Smart Card
Alliance

SMART CARD
DIGITAL SECURITY INITIATIVE
(SC-DSI)

I. Mission and Goals

Mission Statement:

The Smart Card Digital Security (SC-DSI) has been established to increase the size of the smart card market in North America by establishing a broad-based understanding that smart cards are synonymous with security in the networked world and by seeking to resolve any technical or business issues that may exist, or arise, that could make it difficult for a developer or user organization to employ smart cards in their security solutions.

Further it is broadly understood that the primary hurdle to the broad adoption of smart card security solutions is the lack of readers built into network devices. A special task force within the SC-DSI will address this problem.

Goals:

The goals of the Smart Card Digital Security Initiative are:

1) Promote the critical role of smart card technology in securing B2B e-business, enterprise systems, bank card transactions, and consumer Internet applications;
2) Help ensure the smooth implementation of smart card technology for security purposes in internet, credit/debit card, mobile commerce, and network security applications; and,
3) Strongly advocate the inclusion of smart card reader/writers as original equipment on all types of network capable devices including PC's, Internet appliances and mobile phones, to ensure that smart card-based security can be broadly implemented.

II. Background

The SC-DSI effort is an outgrowth of a 6-month long strategic planning process undertaken at the Smart Card Industry Association (SCIA) in early 2000. SCIA is now part of the Smart Card Alliance and its specific interests, those of smart card technology suppliers, are the responsibility of the Vendor Council within ALLIANCE.

During the SCIA planning process it was determined that the organization should focus its energy and resources on a limited number of activities that would have a very high likelihood of making a significant difference in the rate at which the smart card market grows in North America.

A series of meetings were held with representatives of SCIA's core constituency, namely marketing managers from smart card and terminal manufacturers and solution providers. Marketing professionals were selected over technologists, because these are the people with direct communication with current and prospective customers. During these meetings, the group identified and categorized customer concerns and set out to determine which the association could best address.

The meetings lead to the selection of two types of activities that would position the industry for accelerated growth. The primary area of focus was the important role that smart cards should play in the security of the networked world and led to the establishment of this initiative. It was felt that the smart card industry needed to speak with a unified voice of advocacy during this critical time when the infrastructures and architecture of the network world are being established.

Upon accepting this recommendation, the SCIA board of directors determined that the pivotal importance of the initiative demanded that the industry make a united front and approached the Smart Card Forum about jointly undertaking the effort. An announcement of a joint effort was made by the organizations in September 2000.

As a result of the interaction between the SCIA and SCF, it became apparent that the industry would be best served if the organizations took their cooperation one step further in the form of a merger. This led to the creation of the Smart Card Alliance; a combined industry association that will oversee a variety of activities intended to grow the smart card market. The Vendor Council was established in the new Alliance structure to ensure that the Smart Card Digital Security Initiative continued to be the primary focus of cooperation efforts in the industry.

III. The Rationale for Smart Cards in Digital Security

The SC-DSI satisfies the principal criteria established during the SCIA planning process, namely that there be a high likelihood of successfully building industry sales as a result of the effort. By focusing on security, the initiative begins with a very strong base. There is extremely broad recognition that smart card technology is by far the preferred solution for many network security problems, by serving as:

- a secure portable token providing digital identity,
- a hardware-based authentication device, and
- a secure storage device for cryptographic keys and certificates

Most of the major players in the electronics industry have made significant investments in the development and/or integration of the technology. Outspoken supporters of the technology include Microsoft's Bill Gates, Sun's Scott McNeally, and Internet creator Vint Cerf. They recognize that the very growth of networked systems depends on the security, mobility and convenience that smart cards can provide.

It is understood that smart cards are just one component of broader system solutions and a wide variety of approaches are available to address the increasing demand for security in networked systems. However, smart cards <u>are the most attractive approach</u> for many key security battlegrounds. Some of the reasons why are:

- <u>Designed for security</u> - chips designed for smart cards are engineered with a variety of hardware and software protection schemes not found in other types. A partial list of these features is presented in Exhibit A.

Exhibit A

Partial List of Security Features Found in Smart Card Chips*

frequency detectors
voltage detector
Crypto coprocessors
heat detectors
passivation presence detectors
light/UV detectors
constraint (mechanical deformation) detectors
random generators
frequency jitter
random wait states
metallic grid layer
memory witness cells
fuses (physical and/or logical)
memory scrambling
memory ciphering (RAM)
free internal clock

• other security features found in smart card chips are not listed because of their proprietary nature. Not all features found in all products

- <u>Accepted form factor</u> - the plastic card form factor is widely accepted by the vast majority of the population and has been associated with “trusted” applications such as payment systems, drivers licenses and secure identification credentials for over three decades

- <u>Billions Sold per Year</u> - As a result of having produced many billions of cards, the smart card industry has well established and well refined production techniques for both chip components and plastic cards. As a result smart cards provide the most cost effective hardware-based implementation available for logical security. As an example, the implementation of basic DES encryption technology in a smart card adds less than $0.10 to the cost of the card. Full math crypto-coprocessors start at around $2 dollars when populating a smart card chip. This is far lower than any other form factor.
- <u>Windows, Blue, Fusion, GSA’s Common Access ID</u> - Smart cards are the preferred hardware-based authentication method on key programming platforms such as Windows and Java. They are now being issued in large numbers in key industry segments including banking, government and mobile communications. This spectacular leap toward critical mass will result in a standard presence of smart card reader/writers on PCs, workstations and internet devices.
- <u>More items to be added</u>

IV. Operational Plan Overview

The basic structure of the SC-DSI includes three operational units: two committees and one task force[1]. These teams represent the three major areas of activity covered by the effort.

Expert Technical Committee – This panel of experts is charged with addressing any technical issues standing in the way of user organizations, developers and OEMs adopting smart cards for digital security.

Marketing & Communications Committee – Comprised of marketing and communications professionals this group will undertake promotional and educational programs to ensure that user organizations are fully aware of the reliability and cost-effectiveness of smart card security solutions, and

Smart Card Reader Deployment Task Force (SCRD Task Force) – This group, comprised of representatives of user organizations and developers, will conduct a multi-pronged industry advocacy effort to insure that smart card reader/writers become standard equipment on new PCs, workstations, and internet devices.

The key to the success of the initiative is the interaction between the three operational units. As a result there will be a dedicated Executive Director who will guide the day-to-day activities of the initiative and coordinate the relationship between the three work groups. Where appropriate, Internal staff, volunteers from member companies and outside experts, will augment the Executive Director.

SCIA and SCF have committed initial funding of $500,000 to the Smart Card Digital Security Initiative effort in its first two years.

V. Functional Description of Operations

Executive Director

[1] The differentiation between a committee and task force is important. The two committees are populated primarily by representatives of ALLIANCE vendor members, although others who contribute significantly to the work may be invited to participate. The Task Force is comprised primarily of representatives of user organizations whether they are ALLIANCE members or not.

The role of the executive director will be a full-time paid employee dedicated to making the SC-DSI a success. The responsibilities of the Executive Director will include:

- Oversight of the initiative, including:
    - refinement of mission statement
    - refinement of goals and operating plan
    - establishment and tracking of annual budget
    - establishment of metrics for the evaluating the overall success
    - development /production of printed pieces promoting SC-DSI
    - monthly reporting to vendor council including accomplishments during period, budget status, performance against metrics, actions planned for next period
    - coordination of operating unit activities and participation in meetings (see detail below)
    - administration of any supplier or consulting relationships
    - general communications and public relations

- Overseeing the formation and operation of the three operating units including:
    - creation of mission statements
    - refinement of goals and operating plan
    - solicitation of members
    - coordination and communication including distribution of meeting agendas (7 days in advance of meetings), attendance at all in-person and telephone meeting, distribution of minutes (within seven days of meeting conclusion)
    - development of detailed work plans and schedules of meetings for 6 month period
    - administration of any supplier or consulting relationships
    - establishment and tracking of annual budget
    - establishment of metrics for the overall initiative and the individual operating units
    - arranging for production of products and deliverables including print pieces

- Serving as the point person in industry outreach including:
    - speaking at conferences and seminars
    - traveling with the SCRD Task Force
    - talking to the press

Expert Technical Committee

The expert technical committee is to be comprised primarily of representatives of the supplier community who are ALLIANCE members. Additional resources may be called upon from non-ALLIANCE members if agreed to by the group. This includes the use of consultants as allowed by the budget.

The committee has a simple, albeit ambitious goal, to:

> *address any and all issues which could stand in the way of solution providers or user organization adopting smart cards for the purpose of providing security.*

The term issues shall be interpreted broadly. In addition to obvious issues such as interoperability specifications, etc., the group should be willing to address more mundane issues. For instance, it should address issues such as high chip failure rates on cards that are also used in "low shoulder" magnetic stripe readers.

The Expert technical committee does not need to solve every problem with a "perfect" technical solution. In fact it has available to it a variety of actions, including:

- Educational/Outreach: (often these will be implemented with the assistance of the Marketing & Communications committee)
    - Industry circulars: advise industry members on problems and solutions
    - Pamphlets/brochures for dissemination to user organizations (may include actual copies for distribution or layouts for subsequent printing by user organization)
    - Press releases and pubic relations campaigns
    - Speaking at industry events
    - Trade show booths or trade show materials for distribution to members
    - Advertising (as allowed by budget and dictated by need)
- Technical:
    - Formation of a work group to work within the smart card industry
    - Participation with new or existing consortia, association, standards groups.
    - Security Summits: Special meeting meant to bring together the key ALLIANCE supplier members at the highest level to resolve major areas of transience on an important technical issue.

The following tasks shall be among the Expert Technical Committee's activities:

- establish a mechanism for developing an on-going list of technical "road block" issues. List to be generated by 1) committee input, 2) survey/solicitation of ALLIANCE members, 3) survey/solicitation of solution providers and user organizations. The Marketing & Communication Committee is to assist in soliciting the input of the later two sources

- develop methodology for prioritizing and classifying "road block issues".criteria including 1) magnitude of problem, 2) nature of problem (standards, reliability, interoperability, etc.) 3) ability for the SC-DSI to effect change

- develop functional description of each "road block" issue and a plan to address the issue. It is expected that there will be three categories of issue:
    - those that can be address through educational efforts including development of printed materials, public relations campaigns, speaking and other rout reach.
    - those that can be addressed by the industry on a technical basis, such as establishment or endorsement of specifications or standards,
    - those that are beyond the reach of the committee, but require the attention of the smart card community as a whole

- work with the Marketing & Communications Committee to generate materials which will be used in education, outreach and promotional efforts

Marketing & Communications Committee

The Marketing & Communications Committee is to be comprised primarily of representatives of the supplier community who are ALLIANCE members. It is anticipated that the group will consist of marketing and marketing communications managers from major suppliers of cards, terminals and integrated solutions. These individuals need to be available on a regular basis and will be expected to create many of the deliverables of the SC-DSI. Additional resources may be called upon from non-ALLIANCE members if agreed to by the group. This includes the use of contractors, including publications and public relations professionals as allowed by the budget.

The committee has a several responsibilities:

Assist the Expert Technical Committee in its task of identifying “road block” issues. This will be an especially intense activity at the early stage of the project. It will also be an on-going role to provide input to the group about customer concerns, essentially serving as the eyes and the ears of the initiative.

- Produce Educational/Outreach materials and programs flowing from the activities of the Expert Technical Committee:
  - Industry circulars: advise industry members on problems and solutions
  - Pamphlets/brochures for dissemination to user organizations (may include actual copies for distribution or layouts for subsequent printing by user organization)
  - Press releases and pubic relations campaigns
  - Speaking at industry events
  - Trade show booths or trade show materials for distribution to members
  - Advertising (as allowed by budget and dictated by need)

- Develop materials to explain the business case for using smart cards in network security solutions including a templates and case studies which illustrate the cost-effectiveness of the adoption of smart card technology over time.

- Provide a quick-response mechanism (under 24 hours) to respond to any security related incidents that appear in the media. There are two types of incidents that the committee needs to be prepared to respond to:
  - Defensive responses: These would be cases where smart cards, or systems protected by smart card, are compromised either in real world situations or lab type penetrations
  - Offensive responses: These would be cases where systems that do not employ smart cards are compromised. The SC-DSI response would explain how such a situation could be prevented in the future if smart cards are part of the system.

Smart Card and Reader Deployment Task Force

The Smart Card Reader Deployment Task Force (SCRD Task Force) is one of the most important aspects of the SC-DSI. The “chicken or the egg” paradox has plagued smart card industry development for over a decade. In recent months however, the argument for including smart card readers in PCs, workstations, Internet appliances, handhelds and the like has become much stronger. It is time that the industry musters the combined power of its supporters including major banks, government agencies, wireless operators, and industry notables.

The task force has a simple, albeit ambitious goal, to:

> *Convince the suppliers of network hardware that there is about to be a critical mass of smart cards issued in the US. And that this event demands that they include readers in ALL their product offerings.*

Unlike the other operating units within the SC-DSI, the SCRD Task Force is to be comprised primarily user organizations, card issuers, and electronics industry notables. It does not matter if these organizations are ALLIANCE members!

It is important to repeat that the Task Force is made up mostly of user organizations and issuers. These are the people with the best chance of influencing PC and Internet access suppliers. We need to address their biggest requirement…SHOW ME THE CARDS.

There is a secondary benefit to the Task Force effort in that it requires user organizations and card issuers to go on record as being prepared to issue in large numbers.

There are two key elements to the SCRD Task Force:

- SCRD Petition
  The petition is a document expressing philosophical commitment by user organizations and card issuers to having smart cards play a major in the future of their networks. The intent is to have a document that has some teeth, but is open enough that we can actually get the very top person in the organization to sign the document (perhaps electronically, but certainly in ink for the PR effect). We should shot for this being something that Gates, Cerf, McNeally, Chairs/Presidents of banks, Assistant Secretaries in government, etc. will be willing to sign.

- SCRD Tour
  The SCRD Tour is actually a series of two trips to be made in April or May of 2001. A group of representatives from major user organizations and card issuers will visit key electronic equipment suppliers, armed with presentation materials put together by the Marketing & Communication Committee. The group will visit companies like Dell, Palm, Toshiba, Gateway, NCR, Apple, Adaptec, etc. Any touring group should include at least one vendor representative (President or equivalent) to discuss supply and production issues on the industry's behalf.

<u>Smart Card Reader Logo Program</u>
In support of the SCRD effort, the Vendor Council will consider establishing a smart card reader logo that would be administered by the SC-DSI. If adopted, a logo will be developed that OEMs can use to identify products, which have a PC/SC compliant smart card reader. This logo would be licensed and priced to cover legal costs associated with licensing.