

CAC Middleware... Putting the CAC to Work for Information Security



By Tim Russell

As of July 2002, more than one million Department of Defense (DoD) users have been introduced to the Common Access Card (CAC) — the DoD's new standard identification and benefits card that provides active duty and selected Reserve, civilian and contractor personnel with physical access to buildings and secure areas, and authentication for accessing computer networks. While the card represents the most tangible element of the CAC program and the part most visible to DoD personnel, the software that functions to support a user's CAC card on PC workstations is an equally vital part of the equation, even though many users don't realize it or might not even know it's there. But without software, the CAC card can't perform the secure logical access applications for which the card is intended. This August, Datakey was notified, along with three other vendors (Schlumberger, SSP-Litronic and Spyrus), that it had been selected as an approved supplier of middleware for the DoD CAC program.

Working jointly under a partnership agreement with the National Institute of Standards and Technology (NIST) on behalf of DoD agencies, Datakey electronic memory key technology was revised and reengineered to develop a prototype secure token for computer workstation authentication in 1989. Based on this secure token, Datakey manufactured the first cryptographic Smart Card used for digital signatures in 1991. Former President Clinton used Datakey technology on two occasions while in office — to digitally sign an intergovernmental agreement with Ireland in 1998 — and to sign the Electronic Signatures in Global and National Commerce Act (E-SIGN), legislation that took effect Oct. 1, 2000, making electronic signatures as legally valid as signatures on paper in the United States.

Datakey began developing a version of software specifically engineered for the CAC program following the specification requirements, and implemented PKCS #11, MS-CAPI and the DoD-defined Basic Services Interface (BSI), allowing users to take advantage of any DoD CAC card to run their information security applications, including encrypted and digitally signed e-mail, VPN access and PC login applications. Beyond supporting all on-card cryptographic operations, Datakey CAC middleware also includes its supporting software library to perform a complete range of cryptographic operations in software. The middleware provides users with the utilities that are necessary to manage their Smart Card, including a PIN manager, the ability to view digital credentials, and the ability to register certificates within Microsoft environments. Datakey CAC middleware can also be field-enabled to support the full list of current Datakey Smart Card/token options, including all configurations of its Model 330 cryptographic Smart Card, for seamless integration with leading PKI and VPN products.

Datakey also provides GSA-ready Smart Card technology for the Smart Access Common ID Card program. Government customers who have deployed Datakey Smart Card technology include: (1) The Department of State - 40,000 Diplomatic Security users will carry a Smart Card for facility access to DoS buildings and



embassies and for secure network access. In addition to security, benefits include increased efficiencies and user productivity. Personnel can access corporate networks by using the same ID card that grants physical access to buildings. By using a single ID card for many applications and uses, the Department leverages its investment for the greatest possible return on investment. Old paper processes and applications can be securely transitioned online for time savings and 24x7 availability; (2) The Federal Deposit Insurance Corporation - 3,500 field agents and more than 7,000 internal users digitally sign/encrypt e-mail messages and documents, and access corporate facilities. FDIC field agents use an Electronic Travel Voucher (ETV) System application with Smart Cards and laptops for reimbursement of travel expenses. The electronic system interfaces with the National Finance Center (NFC). Previously, it took up to two months for field employees to be repaid, but by using Smart Cards it now takes two days for a direct deposit to an employee's account. The paper reimbursement costs about \$50 per transaction to process, whereas the new process costs less than \$10. Since the FDIC processes 80,000 to 100,000 vouchers every year, this results in savings of about \$3.2 to \$4 million. Due to the success of the ETV pilot program, the FDIC has expanded the program to a fully operational, ongoing cryptographic Smart Card endeavour. Other customers using Smart Card technology include: the Department of Energy, Rocky Flats Environmental Technology Site, the Bureau of Labor Statistics and the Canadian Department of National Defence, which deployed 90,000 Smart Cards.

As more and more DoD users (up to 4 million) receive the CAC card, the missing link is the software required to put the card to work in information security applications (secure network access, digitally signed and encrypted e-mail, etc.). Datakey CAC middleware bridges that gap and enables a powerful, interoperable and CAC-compliant solution that works with any CAC-compliant Smart Card. Through Datakey's contract with the government, any DoD organization can order Datakey middleware and begin taking full advantage of the CAC card.



For more information on CAC Middleware contracts visit the DON IT Umbrella Web site at www.it-umbrella.navy.mil or the DoD ESI site at www.don-imit.navy.mil/esi. DoD organizations can order Enterprise Software Initiative (ESI) CAC Middleware directly from the DON Web site, ITEC-Direct, at www.itec-direct.navy.mil or by contacting a Datakey representative at 1-888-328-2539 or 1-301-261-9150 in Washington, D.C. Tim Russell is vice president and general manager of Datakey Inc. □