Smart Card Alliance

# *Smart Card Technology: The Right Choice for REAL ID*

## States Benefit from Security and Cost Efficiency

### The Only Secure Identity Solution

Smart cards offer the only technology solution that provides a highly tamper-resistant identity credential that can tie the cardholder to the credential and that ensures only those authorized to read the identity information are allowed to have access.

- **Identity Fraud Prevention**: Smart cards deter fraudulent users and can ensure that only the person to whom the card is issued will be able to verify their identity when the card is presented. Smart card technology supports PINs, biometric factors, and visual identity verification. Biometric factors can be stored directly in the secure chip in the smart card and be used to verify that the individual presenting the card is the individual to whom the card was issued. Such verification links the individual cardholder and the document securely together and provides the necessary strong authentication of an individual's identity.
- **Privacy Protection with Encrypted Data**: Smart cards support the encryption of sensitive data, both on the credential and during communications with an external reader. Encryption ensures that only authorized readers and entities have access to the information on the card. In some cases an agency or department may only be authorized to have access to information associated with a specific transaction or process and not to other information on the card that pertains to other transactions or benefits. To ensure privacy, applications and data must be designed to prevent unauthorized access.
- **Prevention of Forgery and Counterfeiting:** Smart cards include a wide variety of hardware and software features capable of detecting and reacting to tampering attempts and countering possible attacks. In the event someone attempts to tamper with the chip on the card, the chip will detect the intrusion and shut itself down, rendering the credential useless. Smart cards are almost impossible to duplicate or forge because of the ability to incorporate cryptography and biometrics. Data stored in the chip cannot be modified without proper authorization (a password, biometric template, or cryptographic access key).

### The Only Technology to Provide the Cost Efficiency, Convenience and Flexibility for Multiple Applications

The ability of smart card technology to support additional applications can generate both cost savings and potential new revenue sources for states. Due to the smart card security features, it is only technology which can support multiple uses of the current driver's license such as: indicating driving privileges; establishing that the cardholder can engage in age-related retail purchases or board an aircraft; enabling additional applications that the state chooses to incorporate to enhance citizen convenience and/or government service efficiency. By using smart card technology for REAL ID, states can choose to use the trusted REAL ID credential for applications beyond Federal purposes according to their needs, budgets, and timeframes.

For example, a smart card-based driver's license could not only indicate driving privileges and allow physical access to facilities and services, it could also allow individuals to take advantage of e-government applications such as filing taxes, requesting official papers (e.g., birth certificates) online, or accessing secure networks. Incorporating these applications into the REAL ID enables a digital workflow that eliminates processing errors, saves time and saves enormous amounts of money.

In addition, smart card technology is flexible. Multiple applications can be enabled on the smart ID card at issuance or can be added after the card is issued, allowing functionality to be added over the life of the driver's license or ID card.

## Citizens Benefit from Convenience and Protections

### One Secure Card = Multiple Uses

A smart card-based REAL ID driver's license or identification card can provide citizens with the basis for accessing government information technology (IT) systems. For example, citizens could use their REAL ID driver's licenses to securely access government online applications (e.g., for filing taxes or requesting official papers online). This provides citizens with a new and important use of their driver's license or identification card and immediately addresses fraud and identity theft and issues around stolen or forgotten passwords.

### Secure Cards Help to Protect Citizens from Identity Theft

Identity theft was identified as a growing threat in 2002 by the General Accounting Office[1] and has been estimated to exceed $50 billion per year in the United States by the Better Business Bureau®[2]. With 60 percent of identity theft complaints relating to Internet activities, the security features supported by smart cards can provide a basis for trusted consumer to-and-from government Internet transactions. Smart cards allow online users to easily verify their identities. In addition, if a citizen loses a smart ID card, the technology enables the card to be "shut down" if compromised, thus immediately protecting the citizen from identity theft.

### The Only Technology to Provide Strong Privacy Protection for Citizens

The privacy of a citizen's personal information endures only as long as security protections are in place to prevent access to, or tampering with, that information. Unlike other identification technologies, smart cards can implement a personal firewall for an individual's data, releasing only the information required and only when it is required. The card's unique ability to verify the authority of the reader and the card's strong security at both the card and data level make the smart card an excellent guardian of a cardholder's personal information. Unlike other forms of identification (such as a printed driver's license), a smart card does not reveal all of an individual's personal information when it is presented.

In addition, information stored on the chip can be protected so that it cannot be surreptitiously scanned or skimmed, or otherwise obtained without the knowledge of the user. Access to personal information stored on the smart card can be controlled through user-presented PINs or passwords or by biometric matches at the place of use, requiring the cardholder to be present. By allowing authorized, authenticated access to only the information required for a transaction, a smart card-based ID system can protect an individual's privacy while ensuring that the individual is properly identified.

## About the Smart Card Alliance

[1] GAO, "Identity Theft: Prevalence and Cost Appear to be Growing," GAO-02-063, March 2002 (http://www.gao.gov/new.items/d02363.pdf)

[2] Better Business Bureau, "New Survey Shows Identity Fraud Growth is Contained and Consumers Have more Control Than They Think," January 31, 2006 (http://www.bbbonline.org/IDTheft/safetyQuiz.asp)

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology.  Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought.  The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America.  For more information please visit http://www.smartcardalliance.org.

The Smart Card Alliance Identity Council is focused on promoting the need for technologies, legislation, and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud, and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.