FIPS-201 - Federally Mandated Security Protocol

Security Integrators who work in the Federal sector are well aware of the ever-changing protocol regarding government standards. We are familiar with air of change because Electronic Security technology is always advancing and evolving. The FIPS 201 standard *(Federal Information Processing Standard Publication 201)* is perhaps the most important federal standard in the field of Security Integration, and its evolution over the past decade is not only elaborate, it continues to change. The latest version, FIPS 201-2, points Security Integrators to the stringent demands of ever-growing data within the confines of secure interoperability. Condortech Services is not only intent to keep abreast of the changes, but is determined to lead the way in understanding them… not only for the Consumer, but for the Integrator as well.

FIPS 201 was birthed out of the response by most federal agencies in the aftermath of the 9/11 attacks. Government entities were unable to identify employee from other institutions within the Federal field. The Bush Administration recognized this limitation, and with the concurrent development of the Dept. of Homeland Security, the HSPD-12 *(Homeland Security Presidential Directive 12*) initiative was the result. HSPD-12 was the answer for agency interoperability and the aim was to have it fully in place by 2008. But as of 2012, only 5.2 million PIV *(Personal Identity Verification)* cards have been deployed and much more have yet to be. Suffice it to say, this is an ongoing process.

At the nascence of FIPS, traditional Access Control would locally produce ID badges within a system. The White House took control of this aspect of access control to ensure the end-goal of interoperability. Everything was to become standardized and NIST *(National Institute of Standards and Technology)* was tasked to develop the inherent protocol. NIST created standards for all aspects of materials, ranging from readers, cameras, etc. and forged into even the most exact of details for devices. In turn, the responsibility of regulating materials developed according to NIST guidelines fell upon GSA *(General Services Administration)* who now approves all Security devices to be used according to HSPD-12 standards. This created a whole other level of codification and certification, where not only products are approved by GSA, but now Security Integrators seek GSA certification in order to demonstrate mastery of HSPD-12 criteria.

Under these standards, the original Access Control set-up entailed a server gathering personal data. While an organization would have a procedure for internal identification, a repository at the federal level could amass information over time which could potentially slow down a system at the local level. Under this precept, dual authentication was the model which would allow a party to be granted access both locally and remotely simultaneously. GSA would issue Smart Cards from a central location for multiple agencies. These cards would hold advanced encryption methods, of which the PKI *(public key infrastructure)* format known as CAK is currently used. At a given door, the card would present an individual's credentials through certificate format. A third-party entity, would issue certificates which would enable authentication remotely. Thus, certificates would be approved onsite and concurrently through information gathered through the IDMS *(Identity Management System)* centralized database.

FIPS 201-2 compliance entails that all access points are authenticating at local repository and through the IDMS system. The latest design includes a PAM module that grabs FICAM *(Federal Identity, Credential, and Access Management)* data and the PKI/CAK credential and delivers it to IDMS while concurrently communicating to the local Access Control. In the beginning, NIST held the understanding that Security systems were like IT systems. But as the scope of HSPD-12 implementation became realized, and correlation with GSA approval procedure became integral, the interoperability sought between Federal agencies became the macrocosm of FIPS-201 evolution. Essentially, for full HSPD-12 compliance to be available, organizations had to work together well and it was going to take time.

This is where we stand as Security Integrators with FIPS-201-2. HSPD-12 is a federally mandated requirement for almost all Federal governmental agencies. As those who wish to push the advent of more secure standards for Electronic Security, we must understand how FIPS-201 has evolved and what it will continue to evolve into. We must understand what full HSPD-12 full compliance means and must push ourselves to deliver our clients true FIPS-201-2 compliant systems.

By Jorge G. Lozano

Condortech Services, Inc.