



## DEPARTMENT OF THE INTERIOR IMPLEMENTING THE SMART CARD INTEROPERABILITY SPECIFICATION

In September 2003, the U.S. Department of the Interior (DOI) became the first federal agency to successfully implement the government's new contactless smart card standard, known as the Government Smart Card Interoperability Specification (GSCIS version 2.1). Beginning at its mammoth Washington D.C. headquarters, the DOI is using contactless smart card technology as a key element in its new physical access control system and will soon begin using the card for logical (computer) access as well as for a digital signature application. With this new technology in place, the DOI is likely to be the first federal agency to meet the government's new contactless security and electronic authentication mandates as well.

The process that culminated in the DOI's ground-breaking adoption of the government's standard for contactless smart cards began in 1993 when a DOI office in Reno, Nevada, was bombed.

Bob Donelson, then business manager for the DOI's Bureau of Land Management (BLM) Nevada region, recalled, "Security, especially access control, became an immediate concern."

After surveying a variety of access control systems, Donelson became concerned at the lack of interoperability between systems. Given the typical federal agency's longevity and scope of operations, the government is uniformly averse to getting locked in to proprietary systems that can't share information with each other and may not be supported in the foreseeable

future. Donelson made it his mission to develop a truly interoperable access control solution.

In 1995, Donelson was promoted and moved back to D.C. Donelson explained, "I found out about the Navy's smart card program and thought I could do something similar to address the BLM's need for an interoperable access control system." One of the Navy's largest smart card pilot programs, known as the Multitechnology Automated Reader Card (MARC) program, sought to test the application of contact smart cards for both physical and logical security across the entire Pacific Command enterprise. The Navy's security systems contractor, Crane, was asked to find a physical access control system that could support smart cards. AMAG Technology, due to its previous experience developing smart card readers for telecom applications, was the only access control developer that had the necessary knowledge to quickly design one of the world's first physical access control systems that used smart cards.

In 1999, Donelson began to assemble a team comprised of individuals who had been involved in the Navy's smart card program. His intention was to leverage their experience to create an interoperable access control system using contactless smart cards. Given the widespread use of proximity cards throughout the BLM, Donelson believed that contactless technology was a more logical choice than contact. Building on an AMAG access control platform, Donelson and his team



"I am pleased with the performance of the system"

developed a pilot enterprise contactless system including multiple BLM facilities in the southwestern U.S. The pilots were a huge success and demonstrated numerous substantial cost-savings opportunities. Propelled by this success, Donelson began developing plans to develop a system that would extend throughout the DOI enterprise.

When Donelson began sharing this concept with peers from other DOI agencies, some expressed a reservation about getting locked into a single-manufacturer system. To address these concerns, Donelson decided to submit his plan to the General Services Administration (GSA) and the National Institute of Standards and Technology (NIST). Both organizations agreed to help Donelson develop a specification for the use of contactless smart cards to be used throughout the federal government. The first step was the creation of an inter-agency committee, the Physical Access Interoperability Working Group (PAIWG). In July 2003, PAIWG completed its two-year mission by publishing a comprehensive specification for the use of contactless smart cards throughout the U.S. federal government.

In mid-January 2003, the DOI had approved the installation of the AMAG Enterprise system at DOI headquarters. PAIWG committee had not yet completed its specifications but AMAG agreed to make whatever modifications were necessary to make the system, including the prototype S731 contact and contactless card reader AMAG engineered specifically for the DOI, compliant when the specifications were published. In addition to the headquarters building, the DOI requested that the DOI building across the street as well as the BLM headquarters be networked to the central server as part of the initial installation.

The AMAG Enterprise system was installed in early September. Over 2,300 smart cards were issued over the following weeks. The new card features a contactless chip conforming to the new GSCIS version 2.1 specification as well as a contact chip that conforms to the earlier GSCIS version 2.0 used by the Department of Defense Common Access Card (CAC). The new AMAG system features an integrated digital video recording system developed by AMAG partner, Integral Technologies. "I am pleased with the performance of the AMAG system," said Steve Hargrave, DOI chief of security. "We are responsible to provide security to over 3,000 employees and other visitors and need to be able to respond to threats, in whatever shape they may take, before they cross our doorstep. The integrated video will help us with that."



**AMAG Technology**

sales@amag.com

www.amag.com