



**Guest
Columnist**
TONY DAMALAS

Back-end may be the new front-end

In the four years since the introduction of HSPD-12, government agencies have adopted countless approaches to achieving compliance with the presidential directive. These diverse approaches have one thing in common: they are designed to deliver control. Control over who enters an agency's facilities, accesses its physical property and leverages its logical assets. And at its foundation, control over the information that enables the identification and authentication of its employees and contractors.

But what agencies may not know is that unless they shift the paradigm of front-end versus back-end security systems, they may sacrifice some of the control HSPD-12 was intended to create.

Traditionally, back-end and front-end system components have very distinct roles within an integrated security solution. The back-end enables the solution, serving as the host and the driver of policy decisions. Typically, the back-end is also the destination for the storage and management of data.

Conversely, the traditional front-end represents the part of the system with which the user directly interacts. The front-end translates user input into data which the back-end can utilize. For example, in a physical access control system (PACS), the server or host is the back-end. That back-end stores identity information, as well as the data that allows the system to determine whether a user is authorized to gain physical access. The access control panels and other field devices -- which enable users to interact with the system -- play the role of the front-end.

In the new world order that is HSPD-12, the back-end is commonly referred to as the identity management system (IDMS). This system is the backbone of the HSPD-12 compliant solution. It stores identity information, creates the system infrastructure, defines workflow processes, enables lifecycle management and more. The terminals and devices that facilitate enrollment, registration and issuance of cre-

dentials are considered the front-end.

The core benefit of this new HSPD-12 environment is the assurance that an agency can establish and maintain a single, unique identity for each of its employees and contractors. Ideally, this single, unique identity can be provisioned for physical and logical access control throughout an agency's multiple locations. One back-end system would store identity information, and agencies would leverage the front-end to make updates to the identity, manage authorization for the use of that identity and seamlessly "onboard" and "offboard" users. To do this, the agency must have control over the IDMS, or the back-end.

But many agencies are opting for a managed-services model, relinquishing that control in favor of allowing a third party, such as U.S. Access, to manage their IDMS. Instead of maintaining the back-end host identity server locally, storing and making identity data accessible on-site and enabling local rules processing and customized workflow configuration, the back-end is being outsourced. While this shared management of the HSPD-12 solution means the agency gains valuable resources for its identity management program, it can also mean that it gives up direct, unfettered access to critical identity management information. In the traditional scenario, because the third party issues the credential, it likely also maintains the back-end, effectively isolating the credential information from the front-end components that typically need such information to make valid authorization decisions.

To overcome these challenges, agencies must transcend the traditional scenario and redefine the back-end and front-end. They must transform the legacy back-end to serve as an intelligent and flexible front-end, allowing critical identity management information to be shared with and leveraged by the local agency's internal systems infrastructure. By implementing a framework of workflow capabilities and links between these internal sys-

tems and the new front-end, a local IDMS is created. This creation restores the agency's control over identity management information, and makes that information available where it can be most useful, at the local level.

This new approach will enable agencies to continue to benefit from the managed-services model, while creating valuable links between the third-party and local identity management systems. The downstream link can serve as a provisioning platform, ensuring that the local IDMS and all internal systems that connect to it maintain the most up-to-date identity information in the form of new enrollments, updates and deletions that are originated by the third party at the host, or central, IDMS. Because it now has control over and access to identity information, the agency can leverage the unique identity credential for a variety of additional systems and applications such as physical and logical access control, single sign-on and more. The IDMS not only takes on enhanced functionality, it increases the return on investment by enabling enhanced usage.

With innovative planning and a willingness to shift their systems architecture paradigm, government organizations can transform their back-end to deliver a new, intelligent, authoritative front-end. Through this transformation, they will create storage for unique identifiers, a forum for automated provisioning, control over policy implementation and business rules processing, a framework for workflow and lifecycle management and a platform for compliance and auditing. And they will realize new value for their identity management system and achieve a safer, more secure environment. After all, that's just what HSPD-12 was conceived to help them do. ■

Tony Damalas is vice president of technology for Diebold and a specialist in HSPD-12 and FIPS 201 solutions. He can be reached at:
tony.damalas@diebold.com