The US Department of Defense (DoD) has started a worldwide issuance of smart card-based ID badges. Years ago, the Department of Defense envisioned the value smart card technology could bring to the re-engineering of a number of government processes. During initial pilots, only simple demographic information was offered, such as name and serial number on the card, and a significant increase in process efficiency was experienced. New technologies have been instrumental in enabling to reach the next generation standard solution, enabling broad deployment of a smart card vision, offering enhanced security through digital signature services, ease-of-use for badge-holders and opportunities for large-scale cost reduction programs.

ActivCard is being deployed worldwide by the DMDC to support the issuance and personalization of 4.3 million Common Access Cards (CAC) using a comprehensive digital identity infrastructure technology. The Defense Manpower Data Center (DMDC) of the US Department of Defense is about to roll out 4.3 million Common Access Cards (CAC) using a comprehensive digital identity infrastructure technology by Nelly Dimei, ActivCard.

The new badges will support a wide range of functionality from building access to financial services to digital identity for access to government services and information containing personnel information and processing credentials that enable digital signature, encryption, and strong user authentication. However, the market for Digital ID technology is much larger, spanning every sector of human activity. From business and healthcare to entertainment, transportation and education, our technology enables the mobility, privacy, security, ease-of-use and digital identity management essential for network delivered applications and services. Digital ID technology has been designed not only for computers and the Internet, but for use with cable and satellite television and with land and mobile phone networks, as well.
Milestones of the project
In February 1997, US Vice President Gore called for the “use of information technology to reengineer the government’s business processes and provide public electronic access to the government’s services and information.” A report published by the federal Electronic Processes Initiatives Committee (EPIC) Card Services Task Force further stated that: “Smart card systems serve as the ideal platform to support the government’s business process reengineering for the future.” In 1998 and 1999, systems were piloted and the Smart Access Common ID requirements were defined. In May 2000, a Government Wide Acquisition Contract (GWAC) was awarded to provide smart card products and services that are competitively priced and support a common, interoperable, multi-application Smart Card solution, worth $1.5 billion over 10 years. Based on extensive return on

The DoD contract will soon represent one of the largest deployments of digital identity for network computing in the world.
investments studies and smart card trials during the past 5 years, the US Government has now selected the best technology and is leading the world in deploying next generation information technology that it has determined will:

- strengthen security - passwords are simply not good enough in today’s Internet connected world, and PKI without a smart card is no better than a password;
- guarantee privacy - digital identity is less about keeping people out and more about allowing only the appropriate people in. Identity is crucial to privacy and privacy is critical if personal, confidential data is used by digital services;
- increase customer satisfaction - the new ID badges bring the ATM user experience to network computing, giving users, what they want, when they what it, from where ever they are in the world;
- improve quality of life - reduce data entry, reduced processing time, reduced time in lines, reduced administration burden and more accurate information processing.

Digital Identity

Digital Identity links people from their physical world to the digital world. Digital Identity is a requirement for businesses using web based computing for their network systems, services and applications. It creates confidence for an inter-connected business process by assuring users and service operators that people are who they say they are and that transactions are sent and received as intended. It enables mobility, terminal independence and single-sign-on. Digital Identity is the foundation for enabling the Internet to be the tool, not just for marketing, but for every business process or communication.

Digital Identity Management

Digital Identity Management is the combination of technology and business processes that manage the issuance, assignment, protection and control of credentials that digital services use to uniquely identify people and transactions. Specific softwares, based on industry standards, enable applications and data that uniquely identify a person to be securely generated and loaded on a personal security device (PSD) such as a smart card or mobile phone. It enables user identity information to be physically linked to a person, which is the critical basis to the effective use of network infrastructure technology such as PKI, digital signature, firewalls, VPN, and digital authentication and authorization.

Digital Identity user software

The new DoD Common Access Cards are used by inserting the card into a smart card reader attached to a PC used by the cardholder to access digital services. The user then enters the correct PIN, similar to an ATM transaction, to enable use of the credentials and data on the card. The PC requires software that understands the communication interfaces through which information on the card can communicate with digital services and through which the card can be managed, updated or modified remotely, after it has been issued. These communication interfaces have been defined by the GSA CAC interoperability standard.