

The Challenge

For Government Facilities



Government facilities are in need of integrated functionalities of video surveillance, access control and related functions for universal coverage across the Enterprise.



THE CHALLENGE IS:

- To provide role based access control for the organization
- To provide support for multi-protocol systems
- To implement a scalable controller architecture—from single point/door controllers to 64 door controllers.
- To implement FIPS 201 Compliance
- To implement PIV Integration
- To add Threat Level Awareness
- To integrate Biometric readers
- To ensure that the security system uses 128 bit encryption -end to end

Electronic security systems that are used in most government facilities are proprietary system solutions with very little interoperability or operational synergy. This has resulted in isolated islands of systems with unique protocols, operational structures and hardware implementations. As security requirements have grown more complex and interrelated, this has led to significantly sub-optimal solutions for many organizations.

Over the past five years, the technical convergence to IP-based products and systems has dramatically illustrated the advantages of open solutions that utilize industry-standard components and protocols for both operational utility and economic efficiency. This process is perhaps most clearly illustrated by the rapid evolution of security video from proprietary [often analog] imaging, communication and processing components, to open IP solutions that can take full advantage of shared communication and data storage infrastructures. This process has not only enhanced the operational utility of security video, but has led to an explosive growth in the use of video within Electronic Security solutions.

The challenge is to implement a unified system that has the open standards of IP (instead of proprietary technology or proprietary web pages) and integrate your legacy equipment and legacy protocols. As you expand, you want to be able to select the vendor of your choice and not be restricted to work with a specific manufacturer. You want to own and control your user interface, including enhancements and upgrades. And last but not least, you want the new system to meet the most demanding scrutiny of the IT Department.

FIPS 201 incorporates three technical publications specifying several aspects of the required administrative procedures and technical specifications that may change as the standard is implemented and used. NIST Special Publication 800-73, "Interfaces for Personal Identity Verification" specifies the interface and data elements of the PIV card; NIST Special Publication 800-76, Biometric Data Specification for Personal

Identity Verification" specifies the technical acquisition and formatting requirements for biometric data of the PIV system; and NIST Special Publication 800-78, "Cryptographic Algorithms and Key Sizes for Personal Identity Verification" specifies the acceptable cryptographic algorithms and key sizes to be implemented and used for the PIV system.

In addition, a number of guidelines, reference implementations, and conformance tests have been identified as being needed to: implement and use the PIV system; protect the personal privacy of all subscribers of the PIV system; authenticate identity source documents to obtain the correct legal name of the person applying for a PIV "card"; electronically obtain and store required biometric data (e.g., fingerprints, facial images) from the PIV system subscriber; create a PIV "card" that is "personalized" with data needed by the PIV system to later grant access to the subscriber to Federal facilities and information systems; assure appropriate levels of security for all applicable Federal applications; and provide interoperability among Federal organizations using the standards.

When protecting sensitive data, government agencies need to have a minimum level of assurance that a product's stated security claim is valid. There are also legislative restrictions regarding certain types of technology, such as cryptography, that require Federal agencies to use only tested and validated products.

Federal agencies, industry, and the public rely on cryptography for the protection of information and communications used in electronic commerce, critical infrastructure, and other application areas. At the core of all products offering cryptographic services is the cryptographic module. Cryptographic modules, which contain cryptographic algorithms, are used in products and systems to provide security services such as confidentiality, integrity, and authentication. Although cryptography is used to provide security, weaknesses such as poor design or weak algorithms can render the product insecure and place highly sensitive information at risk. Adequate testing and validation of the cryptographic module and its underlying cryptographic algorithms against established standards is essential to provide security assurance.

The MAXXESS Solution

The MAXXESS framework is a highly efficient and cost effective solution for providing a unified operational environment for Electronic Security. It offers a true open architecture as defined by the IT standards of today. Unlike most proprietary software, MAXXESS systems create a customer-unique framework that can be connected to any and all security systems and sub-systems, providing the real-time data necessary for effective decision making.

(Continued)

The MAXXESS Solution *(continued)*

MAXxess systems utilize the existing IP-based networking infrastructure distributed throughout your environment as well as any external Internet resources that may be required to provide the appropriate context for effective security operations. It can directly support IP connected systems and sources as well as bridge, via IP-based protocols, to legacy systems that do not, themselves, have direct IP connectivity.

The MAXxess framework allows any manufacturers system to function as part of one unified system, thereby leveraging the existing (and expensive) assets currently installed. The benefit is that these diverse systems can now work together to respond to critical events and perform tasks as one complete system.

MAXxess systems address all levels of integration and comply with FIPS 201. We implement PIV integration and we can augment your DCID compliance program.

Highlights

MAXXESS FRAMEWORKS ARE ADAPTIVE

MAXXESS frameworks provide you with a smart infrastructure that adapts as your requirements evolve. You don't need to adapt to MAXXESS; we adapt to you.

MAXXESS SYSTEMS PROVIDE A BUSINESS ADVANTAGE

Our framework systems are quick and easy to implement. You only need to implement what you need, when you need it.

We protect your previous investments. We allow you to integrate existing infrastructure with the latest in current generation technology providing you a seamless integration experience.

We protect your previous investments. You no longer have to strip out existing infrastructure when implementing new technology.

We consolidate and unify systems. Eight separate systems may require eight different people to administer those systems. MAXXESS allows you to be more efficient and reduce your administration costs.

We significantly reduce your support costs. Our systems can be changed dynamically and, in many cases, are reconfigurable by you, the end user.

We can link major subsystems and processes to the security infrastructure to provide layered security.

We provide an integration to relevant employee programs, such as:

- Contractor Management (time on site), (expiry links to contracts)
- Safety Certification verification
- Drug /Alcohol screening confirmation
- Mustering
- Remote verification

You don't need to make investments in software, infrastructure or training that are not required to meet your immediate objectives — without, in any way, limiting your ability to do so in the future, when your needs change.

WE LEVERAGE IT TECHNOLOGY

We use existing networks and economically run IP networks wherever appropriate and can integrate a world of wireless sensors that are cost effective to install and open up new monitoring opportunities.

Our single integrated display results in more efficient use of security and security-related personnel throughout your organization.

There is no limit to the number of systems or the number of sites or the number of geographic locations that you can integrate.

Our systems can be upgraded remotely.

We provide redundant server solutions to ensure maximum reliability.

We integrate best in class video, operational and security subsystems.

MAXXESS SYSTEMS GO BEYOND TRADITIONAL ENTERPRISE SECURITY

We present instructions on how to handle an event, ensuring that your organization operates under the policies and procedures that you have defined for those events.

We allow for layered decision making in your enterprise which helps you integrate participation at all levels of the organization and provides a tremendous advantage for staff training.

We logically group major event information so that you can see the bigger picture in the context of both internal and external events.

- We alert you in a textual format describing the event.
- We alert you through a graphical floor plan that shows you where and what has happened.
- We display the video that is related to the event.
- We alert you to external events that may affect your operations.
- We combine all the event information and display it simultaneously.
- We provide a uniform way to report and capture exception events
- We integrate to biometric subsystems
- We do all of the above with 128 bit encryption, end-to-end

In summary, we allow you to see the bigger picture, make more informed decisions, respond quicker to events and be able to share critical information throughout your organization.



MAXXESS

MAXXESS Systems, Inc.

Headquarters

1040 North Tustin Avenue
Anaheim, CA USA 92807
Tel 714 772 1000, 800 842 0221
Fax 714 399 9358
Email sales@maxxess-systems.com

MAXXESS Systems Europe, Ltd. Europe, Middle East, Africa

Doncastle House, Doncastle Road,
Bracknell, Berkshire, UK RG12 8PE
Tel +44 (0) 1344 440083
Fax +44 (0) 1344 424658
www.maxxess-systems.com