

## **GROUP TO CONSOLIDATE SERVICES' IDENTIFICATION, AUTHENTICATION EFFORTS**

---

**Date: March 22, 2004**

A new Navy-led panel has been formed to coordinate "identity management" efforts across the Defense Department.

David Wennergren, the Navy's chief information officer and now chair of the new "Identity Management Senior Coordinating Group," said he is planning to meet in early April with officials developing and fielding technologies that identify military personnel -- biometrics, the Common Access Card and Public Key Infrastructure.

"These things of identity management are absolutely crucial to this vision of network centric warfare that we have," said Wennergren during a March 18 seminar on biometrics. "The future of our organization for information is about being able to get access to the intellectual capital of the Department of Defense so that you can do the transactions you need to do from wherever you are."

For the DOD to reach that goal, it will need strong authentication technology to confirm a user's identify, he said.

"Identity management is absolutely essential to that," he said. In the past, development of PKI, "smart cards," and biometrics were "splintered" by not "being together as a single whole," he added.

DOD is in the process of fielding Common Access Cards to each military personnel as the single identification card that will enable access to buildings and computer networks. The card is equipped with PKI technology, which supports e-mail encryption, authentication and tamper detection. Future versions of the CAC are likely to incorporate biometric technology, such as identifying a person by their thumbprint.

Although each area contains similarities, there are subtle differences, he said. For example, PKI or digital certificates will eventually replace passwords, whereas biometrics will operate more like personal information numbers.

Coordinating these identification methods will help build a common policy, according to Wennergren, because there is a point of diminishing returns in each service working individually.

"There's a right break point, where we come to terms with what needs to be done centrally for all DOD in order to get a path that we can all move down from the standpoint of interoperability," he said. "And then what really needs to be done by smaller enterprises is to take advantage of that technology."

The April meeting will entail establishing a road map in choosing the right set of policies and standards for the group to move forward, Wennergren said.

To do so, the group will look at three areas of business, including tactical operations. The group will also “look at the handful of tasks that really need attention right now” and take up a business-oriented approach to its work to eliminate duplication.

The final component is a strategic approach. The group will set forth a vision and policies for identification management, taking on such thorny issues as measuring results, setting standards and coping with privacy matters.

Such concerns will not make transition easy, but the services should not be “risk averse,” Wennergren said.

Challenges will extend beyond authenticating humans. Devices themselves will also have to be identified, he said.

“Devices do transaction requests all the time without human intervention,” he said. “Knowing with authority which device is asking you for a transaction and that that device is the right one, is a place where [identity management] has been much more haphazard.”

Eventually, establishing a DOD policy will help future commanders, Wennergren said. “If I could understand the additional security given to me by the different forms of biometrics and the different forms of cards and PKIs and things, then I as a base commander can make smart choices as to what things I need for what I’m doing rather than guess, which I fear is where we still are.” -- *Jen DiMascio*

ARMY-16-12-15

© 2004 Inside Washington Publishers