

# Defense Pilot Will Pave Way for Department-Wide PKI Use

## General Dynamics Awarded Contract

WILLIAM JACKSON

**T**o see if a commercial certificate authority can meet its high-assurance requirements, the Defense Department has chosen General Dynamics Communications Systems to conduct a one-year public-key encryption pilot.

Within two years, the Department wants to establish a public-key infrastructure to serve users with transaction needs from low- to high-risk.

DoD agencies have begun fielding PKI-ready applications. But the Department must establish a plan for handling digital certificates, using public-private key pairs, to encrypt and sign electronic data. The pilot is part of DoD's PKI Roadmap 3.0, which was released in October and lists requirements for the Department-wide PKI.

The Office of the Assistant Secretary for Command, Control, Communications and Intelligence defined the requirements for the PKI program, which the National Security Agency (NSA) is running.

**Within two years, the Department wants to establish a public-key infrastructure to serve users with transaction needs from low- to high-risk.**

The General Dynamics pilot is the first test of a commercial Class 4 program. Class 4 service, for medium- and high-value unclassified data on secure or unsecured networks, requires placing a digital certificate on a hardware token—in DoD's case, a smart card.

Class 3 service, for medium-value data in low- to medium-risk environments, permits a software token. Class 5, for high-value information in high-risk environments, requires NSA-approved Type 1 cryptography. General Dynamics is the only vendor so far to receive NSA approval of its Type 1 hardware and software cryptography.

When developing the PKI road map, the Department found widespread use of PKI-enabled applications at classes 3, 4, and 5. Eight agencies with Class 4 needs have asked to take part in the pilot, which is limited to 1,000 users.

"The long-term goal is to provide a Class 4 certificate to everyone within DoD and, where appropriate, Class 5 certificates via the target DoD PKI starting in January 2002," the road map document states.

Although commercial PKI products and services are still immature, the authors of the road map said they expect vendor interoperability within four years.

DoD already has tested commercial Class 3 PKI and has established its own decentralized Class 4 program using the Fortezza card for encrypting Defense Message System E-mail.

CyberTrust, a GTE unit in Needham Heights, Mass., will provide the digital certificates for the pilot.

Datakey, Inc., of Minneapolis will supply the smart cards that hold the digital certificates and private keys.

"We are the systems integrator," said Sandra Wheeler, business development manager for General Dynamics Communications Systems, formerly a part of GTE Government Systems. She said General Dynamics would give help desk support and training to integrate PKI into applications such as secure E-mail.

DoD registrars will access GTE's central certificate authority online through a Secure Sockets Layer connection. A registrar must verify in person the identity of each user receiving a digital certificate. A copy of the certificate goes to the certificate authority. Another copy resides on the smart-card token, which generates a public-private key pair with the private key on the token and the public key held by the certificate authority.

Messages are encrypted with a recipient's public key and decrypted with that person's private key.

Messages are digitally signed with the signer's private key and verified with that person's public key.

General Dynamics could act as the registration authority, "but in this model, we see most agencies having their own local registration authority, since it is an in-person identification," Wheeler said.