



## Leveraging Your Investment

The issuance of a universal credential is only the first step to ensuring the protection of your enterprise. And while federal agencies have been working feverishly to meet deadlines for the implementation of card management systems and the issuance of cards, the true benefits of identity management solutions go far beyond the plastic that enables the verification and authentication of identity. Diebold can partner with you to develop a strategy for usage – the ways in which you allow participants to deploy a credential to gain access to assets. Early consideration of usage can enable you to derive the full value of credentialing, resulting in a comprehensive identity management and access system for your agency or organization.

### *One Enrollment, Countless Applications*

Once you've made the investment in capturing the unique identifying credential data of your employees and contractors, that data can be conveyed through a provisioning process for a variety of systems and applications. These applications may be located not only throughout your enterprise, but across multiple government agencies or organizations. [Automated provisioning is now enabled by leveraging the use of a single credential enrollment process for these multiple applications.](#) That means that once your HSPD-12-compliant system is in place and credentials have been issued (or the credential has been issued for you through a managed service), the same credential data also can be used for human resources systems, Physical Access Control Systems (PACS), Logical Access Control Systems (LACS), Single Sign-On (SSO) applications and more.

[In addition to streamlining the identity management process, provisioning also helps ensure that each employee and contractor maintains only one identity.](#) This results in uniform implementation and use of this identity, simultaneous distribution of on-boarding instructions and off-boarding (deprovisioning) and creates more efficient communications between various systems and departments across organizations or departments. It also eliminates the disparate documentation and procedures that often lead to gaps in your agency's protection measures and, ultimately, breaches in security.



### *Physical Access Control (PACS)*

Your single, unique credential can be used to grant employees and contractors access to your organization's physical assets, including facilities, rooms within facilities, documents, supplies, weapons and more. PACS can include a variety of applications, including visitor management and asset tracking. CredentialOne provisioning solutions can PIV- or CAC- enable one or multiple Physical Access Control Systems (PACS) in a single process.

### *Logical Access Control (LACS)*

Data is quickly becoming the most valuable asset an organization seeks to protect. Once established, a credential can also be used to govern access to an organization's wealth of data and information assets. LACS can include computer (workstation) or network logon, access to digital assets and more.

### *Single Sign-On (SSO)*

Your credential can also be leveraged to enable Single Sign-On (SSO), allowing users to complete a single login to gain access to multiple resources, applications and software systems. SSO can help minimize password vulnerabilities and can result in efficiencies throughout your agency's data warehouse.