-virus and anti-spyware software, and keep them up-to-date. If your firewall was shipped in the "off" mode, turn it on.

3. Turn off identifier broadcasting. Most wireless routers have a mechanism called identifier broadcasting. It sends out a signal to any device in the vicinity announcing its presence. You don't need to

broadcast this information if the person using the network already knows it is there. Hackers can use identifier broadcasting to home in on vulnerable wireless networks. Note the SSID name so you can connect manually. Disable the identifier broadcasting mechanism if your wireless router allows it.

4. Change the identifier on your router from the default. The identifier for your router is likely to be a standard, default ID assigned by the manufacturer to all hardware of that model. Even if your router is not broadcasting its identifier to the world, hackers know the default IDs and can use them to try to access your network. Change your identifier to something only you know, and remember to configure the same unique ID into your wireless router and your computer so they can communicate. Use a password that's at least 10 characters long: The longer your password, the harder it is for hackers to break.

5. Change your router's pre-set password for administration. The manufacturer of your wireless router probably assigned it a standard default password that allows you to set up and operate the router. Hackers know these default passwords, so change it to something only you know. The longer the password, the tougher it is to crack.

6. Allow only specific computers to access your wireless network. Every computer that is able to communicate with a network is assigned its own unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses access to the network. Some hackers have mimicked MAC addresses, so don't rely on this step alone.

7. Turn off your wireless network when you know you won't use it. Hackers cannot access a wireless router when it is shut down. If you turn the router off when you're not using it, you limit the amount of time that it is susceptible to a hack.

8. Don't assume that public "hot spots" are secure. Many cafés, hotels, airports, and other public establishments offer wireless networks for their customers' use. These "hot spots" are convenient, but

they may not be secure. Ask the proprietor what security measures are in place.

9. Be careful about the information you access or send from a public wireless network. To be on the safe side, you may want to assume that other people can access any information you see or send over a public wireless network. Unless you can verify that a hot spot has effective security measures in place, it may be best to avoid sending or receiving sensitive information over that network.

Reprinted from
Security Products Magazine
June 2008



Amalgamated Security provides a full range of security services, which include:
Cash Services
Electronic Security
Access Control
Data Storage
Courier Services
Guarding Services
Alarm Monitoring
Response Services