Standardization Trends at GlobalPlatform

Eikazu Niwano† *and Hideki Goromaru*

Abstract

The introduction of smart cards continues to progress in various fields, and technology for loading and managing multiple applications on a single smart card is attracting much attention. This article introduces standardization trends at GlobalPlatform, one of the most influential standardization organizations for multi-application smart card technology.

1. Smart card management technology

The smart card was invented in Japan and France at about the same time in the first half of the 1970s. The original version was single-function and single-purpose. Advances in smart card technology led to the appearance of multi-purpose smart cards by the end of the 1990s. The technology for achieving such multi-purpose use, which is commonly referred to as multi-application smart card management technology, provides mechanisms for performing a range of functions from the issuing of a smart card loaded with applications and keys to the addition of applications after a card has been issued. In short, this technology enables multiple smart card applications to run on a single card. It targets a wide variety of smart cards such as resident registration cards, transit cards, ATM (automatic teller machine) and credit cards for financial services, and SIM (subscriber identity module) cards for mobile communications.

2. GlobalPlatform

2.1 Overview

GlobalPlatform [1], a worldwide standardization organization targeting multi-application smart card management systems, was founded in 1999 based on Open Platform technology developed by VISA. It is one of the most influential smart card standards bodies together with MAOSCO [2] of MasterCard. About 50 companies and organizations from diverse industries have become members of GlobalPlatform. These include credit-related firms like Visa International, MasterCard, and JCB; card vendors such as Gemplus, Axalto, and Dai Nippon Printing; solutions providers like IBM; and communications carriers such as France Telecom and NTT Group.

GlobalPlatform is also a strong advocate of multi-application cards, and in this area, it is developing and deploying guidelines for various fields from an industry-neutral standpoint. In particular, card specifications developed at GlobalPlatform have been adopted at ETSI/3GPP (European Telecommunication Standards Institute and 3rd Generation Partnership Project), which is a telecommunications-related standardization organization, as standards for managing applications in the SIM/UICC (subscriber identity module and Universal Integrated Circuit Card) card for subscriber authentication incorporated in mobile phones. These standards (ETSI: GSM 03.48, TS 23.048, ETSI&3GPP SCP TS 102.225/102.226) are industry standards for smart card application management in mobile-communication systems.

In a similar manner, GlobalPlatform card specifications have come to be included as a representative scheme in the annex to ISO standard 7816-13 together with the framework specified by NICSS (Next Generation IC Card System Group) [3], a Japanese standards organization for public-sector systems, and MULTOS specifications [2] (the license for which has been transferred from MAOSCO, the developer of the specifications, to the StepNexus company).

† NTT Service Integration Laboratories
Musashino-shi, 180-8585 Japan
Email: niwano.eikazu@lab.ntt.co.jp

The ISO (International Standardization Organization) is currently establishing specifications for smart card multi-application management.

2.2 Organization of GlobalPlatform

The organization of GlobalPlatform is shown in **Fig. 1**. The decision-making entity of GlobalPlatform is the Board of Directors, which has 11 elected directors and 3 strategic directors. In addition, but not on the board, there is an executive director for unifying strategy and marketing and a technical director for unifying technology. On the Board of Directors, NTT, Hitachi (treasurer), and JCB are elected directors and Toshiba is a strategic director as Japanese entities. The only other telecommunications carrier on the board besides NTT is France Telecom.

GlobalPlatform has three main committees for establishing technical standards. These are the Card Committee for prescribing card specifications, the Device Committee for prescribing specifications for card accepting devices (terminals in which smart cards are to be inserted), and the Systems Committee for defining not only the server side including card issuers and application (service) providers but also the overall architecture and requirements.

The Advisory Council located between the Board of Directors and these committees was recently established to reflect the opinions and comments of GlobalPlatform users and to drive implementation and deployment of GlobalPlatform standards. This council also serves to interconnect the Board of Directors and the committees, and in this role, it should attain

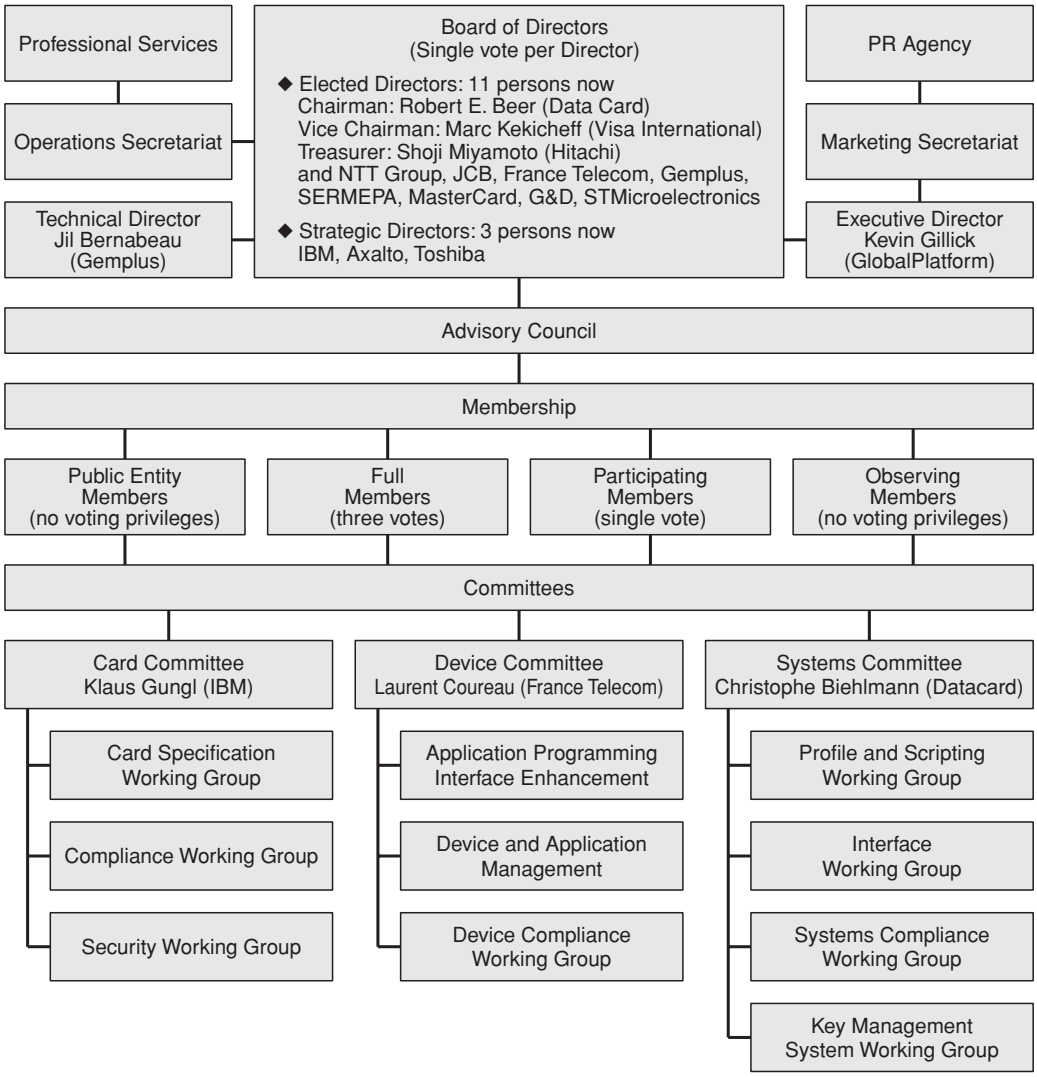


Fig. 1. Organization of GlobalPlatform.

an important position within GlobalPlatform in the years to come.

2.2.1 Card Committee

This committee is the part of the organization where the diffusion and deployment of the most influential specifications in GlobalPlatform move forward. The range of specifications prescribed by the Card Committee includes general card management commands (information display commands, key management commands, etc.), card content management (card application management) commands, secure channel protocol between cards and non-card entities (setup of authentication/encryption channels), and application programming interfaces (APIs) for use by card applications.

The Card Committee established Card Specification V2.1.1 in March 2003 and released V2.2 three years later at the end of March 2006. The main features of V2.1.1 were specifications for symmetric key based secure channel protocols (SCPs) between cards and off-card entities (such as servers), API when using JavaCard, card content management commands (for loading and installing smart card applications from off card entity onto the card) based on those SCPs, and the formats of tokens (permits) and receipts, where the former grants a service provider permission from the smart card issuer to download a smart card application onto a smart card, and the latter indicates execution results. In addition to the above functions, V2.2 provides specifications for PKI-based secure channel protocol, for secure channel protocol for mobile networks, for the PKI based formats of tokens and receipts, for card content management commands which can be combined with PKI-based SCP (additional parameters), and for MULTOS runtime environments. In this way, Card Specification V2.2 incorporates the NICSS based on PKI authentication and MULTOS, thereby covering two of the most powerful standards in the world today.

The Card Committee comprises three working groups. The Card Specification Working Group prescribes industry- and technology-neutral standards for cards and application management on multi-application cards; the Compliance Working Group defines guidelines, processes, and tools for ensuring compliance with card specifications; and the Security Working Group defines security requirements for GlobalPlatform smart cards and develops and maintains the GlobalPlatform Protection Profile based on the Common Criteria methodology.

2.2.2 Device Committee

The Device Committee defines an open architecture and APIs toward the development of applications (called "striplets") on card-accepting devices, such as POS (point of sale) terminals into which multi-application cards are to be inserted, and generally works to facilitate the development and distribution of applications for card-accepting devices. The mechanism for achieving this is the Small Terminal Interoperability Platform (STIP), which is divided into two main sections: STIP Core Framework Technology has common functions and STIP Profile has functions specific to a particular card-accepting device. In more detail, the STIP Core Framework Technology section provides access control, card-owner authentication, and other functions for use by the operating system as a common API for all card-accepting devices (POS terminals and the like that have a reader function). The STIP Profile, in contrast, provides a mechanism for prescribing APIs when using devices that accept specific types of cards. At present, profiles have been prescribed for mobile phones, EFT-POS (electronic funds transfer at point of sale) terminals, and FINREAD (European reader/writer for financial transactions).

This committee was established on the basis of technology developed by the STIP Consortium, which itself was established in 1999 by the Smart Card Accepting Devices (SCAD) working group of the JavaCard Forum to manage common APIs and policies. The STIP Consortium was recently integrated into the Device Committee. Application fields for specifications established by this committee include EFT-POS terminals (STIP EFT-POS profile), ATMs, traffic/transport-related terminals, automatic vending machines, mobile phones, PDAs (personal digital assistants), set-top boxes, home-banking terminals, and personal computers with card readers.

The Device Committee also has three working groups. The Application Programming Interface Enhancement enhances APIs to satisfy business and function requirements of GlobalPlatform members; the Device and Application Management aims to establish a framework for managing devices and applications; and the Device Compliance Working Group provides guidelines, processes, and tools to ensure compliance with the GlobalPlatform Device Specification to achieve the desired level of interoperability.

2.2.3 Systems Committee

The Systems Committee prepares functional

requirements, technical specifications and informational guides for a smart card back-end infrastructure and prepares frameworks to facilitate compliance testing. The committee prescribes the roles and responsibility models for all actors (players such as card issuers and application providers) involved in a multi-application smart card infrastructure and prescribes reference specifications for messaging and data exchange between actors, key-management requirements, and guidelines for smart card personalization.

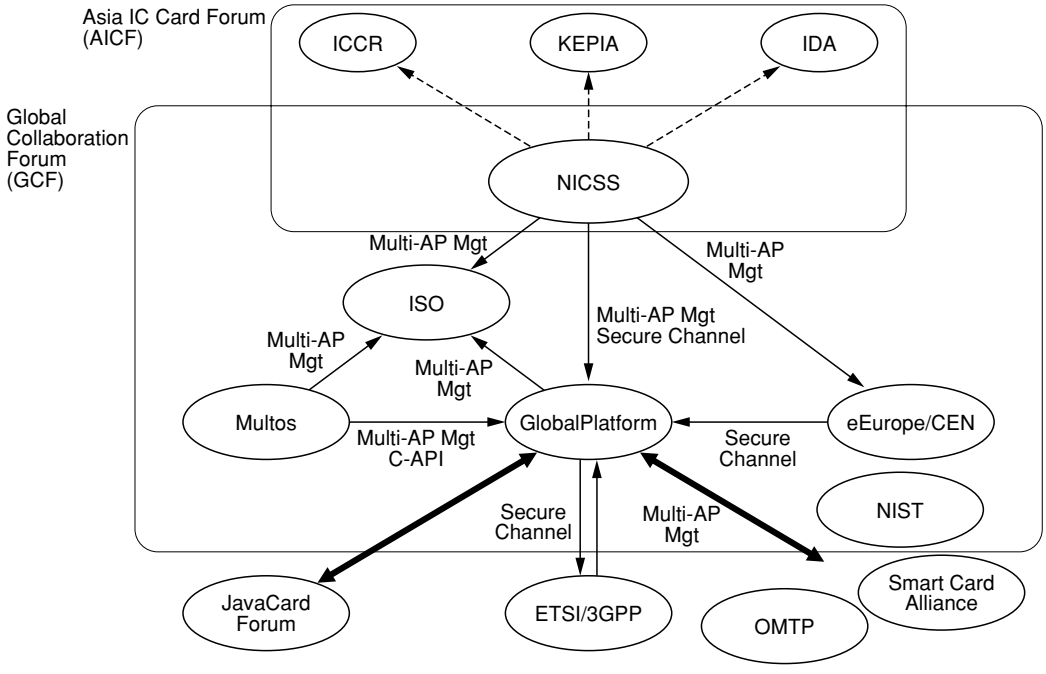
This committee consists of four working groups. The Profile and Scripting Working Group aims to develop open standards for the customization of smart cards (including designs using XML and ECMAScript). The Interface Working Group defines the overall system architecture, which includes card and card-content lifecycles. The Systems Compliance Working Group defines the Systems Compliance Program primarily based on interoperability. The Key Management System Working Group defines interfaces between key-management systems and interoperability between systems that share keys.

2.3 Cooperation with other smart card-related organizations

GlobalPlatform cooperates with many standards-related organizations throughout the world involved in the smart card industry (**Fig. 2**). These include the Asia IC Card Forum (AICF), which consists of Japanese, Chinese, Korean, and Singaporean organizations involved in public-sector smart card systems; the Global Collaboration Forum (GCF) consisting of Japanese, European, and American organizations; NICSS; NIST (US National Institute of Standards & Technology); and, in mobile communications, the Open Mobile Terminal Platform (OMTP) and ETSI, as well as the JavaCard Forum and Smart Card Alliance.

2.4 Implementations

By the end of 2006, the number of GlobalPlatform smart cards in circulation will have reached the 100-million level, and about one billion GSM cards using GlobalPlatform technology will have been issued [4]. Worldwide implementations continue to progress across many industries including finance, healthcare,



ICCR: China National IC Cards Registration Center
KEPIA: Korea Electronic Payment Industry Association
IDA: Infocomm Development Authority of Singapore
AP: application
Mgt: management

Fig. 2. GlobalPlatform and related organizations.

identity (government-related), and communications. Typical examples are Citibank and Sumitomo Mitsui cards in Japan, SK Telecom and KT Corporation telecom-company cards in Korea, the Moscow Social Card, and a public-employee card for the US Department of Defense.

3. Future trends and NTT's involvement

In parallel with its preparation of compliance testing specifications and user guides for e-government systems in relation to Card Specification V2.2, GlobalPlatform is planning to expand into the ID (identity) and government-systems markets. To support this move, a system integrator and government task force has been established within the Advisory Council. GlobalPlatform is already an industry standard in mobile communications and is sure to be a leading industry standard in finance as the next version of Open Platform. Support of PKI authentication in this way should help make GlobalPlatform a leading standard in the ID and e-governments fields as well in the form of national ID cards and resident registration cards. Furthermore, as discussions proceed on the Next Generation Network (NGN) in the field of telecommunications, discussions are also being held on the adoption of SIM specifications as part of standardization activities, and this raises the possibility that the application of GlobalPlatform will expand beyond the mobile network to the fixed network. In addition, specifications prescribed by the Device Committee are beginning to be deployed, and they are expected to undergo further development in the years to come.

Within the above trends, NTT has developed a PKI-based multi-application management architecture [5], has contributed to the establishment of NICSS framework as a major player, has participated in GlobalPlatform since its founding as an elected director on the Board of Directors, and has been the convener of the GlobalPlatform-NICSS Collaboration Expert Group at NICSS since 2002. As a result, the above framework has been adopted in GlobalPlatform Card Specification V2.2 [6], [7] and has come to be recognized as a major worldwide smart card scheme together with the symmetric key-based GlobalPlatform scheme (Card Specification V2.1.1) and the MULTOS scheme.

In the future, we will continue to promote open, dynamic, and secure smart card management through multi-application management based on PKI authentication and developed by smart card standardization organizations. Through these efforts, we aim to support a digital society in which secure information-communication services can be received anytime and anywhere by anyone. Toward this end, we also plan to contribute to the e-Japan strategy and u-Japan policy (information technology strategy and ubiquitous network society policy, respectively) and to efforts to interconnect and link smart card systems around the world.

References

[1] http://www.globalplatform.org/
[2] http://www.multos.com/
[3] http://www.nicss.or.jp/?doc=main_en.php
[4] http://www.globalplatform.org/pressreleaseview.asp?id=398
[5] E. Niwano, J. Hashimoto, S. Senda, S. Yamamoto, and M. Hatanaka, "Smart Card Information Sharing Platform towards Global Nomadic World," IEICE Transactions on Information and Systems, Vol. E87-D, No. 4, pp. 917-927, 2004.
[6] http://www.globalplatform.org/pressreleaseview.asp?id=357
[7] http://www.globalplatform.org/pressreleaseview.asp?id=380

Eikazu Niwano
Senior Research Engineer, Smart Card Platform Development Project, Smart Card Service Promotion Projects, NTT Service Integration Laboratories.

He received the B.S and M.S. degrees in mathematics from Waseda University, Tokyo, in 1987 and 1989, respectively. He joined NTT in 1989 and engaged in R&D of a distributed system architecture. Since 1999, he has headed the development of the concepts and framework of PKI-based multi-application smart card management systems and model-based ubiquitous system. From 2002 to 2005, at NTT's European Office in Paris, he was involved in the globalization of PKI-based smart card management through establishing international projects and joining standardization organizations. He is currently an NICSS Fellow and the Chair of the Global Platform-NICSS Collaboration Expert Group in NICSS. He is Editor of eEurope/Smart Card Charter/TB7/WG4 (multi-application architecture), a member of CEN Workshop on eAuthentication, CEN TC224 WG15 (European Citizen Card) and ISO/IEC SC17 (smart card). He is an active member of the Card Committee and of the Board of Directors of GlobalPlatform. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan, the Physical Society of Japan, and IEEE.

Hideki Goromaru
Smart Card Platform Development Project, Smart Card Service Promotion Projects, NTT Service Integration Laboratories.

He received the B.E. and M.E. degrees in electrical and information engineering from Kagoshima University, Kagoshima, in 1993 and 1995, respectively. He joined NTT Information and Communication Systems Laboratories in 1995. In 2001, he moved to NTT Service Integration Laboratories. He is a member of IEICE.