



## Oracle DoD Common Access Card Solutions from USIT

### Oracle CAC Solutions for the Department of Defense by USIT

In April 2004, the DoD issued directive DoDI 8520.2 (updated October 2007 as 8500.01E) requiring Public Key Infrastructure (PKI) and Public Key Enabling (PKE) for all new information system acquisitions and upgrades. This directive mandates the use of Public Key Infrastructure certificates for positive user authentication during DoD System access, and dictates policy and procedures for developing and implementing PKI with guidance for enabling PKI for authentication, digital signatures, and encryption.

Out of the box, Oracle provides a simple single sign-on (SSO) authentication solution based on a one-to-one relationship between the user and an application or database account. In reality, many Department of Defense (DoD) applications require the user to have multiple database and/or application accounts in order to accomplish their job. The standard for DoD authentication is the Common Access Card (CAC), however, DoD restrictions allow only one CAC to be issued per person. The user with multiple accounts must log out of one account and then, using a different common access card (CAC), log in to another account.

USIT has developed a unique approach to solving this problem. Using Oracle Private Key Enabled/Single Sign-On (PKE/SSO), we have devised a scenario that maps the user certificate information stored in the CAC account to an Oracle Single Sign-On (SSO) account. The SSO account can then be mapped to multiple mid-tier applications and/or database accounts. The result is a Single Sign-on environment employing CAC authentication enabling access to multiple accounts on multiple databases and applications, using the identity information stored on a single CAC.

USIT has three methodologies for enabling CAC registration, login, and account management, each completely secure and manageable.

- We can enable self-service user registration, with simple user account creation.
- We can enable a user login page with a list of valid Applications and Accounts for the user.
- Lastly, we can automatically log the user into his default application and provide a menu displaying a list of authorized application/accounts for the user.

## How do we do it?

USIT uses a proven methodology to enable CAC across multiple applications and databases.

- First, we configure your Oracle infrastructure to accept DoD user certificates.
- Then we install and customize a user certificate registration and self-service web site for users to register and manage their application accounts.
- For each J2EE custom application, we install a filter to help convert existing applications to accept the user authentication without submitting a username/password.
- Oracle Portal, Forms, Reports and Discoverer are enabled to make use of existing Oracle Single Sign-On framework.
- Finally, we provide a SOA web-service to enable SSO for your existing architecture.

With a single CAC, a Government employee can securely access all of their application accounts, without the need to memorize multiple user name and password combinations.

## Why US Information Technologies?

Since 2003, our team of certified Oracle consultants has been helping organizations like yours implement the mandated DoD public key infrastructure into your existing product line. Our solution helps bring best practices to your next DoD PKE implementation, in a quick, efficient, and completely secure process.

We are an Oracle partner with a team of Oracle certified professionals, many of whom are former Oracle employees themselves. We are focused exclusively on Oracle technologies, with years of experience in Oracle software implementations. We know Oracle best and can provide you with comprehensive Oracle service at a reasonable price.

At **USIT**, we are sure that once we work with you, we will become your trusted advisor for all things Oracle.

## Get Started Today

To learn more, contact **U.S. Information Technologies** at 1-877-874-8872, email us at [contactus@usinfotech.com](mailto:contactus@usinfotech.com), or visit us at [www.usinfotech.com](http://www.usinfotech.com)



[www.usinfotech.com](http://www.usinfotech.com).