

行政院衛生署中央健康保險局
(出國類別：考察)

日本、韓國 IC 卡之相關技術及應用

行政院研考會編號欄
I87 / 009007103

服務機關：中央健康保險局

出國人職稱：副總經理 簡任技正 經理

姓 名：江宏哲 王怡人 黃三桂

出國人職稱：經理 經理 科長

姓 名：蔡 魯 李建廷 張禹斌

出國地區：日本／韓國

出國期間：90年12月10日至12月15日

報告日期：91年1月24日

公務出國報告提要

頁數: 44 含附件: 是

報告名稱:

日本、韓國IC卡之相關技術及應用

主辦機關:

行政院衛生署中央健康保險局

聯絡人/電話:

劉彥秀/27029959

出國人員:

江宏哲 行政院衛生署中央健康保險局 副總經理
黃三桂 行政院衛生署中央健康保險局 北區分局 經理
蔡魯 行政院衛生署中央健康保險局 南區分局 經理
李建廷 行政院衛生署中央健康保險局 高屏分局 經理
張禹斌 行政院衛生署中央健康保險局 資訊處 科長
王怡人 行政院衛生署 健保小組 簡任技正

出國類別: 考察

出國地區: 日本 韓國

出國期間: 民國 90 年 12 月 10 日 -民國 90 年 12 月 15 日

報告日期: 民國 91 年 1 月 24 日

分類號/目: I8/資訊科學 J0/綜合(醫藥類)

關鍵詞: IC卡,電子錢包,晶片

內容摘要: 此次行程參訪日本HITACH(日立公司)半導體事業部之甲府廠，瞭解IC晶片趨勢外，日立公司亦表示提供該公司較高規格之型號AE45系列IC晶片作為台灣「健保IC卡建置計畫」之晶片，並實際進入廠區參訪晶片製作過程。並蒐集日本境內IC卡相關組織資料，同時對日本某一健保醫療IC卡實驗計畫作初步瞭解，其存放欄位內容與本國之規劃大部分相似，嚴格來講，日本之IC卡偏向於病歷紀錄，而本國IC卡較不偏向病歷紀錄。日本之醫療保險卡頗受民眾接受及好評，相信台灣的健保IC卡亦能獲得民眾的支持及肯定。韓國僅有健康照護IC卡之構想，但尚未有具體執行計畫，僅在金融上進行發放IC卡計畫，發卡初期，磁條及IC晶片並存，而本國是紙卡及IC卡並存一段時間；首次發卡時民眾不出資，但遺失、換、補卡則民眾需付工本費。在過渡期之作法，本國與韓國發卡方式諸多觀念相同。

本文電子檔已上傳至出國報告資訊網

行政院衛生署中央健康保險局
(出國類別：考察)

日本、韓國 IC 卡之相關技術及應用

行政院研考會編號欄

服務機關：中央健康保險局

出國人職稱：副總經理 簡任技正 經 理

姓 名：江宏哲 王怡人 黃三桂

出國人職稱：經 理 經 理 科 長

姓 名：蔡 魯 李建廷 張禹斌

出國地區：日本／韓國

出國期間：90年12月10日至12月15日

報告日期：91年1月24日

摘 要

此次行程參訪日本 HITACH(日立公司)半導體事業部之甲府廠，瞭解 IC 晶片趨勢外，日立公司亦表示提供該公司較高規格之型號 AE45 系列 IC 晶片作為台灣「健保 IC 卡建置計畫」之晶片，並實際進入廠區參訪晶片製作過程。並蒐集日本境內 IC 卡相關組織資料，同時對日本某一健保醫療 IC 卡實驗計畫作初步瞭解，其存放欄位內容與本國之規劃大部分相似，嚴格來講，日本之 IC 卡偏向於病歷紀錄，而本國 IC 卡較不偏向病歷紀錄。日本之醫療保險卡頗受民眾接受及好評，相信台灣的健保 IC 卡亦能獲得民眾的支持及肯定。韓國僅有健康照護 IC 卡之構想，但尚未有具體執行計畫，僅在金融上進行發放 IC 卡計畫，發卡初期，磁條及 IC 晶片並存，而本國是紙卡及 IC 卡並存一段時間；首次發卡時民眾不出資，但遺失、換、補卡則民眾需付工本費。在過渡期之作法，本國與韓國發卡方式諸多觀念相同。

目次

壹、 考察目的.....	1
貳、 考察過程.....	2
參、 考察內容.....	4
(壹)日本部分.....	4
(貳)韓國部分.....	15
肆、 考察心得.....	17
伍、 考察建議.....	19

壹、考察目的

- 一、 健保 IC 卡係採用日本日立公司(HITACH)半導體部門所研發、生產之 IC 晶片，晶片從設計、開發至生產必須經過一連串的安全保護措施，若因一時疏忽，原始設計資料外流，將會造成整顆晶片遭到破壞，因此，至未來晶片製作場實地瞭解其安全性，並蒐集健保 IC 卡所使用之晶片型號資料。
- 二、 健保 IC 卡建置計畫除了卡片技術外，如何發卡順利亦是一大課題，爰考查日本及韓國等國家之發卡經驗及國內組織。
- 三、 日本境內之健保醫療 IC 卡試辦計畫，其規劃之存放欄位及應用是否有值得本國健保 IC 卡建置計畫借鏡之處。
- 四、 由於健保 IC 卡計畫利用網路來傳輸資料，就傳輸安全之考量，瞭解日本及韓國在這方面如何執行。

貳、考察過程

此行第一行程為參訪日本 HITACH(日立公司)半導體事業部之甲府廠，除聽取公司之簡介、IC 晶片趨勢外，亦實際進入廠區參訪晶片製作過程，第二行程參訪 the New generation Ic Card System Study group(新世代 IC 卡系統研究會，簡稱 NICSS)，蒐集日本境內 IC 卡相關組織資料，並以熊本縣八代市之醫療保險導入 IC 卡實例進行說明，第三行程拜會 Japan Smart card Solution company(日本智慧卡顧問公司，簡稱 JSS)及第四行程韓國 Mondex 公司，瞭解發放卡片之現況及應用，本考察行程如下表：

日期	內 容	拜 會 機 構
12/10	啓程，抵達日本東京；再至新宿搭車至甲府	搭機
12/11	● 甲府工廠簡介 ● IC 晶片發展趨勢 ● 台灣健保 IC 卡採用之晶片介紹 ● 半導體生產工廠實地查訪	HITACH(日立公司甲府廠)
12/12	● 拜會 HITACH CEO 及 CMO ● 蒐集日本境內所有 IC 卡相關組織資料 ● 熊本縣八代市之醫療保險導入 IC 卡實例 ● 瀧川市在商店街主導下導入 IC 積分卡之預付型電子錢包探索	HITACH(日立公司東京總公司) NICSS
12/13	● e-Cash Business 及 CA Business 之	JSS

	說明	
12/14	● 從日本前往韓國漢城 ● 韓國在金融方面發放 MODEX 卡之現況	搭機 韓國 Mondex 公司
12/15	● 返國	搭機

參、考察內容

(壹) 日本部分

一、 參訪日立公司 (HITACH)

(一)HITACH 公司之甲府 (Kofu) 製作廠簡介

日立製作所半導體事業群，從它小平地區(Kodaira)、甲府地區(Kofu)、高崎地區(Takasaki)、小諸地區(Komoro)、那珂地區(Naka)五個製造工廠至其相關的製造廠及公司皆時時保持密切的關係，而每一個個體皆能善用它們特有的優勢在研究、開發及生產活動上。爲了尋求在半導體技術上各方面皆能保持領先的地位，日立製作所以品質、績效及產量等方面將自己定位於世界數一數二的公司。日立製作所生產各種類的高科技產品及技術，此外，也正積極地擴展活動範圍，包括了資訊及通訊的領域、各式的系統、視聽設備、消費性電子應用及汽車電子零件等。

台灣之「健保 IC 卡建置計畫」所採用之晶片係由日立公司提供，並在甲府製作廠製作。甲府地區的工廠主要從事半導體產品的開發及生產。它處理及大量生產晶圓，並完成從設計、開發到製造的一貫的半導體生產過程。它同時也致力於重要資源的研發，並透過與各大學及相關研究機構的合作來開發世界最先進的技術。

半導體及 IC 部門主要是提供優良的半導體產品，在開發、設計、生產及行銷上與關係工廠及企業皆有相互的合作關係。它不僅只是從事製造，同時以其經濟影響力在當地產業社會及針對當地社會更深入的活動中扮演一重要的角色。

該廠自 1964 年成立，佔地 91000 m²，共有 1300 名員工，目前

主要產品為 IC card microcomputer、LCD driver。此次參觀甲府製作廠之新廠房—K6，亦即未來本國健保 IC 卡之 IC 晶片製作場所，K6 具有快速製作之建築結構，同時具備極高的安全系統。

半導體及 IC 部門已在全球三大洲—美洲、亞洲及歐洲設立開發、設計、生產到行銷的完整製造體系，並為了與其海外客戶保持密切的關係，建構了堅強的組織陣容。在海外的設計中心，透過當地人員的直接參與下，使其具有本土化的特色。在設計中心間，彼此以技術交換的方式來達到科技的精密化及多樣化。當製造據點位在相對應的地區，符合當地需求而開發的產品可在各個生產據點立即生產以能迅速地送到客戶手中。由於日本與台灣在地理位置上相鄰近，日立公司針對本計畫擬採由日本製造後再送往台灣，而不採取在台灣生產。

(二)日立公司簡介 IC 卡之發展趨勢

詳細之資料如附錄一。

(三)日立公司提供「健保 IC 卡建置計畫」之晶片介紹

日立公司提供的晶片在健保 IC 卡為 AE450 型號，而在安全模組所提供的晶片為 AE45C 型號，該公司保證健保 IC 卡計畫提供之晶片為 AE-4 系列之晶片，符合 ISO 15408 Common Criteria 之安全認證。

1.AE450 晶片之資料如下表：

Item	Specification
Process	0.35 um CMOS process
CPU	AE-4 – High performance 16-bit CPU

	16 Mbytes Linear Address Space minimum instruction timing: 400 ns for 32-bit addition 2.8 us for 16x 16-bit multiplication
EEPROM	MONOS EEPROM Process 32 Kbytes EEPROM 512 bytes Extra EEPROM Easy access by single instruction 1 to 64 byte programming with one instruction Protected against accidental writing and erasing Data Retention minimum 10 years Programming & erasing voltage generation onchip Endurance greater than 100,000 times Erase time 2ms Write time 4ms Overwrite time 2ms
ROM	128 Kbytes onchip ROM
RAM	4 Kbytes onchip RAM
Coprocessor	1024 bit Key length 512 byte RAM RSA/ECC Cryptography
Onchip functions	Des-Engine for calculation of 56 bit DES key by Hardware, Minimum execution time is 18 clock cycle Watchdog timer to protect software runaways RNG to provide hardware random numbers

	FMU Firewall Management Unit to support multi-application
External Clock	input fclk – 1 MHz to 10 MHz at SV, fclk –1 to 5 MHz at 3V
Operating temperature:	Standard –25°C to +85°C

2.AE45C 晶片之資料如下表：

Item	Specification
Process	0.35 um CMOS process
CPU	AE-4 – High performance 16-bit CPU 16 Mbytes Linear Address Space minimum instruction timing: 400 ns for 32-bit addition 2.8 us for 16x 16-bit multiplication
EEPROM	MONOS EEPROM Process 32 Kbytes EEPROM 512 bytes Extra EEPROM Easy access by single instruction 1 to 64 byte programming with one instruction Protected against accidental writing and erasing Data retention minimum 10 years Programming & erasing voltage generation onchip Endurance greater than 100,000 times

	Erase time	2ms
	Write time	4ms
	Overwrite time	2ms
ROM	96 Kbytes	
RAM	4 Kbytes	
Coprocessor	1024 bit Key length 512 byte RAM RSA/ECC Cryptography	
Onchip functions	Des-Engine for calculation of 56 bit DES key by Hardware Minimum execution time is 18 clock cycle. Watchdog timer supports real time OS & applications with exact time measurements RNG to provide hardware random numbers FMU Firewall Management Unit to support Multi-application	
Power	Single voltage power supply 4.5 V to 5.5 V 2.7 V to 3.3 V Power Consumption Max 10 mA in operation Max 100 uA in sleep mode (clock stopped)	
External Clock	input Fclk – 1 to 10 MHz at SV, fclk –1 to 5 MHz at 3V	
Operating temperature: Standard –25 to +85°C		
Shipping Form 8 inch wafer		

Sawn wafer, unsawn wafer Chip on tape (COT) Module

二、 參訪 the New generation Ic Card System Study group(新世代 IC 卡系統研究會，簡稱 NICSS)

NICSS 的成立目的是要在日本針對 IC 卡系統建立一個共同使用的平台(亦即共通的規格)，透過試驗的方式，採用共同的科技去營造使用者之環境，希望透過此研究會制定共同標準，提供給政府、民間企業、一般大眾遵循。

該會提供日本境內關於 IC 卡組織之資料，詳如附錄二。

該會亦說明日本境內二個實驗計畫供參考，簡略說明如下：

(一)熊本縣八代市之醫療保險導入 IC 卡實例

日本社會保險廳對於平成 7 年(1995 年)到 9 年(1997 年)被保險者證的卡片化進行檢討後，在熊本縣八代市進行使用 IC 卡之「醫療保險卡」的導入實驗。這個實驗使被保險者憑證的機能增加，也記錄健診資料及維護健康資料，以從醫療到健康管理全部能應用的卡為目標。

被保險者憑證的卡片化有如下的優點：

1. 被保險者及被扶養者每個人都能擁有一張卡，在就醫時比一張的被保險者證為全家所共有時更為便利。
2. 平時容易攜帶，在緊急時能及時得到幫助。

3. 因為可以收錄健康診斷等資料，對健康之意識會提高，受診機會也會擴大。

從日本醫療機關立場來看，活用診療時所收錄的健診資訊等，可確保防止病歷表及處方籤轉記時的失誤之外、更有減輕事務的優點。但與本國健保 IC 卡不太相同，日本之 IC 卡偏向於病歷紀錄，而本國 IC 卡較不偏向病歷紀錄。

被保險者憑證的 IC 卡化，健康管理佔了很大的功能。政府掌管健康保險的生活習慣及保健服務，受診結果會記錄在卡片裡，記錄期間為 3 年。與本國健保 IC 卡不太相同，本國健保 IC 卡每紀錄滿六筆就要更新，而日本不需更新，純粹為記錄資料用。這個資料在醫療機關的診療時可做為參考，另外，孕婦的健康指導也可參照健診結果做適切的指導。此外，體力測定的結果也可收錄進去，醫師可根據這個數據做參考進而做成訓練手冊。換言之，日本的這張憑證功能，非常的貼近民眾的生活。例如，被記錄的健康診斷結果、體力測定結果是根據操作「健康建議機器」，自行做健康方面的確認，在這台機器上可看見自己的健康及體力的健康圖表，促進對自我的健康做積極的管理及維持。

醫療保險卡中可收錄的資料如下：

1. 基本情報(保險者號碼、發證日期、被保險者證編號、姓名、出生年月日、本人及眷屬區分、住址、電話號碼等)。
2. 健診資料(健診年月日、接受健診醫療機關、健診結果)。
3. 健康記錄表情報(孕婦指導年月日、指導者名、體力測定結果、實施年月日、實施設施名)。

4. 急救資料(緊急連絡處、血型、藥品副作用、過敏資料)。

為保護個人隱私，對於「讀卡機」之使用對象、IC 卡內的資料項目讀取，都有做對象限定。目前允許的持有身份為：

1. 市府相關業務承辦人員。
2. 醫療機關的醫師、護士、行政人員。
3. 保險者的職員。
4. 八代市健康顧問。
5. 急救隊員。

各種身份的使用者可以閱讀資料範圍各有讀取領域所限定，以加強安全的保護。

日本中央社會保險醫療協議會整理之「關於醫療保險卡的導入效果及影響之調查研究結果」中，關於被保險者憑證的 IC 卡化部份，其具體的效果如下：

1. 提高病歷表的製作效率。
2. 被保險者證編號容易確認。
3. 縮短作業時間。
4. 行政處理效率提高。

被保險者的評價是最大的好處是跟紙的保險證相比，小張且攜帶方便。對於卡片的使用，並沒有特別不滿的評價。

但是不滿的地方則有：

1. 使用範圍不廣。
2. 診療卡跟被保險者證卡必需一起提示。
3. 讀取卡片內記錄的內容的方法不了解等意見。

(二)在商店街主導下導入 IC 積分卡之預付型電子錢包探索

瀧川市的積分卡系統於 1996 年 2 月開始服務，到目前為止已經發行了 3 萬張的 IC 卡(在日本簡稱為元氣卡)。元氣卡的使用一年的消費額為 5 億日元。據瞭解，一開始的目標為一年間會員達一萬人，消費額達一億元日幣，其實驗結果比預想中的目標更佳。

元氣卡當初從營運開始以能與健康管理卡合併做使用為目標。不單限為積分卡，而是以多用途卡做為發展指標。瀧川市的人口為 4 萬 8000 人，消費人口為其人口的半數。其卡片的普及率佔 6 成之多。此外，一個月間的使用者數約 2 萬人，一個人的購物金額平均超過 2 萬 5 千日元，且元氣卡的做法為消費者每買 100 日元就得到 1 點，而 1 點價值 1 日元可以用來購物。消費者完全不需負擔 IC 卡的發行費用。目前元氣卡發行情形如下表。

卡片發行數的累計	約 2 萬 9600 張
加盟店數	110 家店鋪
店鋪末端台數	162 台
1 個月間卡片的消費額	約 4 億 9800 日元
1 個月間積分卡發行數	約 507 萬分

1 個月間手續費收入	約 211 萬日元
1 個月間總利用次數	約 17 萬次
1 個月間利用會員數	約 2 萬人

現在最大的問題是預付型電子錢包的導入，通產省為探討在瀧川市實現上的可行性。並成立「北海道開發問題研究調查會」在其他地方對事例調查及導入上的問題點，做有關的意見交換。但是在市公所的看法是積分卡的滲透度應為優先。對於預付卡功能，不應為優先取決的考量。為了實現預付卡機能，ATM(現金自動預付機)的改造等，會發生新的費用。而其費用的負擔要如何處理，而金融機關取得利益方式需要重新整合。而對 ATM 的操作及卡片所產生的費用所造成心理上的抵抗的使用者能愈來愈少是重要課題。至於加盟店及金融機關之間真正的檢討的開始為止，似乎還需要一些時間。

IC 卡是金融、行政、醫療、交通等的服務利用及多方跨越網路安全、個人認證等。在用途上的使用機能(多媒體應用軟體)全都在一張卡中，對於能集合所有功能及便利性高，未來的發展性被寄予很大的期待。

JSS (此次行程下一個參訪據點) 為促進 IC 卡普及與實用性的提昇，特別利用 MULTOS 等的多功能 IC 卡用作業平台，朝向利用信用卡功能、金融卡功能等，多數有魅力的服務(多媒體應用軟體)的實質化。在領先一般普及的多功能作業平台中搭載應用軟體，實際上從發行、營運、管理等培養出的多樣的技術，擁有專門知識之

不同業種企業組成聯盟，在各別的分野上的先進性充份地活用，檢討、開發拓展 IC 相關業務為對象之各種商務。以提供服務之事業體為目標。

三、參訪 Japan Smart card Solution company(日本智慧卡顧問公司，簡稱 JSS)

JSS 公司於 2001 年 8 月成立的公司，其公司發展重點為：將 IC 卡推展至相關行業，特別是 multi-application 系統之規劃。目前業有二大業務重點，e-Cash Business 及 CA Business，而 e-Cash Business 重點在 MONDEX 的電子錢之推廣；CA Business 重點在 MULTOS CA。而 e-Cash Business 自 10 月至今共發出 2 萬張 IC 卡，尚無發卡上之困難。

JSS 公司針對交易的網路提供二個解決方式，但皆採取透過 INTERNET 的方式進行，不同點在於連結的主機不同，一個是連結 INTERNET 的主機；另一個是交易中心的主機，如果只是一般的下單作業就由 IC 卡經過讀卡機再透過 INTERNET 與 INTERNET 的主機連結處理，涉及加值作業（例如下載金錢）就由 IC 卡經過讀卡機再透過 INTERNET 與交易中心的主機連結處理。詳細資料如附錄三。

該公司所提出之電子錢交易方式是透過 INTERNET，安全顧慮是一大挑戰。日本 IC 卡事業已陸續開始進行推展，像 JSS 公司同類型之公司也一一成立。

（貳）韓國部分

二、 參訪韓國 MONDEX 公司

（一）韓國之 HEALTH CARE CARD

韓國政府原先規劃發放 HEALTH CARE CARD，該卡以 IC 卡為規劃方向，預計採用 8K 的 IC 晶片，共計需八兆韓元（相當於台幣 2222 億元），由於該政府財政困難，無法逐年編列預算，所以該計畫一直延宕，未執行；民間鑑於政府無法近期内執行，遂由該國內三家大型醫院聯合銀行訂定以 IC 卡為主之標準格式及規範，其內容朝多功能規劃，除一般 health care 外，尚有 emergency record、e-billing、credit. . 等功能，待標準確立再由其他醫院一同參與執行，由銀行出資，該案尚在規劃中，執行日期未定。

（二）MONDEX 公司之發卡經驗

韓國在金融方面發放之 IC 卡共計發放約 100 萬張，其中 MONDEX 公司占了 50 萬張，其發卡方式重點如下：

1. 不強迫，由民眾自由選擇。
2. 新申請之卡片，採取磁條及 IC 晶片並存方式發放，並未將磁條取消。
3. 首次發卡由金融機構出資，民眾不需出錢，遺失、換、補卡則由民眾付工本費。
4. 每筆交易透過連線（INTERNET）認證。

雙方經過一連串的經驗交流後，作出下列幾個重點結論：

- 1.該公司佩服本國政府的魄力，願意編列預算執行 IC 卡計畫，並將之列為國家之重點計畫，值得韓國政府學習。
- 2.該公司二年前開始發卡，由於 Infrastructure 建立初期，許多狀況及進度無法掌握，建議本國仍需留意，由於本國發卡量超出韓國甚多，在經驗傳承上能提供的幫助有限。
- 3.雙方發卡方式諸多觀念相同，例如該國磁條及 IC 晶片並存，而本國是紙卡及 IC 卡並存一段時間；首次發卡時民眾不出資，但遺失、換、補卡則民眾需付工本費。
- 4.本國建議韓國 HEALTH CARE CARD 可學習本國經驗，先找一地方試辦，再推行全國。
- 5.本國的健保 IC 卡之內容規劃採分階段執行，但其內容仍以健保資料為主，是否與韓國一樣加入金融功能，有待商榷。

肆、考察心得

本次考察共有參訪健保 IC 卡建置計畫之晶片提供者——日立公司半導體生產部，並實際進入廠內參觀；另外參訪二個日本促進 IC 卡推動之機構 (NICSS, JSS)，並瞭解一個實驗性的 IC 卡計畫，及韓國健保 IC 卡現況 (尚在規劃) 及 Mondex 公司之發卡經驗等，共有以下幾點心得：

- 一、此次參觀行程直接進入 IC 晶片製作場所(無塵室)，親身體會人員安全管制之嚴謹及高科技產品製作過程。HITACH 公司亦非常重視本國健保 IC 卡計畫，願意提供較先進之晶片供本國使用。亦保證該晶片符合 ISO 15408 Common Criteria 之安全認證，應無安全之虞。
- 二、熊本縣八代市之醫療保險卡導入實驗計畫，其存放欄位內容與本國之規劃大部分相似，但本國必須在第二、三階段執行時，才會達到預期效果。嚴格來講，日本之 IC 卡偏向於病歷紀錄，而本國 IC 卡較不偏向病歷紀錄。日本之醫療保險卡頗受民眾接受及好評，相信台灣的健保 IC 卡亦能獲得民眾的支持及肯定。
- 三、瀧川市的元氣卡的成功主要因素是方便民眾使用，所以頗受歡迎，台灣的健保 IC 卡只要能朝便民方向規劃，相信民眾亦能接受。在元氣卡導入預付型電子錢包時，日本政府所考慮的 ATM (自動提款機) 的改造，及與金融機關間之費用關係，在台灣健保 IC 卡若要利用 ATM (自動提款機) 當作民眾更新卡片資料之據點之一時，亦會面臨同樣問題。
- 四、JSS 機構所提出之電子錢交易方式是透過 INTERNET 進行，

在目前 INTERNET 之安全未能有效的防止駭客入侵及破壞前，安全顧慮是一大挑戰；本國之健保 IC 卡擬採用私有網路，即是以網路安全為第一考量。

- 五、日本 IC 卡事業已陸續開始進行推展，像 NICSS、JSS 公司同類型之公司也一一成立，本國健保 IC 卡計畫若能施行順利，國內 IC 卡應用應會陸續發展。
- 六、NICSS 希望訂定一個共通的標準，讓日本境內 IC 卡能遵循，台灣以前有金資中心所訂定的 IC 卡標準，當時諸多 IC 卡皆用該標準，惟因未適用於國際性，已陸續由國際標準取代。健保 IC 卡即採用國際性標準符合世界潮流。
- 七、韓國 HEALTH CARE CARD 因為預算編列問題，使整個計畫暫時無法執行，反而由醫院連結金融機構準備執行，由此可見，IC 卡在健保及醫療上的運用有其必要性。
- 八、韓國之磁條及 IC 晶片並存，而本國是紙卡及 IC 卡並存一段時間；首次發卡時民眾不出資，但遺失、換、補卡則民眾需付工本費。在過渡期之作法，本國與韓國發卡方式諸多觀念相同。

伍、考察建議

- 一、 健保 IC 卡若要方便民眾更新及查詢卡片內資料，而擬利用 ATM（自動提款機）之硬體設施，馬上會面臨 ATM 的改造會發生新的費用，金融機構是否願意吸收該項費用，若不願意，其費用的負擔要如何處理，因此有以下兩種建議方式：

(一)暫時不與金融機構商談 ATM 設備改造事宜，亦即短期間 ATM 不具能讀取及更新健保 IC 卡之功能；而由健保局另行佈建更新機於醫事服務機構。

(二)尋求誘因，促使金融機構主動進行 ATM 設備改造計畫。
至於誘因部分，可考慮釋出健保 IC 卡剩餘之空間。

- 二、 不論日本，還是韓國的 IC 卡計畫，由於皆是試辦型計畫，其發卡規模尚無法讓本國健保 IC 卡建置計畫加以全盤參考，因此，本次發卡作業，健保局將會更加謹慎行事。
- 三、 台灣之 IC 卡事業會隨著健保 IC 卡發放而逐步帶動，NICSS、JSS 類型之公司應會陸續成立，應可將健保 IC 卡之知識及經驗對國際輸出。
- 四、 從日本及韓國的經驗，“電子錢包”屬於未來的趨勢，台灣 IC 卡產業是否跟進，或者健保 IC 卡是否具備電子錢包功能，值得政府再次思考其可行性。

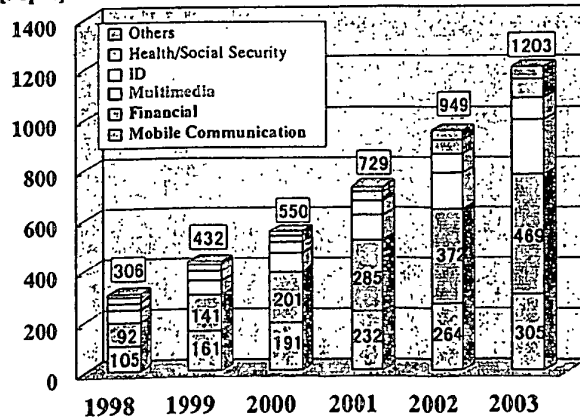
Hitachi Microcomputer for Smart Card

Bureau of National Health Insurance - Taiwan
December 2001

Product Marketing
IC Card Business Unit
Semiconductor & Integrated Circuits
Hitachi, Ltd.

Global Smart Card Market Trend

[Mpcs]

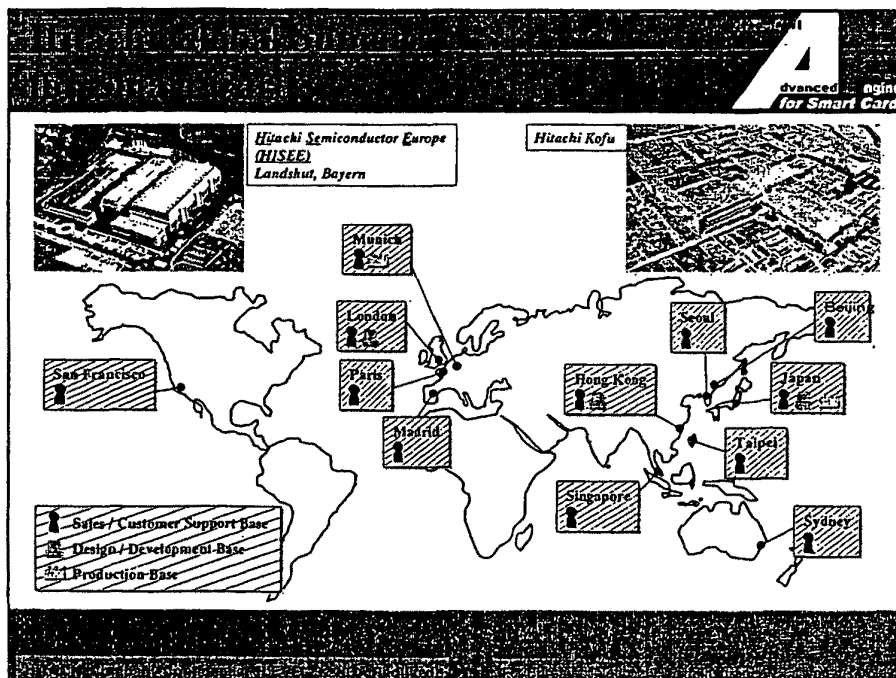
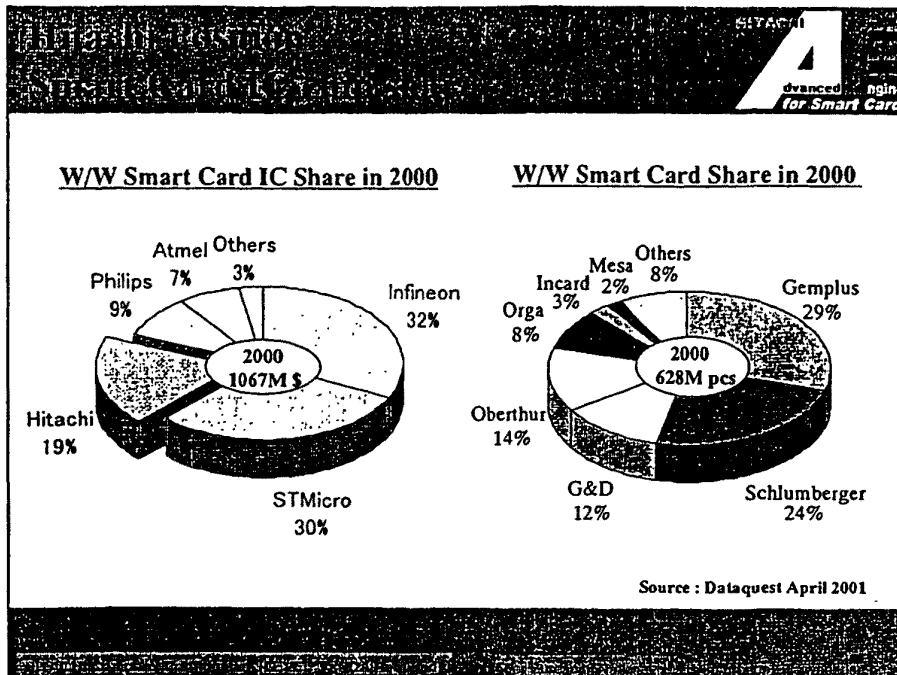


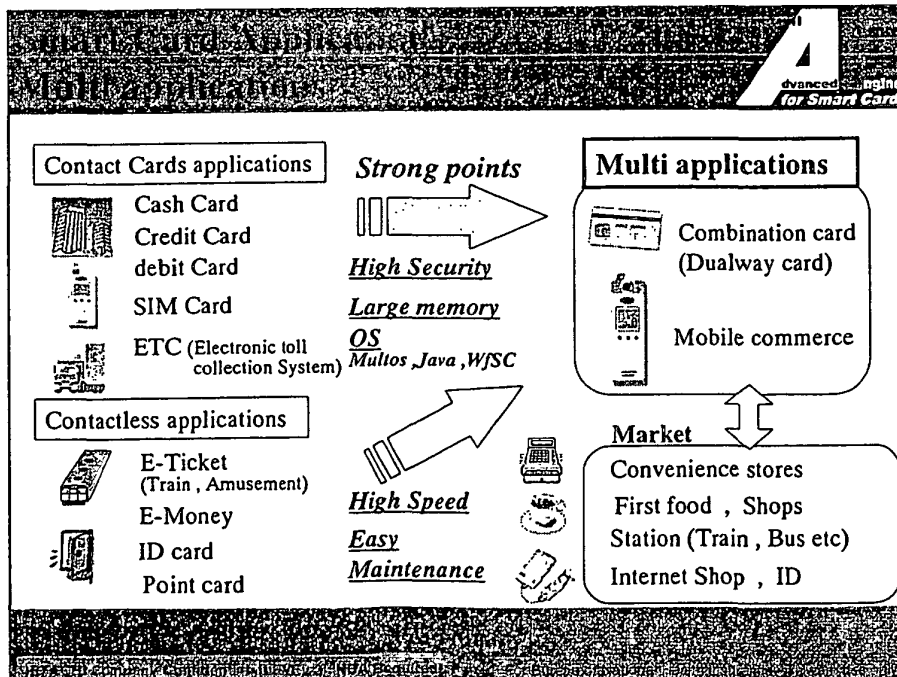
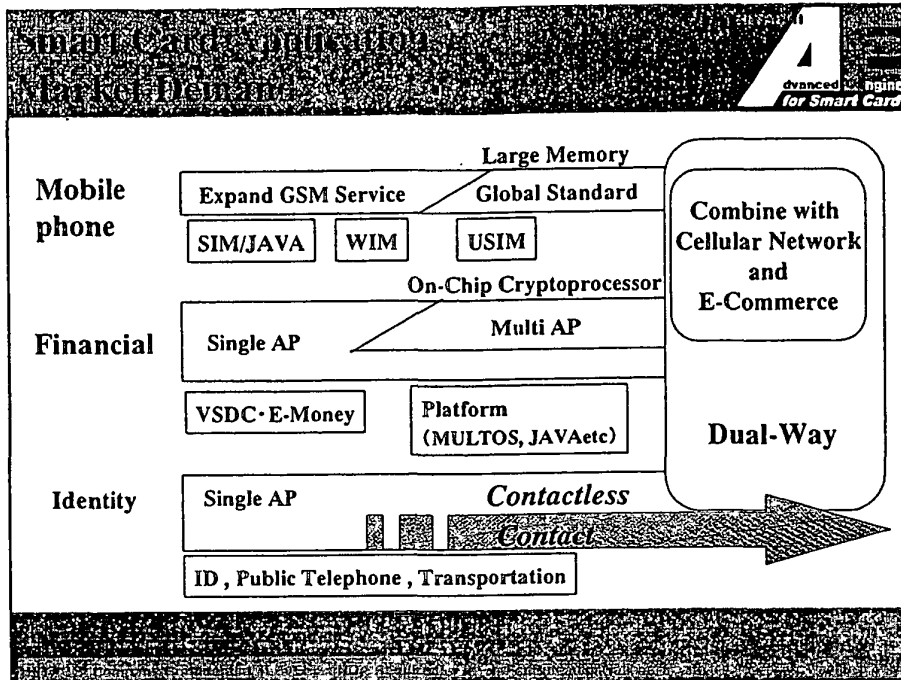
Source : IMS 2000

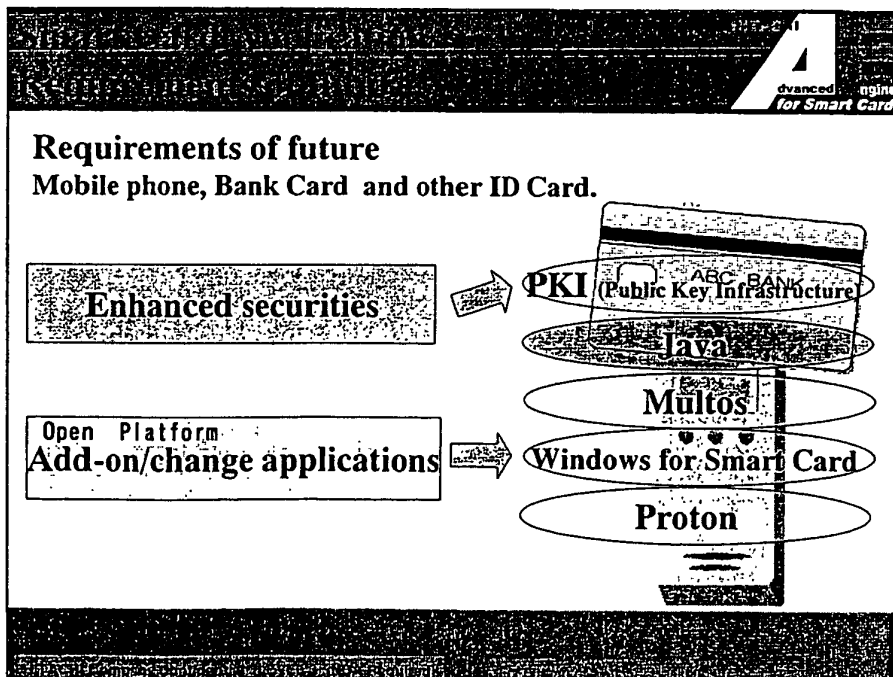
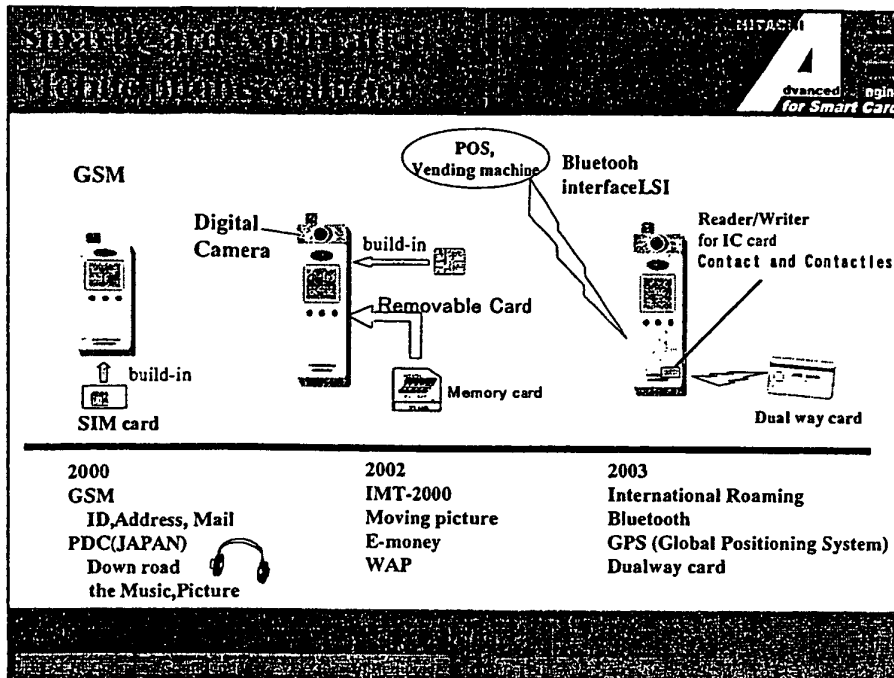
**Toward 2003
Combine**

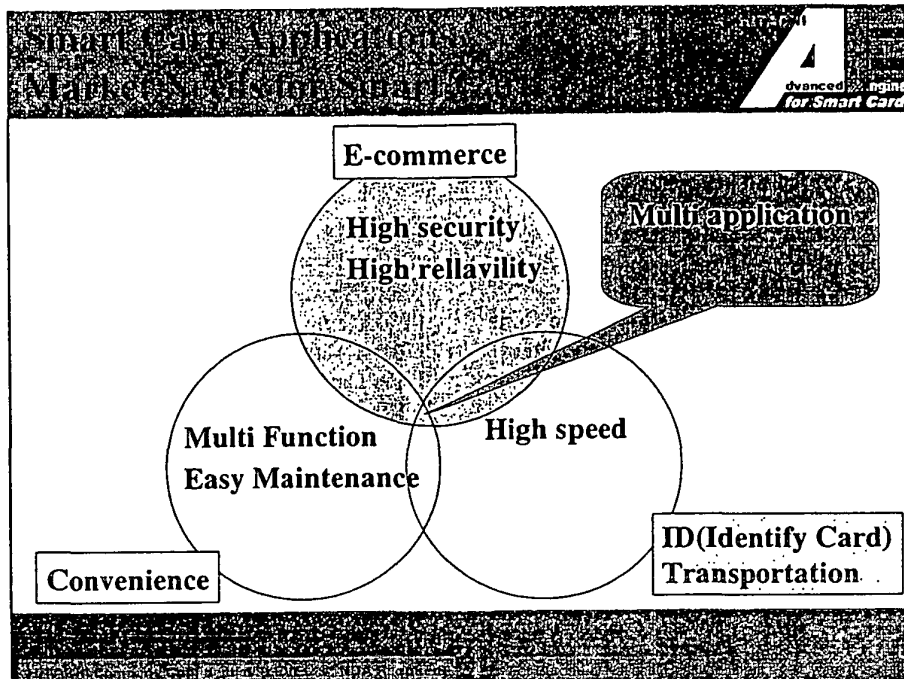
SIM & Financial
(Mobile) (e-commerce)











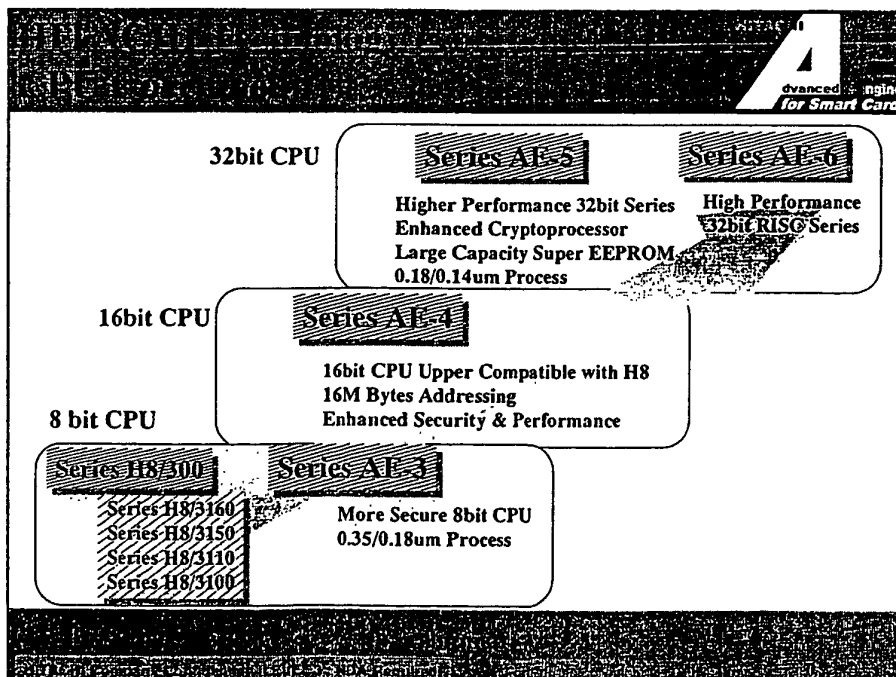
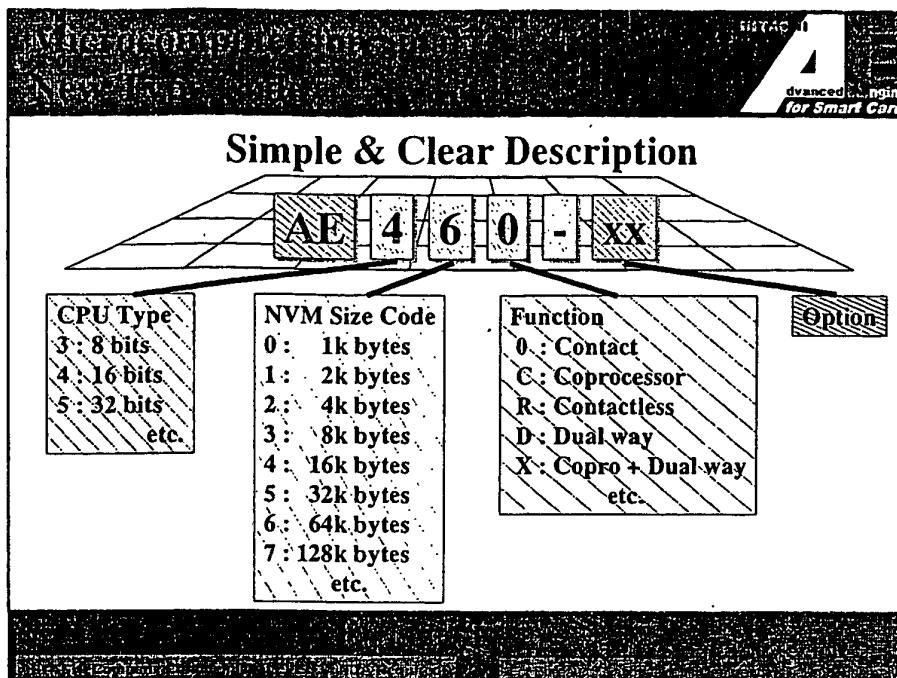
Smart Card Application Market Segments

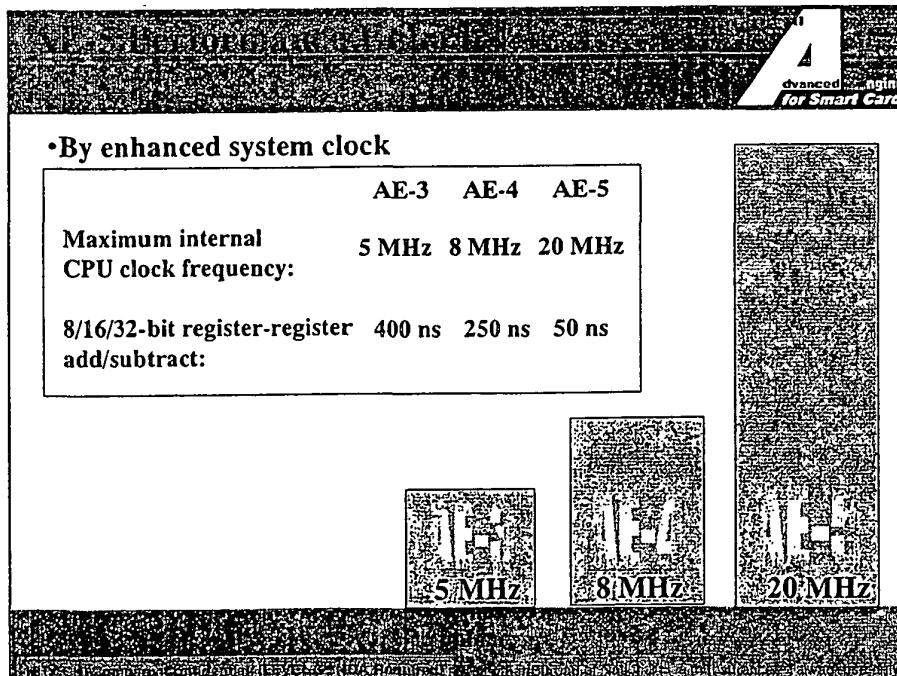
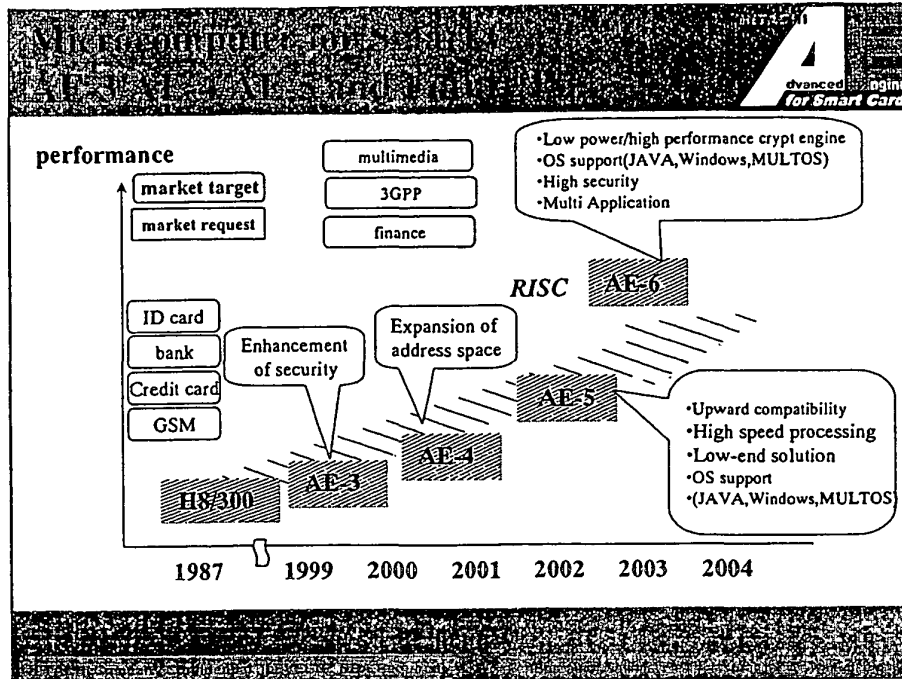
Advanced Engine for Smart Card

- 8 / 16 / 32 bits CPU with linear address space
- Enhanced security
- High performance
- Common ROM and RAM area
- Modular EEPROM sizes
- Selectable crypto functions
- Support for standard OS (JAVA , MULTOS , WfSC)



32K EEP	64K EEP	128K EEP
Clock Multiplier	AE series CPU	
Interval Timer	DES Engine	
Fast I/O	RNG	
ROM	Watchdog	
RAM	FMU	
1024 bit Mod.		
ECC Mod.		

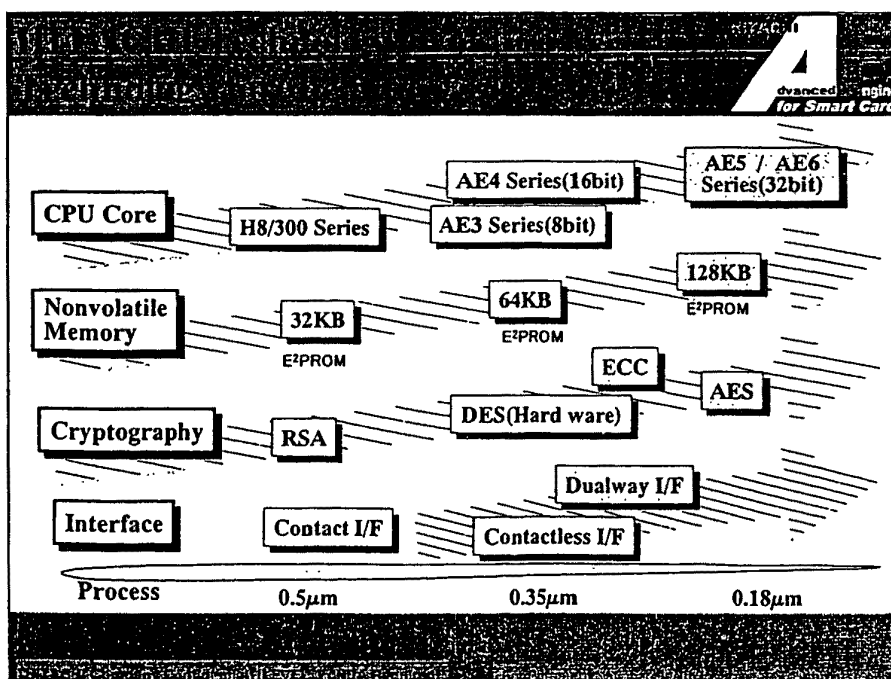


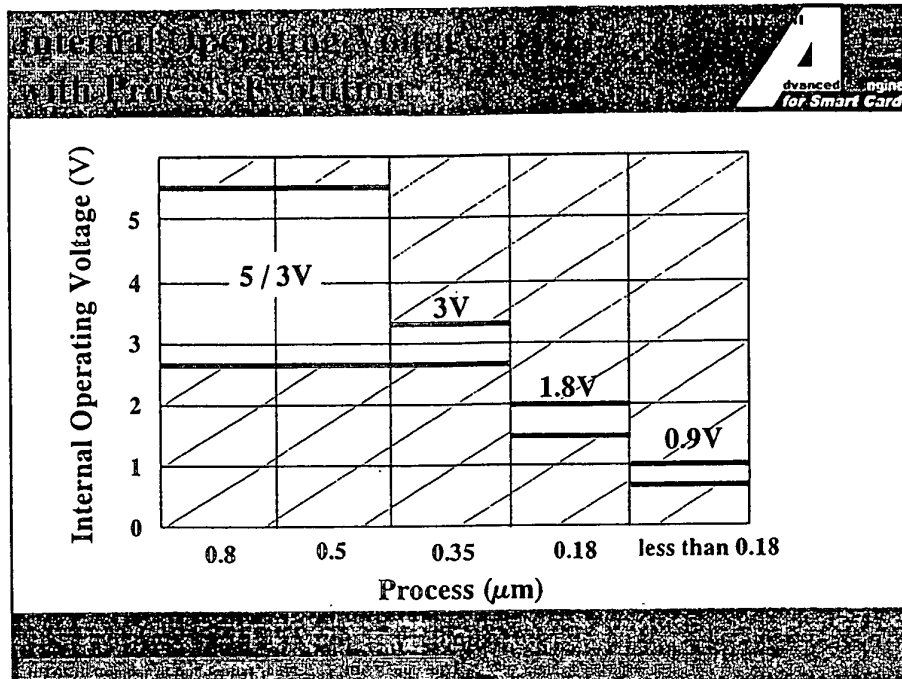


High Performance
Nonvolatile Processor

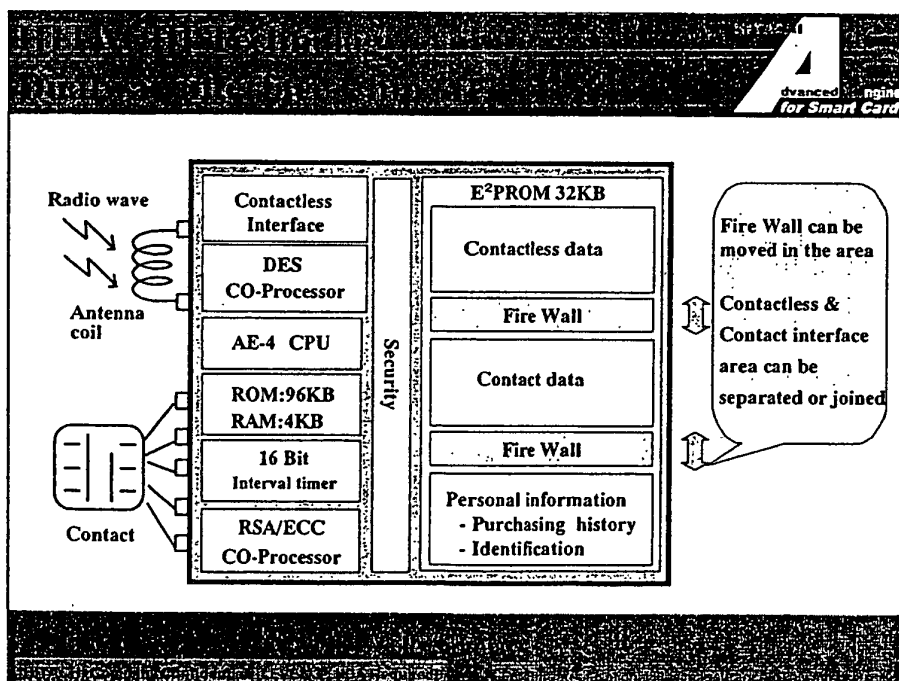
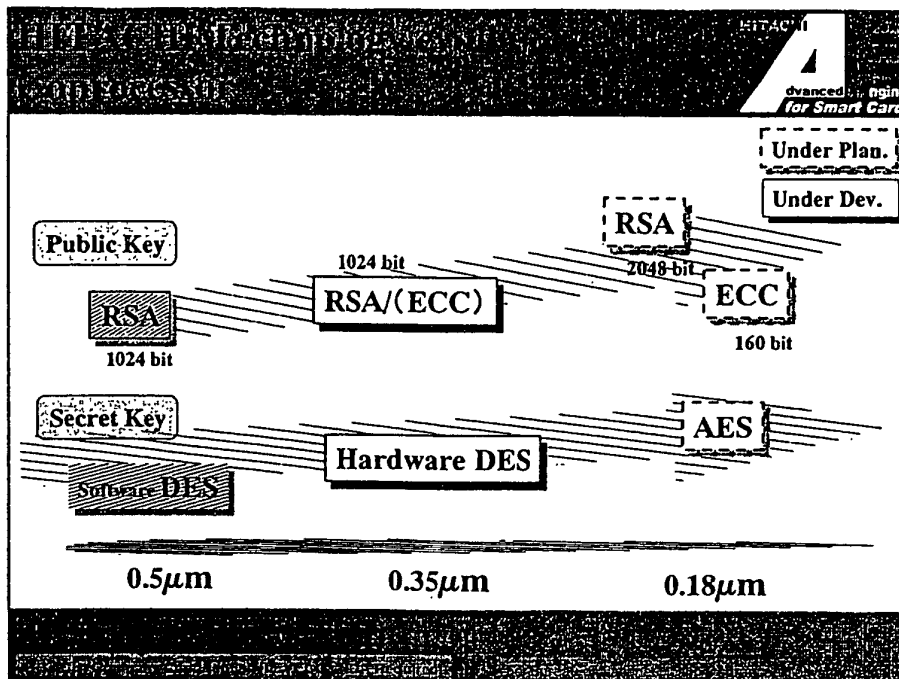


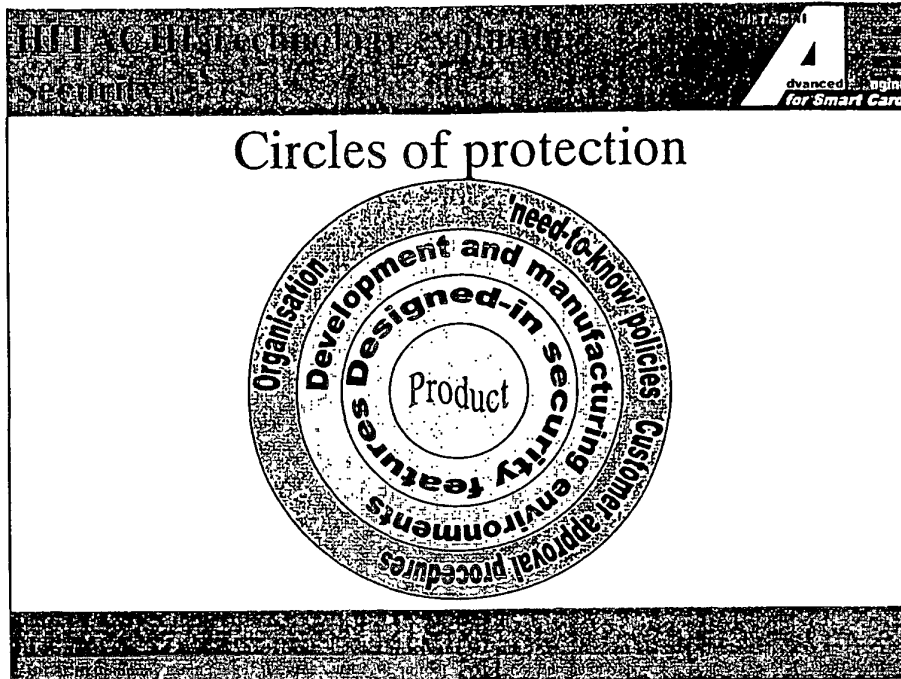
- Upward Compatible to AE-4 and AE-3
- Single cycle instruction execution
- 5 Stage Pipeline
- Enhanced addressing modes for OS
- Extended instruction set
- 20 MHz maximum internal frequency
- Voltage support down to 1.8 V
- Low power static technology
- 0.18 μm - Finest EEPROM process in the world





		MONOS (Hitachi)	FLOTOX (Other)
Memory cell cross section			
Cell Size Ratio (0.35 μm Convert)		1	2.7 (Including ECC)
Characteristics	Merit	- Small size cell - High reliability (Oxide defect resistant) (Soft error-resistant)	- EPROM technology can be used in EEPROM - Simple control logic
	Demerit	Complex control logic	Large defect caused Difficulty of forming a tunnel oxide on N+ diffusion layer

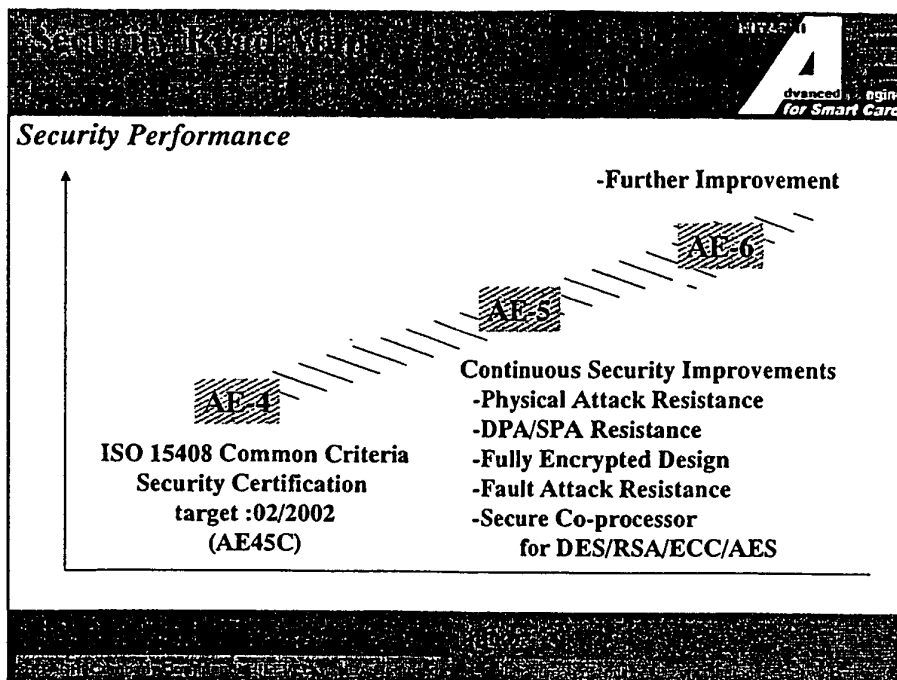




MITAC HP Technology for Smart Card
Security

Silicon security concepts

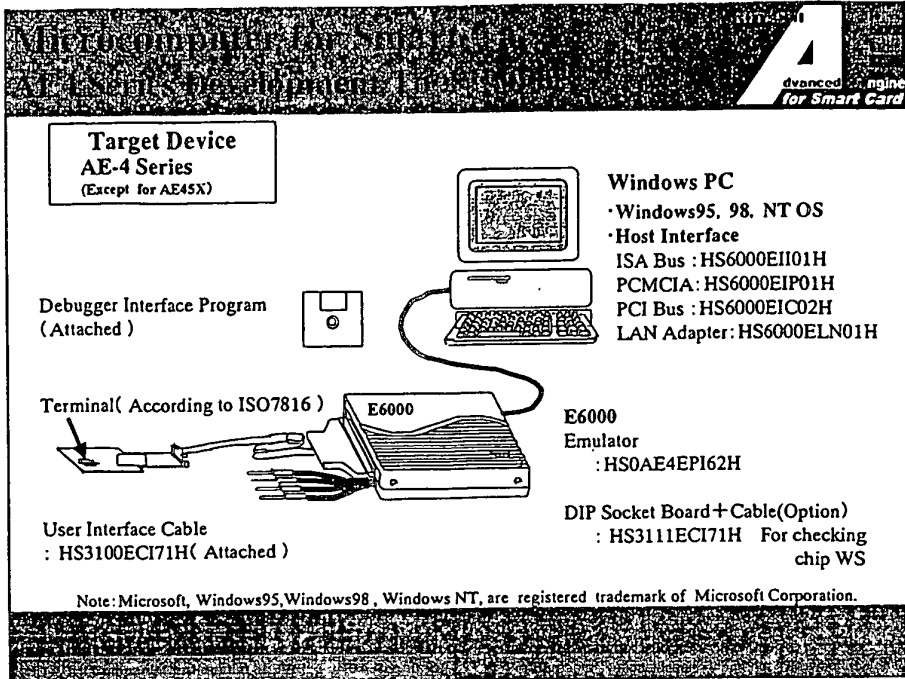
- Specific features built into the product, designed to prevent unauthorised access:
 - secure testing methods
 - control memory: e.g.: traceability data, transport keys, customer EEPROM data
 - out of bounds detectors: voltage, frequency, temperature, light...
 - scrambling of buses, memory topology, etc.
 - data scrambling and encryption
 - use of layout to obscure critical security features: multi-level metal, geometry size,...



International Security Certification
based on ISO15408 (Common Criteria).

First Products	AE45C	
Target Date	Feb. 2002	
Certificate Level	EAL 4+	

Hitachi will design all smart card chips conformed to ISO.

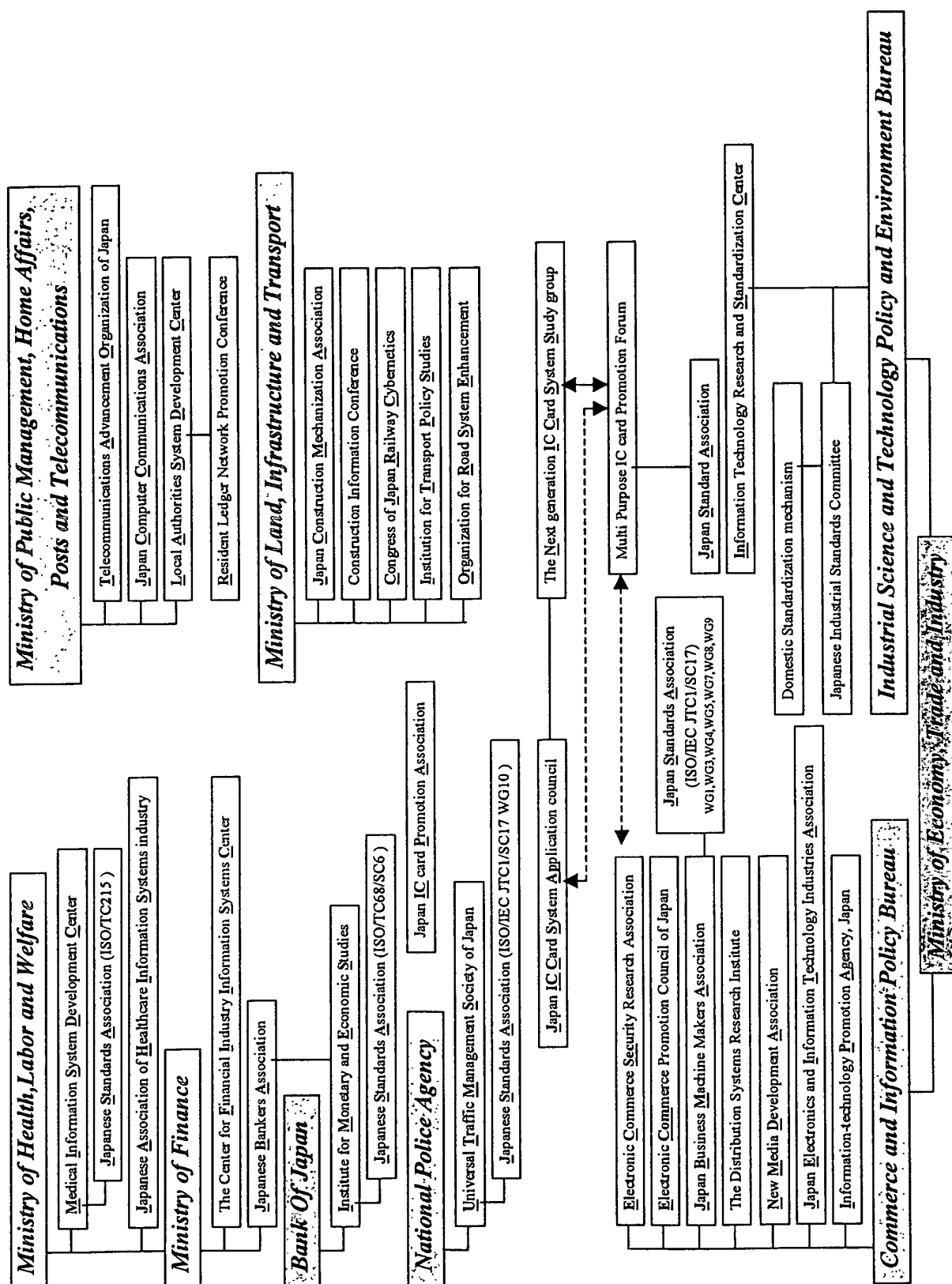


Target Device	ICE Type Number(E6000)	Other
H8/31xx Series	HS3160EPI60H	<u>Host Interface(*1)</u> Windows95, 98, NT ISA bus : HS6000EII01H PCMCIA : HS6000EIP01H PCI bus : HS6000EIC02H LAN Adapter: HS6000ELN01H
AE3 Series		
AE4 Series (Except for AE45X)	HS0AE4EPI62H	<u>DIP Socket Board(*1)</u> : HS3111ECI71H

(*1): Option

THANK YOU FOR
YOUR
ATTENTION

IC card related organization in Japan



国土交通省 日本道路建設振興化協会 日本港湾振興化協会 航行情報化協議会	MUIT JCHA	Ministry of Land, Infrastructure and Transport Japan Construction Machinery Association Construction Information Conference	特許法第30条に基づき(登録)商標の指定を受けていること ・ISO/TC171(土木工学用機械及び装置) ・ISO/TC195(建築用機械及び装置) ・ISO/TC214(保険業(作業者)) 日本工業標準化機構(JIS)の建設機械部門の原案作成は力者としての業務を行っていること 世界貿易機関(WTO)/貿易の技術的障害に関する協定(TBT)の「適正な調整」に基づいて、建設機械関係の団体組織(JCMAS)の審議作成及び制定を行っていること。 改訂システムの調査、調査、調査、調査	英文無し 英文無し 英文無し -	http://www.mlit.go.jp/ http://www.jcha.or.jp/
日本経済産業省 通商政策研究機構	CIRC ITPS	Congress of Japan Railway Cybernetics Institution for Transport Policy Studies	To answer the needs of this new socio-economic environment, the Institute for Transport Policy Studies is conducting research to contribute to the formulation and proposal of new transport related policies. Our research is based on scientific knowledge and advanced research methodology that we apply is comparable to those conducted by leading international universities. The research projects that we undertake concern policy issues relevant to actual social needs. The results of our studies are intended to be practical and easily understood by those parties and individuals at the front-line of transportation administration and transport business.	-	http://www.itrc.or.jp/atgpan/hon
国土交通省 道路システム高度化推進機構	ORSE	Organization for Road System Enhancement	ORSE was newly organized on September 2nd 1993. On the occasion of our launch if ETC, we are planning to link all the information system and communication system and offers standards for the security data and road traffic data for identification enabling privacy protection and fail-safe toll collection. In addition to these tasks, we are going to carry out the promotion for wide use of ETC and to conduct the related research. We, at ORSE, hope to realize more comfortable road traffic environment and to contribute to the national development.	-	http://www.orse.or.jp/
ICカードシステム利用促進協議会 次世代ICカードシステム研究会	JCSSAP NUGSS	Japan IC Card System Application Council The Next Generation IC Card System Study Group	英文無し The IC card technology utilized in the IC card introduction plans and IC card system-related projects of the relevant governmental agencies; the study group makes arrangements for information sharing among the agencies and the corporate members of the study group. At the same time, the group examines the following issues and makes proposals to the government and industry: - Highly efficient and practical common platform for the next-generation IC card systems	-	http://www.icpass.or.jp/ http://www.nugss.gr.jp/meishin
経済産業省 電子商取引安全安心研究所 電子商取引安全安心研究所	MEITI ECSEC	Ministry of Economy, Trade and Industry Electronic Commerce Security Research Bureau Electronic Commerce Security Research Association	Operating as the Electronic Commerce Security Technology Research Association (ECOSE), the organization will conduct research on the security of Economy Trade and Industry and will conduct research relating to security evaluation technology for IT products and systems	-	http://www.meiti.go.jp/ http://www.ecsec.org/
電子商取引推進協議会	ECON	Electronic Commerce Promotion Council of Japan	The Electronic Commerce Promotion Council of Japan (ECON) was established in January 1998 through MITI's EC promotion activities in order to develop a common platform to work for the establishment of electronic commerce and to expand its present expansion of EC	-	http://www.ecom.or.jp/
日本事務機械工業会	JBMA	Japan Business Machine Makers Association	Since its establishment in 1969, the Japan Business Machine Makers Association has been working for the economic development of its member companies, and also conducted a diversity of activities to accelerate the growth of the business machine industry by introducing various measures to cope with trade liberalization and increase employment opportunities, while maintaining close cooperation with other industrial association.	-	http://www.jbma.or.jp/
流通システム開発センター	DCC-JAPAN	The Distribution Systems Research Institute	In future, distribution will progress to the use of EC (Electronic Commerce) through EDI (Electronic Data Interchange), based on such things as JAN (Japan Article Number) and POS (Point-of-Sale) systems which our Center has helped to build. In this process, we must also deal with the blurring of borders between different business fields as well as growing internationalization. Although the challenges facing us are becoming more numerous, through the joint efforts of all concerned, we are making more achievements are being.	-	http://www.dcc-japan.com/

ニューメディア開発協会	NMDA	NEW MEDIA DEVELOPMENT ASSOCIATION	現在、レイアウト/フルカラーシステムや電子インクシステムなどのインクジェット利用装置のためのシステム開発、各種原稿電子保存システムやインクジェット電子印刷システムなどの情報社会を実現するための革新的システムの開発、次世代ICカードシステムの開発、電子ネットワーク実用調査などを行っています。	Non-profit and an auxiliary organization of Ministry of Economy, Trade and Industry Established to develop the information optical visual system. -Refer to City of Light: The Story of Fluor Optics by Jeff Hecht, Oxford University Press 1993 It's promote the spread of New Media and to contribute to the realization of the information society	http://www.nmda.or.jp/
電子情報技術産業協会	JEITA	Japan Electronics and Information Technology Industries Association	このため、政策提言や基礎技術研究の支援、新しいシステムの導入等各種事業を積極的に展開すると共に地球温暖化防止等の環境対策にも積極的に関与しています。	By supporting related government policies and R&D efforts, JEITA is encouraging advancement and restructuring in all areas of business. We are also actively promoting environmental preservation countermeasures, including those to combat global warming.	http://www.jeita.or.jp/
情報処理振興協会	IPA	Information-Technology Promotion Agency, Japan	当協会は、情報処理の促進に関する法律(昭和55年5月21日法律第163号)に基づいて設置された行政機関です。情報処理の振興を図るICプログラムの開発及び利用、情報処理サービス等を営む者に対する助成、ソフトウェアに関する研究開発等の事業を実施しています。	英 文 版	http://www.ipa.go.jp/
ISO/IEC/JTC1/SC1 日本標準協会 工業技術標準センター ICカード多目的化推進フォーラム	ISO/IEC/JTC1/SC1	Japanese Standards Association Industrial Science and Technology Policy and Environment Bureau	ICカードの多目的化を推進するために、ICカード関連団体(参加28団体)を統合したフォーラムを平成12年9月にINSTAC内に設置し、座間ベースでのICカードを多目的化するための問題点の抽出等を図っています。		http://www.iso.or.jp/default.asp
日本規格協会 情報技術標準化研究センター 国内標準化機構 日本工業標準調査会	JSA INSTAC JISC	Japan Standard Association Information Technology Research and Standardization Center Japanese Industrial Standards Committee		What is JISC ? JISC consist of many national committees and plays central role in standardization activities in Japan. In essence, the task of JISC can be summarized as follows: (a) Establishment and maintenance of JIS (b) Participation in International Standardization and Certification Activities (c) Participation and Contribution in International Standardization Activities (d) Development of Measurement Standards and Technical Infrastructure for Standardization	http://www.jisc.or.jp/



JSS Mission Statement

- Make real strides in ensuring the adoption of IC cards, especially toward the adoption of multi-application operating systems and the use of multi-applications.
- Fully utilize the know how and many techniques / skills offered by the alliance of companies in JSS gained through real experience.
- Examine and fully develop all IC card related businesses.

Objectives of Establishment

- Supply leading edge solutions
- Realize the effectiveness of an alliance
- Pursue the latest IT technologies
- Respond swiftly to user needs

JSS Shareholders

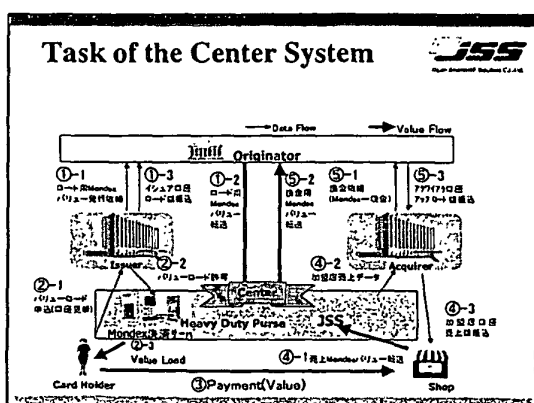
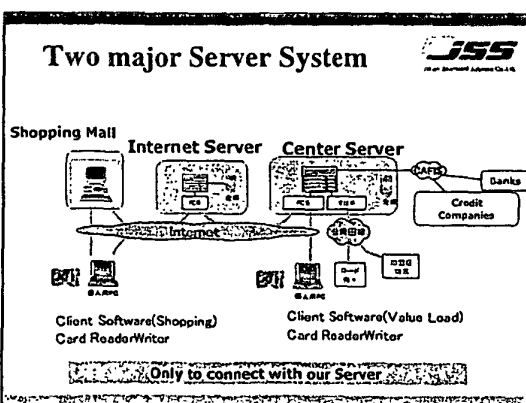
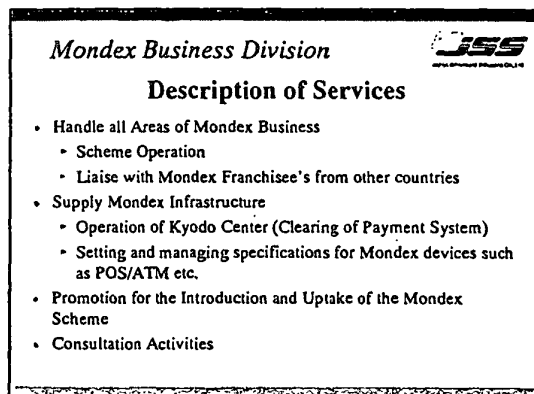
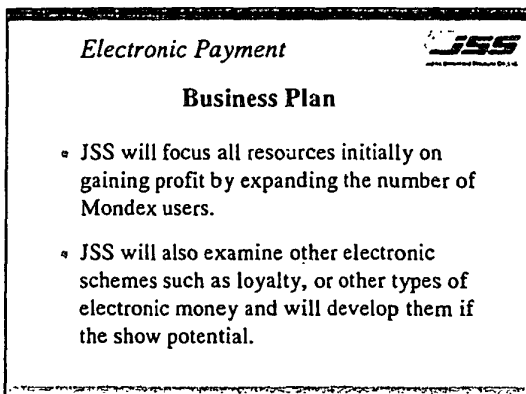
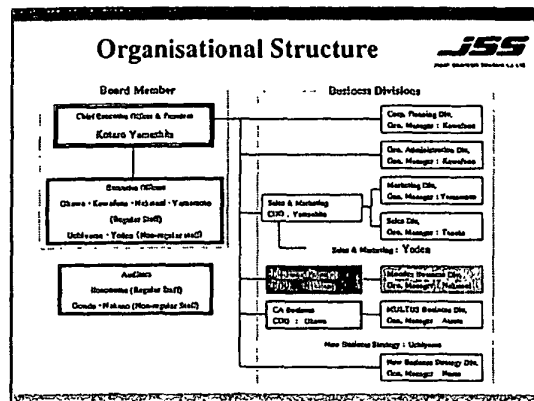
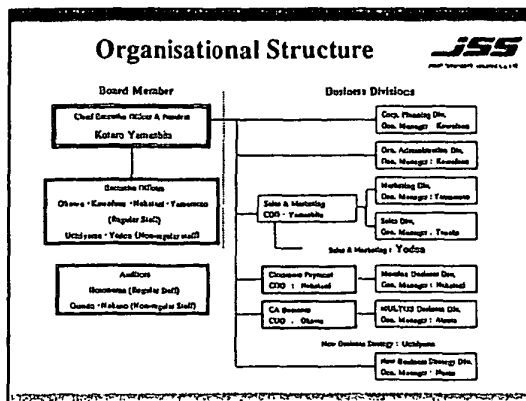
Hitachi, Ltd.	Dai Nippon Printing Co., Ltd.
JCB Co., Ltd.	Nissei Iwai Corporation
Hitachi Software Engineering Co., Ltd.	Sauwa Bank Ltd.
Financial One Card Co., Ltd.	T.I.S. Co., Ltd.
Kyodo Printing Co., Ltd.	Toppan Printing Co., Ltd.
Orico Corporation	Hitachi Capital Co., Ltd.

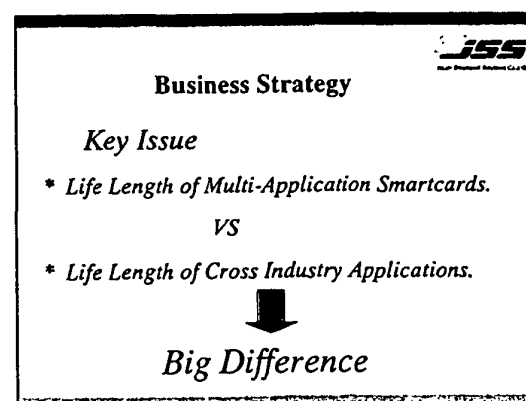
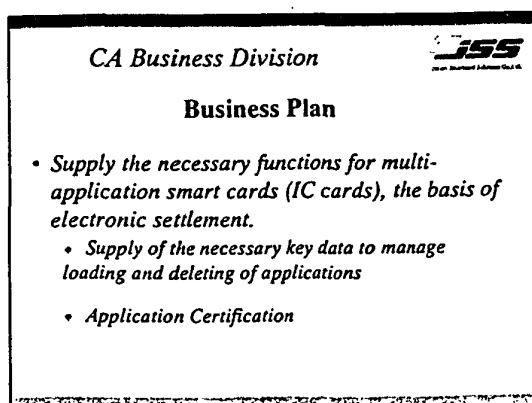
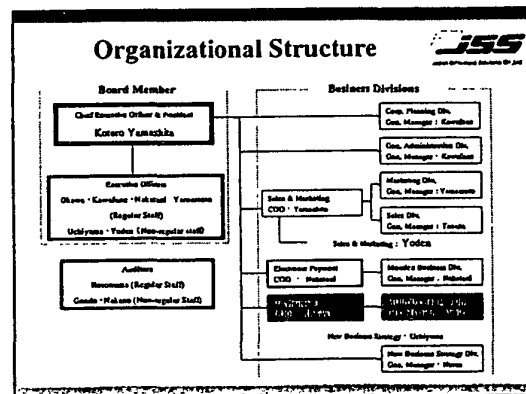
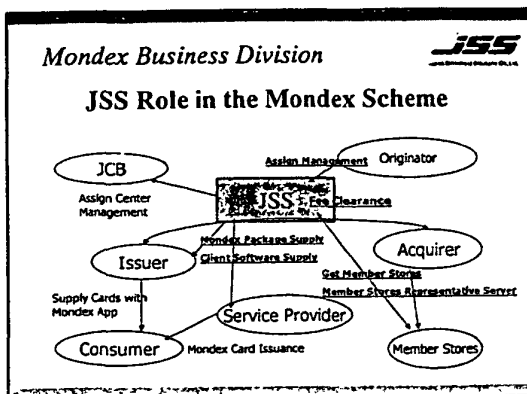
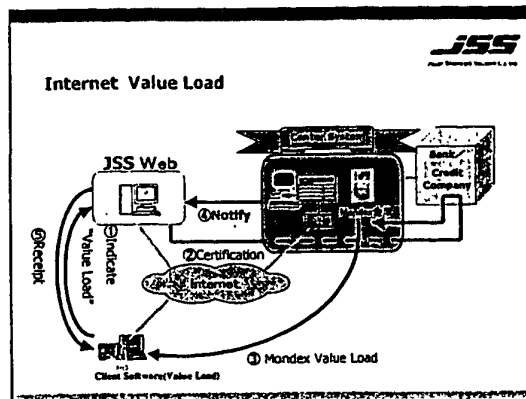
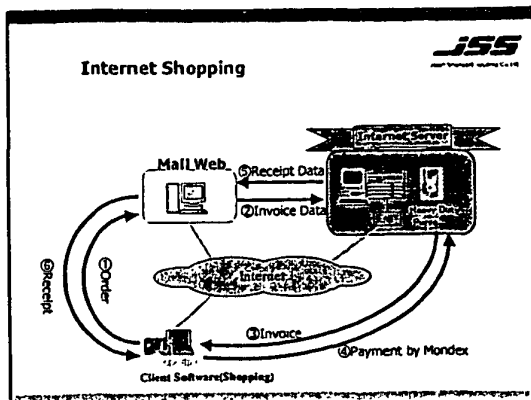
Company Outline

Company Name – Japan Smartcard Solutions Co., Ltd.
 Address – Chiyoda Ward, Tokyo
 Capital – 1,050,000,000 yen (current figure)
 Number of Staff – 9 on establishment (currently 15)
 Date of Establishment – 27th August 2001
 Start of Business – 1st October 2001
 Web Page – www.jssco.net

**Japan Smartcard Solutions Co., Ltd.
Business Focus**

- e-Cash Business
Focusing on MONDEX
- CA Business
Focusing on MULTOS CA





JSS
Japan Smartcard Solutions Co., Ltd.

Business Strategy

Solution
Dynamic Load & Delete Service

JSS
Japan Smartcard Solutions Co., Ltd.

Target

Multi-Application Smartcards

- * *Multi-Application Management Service for any Standardized OS Scheme.*
- * *Key Management Service.*
- * *Application Certification Service for Cross-Industry Applications.*

JSS
Japan Smartcard Solutions Co., Ltd.

MULTOS Features

- (1) *MULTOS OS Supports Multi-Applications*
- (2) *Control for Application Load & Delete*
 - *Post Issuance capability*
- (3) *Extremely High Security (ITSEC E6 High)*
 - *Firewall Separating Applications*
 - *Requires Digital Certificates from KMA*
- (4) *De facto Standard for Financial/Public Use*

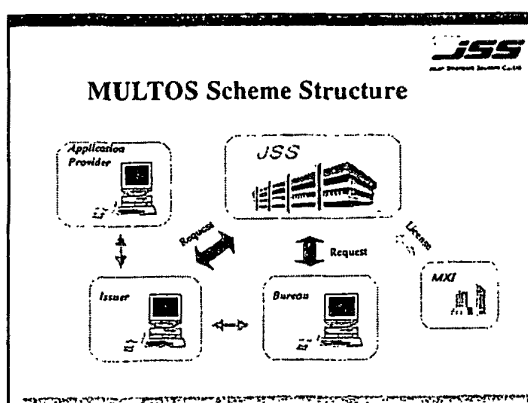
JSS
Japan Smartcard Solutions Co., Ltd.

KMS (Key Management Services)

MULTOS Scheme

**** Parallel Domain ****

- *Card Issuer Registration*
- *Application Registration*
- *Enablement Data (MSM—CD) Generation*
- *Application Load Certificate (ALC)/Application Delete Certificate (ADC) Generation*



JSS
Japan Smartcard Solutions Co., Ltd.

Advantages for the Customer

- (1) *Full Service in Japanese*
 - *Japanese M-SPI Software*
 - *No Export License Necessary*
- (2) *Local Time Support*
- (3) *Pricing in Yen – No Influence by Exchange Rate*
- (4) *Eligible for Use in Public Card Scheme*

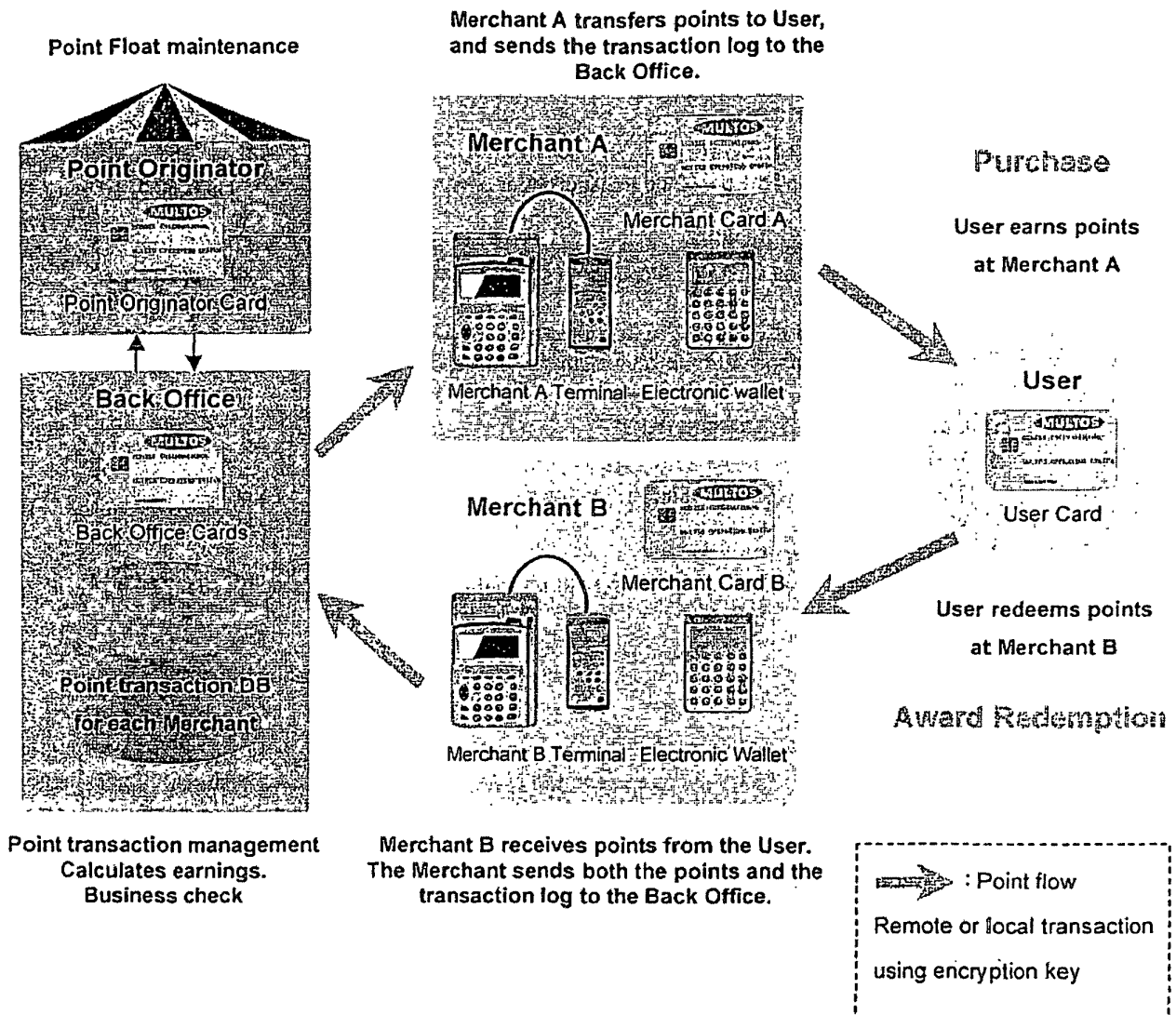
Schedule

2001/11	12	2002/1	2	3	4	5	6	7	8	9	10
Issue / Bureau Application Registration			Issue / Bureau Registration & Application Registration								
Key Generation MSM, CD, ALC, ADC			Key Generation (MSM, CD, ALC, ADC)								
				Key Generation in England				Key Generation in Japan			

HITACHI

MULTOS

Multi Pockets Value Flow



New Financial Systems,
Services & Products Department,
Financial Systems Division
Hitachi, Ltd.



Specifications are subject to change without notice.
© Hitachi, Ltd. 2000

TEL: +81-3-5471-2133
FAX: +81-3-5471-2586
Hitachi Omori 2nd Bldg,
27-18, Minami Oi 6-chome,
Shinagawa-ku,
Tokyo 140-8572, Japan

<http://www.hitachi.co.jp/Div/nfs/index-E.html>

Multi Pockets

Hitachi original loyalty program, "Multi Pockets" is based on MULTOS platform, making card-to-card authentication by encryption key for each transaction. Thus, there is no need to wait for conventional on-line center authentication, making customers comfortable to use like existing cash when they redeem the points. Hitachi's back office system solution will support easy point maintenance and management, providing seamless smart card solutions with optimal technologies.

1. High Performance

- **Fast transaction Speed**
The program enables 1.5 second transaction for a local point transfer. (* Using Hitachi Electronic Wallet)
- **Compact program size**
The program can co-exist with Mondex electronic purse and another application on 16K MULTOS platform.
- **Easy Customization and Enhancement**
Another data management function using authentication key can be incorporated into the user area.

2. Effective Point Management

- **Volume management and redemption monitoring**
The system enables monitoring of total point issuance and returned point flow from users.
- **Card to Card transaction**
Card-to-Card transaction is available both in local and remote transaction mode. The point scheme is completely interactive both for virtual and real world.
- **Low implementation and operating cost**
Reasonable implementation cost and operating cost due to off-line authentication.

3. Security

- **Trustable Encryption**
The program uses highly proficient encryption key. Multi program operation can be possible on one card without any disturbance to each other. The card keeps error log in case of transfer failure.
- **Fraud prevention**
Point transfer can be possible only with recognized counterparts programmed on the card, depending on the scheme. The card prevents any unauthorized point transfer.
- **Efficient Validity management**
Easy point validity management and point recycling by card maintenance program.

Contact:

New Financial Systems, Services & Products Department, Financial Systems Division
Hitachi Omori 2nd Bldg., 27-18, Oi 6-chome, Shinagawa-ku,
Tokyo 140-8572, Japan
Tel: +81-3-5471-2133 Fax: +81-3-5471-2586
<http://www.hitachi.co.jp/Div/nfs/index-E.html>
e-mail: HiMoney-G@comp.hitachi.co.jp