

DOCUMENT SECURITY ISSUES

Part of a Series of Datacard Group White Papers for the Secure Document Issuer

ISO/IEC WORKING GROUPS ARE A KEY DRIVER FOR ID SECURITY

Overview

Industry standards are critical to making the development, manufacture and supply of products and services more efficient, safer and cost-effective.

The International Organization for Standardization (ISO) oversees global standards for thousands of products and processes through a variety of sub-committees and working groups. In the ID card and government ID sector, the major benefits of standardization are to ensure interoperability and commonality between technologies, data elements and interpretation, as well as to make machine-readable documents easier to read and be recognized. In addition, standards provide common criteria for product testing and improvement.

The card industry benefits globally from this through its own dedicated working group, ISO/IEC JTC1 SC17. This paper is intended to provide an overview of SC17 and its nine individual sub-working groups or committees and how they work together globally and nationally to bring a high level of value to the ID industry.

MARCH 2007



ISO/IEC WORKING GROUPS ARE A KEY DRIVER FOR ID SECURITY

Working together and group responsibilities

Work on standards within ISO/IEC and SC17 is organized into several technical committees and is carried out in working groups under these committees. Both the committees and working groups are made up of representatives, who are specialists in their respective fields, from industrial, technological and business sectors, which have a need for standards.

In the US, the industry's national committee for standardization is the American National Standards Institute (ANSI). The technical advisory group, known as INCITS B10, is responsible for US contributions to ISO/IEC's SC17. In addition, other representatives from government agencies, testing laboratories, consumer associations and environmental groups, contribute to this work from time to time as appropriate. There are nine individual working groups (WGs) which comprise SC17.

WG1 is centered around the physical characteristics and test methods relevant to ID cards. This includes embossing, magnetic stripe, conformance and durability of substrates. WG3 was established to prepare revised text for ISO/IEC 7501 for machine readable travel documents such as national IDs and e-Passports. The group monitors and defines standards for these in liaison with the International Civil Aviation Organization (ICAO).

WG4 is concerned with integrated circuit (IC) contact cards and defines specifications related to these. WG5 serves as the group responsible for issuer identification numbers and application provider identifiers, while WG7 is responsible for financial transaction cards. Contactless IC cards fall under WG8, which develops standards dealing with the operation of the contactless IC card. Enhanced optical memory cards (OMCs) are equipped with technologies enabling more data capacity, fast access and high reliability. Existing or new standard technologies for this area come under WG9, which also looks at the software or programming interface for accessing OMC data contents.

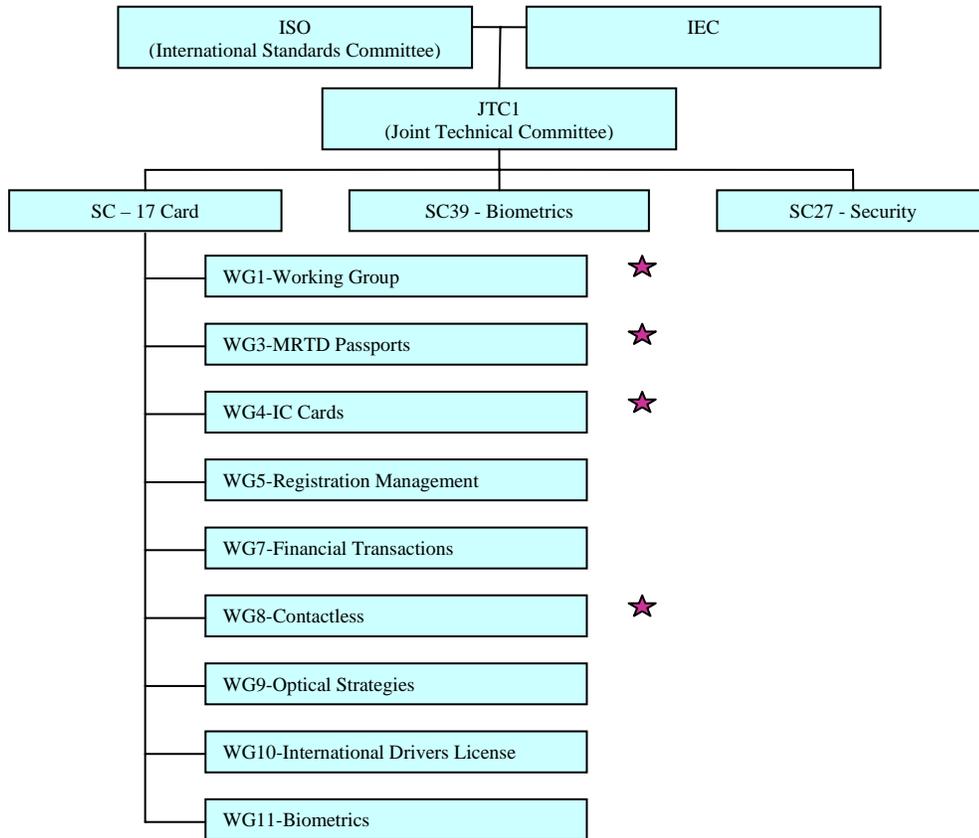
Motor vehicle drivers' licenses and related documents are the domain of WG10, and finally biometrics, one of the fastest emerging technologies, particularly in the field of ID cards and government applications, is the responsibility of WG11. This group is concerned with the interoperability for inter-industry and government solutions using personal identification technologies such as non-generic biometrics.

ISO/IEC WORKING GROUPS ARE A KEY DRIVER FOR ID SECURITY

ISO Standards Structure

There are other subcommittees that are not represented in the graph below.

★ Datacard Group has active participation



National and international participation

The international structure of SC17 exists to aid all sectors involved in ID cards throughout the world. Each member has its own working group or delegation, which meets regularly and feeds into the international body, thus ensuring open lines of communication are maintained. This also means specific regional or national requirements for ID card applications are taken into account when standards are set or modified. In general, existing standards are reviewed and revised by the working groups every 5 years.

As previously mentioned, in the US, the industry's national committee for standardization is ANSI. The technical advisory group (TAG), known as INCITS B10, is responsible for US contributions to ISO/IEC's SC17. This in turn is divided into a number of sub-committees or groups. B10's scope is to develop national and international standards in the area of identification cards and related devices for use in inter-industry applications and international interchange and is currently chaired by a Datacard Group employee.

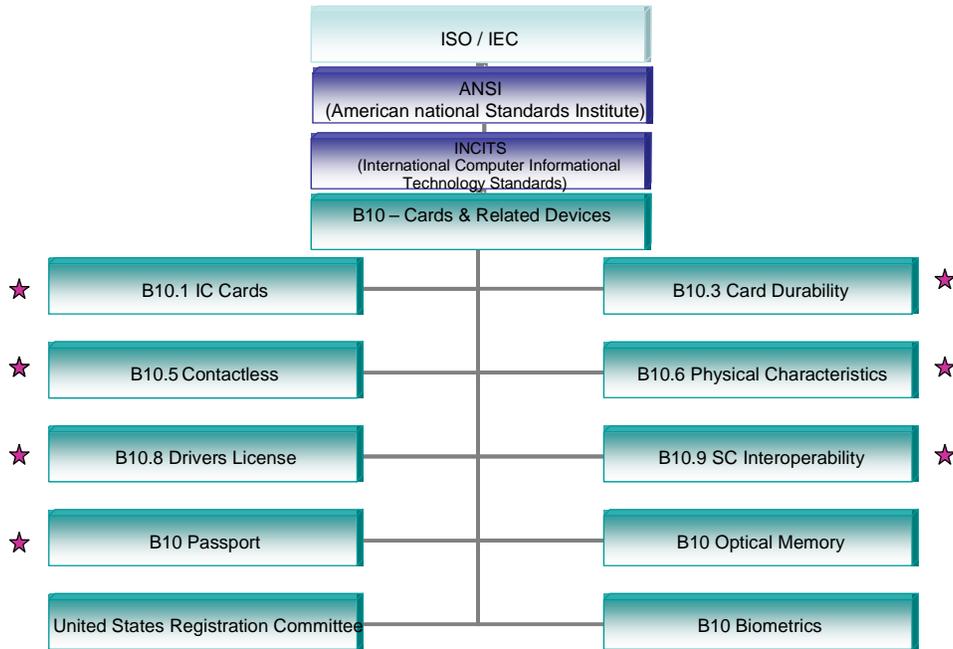
He oversees the focus of all sub-committees' activities. These range from the physical characteristics and test methods for identification cards, integrated circuit cards with contacts and contactless integrated circuit cards to high and low coercivity mag stripe cards and optical memory cards.

ISO/IEC WORKING GROUPS ARE A KEY DRIVER FOR ID SECURITY

Other areas covered include machine readable passports and visas, biometrics, healthcare identification card (ANSI only) and thin flexible cards.

ANSI Structure

(American National Standards Institute)



★ Datacard Group has active participation

Consensus is a key factor

In general, all working groups, both international and their national counterparts, meet to discuss and debate their specific subject or standard development until a consensus is reached on a draft agreement. This is then circulated to the ISO/IEC membership as a whole for comment and balloting. Feedback, which sometimes includes public review, is then taken into account prior to final voting which, if in favor, results in a new international standard being published.

Many aspects of ID card and machine readable security document production, development, personalization and issuance are defined by the work of these groups. For example, the item that carries holder ID information may be a card, ticket, token or document, depending on the standard which defines its size and tolerance. As far as testing is concerned, the methods and apparatus used must provide verification of compliance to the requirements in any given standard.

Development of these tests is a co-operative effort between the working group responsible for the standard and WG1. The relevant working group gives technical detail for the test while WG1 defines the format and acts as project editor.

In the highly secure world of government ID, standards form the foundation for building a specification that meets all the critical aspects for producing such a highly complex product. The ISO/IEC standard includes mandatory and optional requirements and leads to the development of the

ISO/IEC WORKING GROUPS ARE A KEY DRIVER FOR ID SECURITY

application standard such as that for an e-passport or driver's license. This then forms the basis for the application specification, which provides a choice of items from the application standard and national requirements. Finally, this specification, combined with implementation requirements results in product specification and development. This entire process is key to driving security for ID applications.

Standards, which have already been set in this area, are many and varied. Some of these, critical to maintaining security, are ISO/IEC 7501-1 and ISO/IEC 7501-2. The former specifies the form and provides guidance on the construction of machine-readable passports, particularly in relation to the sections of the document containing holder details, which are both visual and machine-readable. Technical specifications include alphanumeric character sets for optical recognition, physical characteristics of ID cards, data elements and country name codes.

The latter, ISO/IEC 7501-2, is related to machine-readable travel documents and visas under ICAO specifications. Other standards falling under SC17 for government ID include specifications for physical characteristics and construction of cards, parameters for card performance in international interchange and encoding techniques. Both contact and contactless IC Cards are also defined by SC17 in terms of power and signal structures, as well as information exchange between cards and terminals.

Security is of the highest relevance when developing standards for government applications. Specifications cover security protocols for use in cards, secure messaging extensions and the mapping of security mechanisms on to cards' functions and services. They also include descriptions of the in-card security technology, data elements for security support, the use of algorithms and certificates, as well as security related commands.

Card applications are also governed by standardization. ISO/IEC 7816-15 specifies the information on cryptographic functionality held within an application. It also facilitates interoperability, enables applications to take advantage of products and services from multiple vendors and allows new technological advances to be employed without re-writing application-level software.

Conclusion

In summary when a government ID application works well with optimum security, it is not only down to the technologically advanced nature of the product or system that supports it. A major aspect of its success is because all its components – from software to hardware, service to support, supplies to business benefits – do conform to standards. This therefore ensures machine-readable documents are easier to read and are recognizable through their interoperability and commonality between technologies, data elements and interpretation.

Additional Resources

For additional information about standards for secure ID documents visit:

- www.SC17.com
- www.incits.org
- www.iso/iec.org