經濟部

參加「第一屆亞洲 PKI（Public Key Infrastructure）論壇」出國報告

The First Asia PKI Forum Meeting Report

June 11-15, 2001

出國人員：經濟部商業司　黃慶堂副司長
經濟部商業司　李淑燕約聘人員
經濟部中小企業處　賴杉桂副處長
經濟部國貿局　余吉政副組長

出國地點：日本　東京

出國期間：九十年六月十一日至六月十五日

報告日期：九十年七月六日

目　錄

一、前言

為助於電子商務與電子化政府的發展，如何做好存取資訊的安全管理，是目前重要議題，其中推動 CA 憑證機構與 PKI（Public Key Infrastructure）架構以解決網路上身分認證問題屬當務之急，而公開金鑰基礎建設是電子認證的最基本架構，這項基本架構正是擴展全球電子商務市場及電子化政府服務的根本要素。隨著網路資訊的腳步愈來愈快，PKI 在企業與企業、國與國之間的資訊安全交易中所扮演的角色也愈來愈重要。

亞洲 PKI 論壇（Asia PKI Forum）成立宗旨在於推動亞洲國家或地區間電子商務與電子化政府的合作應用與公開金鑰基礎建設(PKI)之架構建置，希望在跨國交互認證、法律制度、認證中心間的共用性進行合作，建立亞洲國家間通用的認證規格，統一技術規格與縮小差異，創造可以相互溝通且安全的電子商務環境，進而整合亞洲地區電子商務市場，促進無國界電子政府與亞洲共同電子商務市場的發展。

日本 PKI 推進協議會（Japan Promotional Association for Asia PKI Forum，APKI-J）於 2000 年成立，結合亞洲國家/地區之政府與民間力量，共同成立亞洲 PKI 論壇（Asia PKI Forum），而第一屆亞洲 PKI 論壇（The First Asia PKI Forum）即在 2001 年 6 月 12-14 日於日本東京展開，邀集了亞太區 11 個國家/地區及三個相關組織之政府及民間代表共同參與，這幾天的活動，除了有對外公開的研討會，以及主辦單位為參與國家/地區參加人員所安排的電子化政府及電子商務展示中心參觀之外，同時亦針對此項亞太區 PKI 合作計畫另外召開會員大會（General Meeting），討論此項計畫未來進行方向。

為配合亞洲推動有關公共金鑰基礎建設，本司負責籌組民間組織為推動單位；目前業已成立本國「亞洲公開金鑰基礎建設論壇中華台北推動委員會」(Chinese Taipei Promotion Association for Asia PKI Forum)，並於本（九十）年三月廿六日及五月三日召開第一及第二次籌備會，推舉財團法人NII發展協進會夏漢民董事長為召集人，資訊工業策進會黃台陽副執行長及本司劉坤堂司長二人為共同召集人。此次由日本召開「第一屆亞洲PKI論壇」，本國由委員會夏漢民會長擔任團長，帶領政府及業界相關單位前往日本參加，為我國爭取這項亞太區合作計畫，同時也為我國電子商務資訊安全環境奠定良好基礎。

二、會議相關資料

（一）會議議程

June 12 (Tue) Current status of PKI usage and challenges for its deployment	
13:30	Registration
14:00-14:10	Opening remarks: **Seiichi Shimada** Vice Chairman, PKI-J(※) (Executive Vice President of Mitsui & Co., Ltd.) (※) The Japan Promotional Association for Asia PKI Forum
14:10-14:50	Special speech: **Riccardo Genghini**, Chaiman of the E-Sign Workshop, EESSI(※) "The Current Status and Prospective Use of PKI in the World: A Report on the Efforts of EESSI" (※)The European Electronic Signature Standardization Initiative
14:50-15:10	Break
15:10-17:40	Speeches: Government officials from Asian nations/regions: "Issues on the Deployment of PKI in Asia" ・Report on efforts for PKI deployment ・Challenges and proposals for PKI deployment in Asia
17:40-17:45	Closing remarks
18:00~	Welcome Reception

June 13 (Wed) Towards the establishment of the Asia PKI Forum	
08:30	Registration
9:00-9:15	Opening remarks: **Tsutomu Kanai** Chairman, APKI-J (Chairman of the Board, Hitachi, Ltd.)
9:15-9:45	Congratulatory speeches: Ministry of Economy, Trade and Industry Guests from Asian countries/regions
9:45-10:25	Keynote Speech: Key issue for global deployment of Electronic Commerce: **Michio Naruto,** Co-Chairman, GIIC(※1)Asia and Co-Chairman, GBDe(※2)Overall (※1)The Global Information Infrastructure Commission (※2)The Global Business Dialogue on Electronic Commerce
10:25-10:45	Break
10:45-11:15	Progress reports on the establishment of the Asia PKI Forum **Akira Tachigami**, General Manager, APKI-J ・Policies and planned activities of the PKI-J ・Cooperation towards establishing the Asia PKI Forum
11:15-12:30	Special speeches: "The Current status of and outlook for PKI deployment Worldwide, based on the efforts of the IETF(※) and PKI Forum" **Steve Kent,** Co-Chairman, IETF/PKIX **Lisa Pretty,** President, PKI Forum (※) The Internet Engineering Task Force
12:30-14:00	Lunch

14:00-15:00	Visual presentation: "The future society with the use of PKI"
15:00-15:20	Break
15:20-17:20	Panel discussion: "Scenarios of PKI Deployment in Asia" Panelists: Representatives of Asian governments and PKI promotional organizations Moderator: **Osamu Sudoh**, Professor, University of Tokyo
17:20-17:35	Wrap up: **Akira Tachigami,** General Manager, APKI-J
17:35-17:40	Closing remarks
18:00~	Networking Party

June 14 (Thu): Field visit (only for participants from overseas)	
9:00	Depart New Takanawa Prince Hotel
9:30-12:00	Visit the e-government/e-commerce showroom
12:00-14:00	Lunch

自行安排拜訪行程：

June 14（Tue）

16:00-17:00 拜會 Electronic Commerce Promotion Council of Japan（ECOM）

June 15（Fri）

10:00-10:30 拜會 Japan Promotional Association for Asia PKI Forum

合作會議：

June 12（Tue）

18:30~19:30 Pre-General Meeting

（參加人員：黃慶堂副司長、夏漢民董事長）

June 13（Wed）

12:30~13:30 General Meeting

（參加人員：黃慶堂副司長、夏漢民董事長、余吉政副組長）

（二）參與國家/地區/組織

國家/地區：

日本、新加坡、韓國、香港、馬來西亞、中華台北、泰國、菲律賓、中國大陸、澳大利亞、緬甸

組織：

E-ASEAN（an organization to promote IT business in Asean）

IETF（EU）

EESSI（EU）

PKI Forum in USA

（三）我國參與人員

財團法人中華民國國家資訊基本建設產業發展協進會	夏漢民 董事長
經濟部商業司	黃慶堂 副司長
經濟部商業司	李淑燕 約聘人員
經濟部中小企業處	賴杉桂 副處長
經濟部國際貿易局第四組	余吉政 副組長
行政院 NICI 小組	林登輝 副研究員
財團法人中華民國國家資訊基本建設產業發展協進會	陳怡湞 專案經理
財團法人資訊工業策進會電子商務應用推廣中心	郭淑敏 顧問工程師
財團法人資訊工業策進會科技法律中心	李科逸 專案經理
財團法人資訊工業策進會國家資通安全會報技術服務中心	林劍秋 資深經理
台灣網路認證股份有限公司	林長慶 總經理
中華電信研究所	謝東明 博士
資誠會計師事務所	包化富 副總經理
普華商務法律事務所	蔡朝安 主持律師
普華商務法律事務所	朱瑞陽 律師
太穎國際法律事務所	黃漢臣 經理
中國信託商業銀行（銀行公會代表）	成家瑜 資深經理

三、會議重點摘述

（一）研討會

（1）全球 PKI 運用現況：歐洲電子簽章架構（E-sign Workshop, EESSI）

在歐洲 EESSI 已成立，而亞洲也成立 Asia PKI Forum，歐盟希望藉由這些組織的建立與合作，將標準相互連結，並且根據歐洲技術標準規範，提供亞洲地區 PKI 架構建置參考。目前歐洲已通過 GSN 這樣的協議規範，如建立電子簽名標準化。建立安全系統和信任規則是相當重要，歐洲的經驗可以做為亞洲國家參考，希望在不失技術有利的條件下制訂相關規範，尤其要保障傳統商業交易能在公平、安全及透明化的條件下進行商業活動。中小企業是未來經濟的力量，如何在不提高成本，適時捉住商業機會，以加速中小企業成長。技術轉變迅速，因此各項法規必須順應這快速變遷的資訊革命，做出適當的修改。

EESSI 希望在資訊基本建設達到以下目標：

- 結合現代與傳統商業交易，進行更快速便利的文件傳輸。
- 透過適當的文件傳輸提昇對消費者的透明化及公平性。
- 加強中小企業資訊系統的商業流程整合。
- 鼓勵更多民眾參與相關活動。
- 加強電子化政府運作，減少整體公共管理與行政流程費用。

歐洲在 PKI 基礎建設方面致力相當多心血，尤其針對 B2B 交易。其中一項 93/1999 EC 法規中強調技術中立、隱私權保護、國內與國外相互認知以及無歧視等原則，除此之外，金融保險部分也將擴大規範。目前德國、奧地利、法國都依循歐盟的法律原則，而義大利亦將跟進。歐盟現階段積極與 Asia PKI Forum 進行交流，雖然有許多技術問題，但這樣的交流仍是必備。

（2）澳大利亞和 APEC 之 PKI 規劃
（APEC Telecommunications E-security Task Group Representative of Certification Forum of Australia）

澳大利亞是根據 ISO 和 IETF 來制訂標準，IETF 為僅限於澳洲的標準。**Gatekeeper** 為澳洲進行電子化政府的一項計畫，其中電子檢疫服務是目前正進行建構推動的項目，另外澳洲也與 APEC 部分會員國家共同合作電子通關、電子報稅及電子檢疫等項目。

ABN-DSC（The Australian Business Number–Digital Signature Certificate）是一個獨特的商業鑑定法規，此 ABN 電子簽名法於 2001 年 1 月通過，希望全體國民與州政府機構之間均能使用電子認證，確保商業都接收並核發 ABN 電子簽名目前只適用於商業及政府交易，對於個人交易則不適用。

另外澳洲有四家銀行根據 ABN-DSC 的規格再延伸發展一項商業數位認證，名為 Angus businesses digital certificates，其效力與 ABN-DSC 同樣被民間機構所接受，目前正尋求州政府機構的認同。Gatekeeper/Angus 這兩項計畫方案均根據相關的國際及國內標準來制訂，且規定一家公司只能參與一個國際性認證機構，如 Identrust。參與 Angus 認證機構的會員可以決定所想要的 PKI 服務提供者，而參與 Gatekeeper 認證機構可以核發認證給國內外單位，適當發揮互通性功能。

澳洲電子交易法案於 1999 年通過，採取中立原則，同時也成立了幾個相關單位，如澳洲認證論壇（Certification Forum of Australia）、國家電子認證委員會（National Electronic Authentication Council）及相關工作小組（Working Groups）。

另外澳洲亦於 APEC 組織中成立電子安全工作小組（eSecurity Task Group）、PKI 互通性專家小組（PKI Interoperability Expert Group）及電子商務營運小組（eCommerce Steering Group），由此可看出澳洲對 PKI 整體架構運作的重視程度。

澳洲目前正規劃建立電子認證信賴名單（Signed Certificate Trust Lists），要確認這些名單上的公司是否可以信賴，需要嚴謹的法律規範。澳洲認為不同地區有不同法律、文化背景，不同單位也使用不同術語、技術，目前最迫切進行的即是解決這些差異性，建立共通性標準與方法。

參考資訊：

- Certification Forum of Australia
  http://www.aeema.asn.au/groupings/divs_info.cfm?divisionID=35
- National Electronic Authentication Council
  http://www.noie.gov.au/neac
- Government Public Key Authority（Project Gatekeeper）
  http://www.gpka.gov.au
- Australian Business Number – Digital Signature Certificate
  http://www.govonline.gov.au/projects/publickey/abn-dsc.htm
- Report of the National Electronic Health Records Taskforce
  www.health.gov.au/healthonline/her_rep.htm
- APEC e-Security（Formerly Electronic Authentication）Task Group
  http://www.apectelwg.org/apec/atwg/preatg.html
- Standards Australia
  http://www.standards.com.au/

（3）韓國 PKI 政策與架構

（Korea Certification Authority Central, Korea Information Security Agency）

韓國數位簽章法案於 1999 年通過，並規範認證機構核可條款，其主要立法原則為彈性規範相關條文、共同追求政府與民間機構利益，以及法律穩定性與便利性原則。

認證機構發放條件包括：

- 財務能力：需有超過 800 萬的資本額。
- 技術能力：需有超過 12 位認證業務管理經驗的專家。
- 設備工具：需有雙重的安全認證管理系統、運作系統、資料庫備份等設備。

韓國目前已有四家核可發放的認證機構，然而由於電子簽章使用環境尚未健全，觀念亦不普及，因此認證機構市場成長速度仍緩慢。到 2001 年 5 月為止，韓國共發放了 413,578 件證明書，現階段則是積極推廣認證制度和數位簽章的使用及無線通訊 PKI 架構規劃。

下表為韓國數位簽章使用狀況與未來預測：

單位：萬/人次

	2001 年	2002 年
政府單位	12	33
銀行	127	405
股票市場	71	236
保險/信用	66	194
行動商務	16	101
其他	22	82
總計	314	1,051

（4）透過 PKI 建置一個可信賴的電子商業環境

（Online Development, Infocomm Development Authority, Singapore）

跨國交易需要一個互信的環境，而 PKI 被視為是建立電子商務安全交易環境的重要環節。新加坡電子交易法規於 1998 年通過，相關法規包括電腦濫用處理法（Computer Misuse Act）、著作權法（Copyright Act）及證據法（Evidence Act）等。新加坡亦成立一個由民間主導的 Singapore PKI Forum，希望達到互通性跨國安全交易的目標。

（5）日本 PKI 現況說明

（Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry）

日本電子簽章法於 2001 年 4 月剛通過，利用完整 PKI 架構建立認證系統以達到電子化政府及民間安全的交易傳輸是日本推動 PKI 目標，同時要達到個人認證亦是日本發展 PKI 的主要項目之一，計畫推出公民卡（Resident's Cards）來進行個人認證工作。日本自 1997 年開始即積極推動電子化政府各項重點工作，其中 1999 年 12 月由小院內閣決定的一項千禧計畫（Millennium Project）特別針對電子化政府提出幾點目標，包括：發展政府公開金鑰基礎建設（GPK）、發展 Bridge CA、根據商業登記法發展電子憑證系統、以及電子簽章和電子憑證法律條款之訂定。

2001 年 3 月，日本亦發表了一項日本電子化重點計畫（e-Japan Priority Policy Program），預計在 2003 年達到 90%所有交易運作流程電子化之目標。

日本希望藉由安全及順暢的電子簽章使用加速推動電子商務，進而加強民眾生活品質和促進國家經濟健全發展。

日本一項憑證服務鑑定條款中提到幾項重點：

- 憑證服務提供者可以在不需經過鑑定的情況下自由經營。
- 對於憑證服務提供者的線上鑑定調查可以由指派的調查單位來進行。
- 國外憑證服務提供者亦會收到鑑定通知，而其線上鑑定調查可以由在他國設立且經過認可的調查單位來進行。

日本商業登記電子化相關法案在 2000 年修正完畢，其電子憑證系統是根據原有的商業登記法延伸制訂，希望建立一個便利的申請、申報及商業交易系統之基礎建設。對於整體 PKI 架構，日本認為要建立出新的 PKI 商業模式及網路安全與信賴規範，以期 PKI 未之來健全發展。

（6）美國 PKI Forum 概要（PKI Forum）

美國 PKI Forum 於 1999 年 12 月由 5 個組織共同成立，宗旨為致力於產業合作與市場認知，期許民眾瞭解 PKI 在商業應用之益處與價值。北美洲數位憑證的使用自 1999 年起已相當普及，而對於 PKI 市場的未來發展，美國則預測在 2003 年 PKI 管理服務的營收將達 200 億美元，在 PKI 軟體產品營收將達 50 億美元。

美國 PKI Forum 於第一年運作時期成立 PKI 資源網站（www.pkiforum.org/resources），提供 PKI 相關資訊及網站鏈結。目前約計 11 個會員國，包括北美洲的美國和加拿大、歐洲的 8 個國家、日本以及其他地區。其組織架構共分隱私權與政策工作小組、推廣與教育工作小組、法律工作小組、商業應用工作小組、技術工作小組。

目前有幾個組織持續進行 PKI 標準與規格研究，這些組織包括：International Standards Organization（ISO）、Public Key Cryptography Standards（PKCS）、Internet Engineering Task Force（IETF）。可鏈結到關網頁：http://www.pkiforum.org/resources.html 參考相關標準與規格。

美國 PKI Forum 同時也進行 CA 與 CA 間的互通性計畫，將信賴關係議題擴展到企業與企業，甚至國家與國家之間，而不僅限於企業本身內部。其成立目的在於促進賣方之間的互通性，要達到以企業主導、客戶導向、國際發展與共同合作之目標前進。除了技術議題外，國際間的互通、政策的規範與流程的標準化等均扮演重要角色。

（7）馬來西亞 PKI 現況概述（MSC Trustgate.com）

馬來西亞數位簽章法於 1997 年制訂，將數位簽章與實際簽名視為同等效率，而數位簽章管理規範於 1998 年制訂，條文中詳述 CA 的運作規範。目前有兩家經核可的 CA 來發行數位憑證。對網際網路安全議題的認知是馬來西亞相當重視的議題，另外，如何將數位憑證與國際貿易法規做結合亦是馬來西亞未來計畫重點。

（二）會員大會（General Meeting）

來自亞太區 8 個國家或地區的代表於 2001 年 6 月 13 日東京召開會員會議，共同商討 PKI 合作計畫的成立與未來在電子商務的應用。

此項會員會議彙整出幾項結論：

- 亞洲 PKI 論壇 8 個參與會員國分別為：澳大利亞、中國大陸、香港、日本、韓國、馬來西亞、新加坡與中華台北。
- 亞洲 PKI 論壇第一屆主席由日本推動協進會（APKI-J）會長 Dr. Tsutomu Kanai 擔任，副主席由韓國 PKI 論壇會長 Dr. Y. T. Lee、新加坡 PKI 論壇會長 Mr. Lucas Chow 共同推選擔任，另外中國大陸於會中提出共同擔任副主席意願，因此最後決議副主席由三個會員國代表擔任。
- 所有參與之會員國家代表共同簽署，同意亞洲 PKI 論壇合作計畫章程內容與合作原則，並達成共識為亞太地區建立一個無國界和順暢的電子商務環境，同時希望在公開金鑰基礎建設之法律制度、技術層面與跨國認證部分，建立各國間互通性的安全架構與原則，裨益電子商務整體發展。

亞洲 PKI 論壇合作計畫章程（Asia PKI Forum Charter）內容如下：

條款 1（名稱）

此項組織名稱為“亞洲 PKI 論壇”。

條款 2（目標）

此論壇目標在於推動各國或各地區間公開金鑰基礎建設（PKI）之互通性，並使電子商務在 PKI 領域能充分靈活運用。

條款 3（基本原則）

論壇之參與會員國應遵循以下基本原則，以達到條款 2 所述之目標。

（1）將無邊界、無國界電子商務觀念視為此論壇成立的基本宗旨，亞洲 PKI 論壇將協調各會員國間各項跨國性議題之合作計畫行動，以及尋求這些計畫對所有會員國所產生的多重性利益。

（2）亞洲 PKI 論壇將尊重並支持不同國家/地區提出的各項計畫，例如法律制度及技術發展，全力協助解決跨國議題，以確實達到互通性目標。

（3）所有論壇活動將透過各會員國以自願性參方式共同實踐。

條款 4（相關活動）

亞洲 PKI 論壇將實行以下必要性活動，協助解決跨國性議題，以期達到條款 2 之目標及條款 3 之各項基本原則。

（1）舉辦討論會並提供不同議題之資訊交換。

（2）執行必要性問卷調查、先導性實驗、以及有效的工作小組

討論。

（3）針對不同地區所舉辦的電子商務相關活動共同合作進行並參與。

（4）共同參與會員國間 PKI 技術性標準及 PKI 互通性推廣。

（5）研究並比較相關法律及電子交易系統規範。

（6）推動各會員國之間相互合作關係。

（7）進行任何必要性活動，以達成條款 2 之目標。

條款 5（會員資格）

原則上每個國家/地區由一個單位代表加入亞洲 PKI 論壇會員。營運委員會（Steering Committee）將從每一位候選國家代表提出的申請中審查並選出合格委員。會員會議功能則在於通過由指導委員會提出的各項決定。

條款 6（組織架構）

（1）會員大會（General Meeting）

a) 會員大會一年舉辦一次，由各會員國代表參與。

b) 會員大會功能則在於通過由指導委員會提出的各項決定，並做出與亞洲 PKI 論壇相關活動的各項決議。

（2）營運委員會（Steering Committee）

a) 營運委員會之委員將在會員會議上從亞洲PKI論壇會員國中推選出，每一位委員將代表一個國家/地區。

b) 營運委員會之委員數量將於會員會議中決議。

c) 營運委員會將研究並決定亞洲PKI論壇相關活動和管理上之政策及會員資格，同時尋求會員大會對這些決定的認可。

（3）主席和副主席

a) 主席和副主席（最多三位）將在會員會議中，從各會員國代表推選出來，任期為一年，連選得連任，但以不超過兩任為原則。

b) 主席需在各項活動和管理上扮演領導統域角色，並主持營運委員會和會員大會。

c) 在主席或任何一位副主席無法繼續執行其責任的情況下，亞洲 PKI 論壇將選出一位暫時替代的領導人接續所有職掌。

（4）秘書處

秘書處將設置於主席所在國家/地區，俾利執行相關作業。

（5）其他

工作小組和其他附屬單位需在必要情況下設立。

條款 7（會費）

會費會員應支付會費，並依據會員會議中所核可之決議來支付款項。

條款 8（其他）

其他規定/細則及相關亞洲 PKI 論壇運作方式將由營運委員會或其他委員會決定，並由會員大會核可通過。

（三）廠商拜訪

此次會議，除了主辦單位安排參觀 NEC 及富士通（Fujitsu）兩家公司的電子化政府/電子商務示範性展示中心外，中華台北代表團亦自行安排拜訪 Electronic Commerce Promotion Council of Japan（ECOM）公司和拜會日本 PKI 推進協議會（Japan Promotional Association for Asia PKI Forum, APKI-J）；另利用此次 PKI 論壇空檔期間，前往日本經濟產業省商務情報政策局拜會其承辦課長，了解日本電子簽章法之重要立法內容與推動情形。

NEC 資深經理 Mr. Takeo Sakurai 針對電子化政府與 PKI 相關產品做詳細解說與實地示範。NEC 在日本電子化政府方面致力相當多心血，相關工作包括：政府 PKI 架構、全方位電子化應用、電子結算、民眾申報網站、開放式網路貿易控制系統、校園社區服務、電子醫學系統等等。NEC 積極參與政府會議推動電子化政府，於 2000 年建置電子化政府商業推廣中心（Electronic Government Business Promotion Center）及建置電子化政府展示場，同時提供多項系統解決方案，協助日本推動電子化政府之發展。

富士通公司亦針對其所發展的電子化政府解決方案與 PKI 相關產品進行簡報與 showroom 展示先進設備。富士通參與電子化政府方面有許多作法與 NEC 相似，富士通認為 IC 卡在電子化環境中扮演重要角色，若運用得當，將會是一個多功能且便利的數位工具。

ECOM 公司對於電子商務技術、法律、管理標準制訂等各方面均有深入研究，其針對不同議題分別成立幾個工作小組進行相關計畫。ECOM 在認證部分已有 6 年研究，除了有豐富資訊外並完成多項重要

報告。ECOM 所提出的指導方針、報告、提案及研究調查等均是政府及民間在通動電子商務的一個重要參考來源。ECOM 表示日本有印鑑證明制度，目前由市公所核發，但也有私人企業進行核發動作，法律同樣承認其效力。日本並無強制規定認證機構需經正式核准才能發放認證，有些 CA 並無受政府公認或經過申請，如 VeriSign 在法律制訂之前已受大眾接受，這也是日本採行自由認證機構的原因之一。

拜會日本經濟產業省商務情報政策局之重點如下（因臨時約見，時間非常有限，訪談內容亦受限）：

＊ 日本電子簽章法已於二０００年五月公布，並於二００一年四月正式施行。

＊ 區分「認證業務」與「特定認證業務」：特定認證業務係符合主管機關設定基準而得以認為僅本人始得為之者，加以認證之業務（第四~六條）。

＊ 肯定電子文件之形式證據力（第三條）。

＊ 分別訂定國內認證事業與國外認證事業之認可程序：對外國認證公司（Certification Authority：CA）公司之認可，基本上可由日本政府認許之外國機構檢查或日本 JQA（日本品保協會）前往檢查（第七~十六條）。

＊ 訂定「指定調查機關」及「認可調查機關」制度：該法第十七條至三十條為有關對認證公司之檢查規定，基本上日本政府並不執行對認證之檢查工作，而是委由具公信力之機構代為執行，目前僅有「日本品保協會」（JQA）取得日本經濟產業省

之許可，可執行對 CA 公司之檢查工作，其收費標準約為日幣七０~八０萬元之間，經檢查認可之 CA 公司，給予「信賴標章」，類似我國優良商店認證給予標章一樣，至於未經檢查之 CA 公司，日本政府並未不准其設立，只是不具公信力而已，此項規範，乃日本政府基於自由原則，不給予太多管制，以使該產業有發展空間。

（四）結論與建議

- 由此論壇各國/地區報告中，可以發現歐洲、美國與澳洲之 PKI 活動多且積極，其發展較亞洲快速，此為日本急於尋求亞洲各國成立亞洲 PKI 論壇之主因，新加坡、韓國、日本對 PKI 推動極為積極，新加坡 B2B 電子商務交易量於 2001 年高達 1 千多億美元，跨國的電子商務貿易量於 2001 年亦達 5 百多億美元，因此對整體 PKI 建置有極大需求。

- 對於日本 NEC 及富士通兩家大廠的拜訪，可以感受到他們在 PKI 上的研發與應用的堅強實力。其所應用的軟硬體設備與技術幾乎都是自行研發，或許與歐美相較尚嫌不足，但相信以日本對 PKI 發展所致力的心血來看，在不久將來必很快趕上歐美進度，值得我國做為借鏡。

- 從日本此次「The First Asia PKI Forum」會議的安排時程緊湊性與態度來看，明顯感受到日本對於 PKI 這項合作計畫的推動，以及對 PKI 未來發展的期許相當積極並付出許多精力。這些亦是我國在發展 PKI 時，值得學習及參考之處。

- 本團相關人員此次拜會日本 PKI 推進協議會，與會長 Dr. Tsutomu Kanai 達成共識，希望將電子商務、網際網路與 PKI 共同結合，解決亞洲區相關問題，進而促進亞太經貿更加蓬勃發展。團長夏漢民先生表示 cross-border 為 PKI 合作計畫之重點項目，希望 Dr. Kanai 在之後 PKI 會議上將此訊息表達給各會員國，讓 Asia PKI Forum 推動更為順暢。不論在 IT 領域或電子零組件領域，日本和台灣實有密不可分關係，期許這項亞太區 PKI 合作計畫能加速我國電子商務發展。

- 亞洲各國中，日本、韓國、新加坡、馬來西亞、菲律賓、泰國均已陸續制定電子簽章（或交易）法，而我國尚僅立法院

一讀通過，有必要在下個會期加緊推動立法院儘速通過電子簽章法，以利於在亞洲 PKI 論壇展開積極活動。

- 未來在亞洲 PKI 論壇之營運委員會中（Steering Committee），政府應積極與業者協力在會中爭取設立相關 工作小組（Working Group）並擔任積極角色。

- 中共在亞洲 PKI 論壇中，積極爭取主導角色之企圖心相當明顯，我國未來在此類似活動中，亦應與業者協調配合積極參與，畢竟 PKI 在未來跨國電子商務扮演相當重要角色。

四、附件

（一）研討會資料

（二）會員章程

（三）會員簽署同意書

（四）其他參考資料

附件一

研討會資料

— The First Asia PKI Forum —

Date : Tuesday June 12 - Thursday June 14, 2001
Venue : New Takanawa Prince Hotel, Tokyo
International Convention Center PAMIR

Tuesday June 12

"Current Status of PKI Usage and Challenges for its Deployment"

13:30-	Registration
14:00-14:10	Opening Remarks: Mr. Seiichi Shimada, Vice Chairman, APKI-J(※) (Executive Vice President of Mitsui & Co., Ltd.) (※) Japan Promotional Association for Asia PKI Forum
14:10-14:50	Special Speech: "The Current Status and Prospective Use of PKI in the World: A Report on the Efforts of EESSI" Dr. Riccardo Genghini, Chairman, E-Sign Workshop, EESSI(※) (※) The European Electronic Signature Standardization Initiative
14:50-15:10	Break
15:10-17:40	Speeches: "Issues on the Deployment of PKI in Asia" ◇Report on efforts for PKI deployment ◇Challenges and proposals for PKI deployment in Asia Mr. Steve Orlowski, Chair, eSecurity Task Group APEC Telecommunications and Information Working Group, Representative of Certification Forum of Australia (CFA), Australia Mr. Qin Xu, Deputy Director-General, IT Industries Department of High Technology Industries, State Development Planning Commission, People's Republic of China Mr. Seok Lae Lee, Senior Member of Technical Staff, Korea Certification Authority Center, Korea Information Security Agency, Republic of Korea Dr. Kaizad Heerjee, Assistant Chief Executive, Online Development, Infocomm Development Authority of Singapore, Singapore Dr. Emmanuel C. Lallana, Executive Director of the e-ASEAN Task Force Secretariat Mr. Hajime Furuta, Deputy Director-General, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry, Japan
17:40-17:45	Closing Remarks Mr. Toshihiro Nishimura, Group Executive Vice President, Systems Engineering Group, Fujitsu Limited.
18:00-19:30	Welcome Reception

— The First Asia PKI Forum —

Wednesday June 13

"Towards the Establishment of the Asia PKI Forum"

8:30-	Registration
9:00-9:15	Opening Remarks: Dr. Tsutomu Kanai, Chairman, APKI-J (Chairman of the Board, Hitachi, Ltd.)
9:15-9:45	Congratulatory Speeches: Mr. Takeo Hiranuma, Minister of Economy, Trade and Industry, Japan Dr. Yong-Teh Lee, Chairman, Korea PKI Forum, Republic of Korea Mr. Lucas Chow, Chairman, PKI Forum Singapore, Singapore
9:45-10:25	Keynote Speech: "Key issue for global deployment of Electronic Commerce" Mr. Michio Naruto, GIIC(※1) Asia Co-Chair and GBDe(※2) Overall/Asia-Oceania Co-Chairs (※1) The Global Information Infrastructure Commission (※2) The Global Business Dialogue on Electronic Commerce
10:25-10:45	Break
10:45-11:15	Progress Reports on the Establishment of the Asia PKI Forum: Mr. Akira Tachigami, General Manager, Promotion Division APKI-J ◇Policies and planned activities of the APKI-J ◇Cooperation towards establishing the Asia PKI Forum
11:15-12:30	Special Speeches: "The Current Status of and Outlook for PKI Deployment Worldwide, based on the efforts of the IETF(※) and PKI Forum" (※) The Internet Engineering Task Force Dr. Stephen Kent, Co-Chairman, IETF/PKIX Ms. Lisa Pretty, President, PKI Forum
12:30-14:00	Lunch
14:00-15:00	Visual Presentation: "The future society with the use of PKI"
15:00-15:20	Break

— The First Asia PKI Forum —

15:20-17:20	Panel discussion: "Scenarios of PKI Deployment in Asia" Panelists: **Dr. Ki-Yoong Hong**, Member of Task Force Team, Korea PKI Forum, Republic of Korea **Dr. Mohamed Arif Nun**, Senior Vice President, Multimedia Development Corporation Sdn. Bhd., Malaysia **Dr. Kwok-Yan Lam**, Steering Committee Member, Technology Workgroup Chairman, PKI Forum Singapore, Singapore **Dr. Han-MinHsia**, Chairman, Chinese Taipei Promotion Association for Asia PKI Forum, Chinese Taipei **Mr. Jirou Makino**, Attorney at Law, Chairman of Business Environment Section of APKI-J, Japan Moderator: **Dr. Osamu Sudoh**, Professor, Doctor of Economics, Interfaculty Initiative in Information Studies, The University of Tokyo, Japan
17:20-17:35	Wrap up: **Mr. Akira Tachigami**, General Manager, Promotion Division APKI-J
17:35-17:40	Closing Remarks **Mr. Susumu Miyoshi**, Senior Managing Director, IT&ITS Group, Toyota Motor Corporation
18:00-19:30	Networking Party

Thursday June 14

"Field Visit" (only for overseas participants), 9:30-15:00

Japan Promotional Association for Asia PKI Forum

5F, Daiichi Oda Building, 23-5, Omori Kita 1-chome, Ota-ku, Tokyo 143-0016

TEL:03-5767-0671

FAX:03-3761-3313

E-mail : pkiforum@apki-j.gr.jp

URL : http://www.apki-j.gr.jp/

— The First Asia PKI Forum —

Schedule

Tuesday, June 12

Time	Program	Place
14:00～17:45	Forum -Opening Remarks -Special Speech -Speeches -Closing Remarks	3rd Floor KONRON 'HAKUUN'
18:00～19:30	Welcome Reception	2nd Floor 'FUKUJU'

Wednesday, June 13

Time	Program	Place
9:00～12:30	Forum -Opening Remarks -Congratulatory Speeches -Keynote Speech -Progress Reports on the Establishment of the Asia PKI Forum -Special Speech	3rd Floor KONRON 'HAKUUN'
12:30～13:45	Lunch	3rd Floor KONRON 'KEIUN'
13:45～17:40	Forum -Visual Presentation -Panel Discussion -Wrap Up -Closing Remarks	3rd Floor KONRON 'HAKUUN'
18:00～19:30	Networking Party	3rd Floor KONRON 'KEIUN'

― The First Asia PKI Forum ―

開催日：2001年6月12日（火）～14日（木）
会場：新高輪プリンスホテル 国際館パミール

◇ 6月12日(火)「PKI利用の現状と普及に向けた課題」

13:30-	受付
14:00-14:10	開会挨拶： アジアPKIフォーラム推進協議会 副会長 島田 精一 氏（三井物産株式会社 代表取締役副社長）
14:10-14:50	特別講演： 「世界におけるPKI利用の現状と展望 ～欧州EESSIの活動～」 講演者： EESSI（欧州電子署名標準化イニシアティブ）電子署名グループ 議長 Riccardo Genghini 氏
14:50-15:10	休憩
15:10-17:40	講演： 「アジアにおけるPKI普及のための課題」 講演者： APEC eSecurity タスクグループ議長 オーストラリア認証協議会 代表 Steve Orlowski 氏 中国国家発展計画委員会高技術産業発展司副司長 Qin Xu 氏 韓国 Information Security Agency 上席技術スタッフ Seok Lae Lee 氏 シンガポール Infocom Development Authority ｱｼｽﾀﾝﾄﾁｰﾌｴｷﾞｭｾﾞｸﾃｨﾌﾞ Kaizad Heerjee 氏 e-ASEAN 事務局長 Emmanuel C.Lallana 氏 経済産業省商務情報政策局 審議官 古田 肇 氏
17:40-17:45	閉会挨拶 富士通株式会社 取締役 西村 敏洋 氏
18:00-19:30	レセプション

― The First Asia PKI Forum ―

◆ 6 月 13 日（水）「アジア PKI フォーラム設立に向けて」

8:30-	受付
9:00-9:15	開会挨拶 アジア PKI フォーラム推進協議会 会長 金井 務 氏（株式会社日立製作所 取締役会長）
9:15-9:45	ご来賓挨拶： 経済産業大臣 平沼 赳夫 氏 韓国 PKI フォーラム会長 Yong-Teh Lee 氏 PKI フォーラムシンガポール会長 Lucas Chow 氏
9:45-10:25	基調講演： 「電子商取引のグローバル展開と普及のための課題」 講演者： GIIC（世界情報基盤委員会）アジア地区共同議長 及び GBDe※共同議長 鳴戸 道郎 氏 ※ GBDe：Global Business Dialogue on Electronic Commerce
10:25-10:45	休憩
10:45-11:15	アジア PKI フォーラム設立に向けた活動について アジア PKI フォーラム推進協議会 推進本部長 舘上 章 氏
11:15-12:30	特別講演： 「世界における PKI 利用の現状と展望 ～IETF 及び PKI Forum（米国）の活動～」 講演者： IETF（Internet Engineering Task Force）/PKIX 共同議長 Stephen Kent 氏 PKI Forum 議長 Lisa Pretty 氏
12:30-14:00	昼食
14:00-15:00	映像とデモンストレーション： 「PKI が実現する未来社会のイメージ」
15:00-15:20	休憩

― The First Asia PKI Forum ―

15:20-17:20	パネルディスカッション： 「アジアにおける PKI 普及のシナリオ」 パネリスト： 韓国 PKI フォーラムタスクフォースメンバー Ki-Yoong Hong 氏（韓国） マルチメディア開発公社 副総裁 Mohamed Arif Nun 氏（マレーシア） シンガポール PKI フォーラム推進協議会技術ワークグループ議長 Kwok-Yan Lam 氏（シンガポール） Chinese Taipei アジア PKI フォーラム推進協議会会長 Han-Min Hsia 氏（Chinese Taipei） APKI-J ビジネス環境検討部会 部会長・弁護士 牧野 二郎 氏（日本） モデレータ： 東京大学大学院情報学環教授 経済学博士 須藤 修 氏
17:20-17:35	アジア PKI フォーラム設立について アジア PKI フォーラム推進協議会 推進本部長 舘上 章 氏
17:35-17:40	閉会挨拶 アジア PKI フォーラム推進協議会 副会長 三吉 暹 氏（トヨタ自動車株式会社 専務取締役）
18:00-19:30	懇親パーティ

◆ 6 月 14 日（木）「フィールドビジット」（海外参加者のみ）

アジア PKI フォーラム推進協議会
〒143-0016 東京都大田区大森北 1 丁目 23 番 5 号 第 1 小田ビル 5 階
TEL:03-5767-0671
FAX:03-3761-3313
E-mail: pkiforum@apki-j.gr.jp
URL ：http://www.apki-j.gr.jp/

― The First Asia PKI Forum ―

会場スケジュール

6月12日（火）

時間	プログラム	会場
14:00～17:45	フォーラム ・開会挨拶 ・特別講演 ・講演 ・閉会挨拶	3F 崑崙「白雲」
18:00～19:30	レセプション	2F 「福寿」

6月13日（水）

時間	プログラム	会場
9:00～12:30	フォーラム ・開会挨拶 ・ご来賓挨拶 ・基調講演 ・アジア PKI フォーラム設立に向けた活動について ・特別講演	3F 崑崙「白雲」
12:30～13:45	昼食	3F 崑崙「慶雲」
13:45～17:40	フォーラム ・映像とデモンストレーション ・パネルディスカッション ・アジア PKI フォーラム設立について ・閉会挨拶	3F 崑崙「白雲」
18:00～19:30	懇親パーティ	3F 崑崙「慶雲」

Notes

For Forum Participants

1: Please refrain from smoking in the hall. Smoking is permitted only in smoking areas in the lobby.

2: Please refrain from using a cellular phone in the hall in order not to trouble other participants. Please use the silent mode on your cellular phone.

3: The nametag and handouts are used for 2days. Please be to bring them on the 2nd day. Entrance to the hall is not permitted without the nametag.

4: Please leave the translation receiver left on the desk.

5: Participants in the field visit (only overseas participants) need to bring the nametag used in the Forum.

ーフォーラムに関する注意事項ー

1：会場内は禁煙とさせて戴きます。喫煙場所は各階ロビーにございます。

2：周りのお客様のご迷惑になりますので、会場内の携帯電話ご使用はお控え下さい。また、着信音のマナーモード利用をご協力お願い申し上げます。

3：名札および配布資料は２日間共通となりますので、２日目も忘れずにご持参下さい。名札をお忘れになると、会場内にお入り戴けない可能性がございます。

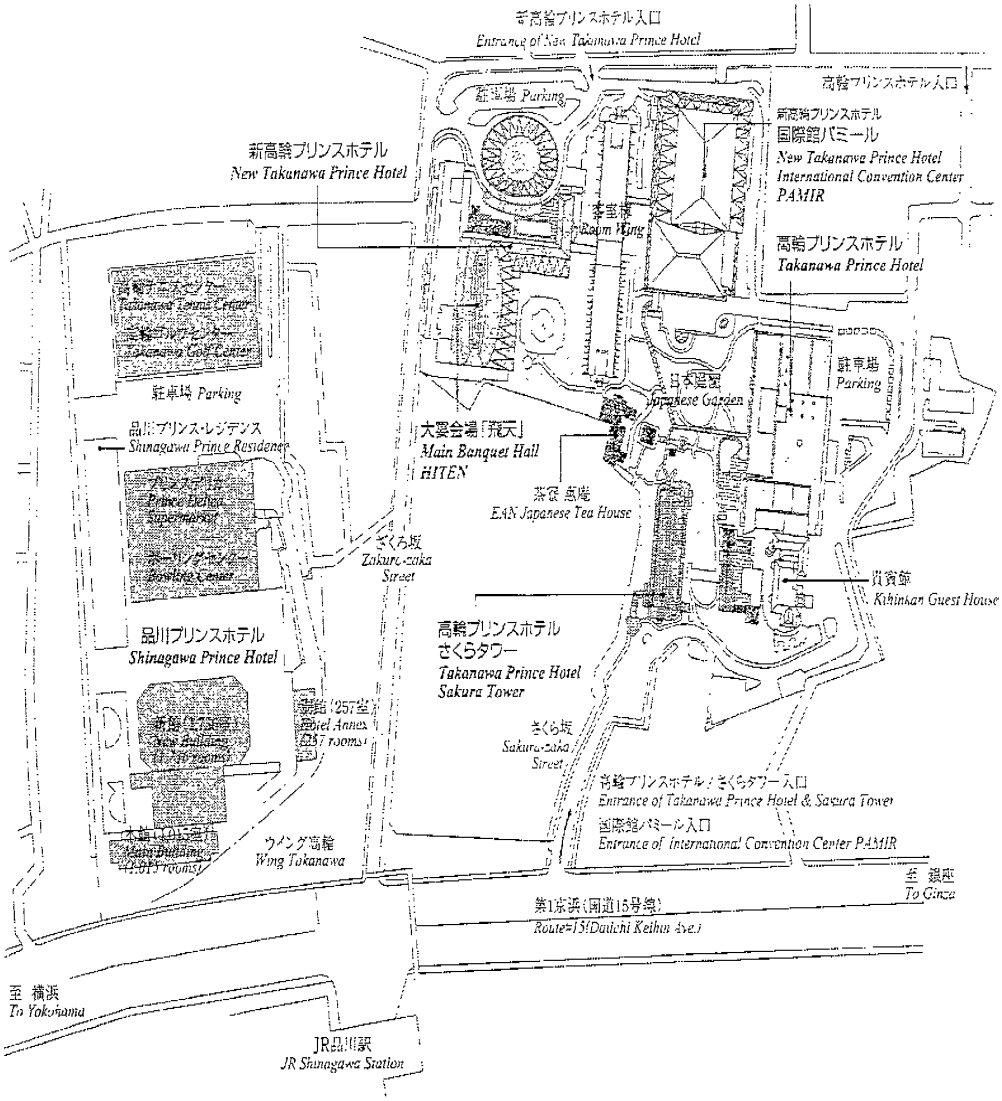
4：同時通訳レシーバは２日間とも机の上に置いたままでお帰り下さい。

5：フィールドビジット（海外参加者のみ対象）へ参加される方は、フォーラムで使用戴きました名札を忘れずにご持参下さい。

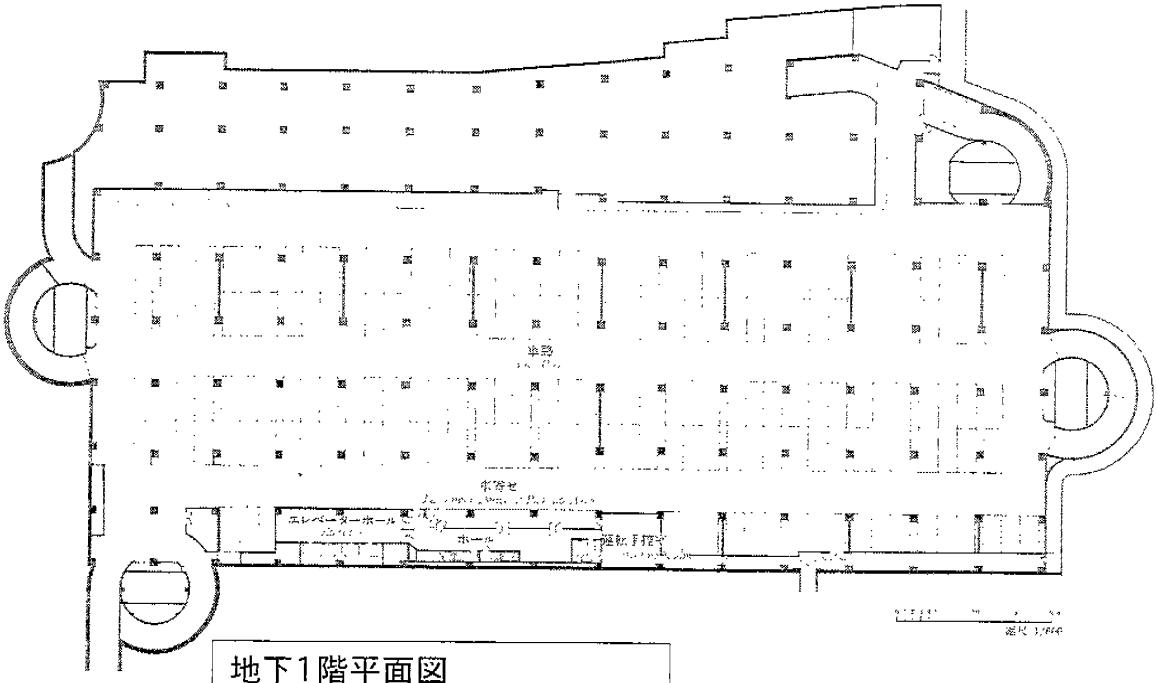
ー以　上ー

Place Information

【 Around New Takanawa Prince Hotel 】

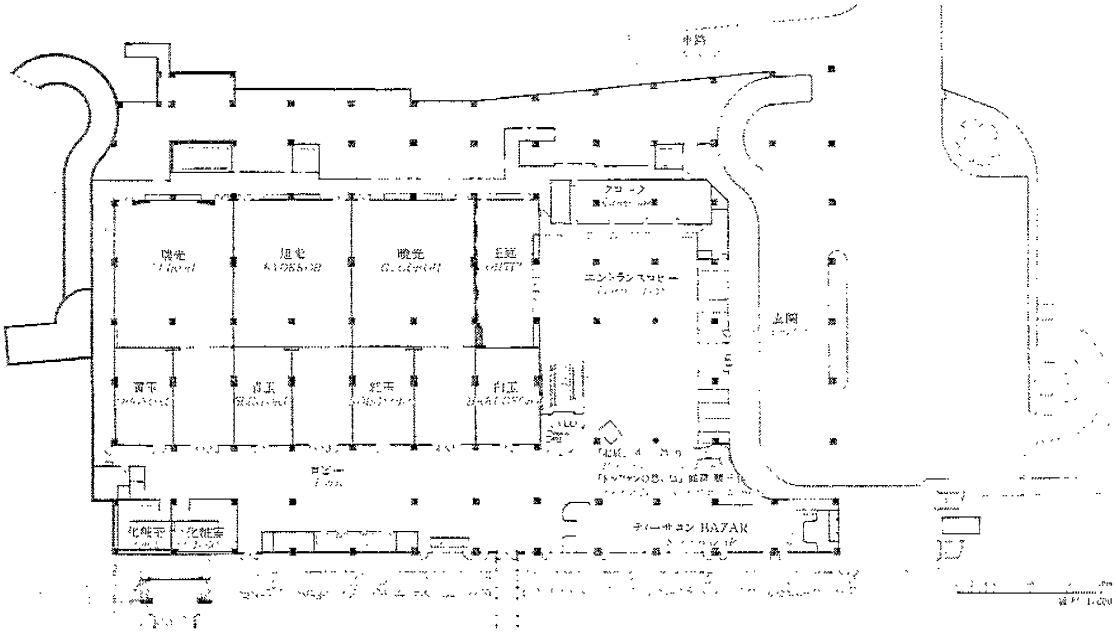


【Floor Plan-A】



地下1階平面図

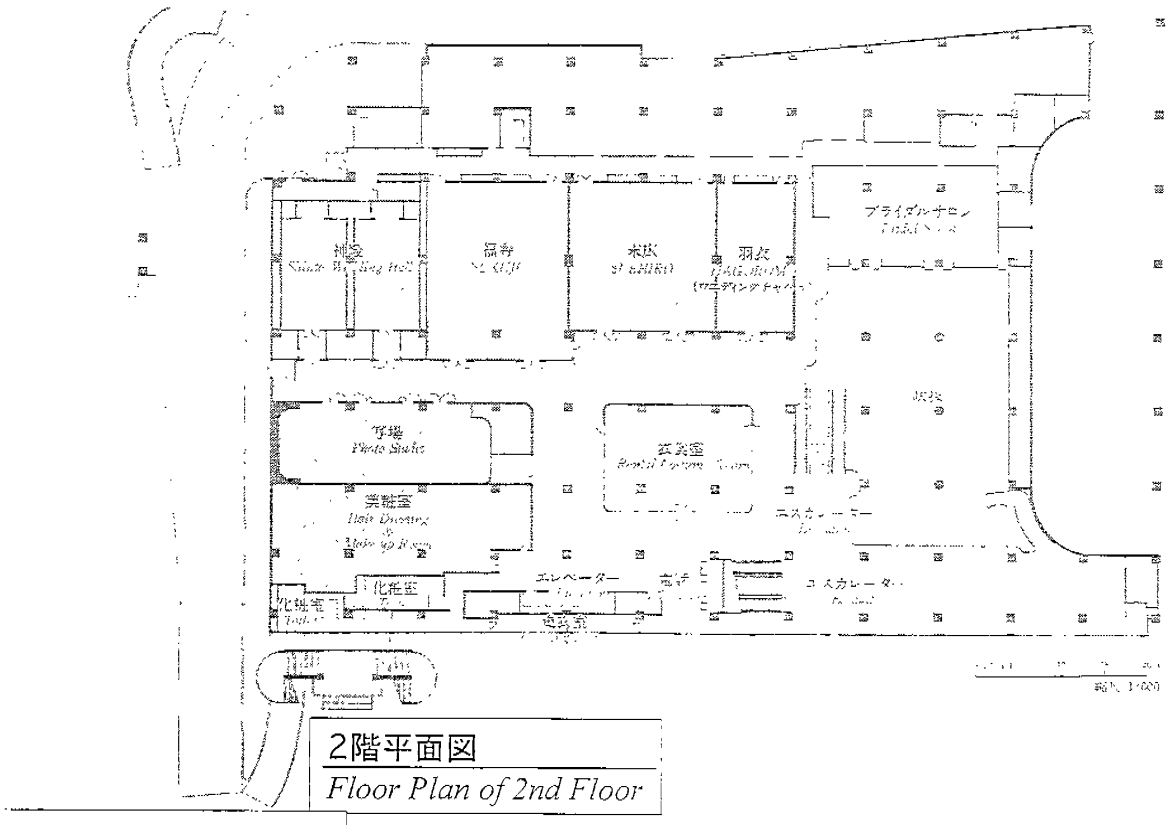
Floor Plan of Basement 1 Floor



1階平面図

Floor Plan of 1st Floor

【Floor Plan-B】


2階平面図
Floor Plan of 2nd Floor

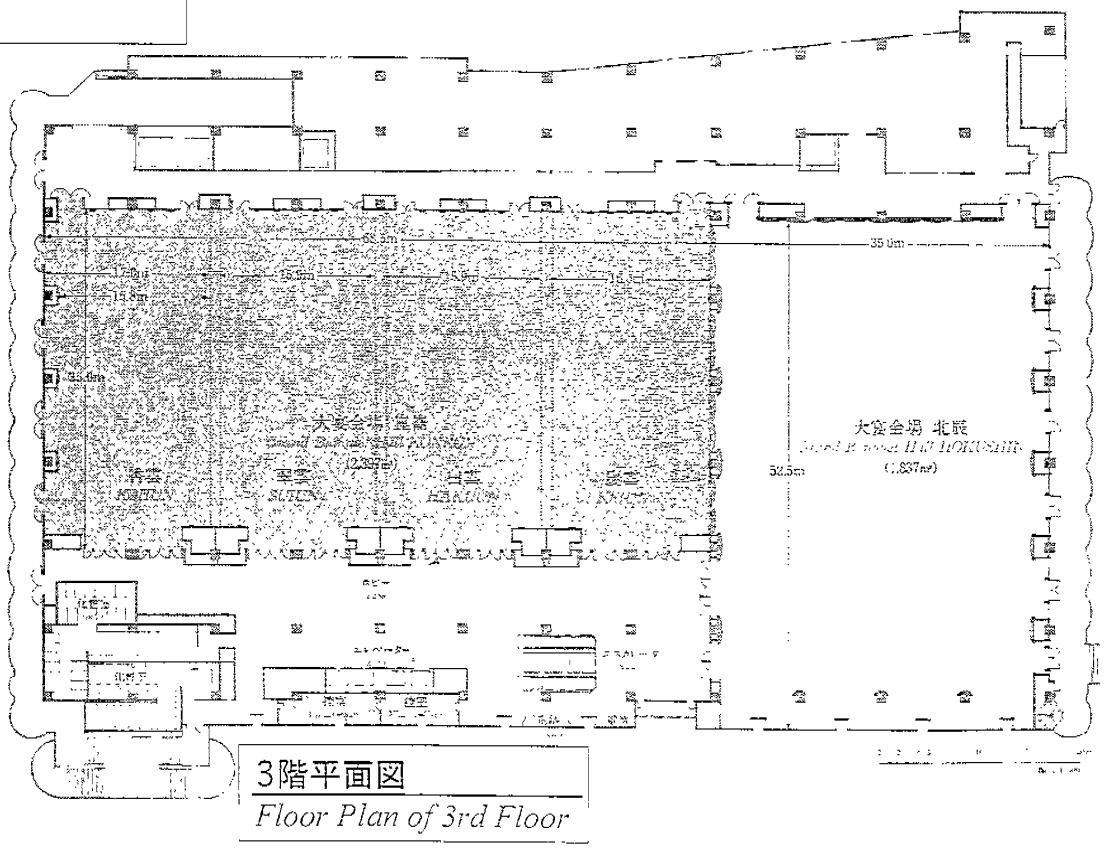

大宴会場 北館
35.0m
52.5m
3階平面図
Floor Plan of 3rd Floor

Table of Contents

《Tuesday, June 12, 2001 》

《Wednesday, June 13, 2001 》

The First
Asia PKI
Forum

DOCUMENT NO.01

TITLE : The Current Status and Prospective Use of PKI in the World: Electronic Signature infrastructure for Europe

SUBMITTED BY : Dr.Riccardo Genghini
Chairman,E-Sign Workshop,EESSI

Electronic Signature Infrastructure for Europe

Riccardo Genghini

Assumptions (1)

- National legislation has few impact on (Internet) technology evolution
- (Internet) Technology influences more law then vice-versa
- Over regulation stifles competition and IT development

Assumptions (2)

- Technology is not trustworthy by itself
- There is the need to have a reasonable trust in technology
- Technology changes very quickly, so that national legislator cannot cope with such frantic evolution

Goals for the infrastructure (1)

- Carve advantages of IT without losing that of paper: i.e. long term availability
- Combine the freedom and anonimity of traditional commercial transactions, with a better documentation
- Increase transparency and fairness towards consumers, through appropriate documentation

Goals for the infrastructure (2)

- Allow integration of business procedures into the IT systems of SMEs and VSEs
- Allow more participation of citizens to their institutions activity
- Allow e-government reducing overall costs of public administration

Problems of the infrastructure

Legal relevance

Liability and risk management

Balance between security and data protection

Objective assessment of IT security

Social acceptance

Effective business models

Principles of 93/1999 EC (1)

Principle of co-regulation:

- Legislator sets goals
- Technical self-regulation defines ways in full respect of existing international standards

Principle of technical neutrality:

- Law should not stifle innovation
- Law should not distort competition

Principles of 93/1999 EC (2)

Privacy Protection (art. 8):

- Electronic signatures shall not make data mining easier!
- Freedom of pseudonimity is a granted individual right

Consumer Protection (Art. 3, 6 and Annexes I, II and III):

- Minimum liability (art. 6)
- Make technology transparent to users (art. 3 + 6):
  - secure signature creation device (Annex III)
  - qualified certificates (Annex I)
  - trustworthy systems (Annex II)

Principles of 93/1999 EC (3)

No discrimination (art. 3):

- National legislator shall not discriminate electronic signatures coming from other member states
- Independent and transparent supervision of TSPs

EU Mutual recognition (art. 5):

- A common framework of technical standards has been set up and is further developed by Cen-ISSS and ETSI
- 93/1999/EC refers to such standards
- Multilateral co-operation between supervisors started

Principles of 93/1999 EC (4)

International recognition (art. 7):

- of third countries CSP if:
  - It fulfils the requirements of the directive and has been accredited under a voluntary accred. scheme
  - The certificates are guaranteed by a CSP established within the EU
  - Is recognised under an international agreement with third countries or international organisations

Principles of 93/1999 EC (5)

No licensing (art.3):

- Accreditation is voluntary
- Supervision is mandatory for each member state

Legal relevance (art. 5):

- Advanced signatures, created with a Secure Signature Creation Device for which a Qualified Certificate has been issued, are equal to handwritten signatures (5.1)
- To other legal relevance cannot be denied in principle

93/1999/EC implementation

Member States shall implement the directive before July 18th 2001

- Legislation shall be completed
- Supervisory schemes shall be in place
- National Supervision bodies shall be notified to the Commission
- Accredited CSPs also shall be notified to the Commission

93/1999/EC Implementation

- Germany, Austria, France have fully implemented the directive
- The other Member States already have legislation on electronic signatures and are amending it
- Except Greece and Finland which are finalizing their legislation

Open Issues

EESSI Standards
first step towards

- European Interoperability
- European co-ordination of Supervision
- Europüean Accreditation Schemes
- European Root Authority

EESSI European Electronic Signature Standardisation Initiative

EESSI SG

Comitée Européen de Normation
Information Society Standardisation System

European Telecommunications Standards Institute

Industry and business, assisted by European standard bodies

EESSI Implementation Plan (1)

Phase 2 (2000) completed 2Q2001
Phase 3 (2001) deliverables to be published by the end of 2001

ETSI ESI Working Group

- Result: ETSI Technical Specifications
- 40-50 Participants, funded Specialist Task Force, STF155, 178
- Chairman: gyorgy.g.endersz@telia.se

CEN/ISSS E-SIGN Workshop

- Result: CEN Workshop Agreements
- 50-70 participants, funded Expert Teams
- Chairman: riccardo.genghini@sng.it

EESSI Implementation Plan (2)

PHASE 2 APPROVED STANDARDS: Cen-ISSS E-Sign

- Cen Workshop Agreements (CWA)
  1. Signature Creation Process (Area C1) CWA 14170 *Signature Creation Process and Environment*
  2. Signature Verification Process (Area C2) CWA 14171 *Signature Validation Process and Environment*
  3. Signature Creation Device (Area F) CWA 14168 – 14169 *Security Requirements for Secure Signature Creation Devices*

EESSI Implementation Plan (3)

PHASE 2 APPROVED STANDARDS : ETSI ESI

- ETSI Technical Standards
  1. *Time Stamping Profile (ETSI TS 101 861)*
  2. *Electronic Signature Formats* (ETSI TS 101 733)
  3. *Policy Requirements for Certification Authorities issuing Qualified Certificates* (ETSI TS 101456)
  4. *Qualified Certificates Profile* (ETSI TS 101 862) based on IETF *X.509 Public Key Infrastructure Qualified Certificates Profile*

EESSI Implementation Plan (4)

PHASE 2 ALMOST READY STANDARDS:

- Cen Workshop Agreements
  1. *CWA 14167 "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures"*
     - *14167-1 (Area D1) Trustworthy Systems*
     - *14167-2 (Area D2) Security of cryptographic modules*
  2. *CWA 14172: (Area V) Conformity Assessment Guidance*

EESSI Implementation Plan (5)

PHASE 3 ONGOING ACTIVITIES:

- Cen-ISSS E-Sign Working Groups
  1. Area AA: Extension of SSCD requirements towards specific applications/environments and towards e-commerce applications (Art5.2)
  2. Area K: Smartcards
  3. EESSI Algorithm Group (Voluntary Research)

EESSI Implementation Plan (6)

PHASE 3 ONGOING ACTIVITIES

- ETSI ESI Working Groups
  1. Security management and certificate policy for CSPs issuing time stamps
  2. Security management and certificate policy for CSPs issuing other than qualified certificates
  3. Electronic signature syntax and encoding formats
  4. Signature policies
  5. Provision of harmonised status information on CSPs and other Trust Service Providers
  6. Maintenance of TS101456 TS101733 TS101862 TS101861

EESSI References

ETSI:
http://www.etsi.org/sec/el-sign.htm
sign up from Web-site to open El Sign mailing list

CEN:
http://www.cenorm.be/isss/workshop/e-sign

EESSI:
http://www.ict.etsi.org/eessi/EESSI-homepage.htm

Asian PKI Forum

- Asian Legislation should boost the productivity potential of IT industry
  - Enhance co-regulation, use international standards
  - Avoid too strict state led infrastructure and "national" solutions
- Asian Interoperability with EU 15 strategically relevant for also for EU

Asian PKI Forum

- Accept open-market principle
- PKI are the organisative/security backbone of the new millennium so they have to think and act
  - Globally (international standards)
  - Transparently (open source no proprietary solutions)
  - Freely (self-regulation + co-regulation not only state-legislation)

Dr. Riccardo Genghini - SNG

Notary Public in Milan - Italy

Cen - ISSS E Sign Chair 2001

Founder of the law firm "SNG"

R&D with leading EU Universities

IT Consulting since 1995

IT Law research since 1982

Present also in Germany, Austria, UK

www.sng.it

SNG's Offices

Via Libertà, 89
20092 Cinisello B. (MI)
tel 02 660991
fax 02 66099666
cinisello.office@sng.it

Via S. Pietro all'Orto, 17
20121 Milano
tel 02 76303011
fax 02 76303029
milano.office@sng.it

Via G. Boccherini, 3
00198 Roma
tel 06 85356919
fax 06 8540260
roma.office@sng.it

STUDIO NOTARILE DR. GENGHINI

The First
Asia PKI
FORUM

DOCUMENT NO.02

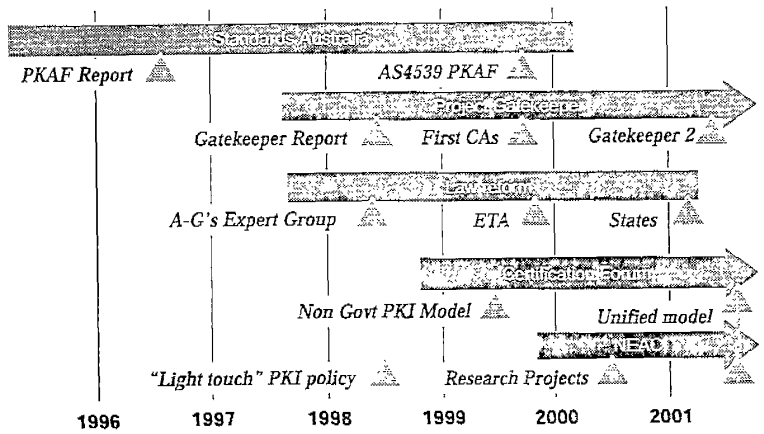
TITLE : AUSTRALIAN AND APEC PKI INITIATIVES

SUBMITTED BY : Mr.Steve Orlowski
Chair,APEC Telecommunications E-security Task Group Representative of Certification Forum of Australia(CFA)

AUSTRALIAN AND APEC PKI INITIATIVES

Steve Orlowski
AUSTRALIA

Evolution of PKI in Australia



Standards

PKAF strategy report

Working group on PKI standards

Standards for public key framework, algorithms, certification authorities

Based on ISO and IETF material

Working group on IT security standards

- integrate with PKI standards

Gatekeeper

Policy framework for PKI in government

Federal agencies must use PKI products from Gatekeeper accredited service providers

Accreditation:

- BCAPL, e-Sign, ATO, HeSA
- 10 have applied

States sign up (November 2000)

Gatekeeper Implementations

Australian Tax Office certificates for GST returns

Australian Securities & Investment Commission

HealthConnect national health network

Australian Customs Service (planned)

Australian Quarantine Inspection Service (planned)

ABN-DSC

The Australian Business Number - Digital Signature Certificate

ABN - A unique business identifier

Agencies to use the ABN

ABN-DSC

Announced December 1999

States in principle agreement November 2000

ABN-DSC specification final January 2001

Based on standard Gatekeeper organisational certificate with ABN

Multi agency use planned

ABN-DSC scope

All Commonwealth and State agencies using digital certificates to identify business are to issue/accept ABN-DSC

For commercial and regulatory transactions with government

The ABN-DSC not for transactions with individuals as individuals

ABN-DSC outcomes

For business

only one identity and certificate needed for dealing with government/s

For government

efficiencies; reduced cost in providing identity, improved business cases

For the economy

for use with government but will facilitate e-commerce

Project Angus

Four major banks

Angus businesses certificates that conform to ABN-DSC specification will be regarded as ABN-DSCs

The Government will also accept other providers' ABN-DSCs

Angus members to obtain Gatekeeper accreditation as RAs

Each Angus member to be cross recognised

Effect

Project Angus digital certificates will be regarded as ABN-DSCs and accepted by Commonwealth agencies

Seeking States' agreement

ABN-DSCs able to be issued by others

Not an exclusive deal

Facilitate B2B e-commerce

Gatekeeper/Angus Interoperation

Both schemes are based on relevant international and national standards

Accredit each Angus member with Gatekeeper

Not cross recognise Identrus scheme

Angus member to determine their PKI service provider

Angus members to achieve Identrus accreditation prior to cross recognition

Cross-recognition involves comparing accreditation criteria and factors such as the regulatory framework

Gatekeeper Accreditation Certificate

Electronic certificate signed by Gatekeeper

Issued to Gatekeeper accredited CAs

Issued to other CAs/schemes recognised by Gatekeeper (including overseas)

Facilitates interoperability

Legal Effect

Electronic Transactions Act 1999 (Federal)

Based on UNCITRAL Model Law on Electronic Commerce

Technology neutral

States in the process of implementing Uniform Electronic Transactions Bill

Certification Forum of Australia

Authentication sector industry group
- lobbying & position papers
- awareness & education
- standards based accreditation model
- Code of Practice & control model
- seat on NEAC

Members
- PKI services and vendors
- users & user groups
- governments
- lawyers, auditors, insurers

National Electronic Authentication Council

Chaired by NOIE.

Members: IT industry, retailers, Small Business Coalition, Australian Bankers Association, Australian Consumers Association, government

Mission is to build industry and consumer confidence in the use of authentication technologies including, but not exclusively PKI

Working Groups

Building consumer and industry confidence

International policy/legal and liability issues

Systems integration and authentication frameworks for industry

Current Activities

Small business/consumer guide to authentication

Legal liability of eTransactions

International policy on authentication

Business applications for private sector

APEC

eSecurity Task Group
- issues paper on electronic authentication
- technical annexes including PKI

PKI Interoperability Expert Group
- PKI interoperability paper
- PKI interoperability mapping

eCommerce Steering Group
- paperless trading initiative

PKI Interoperability Mapping

High degree of consistency

Inconsistencies
- approach to inter-operability and cross-certification
- performance of security function
- policy function and existence of policies

Signed Certificate Trust Lists

Trust list generated by trusted body (eg national body)

Digital signed by trusted body

Imported into browser or application

Evidence of legal effect

Does not require relationship between CAs

Requires check of trust list as well as certificate

APEC TEL Future Activities

Clarification of terminology

ISO, IETF, EESSI, PKI Forums

Interoperability of different approaches

APEC, OECD, PKI Forums

Development of standards

ISO, EESSI, IETF

References

Certification Forum of Australia
http://www.aeema.asn.au/groupings/divs_info.cfm?divisionID=35

National Electronic Authentication Council
http://www.noie.gov.au/neac

Government Public Key Authority (Project Gatekeeper)
http://www.gpka.gov.au

Australian Business Number - Digital Signature Certificate
http:/www.govonline.gov.au/projects/publickey/abn-dsc.htm

References (2)

Report of the National Electronic Health Records Taskforce
www.health.gov.au/healthonline/ehr_rep.htm

APEC e-Security (formerly Electronic Authentication) Task Group
http://www.apectelwg.org/apec/atwg/preatg.html

Standards Australia
http://www.standards.com.au/

The First
Asia PKI
Forum

DOCUMENT NO.03

TITLE : PKI Policy & Framework in Korea

SUBMITTED BY : Mr.Seok Lae Lee
Senior Member of Technical Staff,
Korea Certification Authority Central,
Korea Information Security Agency

PKI Policy & Framework in Korea

12 June 2001

Korea Information Security Agency, Korea

Seok-Lae Lee

I. Overview of PKI in Korea

1. The Digital Signature Act
2. Licensed certificate
3. Overview of certificate [illegible]
4. Applications [illegible]

1.1. The Digital Signature Act - Enactment

- Ensuring the security and reliability of electronic messages processed over the networks
  - Promotion of e-commerce, implementation of e-government and the usage of e-money
  - Promotion of informatization and public welfare
- Feb. '99: Digital Signature Act proclamation
  Jul. '99: Enforcement

1.2. The Digital Signature Act - Principles

- Principle of minimum regulation
  - Flexibly responding to technological change, social regulations to protect subscribers
- Harmony between public and private benefits
  - Pursuit of public interests and profits by supervising both public and private sectors
- Harmony between legal stability and convenience
  - Legal system, technology, policy, profitability, convenience, customer protection
  - Trade-off in security, reliability(legal stability) and convenience(profitability)

1.3. The Digital Signature Act - Major contents

- Grant legal effect on digital signature certified by licensed certificate authorities
- Minister of Information and Communication license the certificate authorities
- Managing system for assuring continuity and reasonability of certificate practice
- Certificate issuing procedure and validity of certificates
- Personal information security related certificate practice
- Mutual recognition of certificates between countries

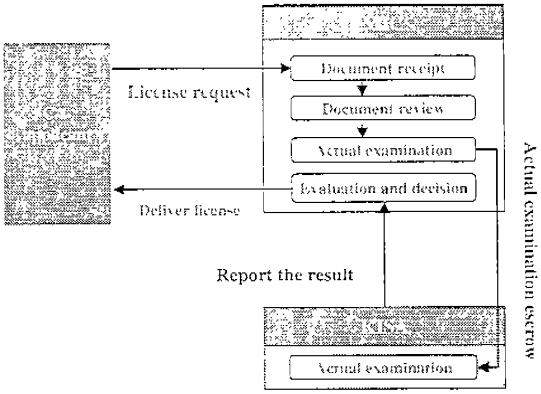
2.1. Comparison between the licensed and the private CA

- **Licensed certification authorities**
  - Licensed pursuant to article 4, the Digital Signature Act
  - Hold legal effect on digital signature certification
  - Assume strict obligation to ensure credibility
- **Private certification authorities**
  - No legal restriction or obligation
  - Not legally valid on digital signature certification
  - Corporate or foreign certification authorities, etc.

2.2. Requirement for licensed CAs

- **Financial capability**
  - Capital : more than 8 million dollars
- **Technological ability**
  - More than 12 certification practice management engineers
- **Facilities and equipment: dualization**
  - Verifying subscriber's identity and registration
  - Digital signature key and certificate management (dual operation)
  - Security equipment for certification management system
  - Physically dualized data backup

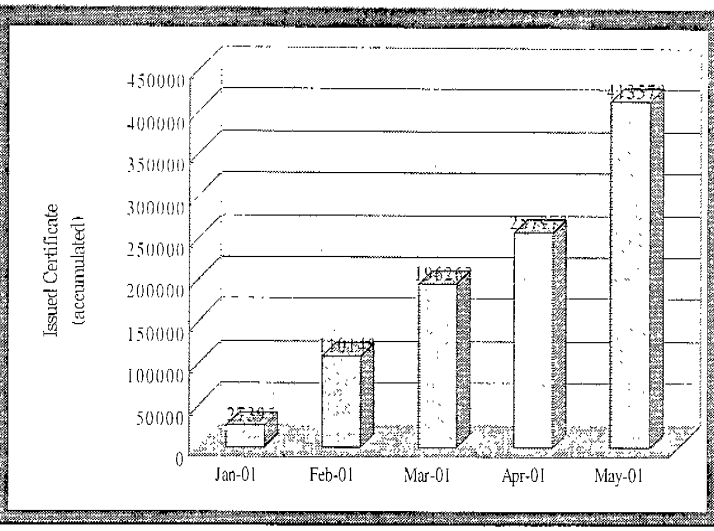
2.3. CA license procedure



3.1. Overview of certification market in Korea

- **Licensed certification authorities**
  - KICA, KOSCOM, KFTC, NCA
- **The market is not stimulated yet due to the lack of perception and the absence of an environment for using digital signature**
  - **An environment is being formulated at financial institutions and companies**
  - **The market is expected to rapidly expand as individual subscribers increase**

3.2. Overview of certification market in Korea



4. Application fields of the certificates

- **The public sector**
  - Civil affair, license application, home tax service, government procurement, customs, official document circulation and electronic patent application, etc.
- **The Financial sector**
  - Internet banking, cyber securities transaction, electronic money, etc.
- **Others**
  - Internet Shopping, various reservations and purchase of entrance tickets, Medical chart·prescription, electronic notary, etc.

II. Major PKI policy direction

- [illegible]
- Year 2001 [illegible]
  - signature [illegible]
- Attract 10 million [illegible]
  - subscriber [illegible]

1. Activation the use of certificates

- Government and public agencies
  - The MIC launched a pilot project in secured mails using certificates within its organizations
  - The project will gradually spread to other administrations and public institutions
- Private enterprises
  - Establish a PKI forum to promote PKI usage in B2B sector
  - Start WPKI service in preparation for a vibrant m-Commerce
- Individuals
  - Advertise the need for PKI and usage procedure, etc.

2. Incentive programs for more users

- Reduction of certificate issuance cost
  - 6 months' free service for a certificate issued for the first half of this year
  - Relative cost reduction by using one certificate in various applications
- Reduction of business execution cost
  - 10% reduction in procurement fee when public institutions use EDI system for procurement (since Jun. 2000)
  - Drawing up a plan of tax reduction for a taxpayer using certificate in electronic report, notification and payment

3. Laws/regulations improvement

- A person can be identified through the digital certificate when opening a bank account
  - Now, the resident registration card is the only means to identify a person
- The digital signature will determine over the Internet whether a person is an adult.
- The Digital Signature Act will stipulate a digital certificate can identify a person

4. The construction of wireless PKI

- Directions of promoting wireless PKI
  - Construct wireless PKI which can accommodate all of wireless Internet protocol such as WAP and MIP
- Maximum use of the licensed certification authorities
  - The existing licensed certification authorities will perform authentication work in wireless field
- Construction plan
  - KISA provides technical standards

5. Digital signature mutual recognition

- APEC actively pursues mutual recognition
  - Canada and Singapore suggest the common evaluation method on digital signature
  - Introduction the concept of Cross Recognition
  - 5 countries (Korea, Australia, Hong Kong, Canada and Singapore) will join
- Develop mutual recognition technology
  - A technology that can embrace different certification system and policy of each nation
  - KISA leads the technology group
  - 1 million dollars will be invested from 2000 to 2001

III. Our chances and challenges

1. Digital signature user forecast(Korea)

(unit: 10,000 person)

	2001	2002
Gov't/Public	12	33
Bank	127	405
Stock market	71	236
Insurance/credit	66	194
m-Commerce	16	101
Other	22	82
Total	314	1,051

2. Our chances and challenges

Information and knowledge are competitive power in the Internet

Internet user per population: Korea ranks top among the Asian countries (as of now, Korea 20mil)

Public Key Infrastructure for the secure circulation of information and knowledge

Korea aims to jump into the top 10 nations in terms of the information and knowledge advancement in the 21C

The First
Asia PKI
Forum

DOCUMENT NO.04

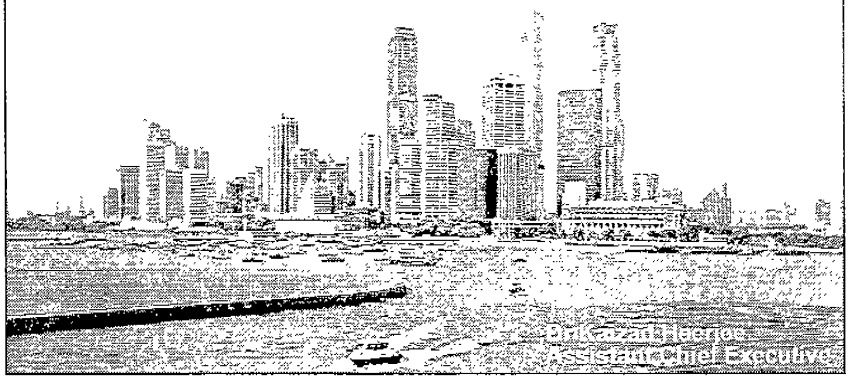
TITLE : Creating a Trusted e-Business Environment through PKI

SUBMITTED BY : Dr.Kaizad Heerjee
Assistant Chief Executive,Online Development,Infocomm Development Authority,Singapore

iDA

INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

Creating a Trusted e-Business Environment through PKI



Dr Gazali Jaafar
Assistant Chief Executive

iDA

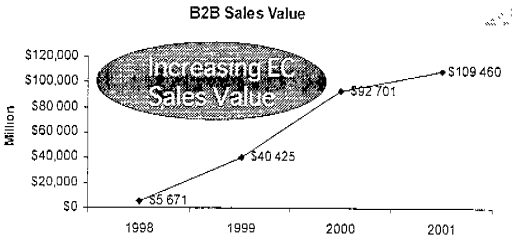
Focus of today's presentation

- Why Trust & Confidence are important
- Key focus areas for making Singapore a Trusted Hub
- Programs for driving PKI Adoption

Catalyst for Change

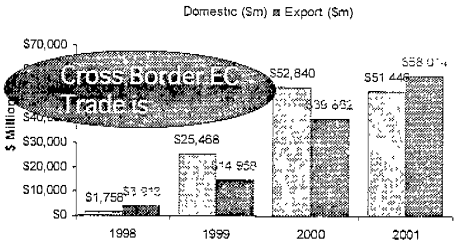
iDA

E-Commerce in Singapore



757% of surveyed companies have web sites

More companies are adopting EC



Catalyst for Change

iDA

Virtual World Requires Trust

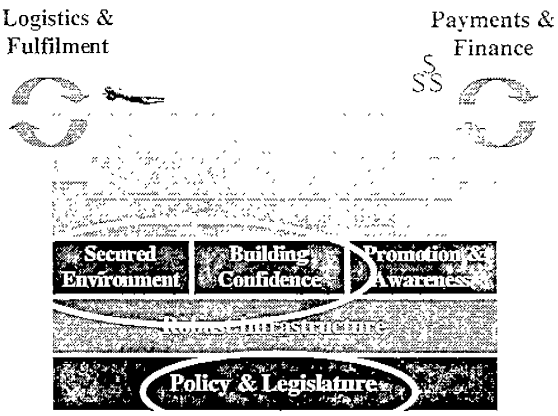
- Knowing reliability of parties involved
- Robust Transmission Infrastructure
- Secured Transmission
- Transaction Recognized and Protected

>> Trust is Critical for E-Commerce

Catalyst for Change

iDA

Singapore - Building of a Trusted Hub



Catalyst for Change

iDA

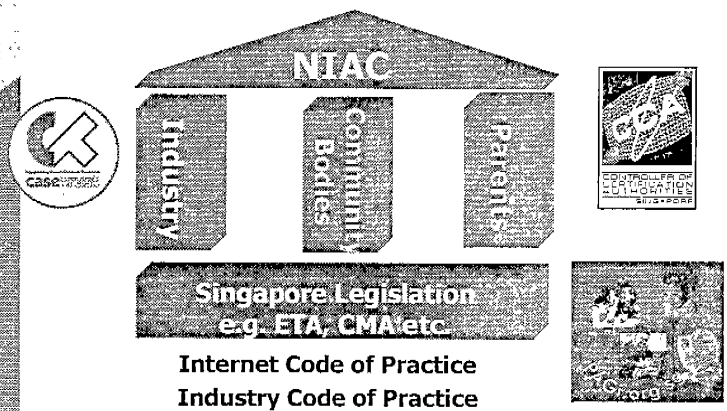
The Need to Build Trust and Confidence

- Industry consultation launched.
- Trust & confidence crucial to EC growth & adoption.
- PKI identified as potential apps to build secured environment.

Catalyst for Change

iDA

Singapore's Approach:A Combination of Self-Regulation, Education & Legislation



Catalyst for Change

7

iDA

Legal Framework: Where We Are Now

- **Legislation**
  - Electronic Transactions Act & Regulations
  - Computer Misuse Act
  - Copyright Act
  - Evidence Act
- **Self-Regulation**
  - National Trust Council (TrustSg Programme)
  - Singapore IT Dispute Resolution Advisory Committee
  - Internet Code of Practice
  - E-commerce Code for Protection of Personal Information
  - Guidelines for IASPs on Scanning
  - Professional Code of Conduct

Catalyst for Change

8

iDA

Adopting a Public Key Infrastructure
for a secured environment

Catalyst for Change

PKI Forum Launched,

PKI forum formed

Nineteen infocomm industry players have joined hands to boost online security with the formation of the PKI (public key infrastructure) Forum Singapore.

Initiated by the infocomm Development Authority (IDA) of Singapore, PKI Forum Singapore will the key platform

Low awareness
Need for inter-operability
Lack of key applications

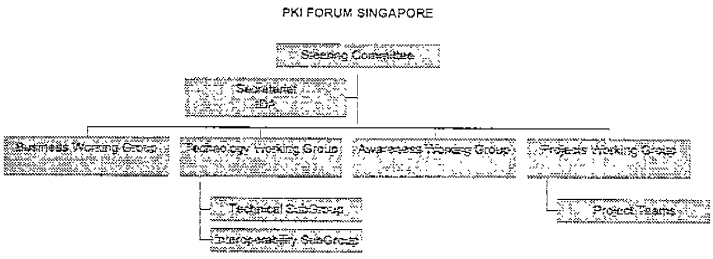
PKI Forum Singapore formed
Conferences/seminars to raise awareness
Identify & pilot key projects

9

iDA

The Singapore PKI Forum

- Charter & Objectives
- Organisational Structure



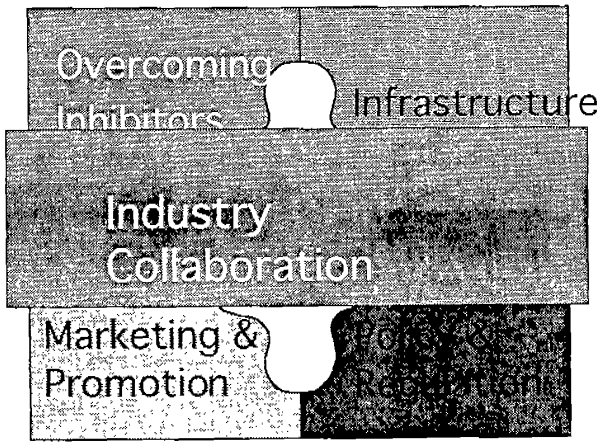
>> PKIFS is an industry led organisation

Catalyst for Change

10

iDA

PKI - Our Strategies ...



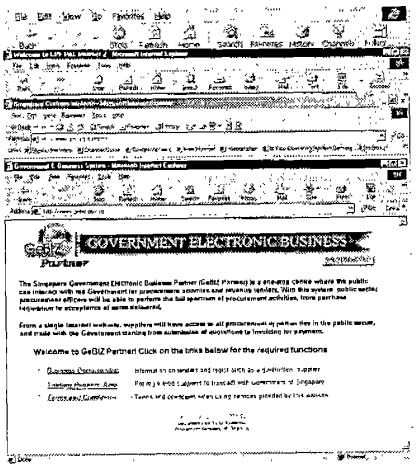
Catalyst for Change

11

iDA

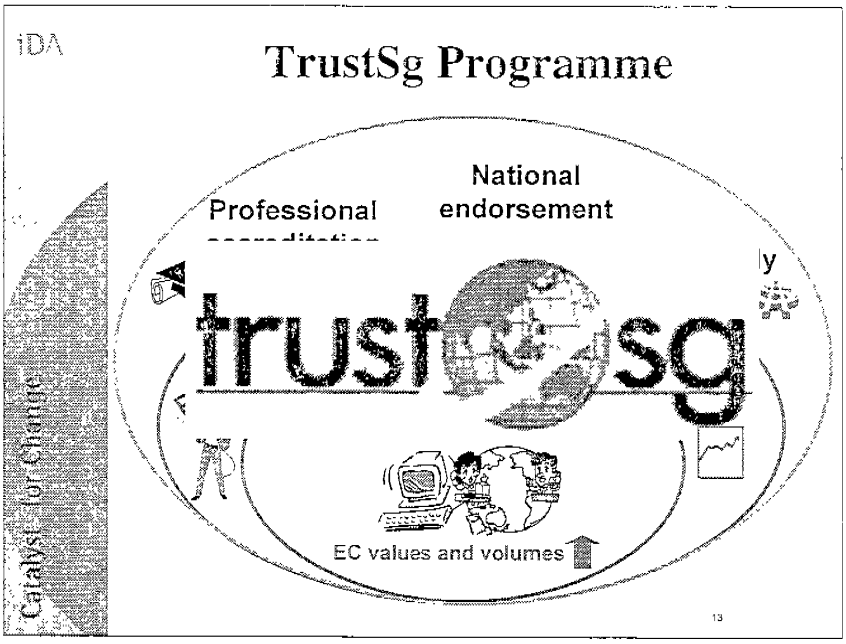
Our PKI Implementation

- 65,000 Public Service Card Users
- Central Provident Fund Board
- Customs & Excise Department
- Government ProcurementPortal



Catalyst for Change

12


iDA
TrustSg Programme
Professional
National endorsement
trustsg
EC values and volumes
Catalyst for Change
13


iDA
Singapore, a Trusted e-Business Hub
Thank You
www.ida.gov.sg
Catalyst for Change
14

The First
Asia PKI
FORUM

DOCUMENT NO.05

TITLE : ISSUES ON THE DEPLOYMENT OF PKI IN ASIA:THE e-ASEAN INITIATIVE

SUBMITTED BY : Emmanuel C.Lallana.Ph.D
Executive Director,e-ASEAN Task Force

ISSUES ON THE DEPLOYMENT OF PKI IN ASIA:

THE e-ASEAN INITIATIVE

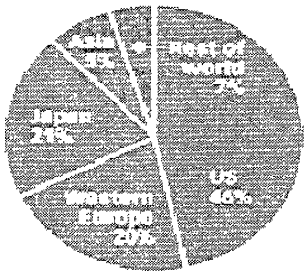
Emmanuel C. Lallana, Ph.D.
Executive Director, eASEAN Task Force

Global eCommerce, 2000 & 2004

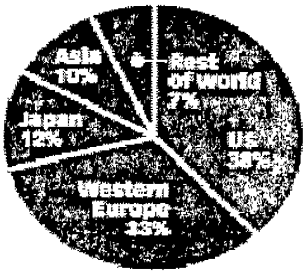
US$350.38 b	US$3.14 t
2000	2004

Source: IDC, 2001

Worldwide eCommerce Revenue, 2000 & 2004
(as a % share of each country/region)



2000



2004

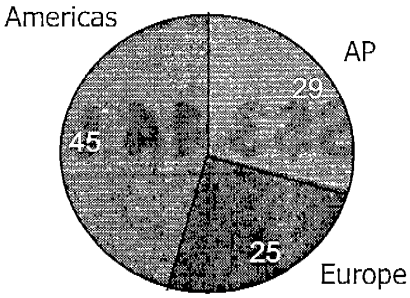
Source: International Data Corp., 2001

 www.eMarketer.com

WORLDWIDE COMMERCIAL PAYMENTS

Domestic

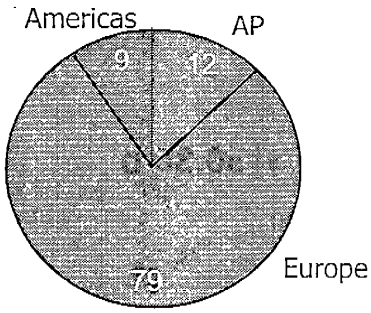
100% = US$ 24,130 billions



AP	6,998
Europe	6,260
Americas	10,871

Cross-border-intra-region

100% = US$ 5,380 billions



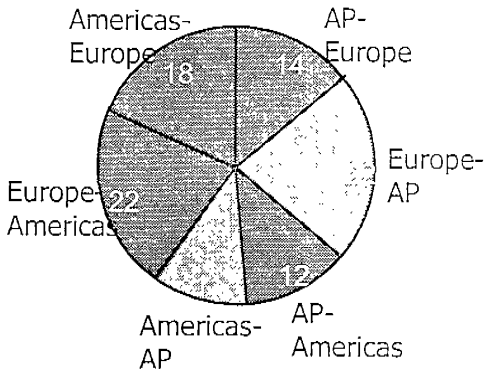
Intra-AP	665
Intra-Europe	4,232
Intra-Americas	484

Source: BCG 1997, WTO, EIU, interviews, team analysis

WORLDWIDE COMMERCIAL PAYMENTS (2)

Cross-border-inter-region (100% = US$ 5,441billions)

AP-Europe	771
Europe-AP	1,213
AP-Americas	658
Americas ¥-AP	611
Europe-Americas	1,210
Americas-Europe	979



Source BCG 1997 WTO EIU interviews team analysis

eASEAN Task Force

To develop a broad and comprehensive action plan with the objective of evolving an ASEAN e-space, and to develop competencies within ASEAN to compete in the global market

ASEAN Framework Agreement on ICT Products, Services and Investment

Elements of e-Agreement

- ***Infrastructure or AII***
- ***e-Commerce***
- ***Common ICT Marketplace***
- ***Capacity building and e-Society***
- ***e-Government***

e-ASEAN CA Forum

- ***Promote interoperability of regional CAs***
- ***Accelerate the use of PKI-based applications***
- ***Promote the exchange of ideas and information***
- ***Educate the region on PKI***
- ***Assist in the narrowing of the digital divide***

e-ASEAN CA Forum Issues

- ***Legal Infrastructure***
- ***PKI-based applications***
- ***Awareness, Education & Training***

Legal Infrastructure

Singapore: eCommerce Electronic Transaction Act 1998

Malaysia: Communications & Multimedia Act 1998, Digital Signature Act 1997, Computer Crimes Act 1997, and Copyright Amendment 1997

Philippines:eCommerce Law 2000

Legal Infrastructure (2)

- ***NO ASEAN CA but member countries should work together as equal partners.***

  Public CAs
  - ***Singapore:*** ***Netrust Pte Ltd***
    ID.Safe Pte Ltd
  - ***Malaysia :*** ***Digicert***
    MSC Trustgate.com

Legal Infrastructure (3)

- ***Legal Interoperability***
- ***Digital Signatures***
- ***Legal Harmonization***
  - ***harmonization of 8 key provisions:***
  - ***minimum regulatory standards for CAs***
  - ***recognition of foreign digital signatures***

Legal Infrastructure (4)

- ***impact on liability of subscribers and CAs***
- ***legal presumptions***
- ***dispute resolution & enforcement***
- ***choice of law***
- ***fulfilling government obligations***
- ***scope of law***

PKI-based Application

- ***ASEAN should promote PKI through:***
  - ***PKI-enables projects***
  - ***secured email program by ASEAN Secretariat***
  - ***PKI-enabled repository for e-ASEAN work groups***
  - ***PKI readiness study***

Awareness, Education & Training

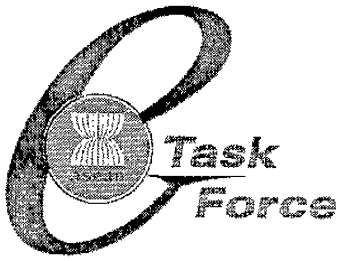
- ***PKI information/resource at the e-ASEAN website***
- ***Roadshows***

Challenges

- ***Formulate harmonised laws and policies (UNCITRAL model law base)***
  - ***Formulate common regulatory requirements for foreign CAs vis-à-vis domestic CAs***

Challenges (2)

- ***Create an interoperability PKI***
- ***Promote use of PKI to achieve trusted e-Commerce***
- ***Reflect PKI importance to e-Agreement***



e-ASEAN Task Force

http://www.e-aseantf.org

The First
Asia PKI
Forum

DOCUMENT NO.06

TITLE : Public Key Infrastructures in Japan

SUBMITTED BY : Mr.Hajime Furuta
Deputy Director-General,
Commerce and Information Policy Bureau,
Ministry of Economy, Trade and Industry

Public Key Infrastructures in Japan

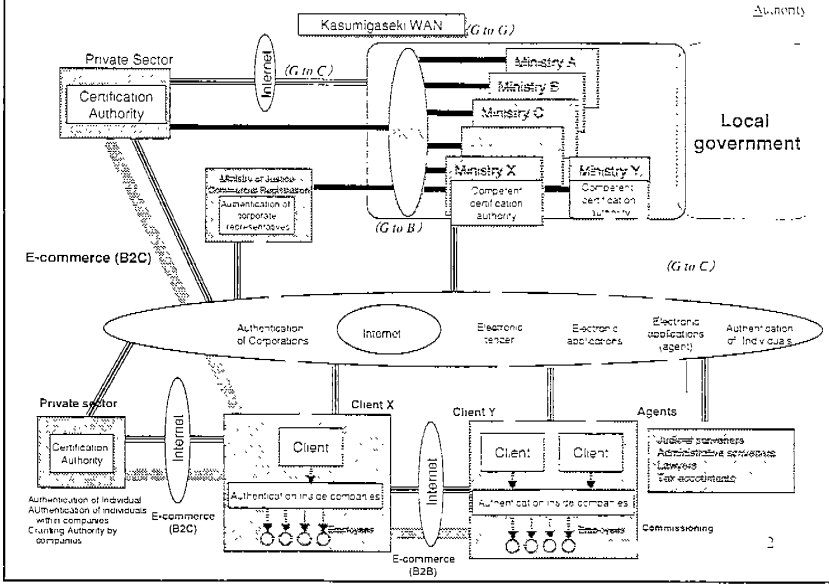
June 12, 2001

Commerce and Information Policy Bureau,
Ministry of Economy, Trade and Industry

1

Structure of Japan's PKI (Image)

※BCA Bridge Certification Authority



2

Table of Contents

1. Policy related to PKI and the e-Government Concept in Japan

The e-Government Concept and PKI

Reducing the burden in administrative procedures and improving administrative services

Computerizing procedures

Authentication of individuals is one of the main issues in procedures

Achieving e-government

<Establishing Authentication System using PKI (Public Key Infrastructure)>

- Applications and notifications to government — GPKI (Government PKI)
- Applications and notifications to local government — LGPKI (Local Government PKI)
- Computerizing Certification
  - Certified copies of commercial registration, certified copy of real estate registry (Regional Legal Affairs Bureau)
  - — Electronic Certification System based on the Commercial Registration provided through Internet
  - Resident records (municipalities) — Infrastructure for Authentication of Individuals

e-Government Concept in Japan's IT Policy

Dec. 1997 Revision of "The Master Plan for Promoting Government-wide use of IT"

Five-Year Plan from FY1998 to FY2002
→Aiming towards the realization of e-government by the beginning of the 21st century

Dec.1999 Millenium Project (Decided on by Prime Minister)

July 2000 Establish IT Strategy Headquarters

To promote comprehensively as a nation measures which strive towards the formation of an globally competitive IT nation, in which the benefits of the IT revolution can be enjoyed by all

Nov. 2000 *Enactment of the Basic Law on the Formation of an Advanced Information and Telecommunications Network Society (IT Basic Law)* → Came into force January 6, 2001

January 6, 2001
Establish Advanced Information and Telecommunications Society Promotion Headquarters = IT Strategy Headquarters

January 22, 2001 Finalization of the e-Japan Strategy
A project to create the world's leading IT nation by 2005

March 29, 2001 Finalization of the e-Japan Priority Policy Program
・Promote computerization of administration and utilization of information and telecommunications technology in the public sector

① Promote as a priority issue reform of operations to achieve the digital provision of administrative information, the computerization of application and notification procedures, the move to paperless operations, and information sharing and utilization through information network.
Strive to achieve an e-government in which digital information is handled in the same way as paper information by FY2003

Milestone Plan

December 1999 (Decided on by Prime Minister)

Three pillars

Response to computerization | Response to aging of society | Response to environment issues

Six projects

1. [illegible]uthentication infrastructure
2. Development of common infrastructure technology
3. Computerization of application and notification procedures
4. Pilot Projects in application and notification procedures
5. Computerization of government procurement procedures
6. Pilot Projects to lead the computerization of local government

(1) Develop Government Public Key Infrastructure (GPKI)
(2) Develop bridge certification authority
(3) Develop electronic certification system based on the commercial registration
(4) Provision of legislative systems for electronic signatures and digital certificates

Issues to be addressed in realizing e-Government

The Computerization [illegible] Policy Program

Specific measures concerning the computerization of administration

Inside administrative organizations

Move to paperless operations

Improve information literacy

Contact points with public and corporations

Public, corporations

- Reduce burden in administrative procedures
- Improve quality of administrative services
- Improve efficiency of administrative services

Digital provision of government information

Computerization of application and notification procedures

Promotion of outsourcing

Computerization of government procurement

Computerization of government revenue and expenditure

Basic specifications for IC cards

Kasumigaseki WAN

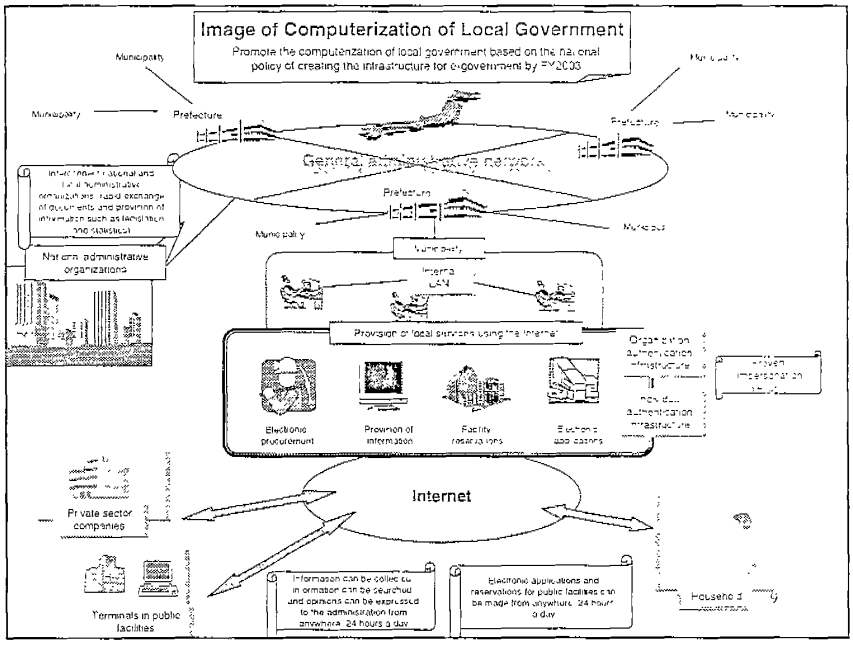
Ministry of Economy, Trade and Industry

LGWAN

Support for the initiatives of local government

Revision of existing legislation/formation of new action plan

Assessment of system development, etc.



2. Laws Concerning Electronic Signatures and Certification Service in Japan

Contents of the Electronic Signatures Law

A Presumption

Presumption given when electronic documents are accompanied by electronic signatures

To make sure the legal position of electronic signatures

B Voluntary accreditation

To ensure the reliability of CA

i. Voluntary accreditation of certification service (Article 4 to Article 16)
- Requirements for accreditation (Article 6)
- Accreditation of certification service provided in foreign countries (Article 15 (Direct accreditation), Article 16 (Sort of mutual recognition))

ii Designated investigating organization (Article 17-32)

iii. Penalties (Article 41-47)

C Other items

i. Support, etc. for certification service (Article 33)

ii. Public education activities and public information activities (Article 34)

Promote of EC through securing the smooth utilization of electronic signatures

Improving citizen's quality of life and the sound development of the national economy

A Presumption of the authenticity of an electronic document

Handwritten signatures / seals

○ **The law of Civil Procedure Article 228 Paragraph 4**

"A private document is presumed to be authentic if it bears the signature or seal of the party concerned."

Document

Signature or seal

If it bears the signature or seal of the party concerned ...

Presumption of the authenticity of the document (=presume that document is signed or sealed with the intent of that person)

Introduce a similar setup for electronic signatures

Electronic signatures

○ **The Electronic Signatures Law, Article 3**

"An electronic document ..... shall be presumed to be authentic if an electronic signature ..... is performed by a specific person in relation to ..... said electronic document."

* **Electronic signature:** A cryptographic or similar measure which has the objective of indicating the creator of information recorded in an electronic record, and which is capable of providing verification of change if the record is changed.

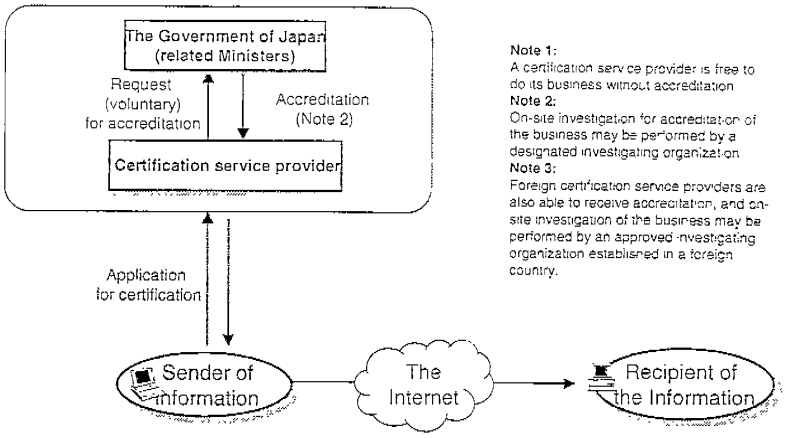
Information

Electronic signature

If the electronic signature of a person has been performed by that person ...

Presumption of the authenticity of the electronic document (presume that document is signed with the intent of that person)

B-1 Provisions for voluntary accreditation of certification services

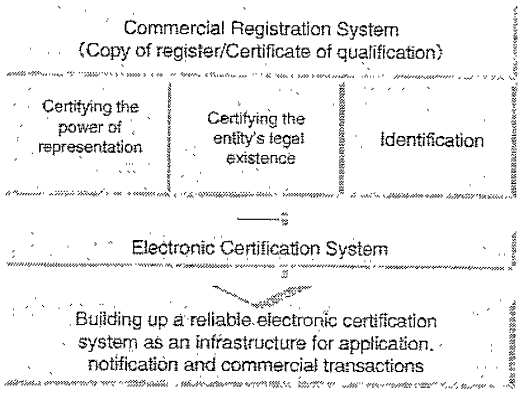


Note 1:
A certification service provider is free to do its business without accreditation
Note 2:
On-site investigation for accreditation of the business may be performed by a designated investigating organization
Note 3:
Foreign certification service providers are also able to receive accreditation, and on-site investigation of the business may be performed by an approved investigating organization established in a foreign country.

Electronic commerce, etc.

3. Certification System for Commercial Registration

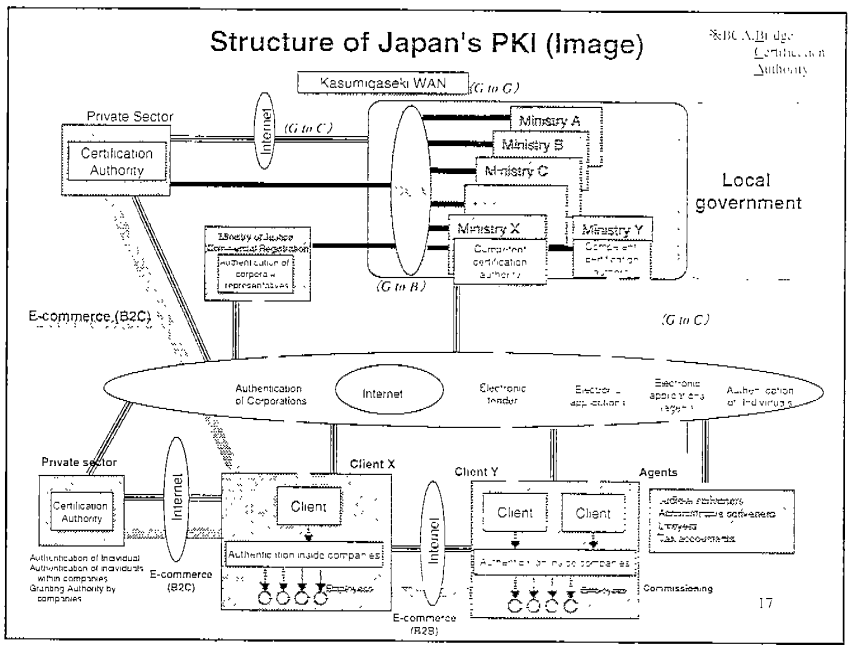
A. Amendment of Commercial Registration Act (Electronic Certification System based on the Commercial Registration)



A. Amendment of Commercial Registration Act (cont'd) The significance of using commercial registration system

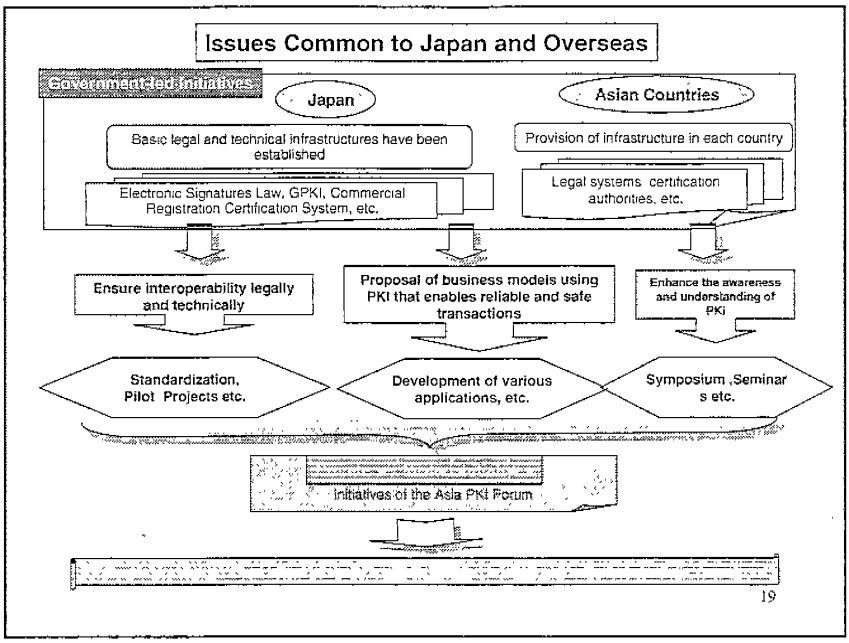
(1) it is possible to organize a reliable electronic certification system using the information registered in the commercial registers, which cover about 3.5 million companies, as a social resource

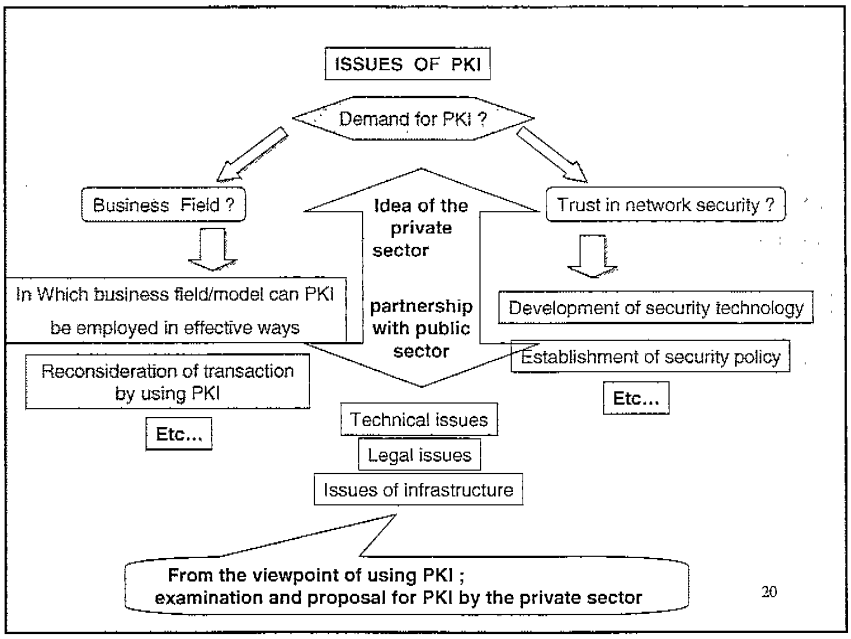
(2) changes in information registered in the commercial registers can be reflected in the information necessary for electronic certification



4. Toward the Development of PKI in Japan and Asia

18


Issues Common to Japan and Overseas
Government-led initiatives
Japan
Asian Countries
Basic legal and technical infrastructures have been established
Provision of infrastructure in each country
Electronic Signatures Law, GPKI, Commercial Registration Certification System, etc.
Legal systems certification authorities, etc.
Ensure interoperability legally and technically
Proposal of business models using PKI that enables reliable and safe transactions
Enhance the awareness and understanding of PKI
Standardization, Pilot Projects etc.
Development of various applications, etc.
Symposium ,Seminar s etc.
Initiatives of the Asia PKI Forum
19


ISSUES OF PKI
Demand for PKI ?
Business Field ?
Idea of the private sector
Trust in network security ?
In Which business field/model can PKI be employed in effective ways
partnership with public sector
Development of security technology
Reconsideration of transaction by using PKI
Establishment of security policy
Etc...
Etc...
Technical issues
Legal issues
Issues of infrastructure
From the viewpoint of using PKI ;
examination and proposal for PKI by the private sector
20

The First
Asia PKI
Forum

DOCUMENT NO.07

TITLE : Keynote Issues for the Global Deployment of EC

SUBMITTED BY : Mr.Michio Naruto
GIIC Asia Co-Chair and GBDe Overall/Asia-Oceania Co-Chairs

The First Asia PKI Forum Keynote Speech

Keynote Issues for the Global Deployment of EC

MICHIO NARUTO
GIIC Asia Co-Chair
GBDe Overall Co-Chairs & Asia / Oceania Co-Chairs
June 13, 2001

1

Today's Topics

1. The IT Revolution and Its Social Impact
2. Internet Legal and Policy Issues
3. Expectations for the Asia PKI Forum

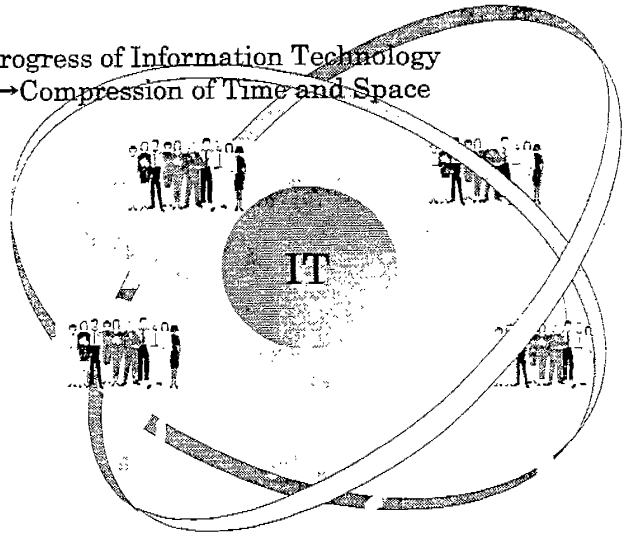
2

1. The IT Revolution and Its Social Impact

3

What is the IT Revolution?

- Progress of Information Technology
  →Compression of Time and Space



4

The First
Asia PKI

DOCUMENT NO.08

TITLE : Progress Reports on the Establishment of Asia PKI Forum

SUBMITTED BY : Akira Tachigami
General Manager,APKI-J

Progress Reports on the

Establishment of Asia PKI Forum

June 13, 2001

Akira Tachigami

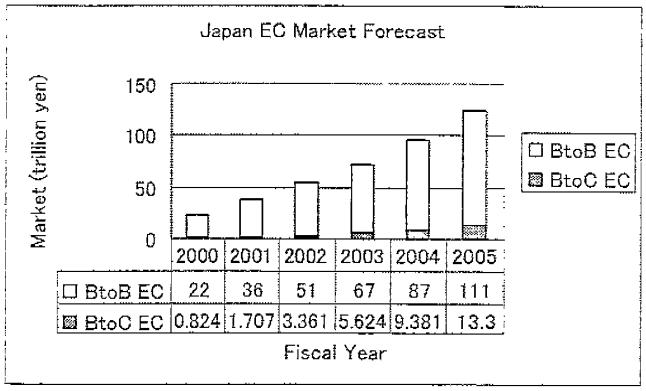
Japan Promotional Association for
Asia PKI Forum

Agenda

- Policies and planned activities of Japan promotional Association for Asia PKI Forum (APKI-J)
- Cooperation towards establishing Asia PKI Forum

I. Policies and planned activities of APKI-J

Growth of EC Market



	2000	2001	2002	2003	2004	2005
BtoB EC	22	36	51	67	87	111
BtoC EC	0.824	1.707	3.361	5.624	9.381	13.3

Rise of the Internet

- Characteristics of the Internet
  - anonymity
  - unspecified number of participants
  - little traceability

    ⇒ Necessity of PKI itself

  - globalization

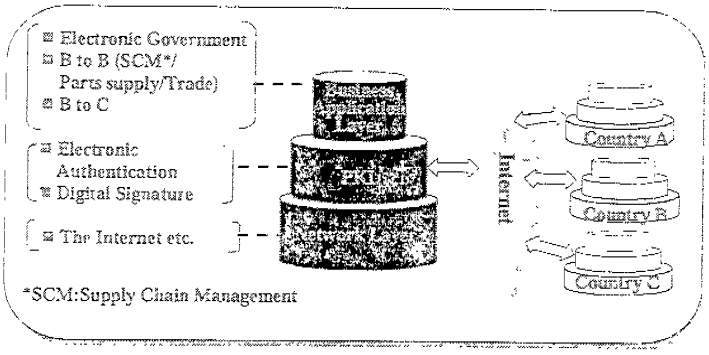
    ⇒ Interoperability among Countries regions

Maturity of the Internet Business Application

- Early stage: E-mail, web browsing
  (simple C to C or B to C use)

- Mature stage: Internet Banking, Electronic Settlement, Trade EDI, e-Government, SCM, e-Marketplace, etc.
  (B to B, B to G...)

Overview of PKI



PKI - The infrastructure indispensable to development of electronic government and electronic commerce (Public Key Infrastructure)

Outline of Japan PKI Activities

Japan PKI Activities

Private	Public		
ECOM etc.			
Standardization of electronic certificates used in private area	Electronic signature law	Commercial registration	GPKI
Japan Electronic Certification Systems Promotion Initiative (METI / MOJ)	METI/MOJ/ MPHPT	MOJ	MPHPT/ METI

METI Ministry of Economy, Trade and Industry MOJ Ministry of Justice
MPHPT Ministry of Public Management, Home Affairs
Posts and Telecommunications
ECOM Electric Commerce Promotion Council of Japan
GPKI Government PKI

Law Concerning Electronic Signature and Certification Services

Went through ordinary diet session in May 24, 2000, and in force in April 1, 2001.

Force of Electronic Signature

- Electronic Signature has the same force as ordinary handwritten signature, or sealed private paper.

Details

- Definition and range of effectiveness
- Accreditation system on designated certification services
- Penalty provisions, etc.

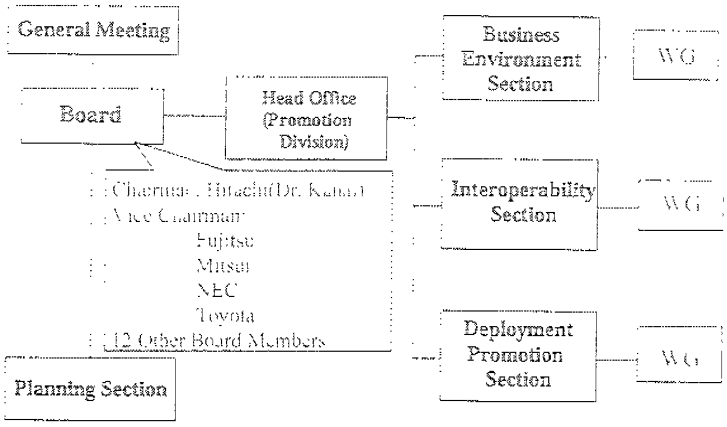
Point: IT systems, from now on, may be urged to be implemented to fill this Electronic Signature Law.

Launch of APKI-J

Japan Promotional Association was formally established on 15 Dec/'00 with 71 Members.

- Information System Vendors
- Certification Service Providers
- Trading Companies
- Financial Institutions & Others

Organization of APKI-J



Activities of APKI-J

(1) Approach to Asian/Oceanian countries/regions for participation in the Forum

(2) Host the First Asia PKI Forum

(3) Promote and implement Trials/Pilotting in Asia/Oceania

(4) Efforts toward the globally interoperable PKI (by tying with not only Asian/Oceanian partners but others)

II. Cooperation towards establishing Asia PKI Forum

Asian IT Revolution and Need of PKI

Economic complementarities
Geostrategic reality

→ Growing trade, investment....

...the process of globalization offers ASEAN and Japan an opportunity to create "a common economic space" to profit from the advantages of the IT revolution.

---Towards Vision 2020 ASEAN - Japan Consultative Conference on the Hanoi Plan of Action: *The Final Report with Recommendations*. Nov. 2[illegible]

... They agreed to work towards an Asian IT Belt to link up cities of IT excellence in Asia. This will create an environment of opportunities that would engage our best talents to develop Asia.

---*Press Statement by Chairman, 4th ASEAN Informal Summit*, Singapore, 25 Nov 2000*

** ASEAN Countries, China, Korea, and Japan attended at this meeting.*

The Answer: **Asia PKI Forum**

Cooperation by Asian/Oceanian Countries / Regions for;

(1) Interoperability between Certification Authorities
Cross-Certification, Adjustment of Legal System, etc.

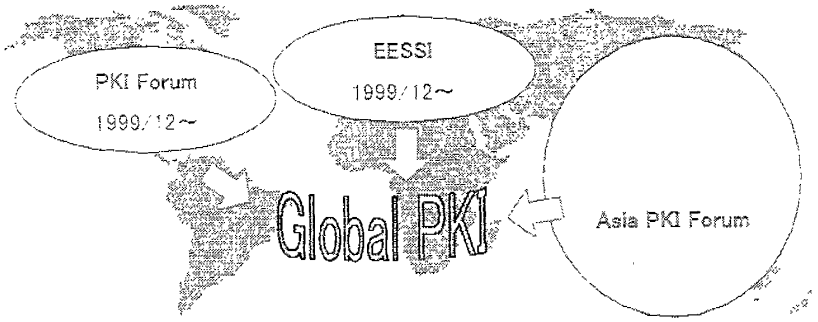
(2) Deployment Promotion of PKI

Objectives

Establishment of Common Infrastructure for Asian/Oceanian Countries Regions

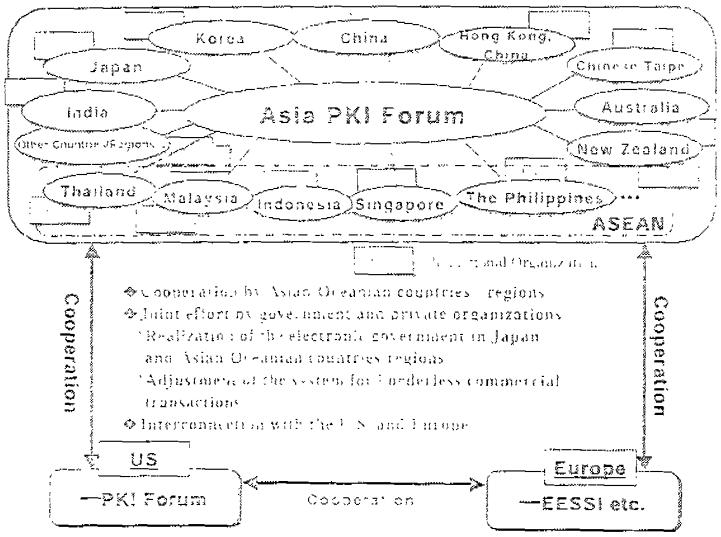
- Global Electronic Commerce
- Seamless Electronic Government
- Electronic Commerce Market common to Asia/Oceania

PKI Promotion Activities in the World



*EESSI : European Electronic Signature Standardization Initiative

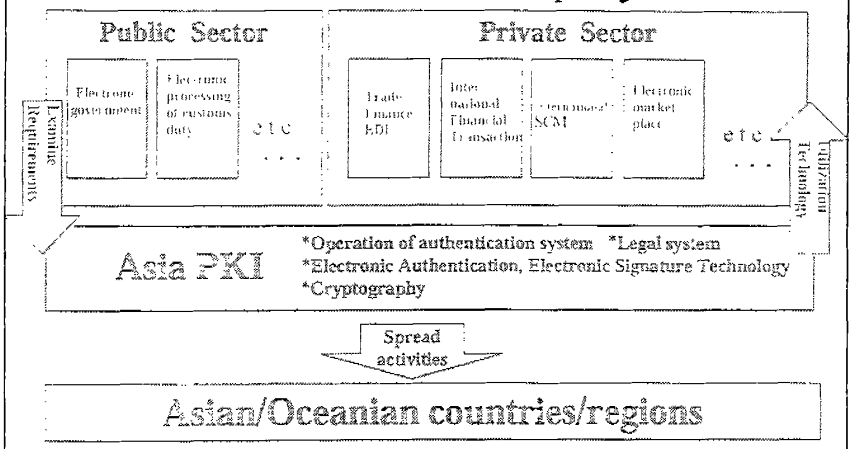
Concept of Asia PKI Forum



Items to be Considered

- **Interoperability**
  - Cooperation between certification authorities
  - Use of common electronic certificates
- **Business Environment**
  - Adjustment of legal systems and certificates management
- **Deployment Promotion**
  - Examination of the requirements for various application fields
  - Supply of utilization technologies

Promotion of PKI Deployment



- Examination of the requirements for PKI in each application field, and interoperability
- Supply of utilization technology to each application field
- PKI deployment promotion activities to Asian/Oceanian countries/regions

Waiting to Start!: Technical Working Group

- Identify similarities/differences of authentication structure (technologically, operationally, legally) of each country
- Investigate an interoperable model
- Process of arrangement among CAs in Asian/Oceanian countries/regions

Conclusions

- PKI is the one of the most essentials to realize the seamless, borderless, and affluent society.
- Great effort have to be made to secure interoperability among national/regional PKIs
- Let's collaborate to realize them by creating **ASIA PKI FORUM**.

The First
Asia PKI
Forum

DOCUMENT NO.09

TITLE : IETF Security Standards & Public Key Infrastructure

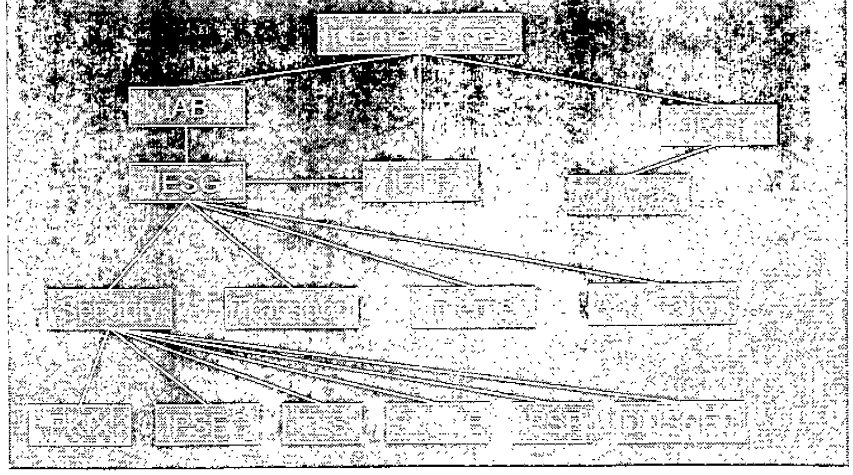
SUBMITTED BY : Dr. Stephen Kent
Co-chair - PKIX Working Group (IETF)
Chief Scientist - Information Security

IETF Security Standards & Public Key Infrastructure

Dr. Stephen Kent
Co-chair - PKIX Working Group (IETF)
Chief Scientist - Information Security

BBN TECHNOLOGIES
A Verizon Company

The IETF Structure



IETF Security Area Working Groups

- Under the Security Area Directorate
- Major PKI-related working groups
  - X.509 Public Key Infrastructure (PKIX)
  - IP layer VPNs (IPsec)
  - Secure web access (TLS)
  - Secure E-mail (S/MIME)
- Plus AAA, AFT, CAT, DNSSEC, OTP, OPCP, SSH, STIME, LINK, IPSP, IPSRA

PKIX

- Charter
  - profile of X.509 standards & creation of new, Internet PKI standards based on X.509
- Major RFCs
  - certificate & CRL syntax and processing
  - certificate request, renewal, reissue and revocation protocols (CMP, CMC)
  - certificate status checking (OCSP)
  - directory conventions (LDAP)
  - Qualified certificates

PKIX Directions

- Revising certificate & CRL syntax and processing
- Time stamping protocol (new)
- Delegated path discovery & validation
  - Requirements being defined
  - Candidate approaches:
    - OCSP v2
    - SCVP

IPsec

- IP layer, crypto-secure VPNs via AH & ESP
- Key management protocol: IKE
- IKE can use certificates for authentication
  - certificates for signature algorithms (RSA, DSA)
  - identity is user name (RFC822 address), system name (FQDN), IP address, or DN
- IKE can transport certificates and CRLs, removing need for real-time directory access

IPsec Directions

- Revisions underway for core RFCs:
  - Security architecture, ESP & AH
  - Son-of-IKE
- Security policy language, negotiation (IPSP)
- Remote user access (IPRSA)
- Kerberos-based key management (KINK)
- No IETF standard detailing PKI use or PKI support in IPsec products!

TLS

- TLS v1 (RFC 2246) the IETF version of SSL
- Transports certificates for server and client authentication
- Like SSL, can transport certificates in protocol, but not attribute certificates or CRLs
- But, HTTPS, not TLS specifies how to use certificates, CRL checking, ...
- HTTPS is largely undocumented, a de facto standard, controlled by Netscape & Microsoft
- Is TLS (vs SSL) significant?

S/MIME

- Secure e-mail based on RFC 822 & MIME
- S/MIME v3: CMS, certificate handling conventions, enhanced services (RFC 263x)
- Good, thorough integration of PKI into a security protocol
- Support for certificate, attribute certificate and CRL transmission inline
- Standards for managing signatures for non-repudiation

A Role for the Asia PKI Forum?

- IETF standards generally do not define test suites for compliance
- Standards compliance is essential for interoperability, user acceptance
- The Asia PKI Forum could do a great service for users and industry by
  - defining test suites (they might become informational RFCs)
  - Certifying or establishing independent testing facilities

Summary

- Standards groups focusing on security issues abound, and more are coming!
- Many make use of PKI of some sort, almost all based on X.509
- But, most security protocol standards fail to complete the job, profile PKI use, ...
- Ambiguities lead to non-interoperability, frustrated customers!
- Test suites and independent test facilities could help

The First
Asia PKI

DOCUMENT NO.10

TITLE : PKI Forum Overview

SUBMITTED BY : Ms.Lisa Pretty
President,PKI Forum

PKI Forum Overview

Presentation for
Asia PKI Forum
June 12-14, 2001

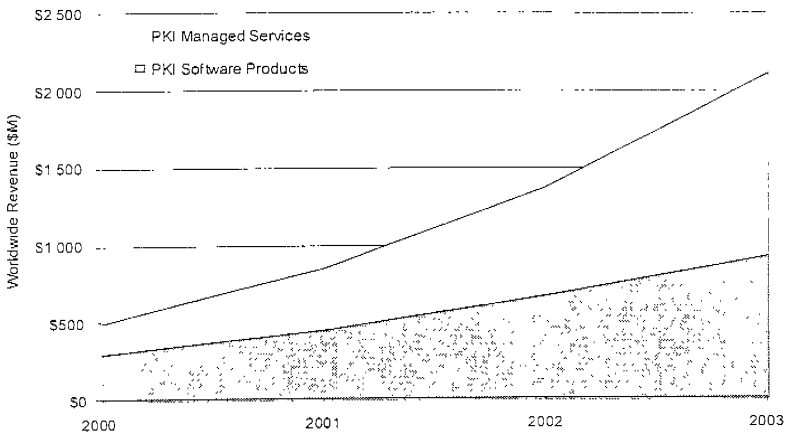
PKI forum

Our Mission

"The PKI Forum is an international, not-for-profit, multi-vendor and end-user alliance whose purpose is to accelerate the adoption and use of Public-Key Infrastructure (PKI). The PKI Forum advocates industry cooperation and market awareness to enable organizations to understand and exploit the value of PKI in their e-business applications."

PKI forum

PKI Market Forecast, 2000-2003

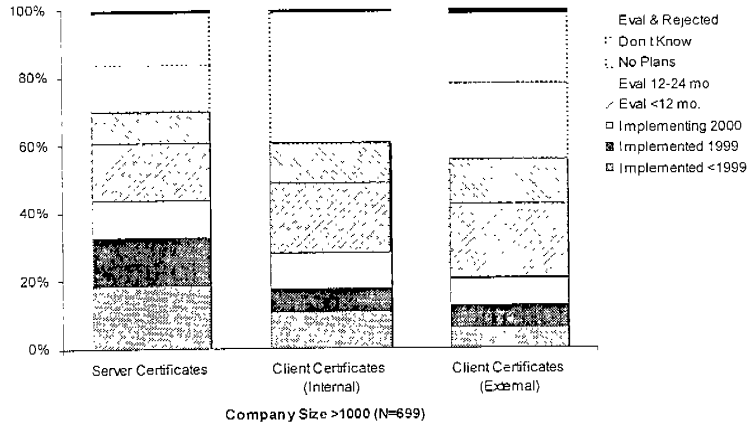


Source IDC December 2000

PKI forum

Digital Certificates

Market Penetration (North America)

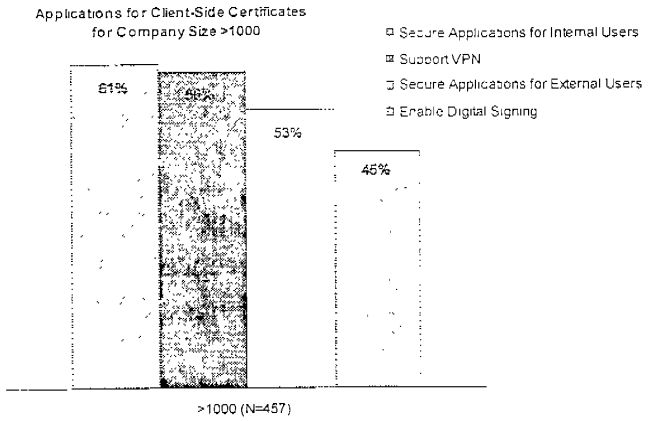


Source: International Data Corp., "Security Technology Survey", November 2000

PKI forum

Digital Certificates

Application Drivers (North America)



Source: IDC "Security Technology Survey", November 2000

PKI forum

Where we started

- Identified inhibitors to the rapid deployment of PKI-based products and services
  - Multi-vendor Interoperability
  - Market Awareness
- Founded in December 1999 by 5 organizations
- First members meeting in March 2000
- Organizations with executive board and working groups put in place

PKI forum

During the first year

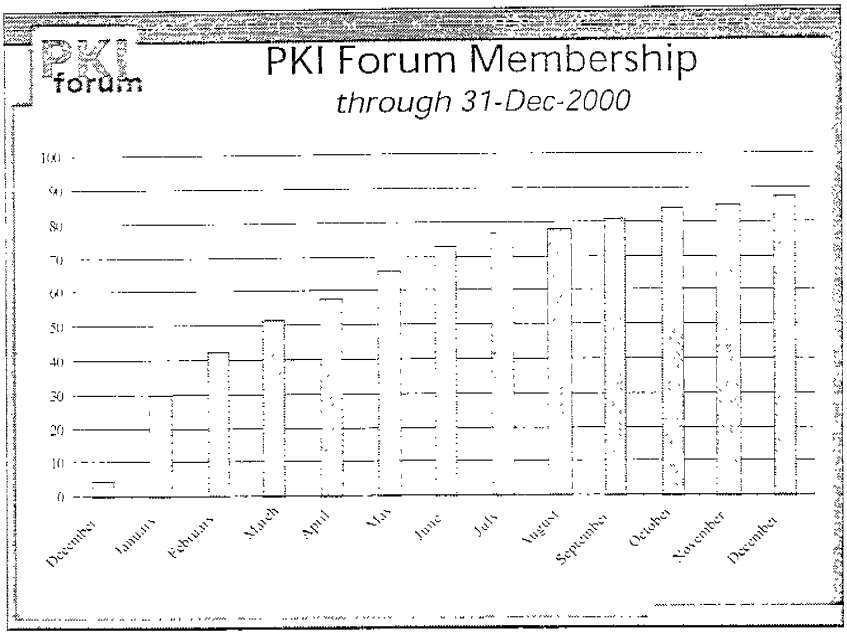
- Rapid Growth in Members
- Held quarterly meetings (4 regions)
- Fine Tuned working group structure with focused deliverables
- Initiated Liaison Relationships
- Launched PKI Resources Webpage
- Promoted PKI at industry conferences & seminars
- Incorporated and contracted services to Virtual Inc.

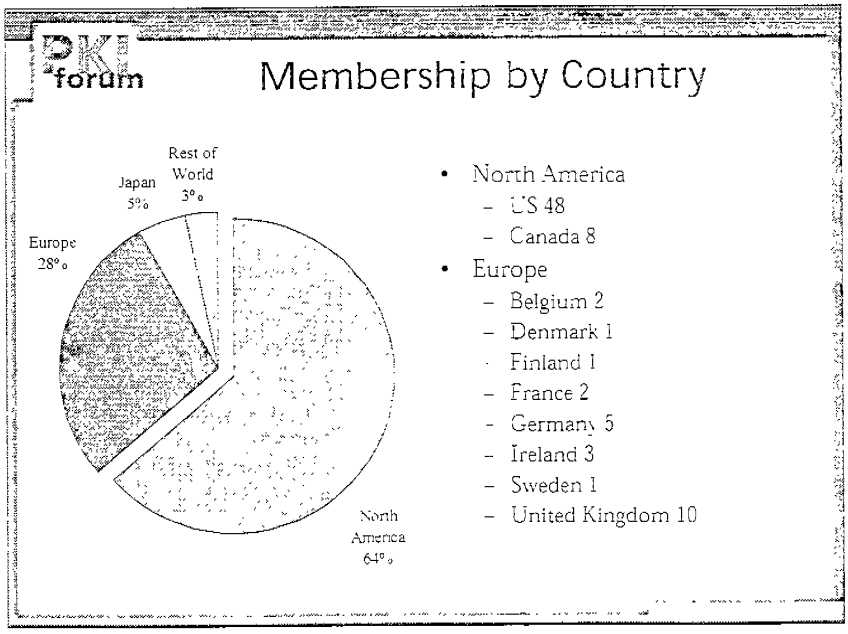
PKI forum

PKI Resources Webpage

- One stop for PKI information
- Place to publish PKI Forum deliverable
- Links to wide range of PKI sites
- Promotion of PKI Members

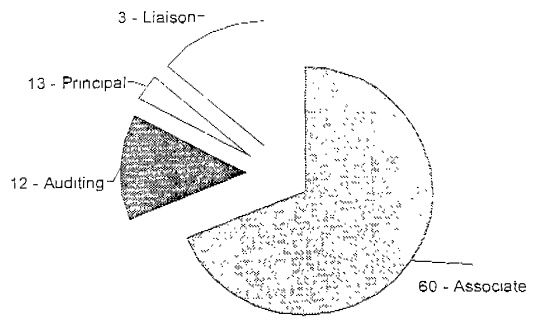
www.pkiforum.org/resources


PKI forum
PKI Forum Membership
through 31-Dec-2000
100
90
80
70
60
50
40
30
20
10
0
December
January
February
March
April
May
June
July
August
September
October
November
December


PKI forum
Membership by Country
Rest of World 3%
Japan 5%
Europe 28%
North America 64%
North America
US 48
Canada 8
Europe
Belgium 2
Denmark 1
Finland 1
France 2
Germany 5
Ireland 3
Sweden 1
United Kingdom 10

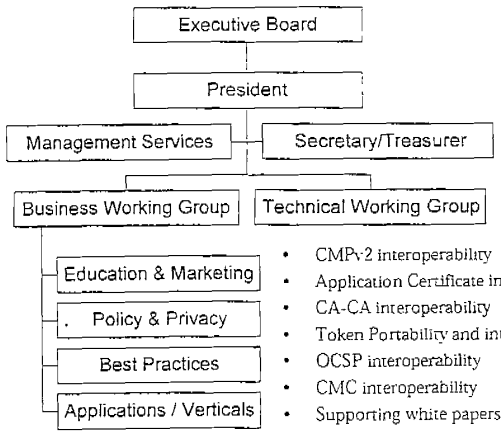
PKI forum

PKI - Membership Levels



PKI forum

PKI Forum Organization & Major Work Areas



- CMPv2 interoperability
- Application Certificate interoperability
- CA-CA interoperability
- Token Portability and interoperability
- OCSP interoperability
- CMC interoperability
- Supporting white papers, etc.

PKI Forum Leadership

- Executive Board
  - Derek Brink, RSA Security
  - Steve Lloyd Entrust
    Warwick Ford, VeriSign
  - Max Rodriguez, IBM
  - Jackson Shaw, Microsoft
  - Bill Garvin, Baltimore
  - John Sabo, Computer Associates
- PKI Forum Staff
  - Lisa Pretty, President
  - Virtual Inc. staff
- Technical Working Group
  - Andrew Nash, RSA Security
  - Mark Davis, Tivoli/IBM
- BWG Education & Marketing
  - Brita Schulz, RSA Security
- BWG Policy & Privacy
  - Jan Lovorn, Protegrity
- BWG Best Practices
  - Blair Canavan, Chrysalis-ITS
- BWG Applications
  - Sandra Salvatori, VISA International

PKI Forum Members Meetings

The PKI Forum has held quarterly meetings since its formal launch last March. Meetings consist of one day of plenary sessions followed by two days of working group sessions.

- March 2001 - San Jose, CA
- June 2001 - Munich, Germany
- September 2001 - Toronto, Canada
- December 2001 - Singapore

PKI forum

Privacy & Policy Business Working Group

Mission Statement:

"To provide information and guidance on the policy and privacy needs and issues related to the development, implementation, and usage of PKI."

Work Items:

- PKI Policy Principals
- PKI Policy Note
- Whitepapers, regulatory review

PKI forum

Marketing/Education Business Working Group

Mission Statement:

"To create informational pieces that help promote the understanding and value of PKI from both a business and technical perspective."

Workitems:

- Whitepapers, notes and presentations

PKI forum

Best Practices Business Working Group

Mission Statement:

"To reach a consensus on an agreed-upon set of internationally recognized standards, policies and audit procedures that ensure the overall integrity, effectiveness and interoperability of trusted PKI-enabled implementations."

Workitems:

- Collection of pieces for Best Practices Whitebook

PKI forum

Applications Business Working Group

Mission Statement:

"To provide a forum that encourages sharing business experience, and to produce deliverables that highlight the driving PKI applications within Financial Services, Healthcare, Government, and other influential vertical markets."

Workitems:

- Case Studies and Industry overview
- Healthcare Industry Overview (PKI Note Series)

Technology Working Group

- Mission Statement:

"To accelerate the adoption of PKI by championing product interoperability through testing, demonstrations, white papers and profile development."

Work Items

- Interoperability Framework
- CA-CA Interoperability
- CMP Interoperability
- Application Certificate Interoperability
- Token Portability & Interoperability
- Whitepapers: LDAP, OCSP, Path Construction, Interoperability, etc.
- Interoperability Profiles

Why is Interoperability Important?

- Flexibility and choice
- Mitigation of risk
- Ultimately, the fundamental goal is to provide seamless application-to-application interoperability

PKI forum

The Role of Standards

- By definition, standards are typically designed to be generic and flexible
- Thus, standards promote interoperability - they do not guarantee it
- Profiling standards and interoperability testing are essential in order to achieve multi-vendor interoperability

PKI forum

PKI Related Standards & Specifications

- Several organizations are working on standards and specifications in the PKI space
  - International Standards Organization (ISO)
  - Public Key Cryptography Standards (PKCS)
  - Internet Engineering Task Force (IETF) ...

Visit:

http://www.pkiforum.org/resources.html for links to several standards and specifications

PKI forum

Interoperability Initiatives

- PKI Forum *several projects underway*
- European Electronic Messaging Association (EEMA) *PKI Challenge 2 year project*
- Communications – Electronics Security Group (CESG) *recently completed interoperability bake-off*
- Other initiatives:
  - USA Fed Government
  - Asia PKI Forum
  - Vertical market specific initiatives

The PKI Forum works in a co-operative manner with other organizations with a goal of sharing results and minimising work effort – liaison efforts are underway with many organisations performing interoperability testing.

PKI forum

CMPv2 Interoperability Project

- Co-sponsored by ICSA and PKI Forum
- Significant number of vendors involved
- Includes the following CMP messages:
  - Initialization request/response
  - Certificate request/response
  - Key update request/response
  - Self-revocation request/response
  - Cross-certification request/response
- Lessons learned filtered into CMP Version 2
- Testing ongoing
- Press release (January 2001) available from PKI Forum Web site

PKI forum

Application Certificate Interoperability Project

- Purpose is to demonstrate interoperability of certificates issued by different vendors in several application contexts
  - SSL
  - S/MIME
  - Certificate path processing
- Results /lessons learned to be documented once completed

PKI forum

CA-CA Interoperability Project

- Purpose is to produce a white paper focused on inter-domain "trust relationship" issues
- Topics discussed include:
  - Technical options for establishing inter-domain trust relationships
  - Survey /synopsis of related initiatives
  - Role of CP, CPS and PDS
  - Recommendations
- Paper can be retrieved from PKI Forum Web site

PKI forum

Token Portability and Interoperability Project

- Purpose is to "explore the problems with token interoperability and how the lack of token interoperability inhibits the deployment of PKI"
- Specific areas to be addressed include:
  - Identification of business requirements
  - Applicable environments (Windows, Java, etc.)
  - Applicable technologies (CAPI, PKCS#11, PKCS#15, IETF Sacred, etc.)
  - Requirements for conformance testing
  - Identification of any liaison requirements
  - Assess the need for a "Token Best Practices Guide"

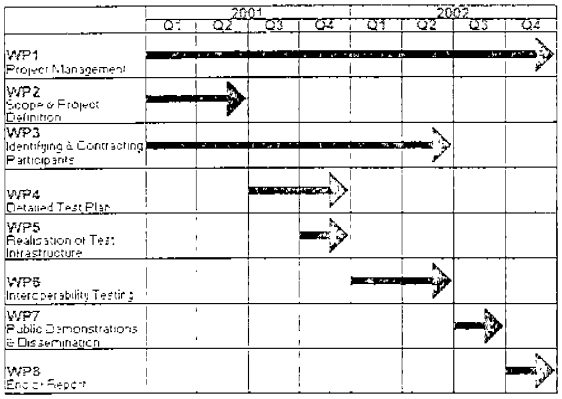
PKI forum

EEMA: PKI Challenge (pkiC)

- Two year project started January 2001
- Fully funded by European Commission
- 14 members in consortium
- Participation open to technology providers and end user community
- Currently working on a common agreed framework for testing

PKI forum

pkiC Time-line



•For more information visit www.eema.org/pki-challenge

PKI forum

CESG (UK Government)

- PKI & Secure Messaging interoperability project (Government Focus) to demonstrate interoperability between different commercial PKI CA/RA products for signed email application
- Phase I completed with 11 vendors testing during a week long bake off (February 2001)
- Considerable progress with respect to interoperability was noted and risks of implementing a PKI (for signed e-mail) were considerably reduced
- Phase I Report available at http://www.cesg.gov.uk/cloudcover/PKIdemonstrator.htm
- Phase II will focus on encrypted S/MIME messaging and 16 vendors have expressed interest in participating

PKI forum

Summary /Observations

- Multi-vendor interoperability considered by many to be an essential ingredient to the success of large-scale PKI deployments
- PKI Forum established to help expedite multi-vendor interoperability
  - Vendor-led, Customer-driven
  - International
  - Co-operation through liaison relationships
- Issues go beyond technology to achieve global interoperability – policy and procedures play a large role
- Progress is continuing to be made based on the work of many organisations working together

PKI forum

QUESTIONS?

PKI Forum's Unique Role

ADVOCATING
industry cooperation

ADVANCING
market awareness

ACCELERATING
PKI adoption

www.pkiforum.org
Info@pkiforum.org
+1.781.876.8810

The First
Asia PKI
Forum

Scenarios of PKI Deployment in Asia

The First
Asia PKI

DOCUMENT NO.11

TITLE : Digital Revolution and Secure Networks
Digital Development and PKI

SUBMITTED BY : Dr.Osamu Sudoh
Professor,Doctor of Economics,
The University of Tokyo

Scenarios of PKI Development in Asia

Digital Revolution and Secure Networks
Digital Development and PKI

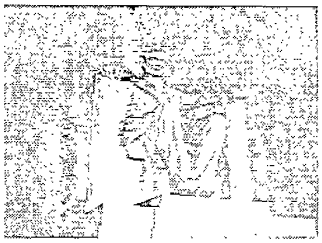
- Osamu Sudoh
- Professor, ph.D. on Economics
- The University of Tokyo

1

Digital Economy

- Constructive Destruction

The emerging digital economy can be seen as a "constructive destruction" of the existing economic order and its replacement with a new one hinged on the Internet.



2

What is the Identrus ?

Digital Certification Project which main financial institutions will be involved

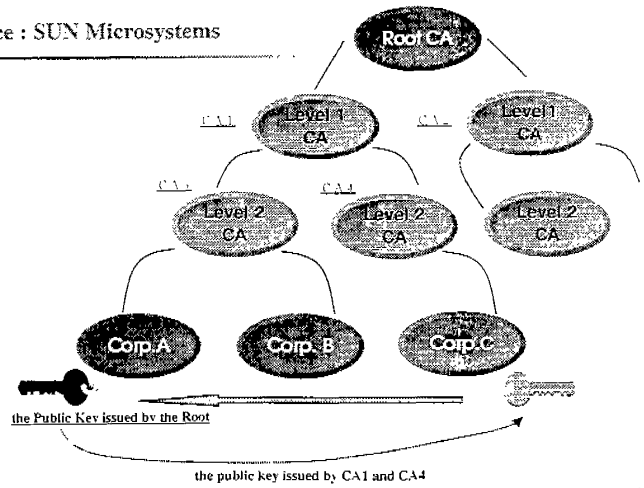
Expected Global Standard of Digital Certification Service

- Identrus LLC, at New York, US
  - decides the rule of CA which financial institutions recognize
  - decides the condition of standard CA system
  - controls the Root CA
- attending financial institutions
  - manages the CAs according to Identrus
  - issues the digital evidence document according to Identrus for client corporations

3

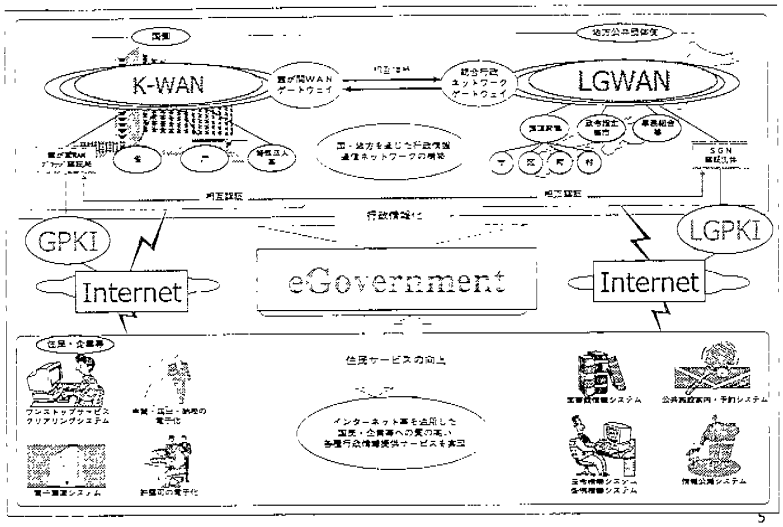
Certification Model of Identrus

Source : SUN Microsystems



4

E-Government



5

Infrastructure For Electronic Procurement and Bidding

- The Kasumigaseki WAN
- GPKI (Central Government)

- 3200 Local Governments' WAN
- LGPKI (Local Governments)

- RA(Registration Authority)
- CA(Certification Authority)

6

PKI in the Future

- Cross Certification
- Legal Problems
- Interoperability

7

The First
Asia PKI

DOCUMENT NO.12

TITLE : PKI in Korea

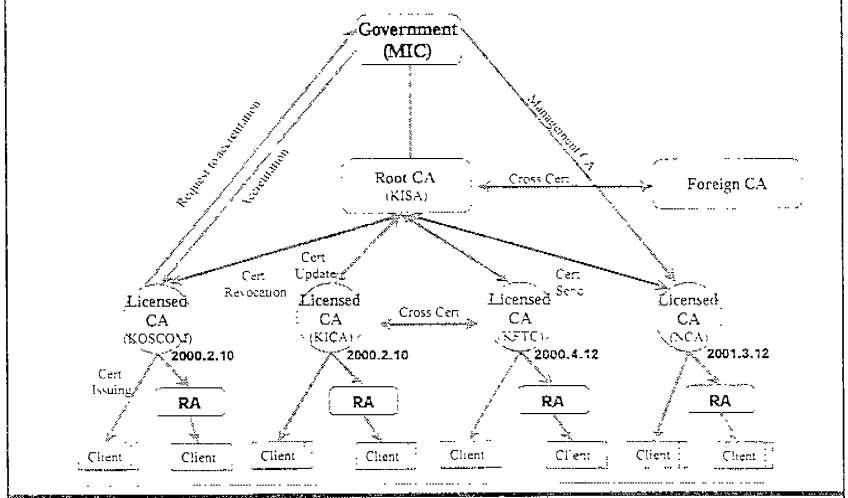
SUBMITTED BY : Dr.Ki Yoong Hong
Member of Task Force Team,
Korea PKI Forum, Korea

PKI in Korea

Ki-Yoong Hong, Ph.D., P.E.

kyhong@ksign.com

PKI Structure in Korea
(Licensed CA)



Environments for utilization & PKI themes

- Numbers of Internet users in Korea : about 20,930,000 [March, 2001]
- February. 1999, released date of Digital Signature Act, to retain secure e-Commerce.
- State of Certificate issuance (approx. 456,500) [May, 2001]
  server : 103, corp. : 83,170, private : 373,240
- GPKI : The MOGAHA prepares to do certificate service for Government
  - MOGAHA : Ministry Of Government Administration and Home Affairs
- Status of Wireless PKI
  - Mobile Telecom Company
    - SK-Telecom : 011, 017
    - KTF : 016, 018
    - LG-Telecom : 019
  - m-Commerce will be based on environment of Licensed CA
- By year 2002, 10M people will use Digital Signature in Korea

4

- Activities
  - Criteria and guidelines for Internet & Wireless PKI
  - Technology & Standardization
    - CA & RA server, Key Management System and etc
    - Digital Signature/Encryption Algorithm
    - Protocols
    - Interoperability and etc
  - e-Government (Government PKI)
  - Wireless PKI : Mobile, PDA, IMT2000 etc
- PKI Applications

E-mail Security	XML, DRM
Server Security	Web mail
Internet Banking	VPN, IDS
Cyber trading etc	Digital Invoice
	Digital Prescription
	Validation Services
	e-dealing with the civil petition etc

4

Measures to activate PKI utilization

- **Recommendation to use certificate**
  - ❑ Development of many application area
    - Cyber trading
    - Validation of the e-transaction
    - Exercise of the e-vote
    - The issue of e-coupon and e-money
    - e-dealing with the civil petition
    - Administrative e-Documents
    - Electronic Government Seal
    - e-Prescription
    - Digital Tax Service
- **Promotional and educational activities**
  - ❑ PKI Promotion Leaflet & Campaign
  - ❑ WPKI Certificate Testing Service
  - ❑ Seminar and conference on the PKI
    - Security World Expo 2001
    - PKI Conference
- **Revision of the related laws**
  - ❑ The benefit of the tax credit
  - ❑ Revision of the Digital Signature Act

Thank You !!

The First
Asia PKI

DOCUMENT NO.13

TITLE : Scenarios of Public Key Infrastructure(PKI) in Malaysia

SUBMITTED BY : Dr. Mohamed Arif Nun
Chairman,MSC Trustgate.com

Scenarios of Public Key Infrastructure (PKI) in Malaysia

By

Dr. Mohamed Arif Nur
Chairman,
MSC Trustgate.com

msctrustgate.com

AGENDA

MSC Trustgate.Com

1. Progress of Digital Transactions in Malaysia.
2. Utilization (status) of P.K.I. in Malaysia.
3. P.K.I. issues in Malaysia.
4. Future P.K.I. Plans in Malaysia.
5. Summary.

Progress

- **Security has always been a major concern in Internet transactions.**
- **Digital Signature Law was established in 1997.**
  - recognizing Digital signature to be as good as physical signature.
- **Digital Signature Regulation was established in 1998.**
  - Guiding the establishment and operating of Certification Authority (C.A.)

Current Status

- **Currently, all Flagships in MSC, like e-Procurement and e-Government are designed to make use of PKI.**
- **e-Banking is also embracing PKI.**
- **G.M.P.C. is designed to incorporate Digital Certificates.**
- **There 2 fully licensed National C.A. to issue digital certificates.**

CURRENT ISSUES ON P.K.I

- Awareness is a big issue (many are still not willing to budget for Internet Security).
- **Beyond the border inter-operability is another big issue.**
- **Harmonization between the various "trade laws" in recognizing Digital Signature is still an issue.**

Current issues on P.K.I

- The laws, which was established in 1997 and 1998 was pioneering. **Is it due for review?**

FUTURE PLANS

MSC Trustgate.Com

- Harmonizing all National Trade Laws to recognize Digital Certificates.
- Updating the current Digital Laws to the current progress of digital world.
- Increasing awareness to the needs of Internet Security for e-transactions.
- Encouraging countries (especially ASEAN) to achieve "inter-operatibility" in Digital Certificates.

Future Plans – Area of Interoperability

MSC Trustgate.Com

3 KEY AREAS OF INTEROPERABILITY BETWEEN NATIONS

1. **Legislations**
   - Digital Laws must be harmonized. It must be inter-operable. Very difficult - requires national cooperation.
2. **Practices (Procedures)**
   - Trust policies for mutual acceptance of Digital Certificates must be harmonized. Also requires national cooperation.
3. **Technology**
   - Market will dictate the interoperability of technology. Its changing. National intervention least required here.

Summary...

- Foundation for Digital Transactions is ready in Malaysia.
- Though awareness is still low, uptake has started.
- As a grouping, we must be ready to discuss the inter-operability issue NOW!!
- Malaysia is on the next wave of implementing Digital Transactions – harmonizing the "Trade Laws" and enhancing current Cyber Laws.
- We are happy to be of assistance, if required.

Thank You

arif@mdc.com.my

The First
Asia PKI

DOCUMENT NO.14

TITLE : Asia PKI Forum Panel Discussion

SUBMITTED BY : Dr.Kwok Yan Lam
Steering Committee member
Technology Workgroup Chairman,
PKI Forum Singapore

Asia PKI Forum Panel Discussion

Dr Lam Kwok Yan
PrivyLink International Limited

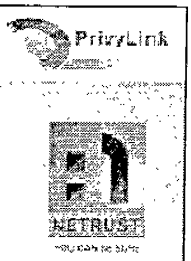
13 June 2001

Agenda

PrivyLink

- Current status of PKI in Singapore
  - Public CAs
  - PKI-based applications
- Issues encountered
  - adoption rate
  - technical issues
- Plan for expansion/deployment of e-transactions
  - Singapore PKI Forum
  - Cross-country interoperability
  - Direction for PKI applications
  - Example

Public CAs

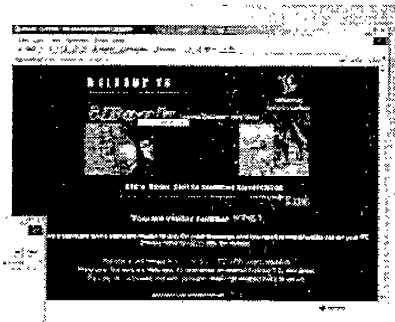


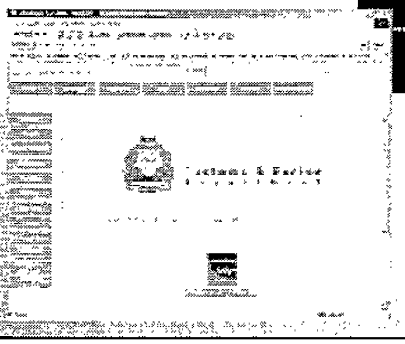
- Netrust Pte Ltd
  - 1st Public CA in South East Asia
  - Formed in July 1997
  - JV between Keppel T&T Ltd and NETS
  - http://www.netrust.net
- ID.Safe Pte Ltd
  - 1st Licensed CA in Singapore
  - Incorporated in June 1999
  - Operational since 1 Feb 2000
  - JV between CISCO Computer Services and Singapore Post
  - http://www.id-safe.com.sg

Government Applications

Singapore Sports Council

- Online booking of sports facilities (badminton, basketball, soccer, etc.)





Customs & Excise Dept

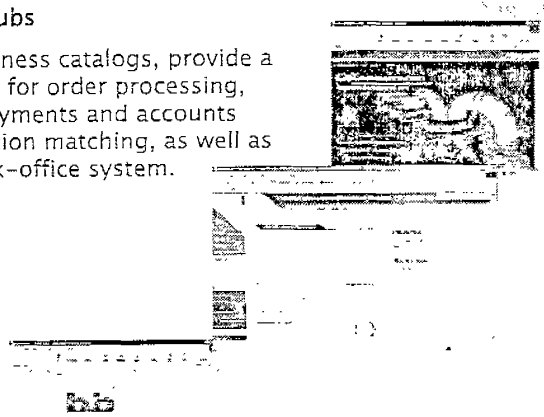
- Closed Web-based application for submission of customs declaration and payment.

Enterprise Application

PrivyLink

B2B E-Commerce Hubs

- Typically host business catalogs, provide a transaction engine for order processing, invoice inquiry, payments and accounts receivable transaction matching, as well as integration to back-office system.



Issues

PrivyLink

- PKI may not be suitable for all applications
  - match security protection vs risk exposure
  - match cost effectiveness vs cost of rollout e.g. smart card
- Market Awareness of Risk is low
- Little or no interoperability of enterprise applications
- Least of all, cross-border, cross-application interoperability
- Low Adoption Rate

Low Adoption of PKI

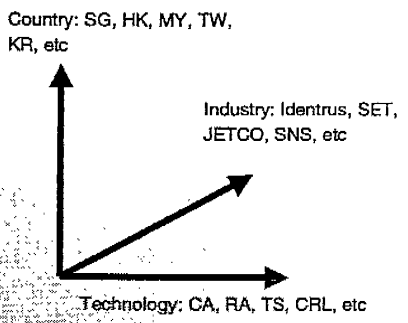
PrivyLink

BARRIERS

- Impact on performance of applications
- Lack of awareness
- Interoperability
- Ease of use
- Cross border issues
- Cost & complexity of deployment
- Lack of demand
- Lack of killer applications

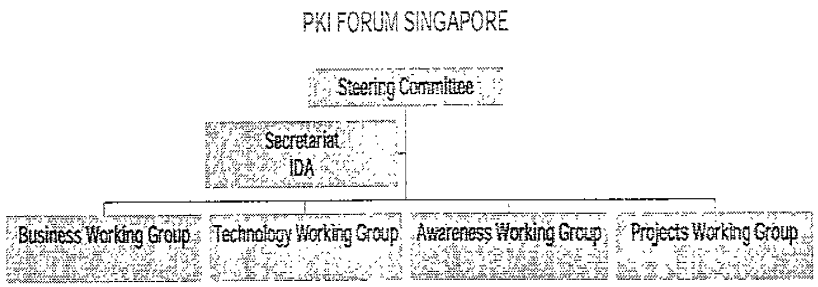
The Interoperability Challenge

PrivyLink



- Many initiatives driven by countries, application and technology providers
- Lack of consistent legal framework
- Non-benchmarkable quality of CA Operations

The Singapore PKI Forum



The Technology WG

- Recommend solutions to address issues relating to interoperability, legal, policy and technical barriers
- Address PKI technology related issues, including the technical difficulties of implementing PKI in Electronic and Mobile Commerce
- Conduct technical and policy research and develop recommendations
- Liaise with the National IT Standards committee in developing the recommended PKI standards

The Direction of Technology WG

PrivyLink

- Technology-driven effort is hard to succeed
  - PKI is difficult to use
  - CAs are getting more complicated and difficult to understand
- Application-oriented PKI initiatives are better adopted
  - It's easier to promote PKI in selected communities
  - users see more compelling reasons for PKI

Our Development Philosophy

PrivyLink

- Fit-for-purpose
  - killer-applications
- Cost-effective
- Multiple delivery channels
  - Internet, mobile, PDA
- Flexible end-user devices
  - PC , GSM, Set-top box, PocketPC, Palm
- Service provider independent
  - CA, ISP, Telco, ASP

Recent Activities

- Secure Document Exchange for B2B E-Commerce
- Aim to develop secure platform for supporting cross-country B2B e-commerce
- SDX platform that interoperable with most regional CAs
- SDX platform:
  - SLIFT from PrivyLink
- Regional CAs:
  - DigiCert, HK Post, ID.Safe , JETCO , KSIGN, Netrust, Taiwan-CA

PrivyLink International Limited

http://www.privylink.com/

PrivyLink (HK) Limited
Portion B, 38/F
Bank of China Tower
1 Garden Road
Hong Kong
Tel: (852) 2523 3908
Fax: (852) 2501 5503

PrivyLink Pte Limited
77 Science Park Drive #02-05/07
CINTECH III
Singapore Science Park I
Singapore 118256
Tel: (65) 882 0700
Fax: (65) 872 5490

The First
Asia PKI
FORUM

DOCUMENT NO.15

TITLE : Scenarios of PKI Deployment In Chinese Taipei

SUBMITTED BY : Dr. Han Min Hsia
Chairman,
Chinese Taipei Promotion Association for Asia PKI Forum

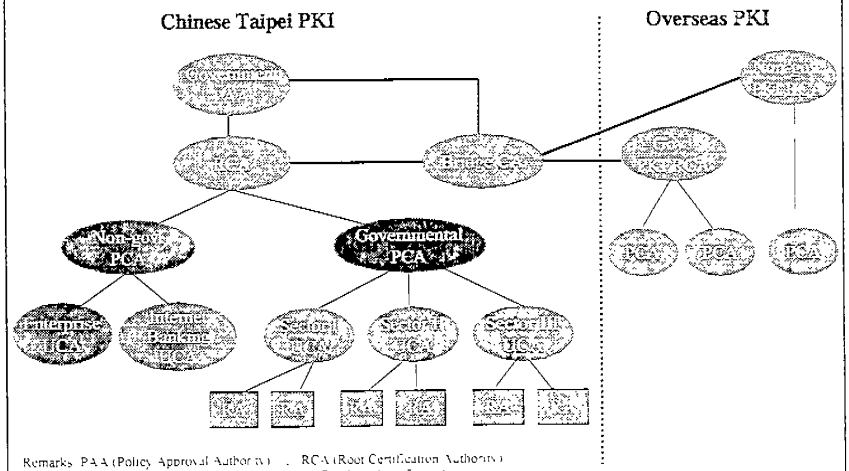
Scenarios of PKI Deployment In Chinese Taipei

Chinese Taipei Promotion Association for Asia PKI Forum

Dr. Han-Min Hsia
Chairman
June 13, 2001

1

PKI Structure -- Chinese Taipei Status



Remarks: PAA (Policy Approval Authority), RCA (Root Certification Authority)
PCA (Policy Certification Authority), UCA (User Certificate Authority)
RA (Registration Authority)

2

E-Transaction Status

EC Market Value

Unit: $ billion

	Item	1999	2004
Chinese Taipei	B2B eCommerce	5.22	57.8(60%)
	B2C eCommerce	0.38	1
	Overall eCommerce	5.6	58.8

Source: 05 2000 Institute for Information Industry
The number inside ( ) stands for CAGR

High market value → High trust requirement → High PKI requirement

On-line Business

Example: TradeVan (source: 2000 year)

Customs Declared Tariff : ***US$*** 1.7 billion
Number of Customs Tariff Declaration : 155,350

High overseas trading rate → High cross-PKI requirement

Principals for CA Structure

- Market-lead development and management
- Follow up international standard and rule
- Few involvement by Gov. and Self-constraint by industries
- Promote CA risk management and insurance system
- Encourage CA information transparency
- Protect consumer privacy and rights
- Encourage competitiveness between industries

Electronic Signature

Legislation Principles

Follow international legislation principles, including:

- Technology Neutrality
- Freedom of Contract
- Market-Lead

Legislation Current Status

1999 Dec. — Passed The Proposal for Electronic Signature Bill by The Executive Yuan

2000 Mar. — Finished submission process to The Legislative Yuan

2001 May — Approved first review procedure by The Legislative Yuan

One of the key amended ordinance of Electronic Signature Bill focuses on the encouragement of international reciprocal cooperation

Environments for Asia PKI (observation)

From culture point of view:

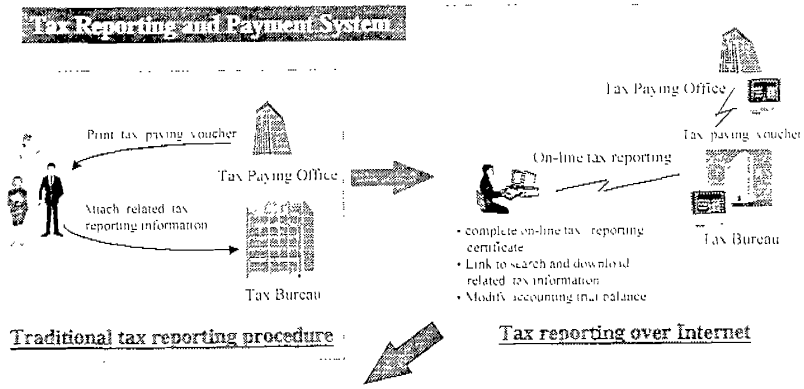
- Lack of transparency in Asia market
- Conservative investment concept (don't want to take risk)
- Lack of deadline sensibility
- Particular consumption model
- Distinction between Asian & Western
  Seal Certificate in Japan and Chinese Taipei
  (Seal Certificate is more adoptable for Asian rather than Western countries due to the culture discrepancy.)

From operation point of view:

- Follow up the international standard and management.
- 3 kinds of CA structure including Bridge CA Model, Hierarchical Model and Mesh Model.
  Chinese Taipei tends toward Bridge CA Model due to its flexible characteristics and market-lead consideration.

Measures to activate PKI utilization (I)

Tax Reporting and Payment System

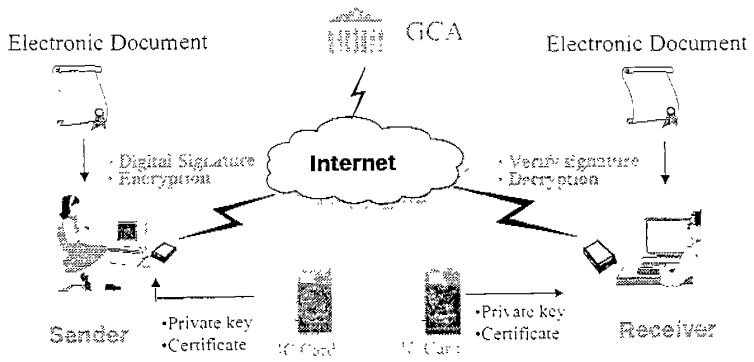


Benefits:

- Enhance data accuracy, raise 70% operation efficiency
- Successful tax reporting are over 11,000 records. (2000, March)
- Fill out and review income information, and digitally signed reports to pay taxes via banking accounts automatically

Measures to activate PKI utilization (II)

Secure Government Messaging over e-mail



- Developed a non-repudiation mechanism for electronic messaging. (1998)
- More than 1,000 government units and more than 3,000 officers exchanging signed mails over GSN.

8

Measures to activate PKI utilization (III)

Procurement Bidding Electronic System

Procurement Institute

Financial Institute

5 Customary fee wire-transfer

1 Bid document upload

4 Bid proposal document download

Customary fees submission and confirmation

Government Procurement Bidding Networks

3 Bid deposit submission and bid proposal document upload

CA

0 Search and apply for certificate

2 Bid document download and registration fee submission

Industries

- Established Electronic Bulletin system and the Electronic Bidding system
- More than 300 government sectors participated in this program

Measures to activate PKI utilization (IV)

Other Applications

- Secure Bank Monthly Report
- Secure Central Payment Admission
- Mobil Vehicle Business Service

The First
Asia PKI

DOCUMENT NO.16

TITLE : WHERE WE ARE,WHERE WE ARE HEADING FOR

SUBMITTED BY : Mr.Jiro Makino
Attorney at Law,Chairman of Business Environment Section of APKI-J

WHERE WE ARE, WHERE WE ARE HEADING FOR

2001.6.13

ASIA PKI FORUM

JIRO MAKINO

The Chairman of Business Part of APKI-J. Attorney at Law

WHERE WE ARE

Our Standpoint and Internet in Japan

1999.4 IT Action Plan(Japanese Government)

1999.12 Millennium Project (Japanese Government)

2000.4.11 Amendment of Commercial Registration Law
The Electronic Authentication Systems
Based on the Commercial Registration System

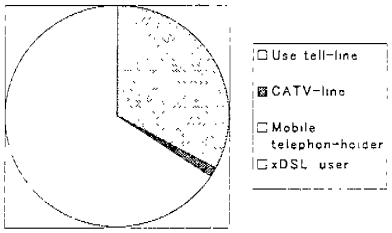
2000.5.31 Law Concerning Electronic Signatures and
Certification Services

2001.4.1 This System Started

Internet in Japan

Internet users in Japan
2001

		Ten thousands of users
Use tell-line	1723	125
CATV line	[illegible]	[illegible]
Mobile telephone holder	157	0.76
xDSL line	7	0.03
Total	2067	100



Monthly movement of the number of subscribers

(The last day of Month)

Year Month	Total (thousand-lines)	Number of subscribers: Mobile Telephone, PHS, Tsudo Phone, Cable and Internet Provider Services, Mobile Telephone
[illegible]	(65944) 67 877	[illegible]
[illegible]	(61567) 68 [illegible]	[illegible]
[illegible]	(60 565) 60 163	[illegible]
[illegible]	59 903	[illegible]

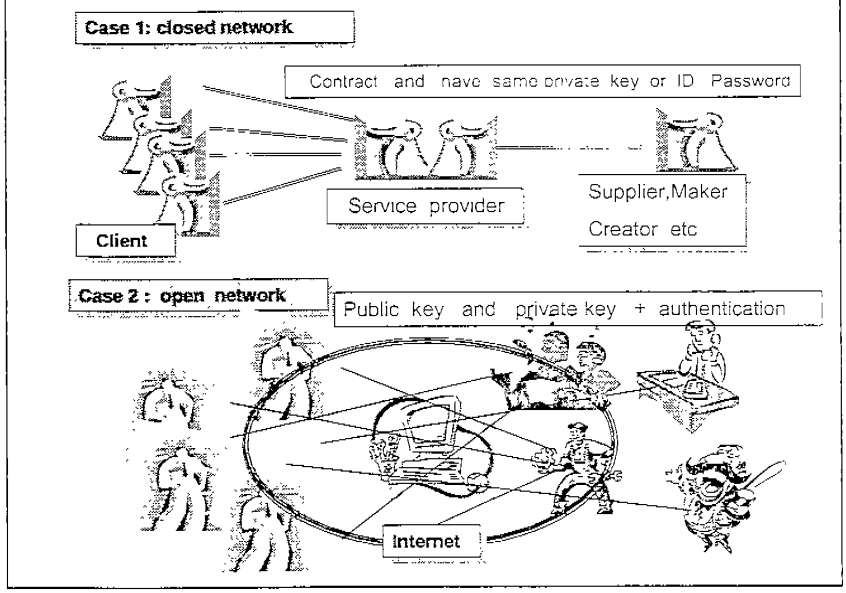
(Rounding up less than 1000 unit for Number of subscribers)

[illegible] Telecommunications carriers [illegible]

Where we are heading for ?

Digital Signature Digital authentication

- Are there any business models ?
- What kinds of services will appear ?
- Is the system safety ?
- What is the merit to use ?
- What will happen from human error ?



附件二

會員章程

Asia PKI Forum Charter

Twentieth-century business styles and lifestyles are changing dramatically in the 21st century with the rapid development of IT and the spread of advanced networks, such as the Internet. E-commerce made possible by IT has rendered the conventional relationships among enterprises and between the government and citizenry more flexible and diversified. As a result, society now holds more possibilities and diversities than ever before. E-commerce in the Asia/Oceania Region (hereinafter "the Region") has the potential to create a seamless, borderless, and affluent society that exceeds conventional communities and national borders.

To realize the society described above requires high-security infrastructures for information distribution and trade. Building Public Key Infrastructures (PKIs) is one of the essentials in achieving this goal. The PKI of a country should reflect that country/area's legal system and technology and thus will not necessarily be interoperable with other PKIs. Therefore, great effort must be made to secure interoperability among national PKIs as the infrastructures are developed. The private sector, which will utilize e-commerce, must strive to overcome the various barriers unique to each country or area.

Based on the above understanding, we hereby announce the creation of the Asia PKI Forum and agree to collaborate to provide solutions to common issues in order to promote the establishment of interoperable PKIs throughout the Region and the realization of borderless and seamless e-commerce.

Article 1 (Name)
The name of this organization is "Asia PKI Forum" (hereinafter "the Forum").

Article 2 (Objectives)
The objectives of the Forum are to promote interoperability among PKIs in countries/areas in the Region and to activate e-commerce utilizing the PKIs in the Region.

Article 3 (Fundamental Principles)
The members of the Forum shall observe the following fundamental principles for achieving the objectives as specified in Article 2.

(1) Recognizing that the first priority is to realize seamless and borderless e-commerce in the Region, the Forum will coordinate members' cooperative actions toward identifying cross-border issues and their solutions for the mutual benefits of all the members.
(2) In all its activities, the Forum will respect differences in areas such as legal systems and technology development in member countries/areas, and will make every effort with full support of all the members to help resolve cross-border issues in order to achieve interoperability.
(3) All of the Forum's activities will be implemented through the voluntary efforts and initiatives of members.

Article 4 (Activities)
The Forum will implement the following activities necessary to help resolve the cross-border issues so as to achieve the objectives as specified in Article 2, as well as to observe the fundamental principles as specified in Article 3.

(1) Hold forums and promote information exchange with the aim of identifying cross-border institutional and technical issues.
(2) Conduct necessary surveys, pilot experiments, and facilitate discussions in the working groups to identify and address in detail the issues involved.
(3) Collaborate effectively with various activities regarding e-commerce in

other regions.

(4) Participate in technology standardization of PKI and promote PKI interoperability among the Forum members.

(5) Study and compare legal acts and systems regarding electronic-transactions.

(6) Promote friendly relations among the Forum members.

(7) Undertake any necessary and appropriate activities to achieve the goals set forth in Article 2.

Article 5 (Membership)

Basically only one PKI promoting organization in a country/area in the region shall be admitted as a member of the Forum. The Steering Committee shall define the eligibility of membership and screen each application for membership submitted by candidates. The General Meeting shall approve decisions made by the Steering Committee.

Article 6 (Organization)

(1) General Meeting

a) A General Meeting shall be held once a year with the attendance of members' representatives.

b) The General Meeting shall approve decisions made by the Steering Committee and make important resolutions regarding the activities of the Forum.

(2) Steering Committee

a) The members of the Steering Committee shall be elected at the General Meeting from among the members of the Forum and each member shall exclusively represent the respective country/area in the Region.

b) The number of Steering Committee members shall be decided at the General Meeting.

c) The Steering Committee will study and decide policies on the activities and management of the Forum and member eligibility, and seek General Meeting's approval of these decisions.

(3) Chairperson and Vice Chairpersons

a) The Chairperson and up to three Vice Chairpersons shall be elected at the General Meeting from among the representatives of the members. The term of service shall be one year. The Chairperson and the Vice Chairpersons may be re-elected for a second consecutive term. In any event, the term of the Chairperson and the Vice Chairpersons shall not exceed two consecutive years.

b) The Chairperson shall take a leadership role in the activities and management of the Forum and shall chair the meetings of Steering Committee and the General Meeting.

c) Should the Chairperson or any Vice Chairperson become unable to execute his or her duties for any reason, the organization from which such officer is elected may nominate a temporary or permanent substituting officer to take over all the duties and responsibilities of the previous officer for the rest of office term.

(4) Secretariat

The secretariat shall be set up at the Chairperson's country/area to perform the required tasks.

(5) Others

Working groups and other subordinate organizations shall be formed as necessary.

Article 7 (Membership Dues)

Membership dues shall be collected and members shall pay their dues according to the resolution, which shall be approved at the General Meeting.

Article 8 (Miscellaneous)

Other rules/bylaws and matters necessary for the operation of the Forum shall be determined by the Steering Committee and/or other Committees and shall be approved at the General Meeting.

附件三

會員簽署同意書

Joint Communiqué

(Tokyo, June 13, 2001)

On June13, 2001, representatives of PKI promoting organizations from 8 countries and areas* in Asia and Oceania region had a meeting in Tokyo to discuss establishment of a regional organization for promoting PKI, and facilitating e-commerce in the region.

At the meeting, the establishment of "Asia PKI Forum" was agreed and the content of a Charter, which incorporates the principles of "Asia PKI Forum", was also agreed by the representatives.

These principles address the fact that 20th century business styles and lifestyles are changing dramatically in the 21st century with the rapid development of IT and the spread of advanced networks, such as the Internet. E-commerce made possible by IT has rendered the conventional relationships among enterprises and between the government and citizenry more flexible and diversified. As a result, society now holds more possibilities and diversities than ever before. E-commerce in the Asia/Oceania region has the potential to create a seamless, border-less, and affluent society that exceeds conventional communities and national borders.

To realize the society described above requires high-security infrastructures for information distribution and trade. Building Public Key Infrastructures (PKIs) is one of the essentials in achieving this goal. The PKI of a country should reflect that country/area's legal system and technology and thus will not necessarily be interoperable with other PKIs. Therefore, great effort must be made to secure interoperability among national PKIs as the infrastructures are developed. The private sector, which will utilize e-commerce, must strive to overcome the various barriers unique to each country or area.

Dr. Tsutomu Kanai, Chairman of Japan Promotional Association for Asia PKI Forum (APKI-J), was elected as its first Chairperson.
Dr. Y.T. Lee, Chairman of Korea PKI Forum, and Mr. Lucas Chow, Chairman of PKI Forum Singapore, were elected as Vice Chairpersons. It was agreed that the representative of an organization from the People's Republic of China would be the third Vice Chairperson, if identified within two months from the date of the meeting.

The Forum will make further efforts to invite similar PKI promoting organizations in the region to join the Forum for realizing the regional interoperability of PKI.

(*8 countries and areas are Australia / People's Republic of China / Hong Kong, China / Japan / Republic of Korea / Malaysia / Singapore / Chinese Taipei)

This Joint communique, dated 13 June, 2001, is jointly issued by the representatives at the First General Meeting of Asia PKI Forum, held in Tokyo, Japan

---

Australia

Steve ORLOWSKI

Representative
Certification Forum of Australasia (CFA)

People's Republic of China

Qin XU

Deputy Director-General
State Development Planning Commission (SDPC)

Hong Kong, China

Ping-Chuen LUK

Postmaster General
Hongkong Post

Japan

Tsutomu KANAI

Chairman
Japan Promotional Association for Asia PKI Forum

Republic of Korea

Y.T. LEE

Chairman
Korea PKI Forum

Malaysia

Mohamed Arif NUN

Senior Vice President
Multimedia Development Corporation Sdn.Bhd.

Singapore

Lucas CHOW

Chairman
PKI Forum Singapore

Chinese Taipei

Han-Min HSIA

Chairman
Chinese Taipei Promotional Association for PKI Forum

The representatives at the First General Meeting of Asia PKI Forum, held in Tokyo, Japan, jointly issue this Joint communiqué, dated 13 June 2001

Australia

Steve ORLOWSKI

Representative
Certification Forum of Australasia (CFA)

People's Republic of China

Qin XU

2001. 6. 13.

Deputy Director-General
State Development Planning Commission (SDPC)

Hong Kong, China

Ping-Chuen LUK

Postmaster General
Hongkong Post

Japan

Tsutomu KANAI

Chairman
Japan Promotional Association for Asia PKI Forum

Republic of Korea

Y.T. LEE

Chairman
Korea PKI Forum

Malaysia

Mohamed Arif NUN

Senior Vice President
Multimedia Development Corporation Sdn.Bhd.

Singapore

Lucas CHOW

Chairman
PKI Forum Singapore

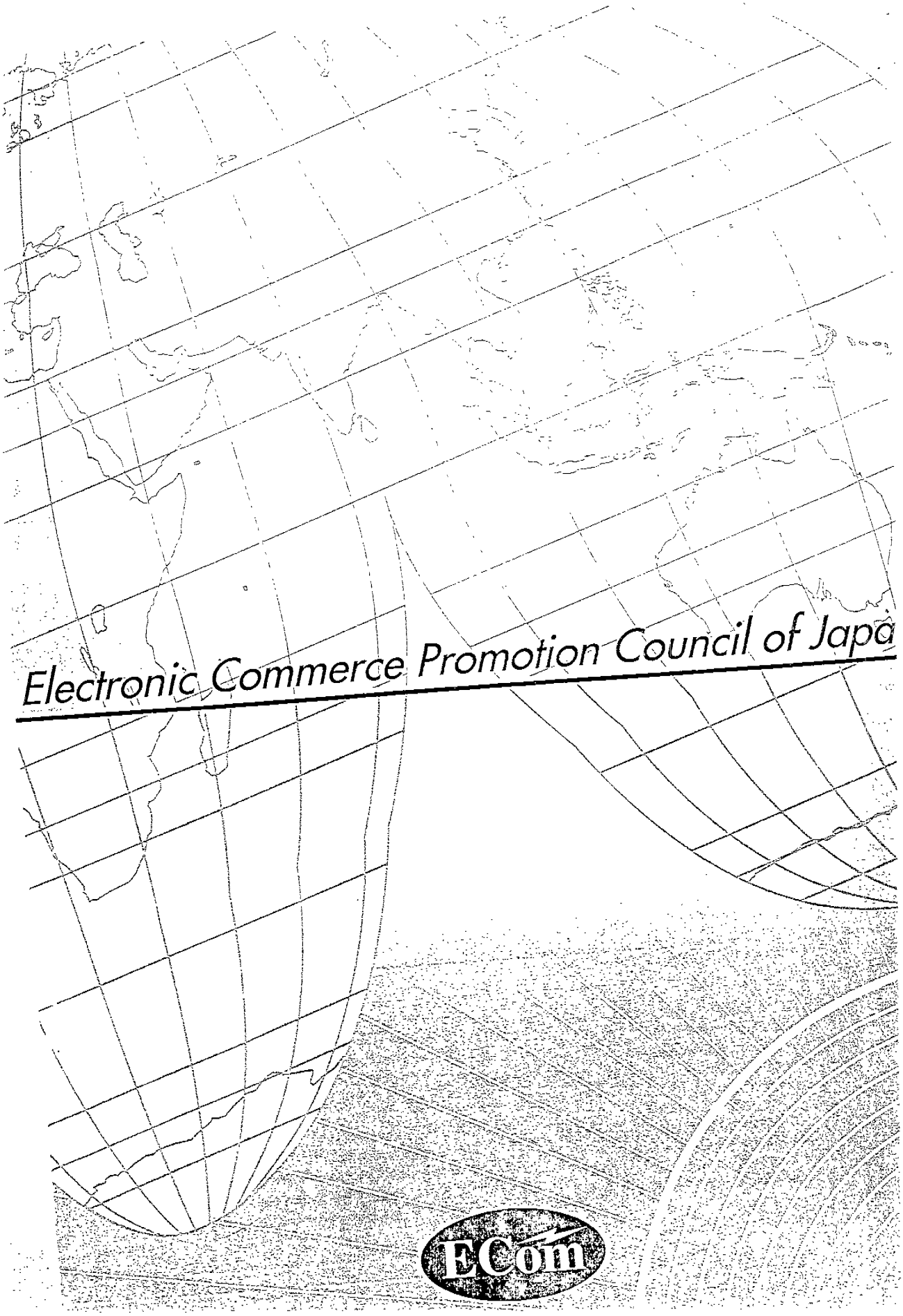
Chinese Taipei

Han-Min HSIA

Chairman
Chinese Taipei Promotional Association for PKI Forum

附件四

其他參考資料


Electronic Commerce Promotion Council of Japa
ECom

Founding Prospectus
Electronic Commerce Promotion Council of Japan (ECOM)

The rapid expansion of electronic commerce (EC), governmental promotion of electronic government projects, and other factors are accelerating Japan's digital revolution. Revolutionary changes are predicted in our economic and social structures, and in the structure of value added creation activities (the value chain) in existing industries to one differing from what we know today, while the daily lives of the average consumer will change, as well.

Revolutionary changes of this magnitude will most likely be accompanied by extensive rationalization in the existing enterprises, while consumer protection and other issues fail to keep pace even now. The transition to computes and electronic commerce cannot be painted entirely in colors of rose.

If Japanese industry procrastinates in computerization, however, not only will foreign industry snatch up domestic demand, but hope of its popularization among the people will be lost as well. If we want to strengthen Japan's economic activities and industrial competitiveness, we must vigorously develop EC.

By computerization, we do not mean just the introduction of the systems. In the process of electronic commerce's rapid growth in the real community, many conventional systems and arrangements will have to be changed to adapt to the digital community, or entirely new systems and arrangements will have to be made.
These new rules will be directed by industry and the people, and must have a global perspective. As can be seen in the developments of Global Business Dialogue in EC (GBDe), there is a growing trend among the global industrial community to meet to draw up unified policy frameworks which transcend individual interests on various EC issues, to take a global perspective in making and practicing its own rules, and to make specific recommendations to their respective governments. Japan, as the leader of the Asian digital revolution, must take part more independently, more actively, and more strategically than it has in the past, alongside Europe and the US, in drawing up the international rules of the digital community.

In order to do so, Japan, too, must collect the wisdom and experience that it has cultivated concerning EC and join this important movement.

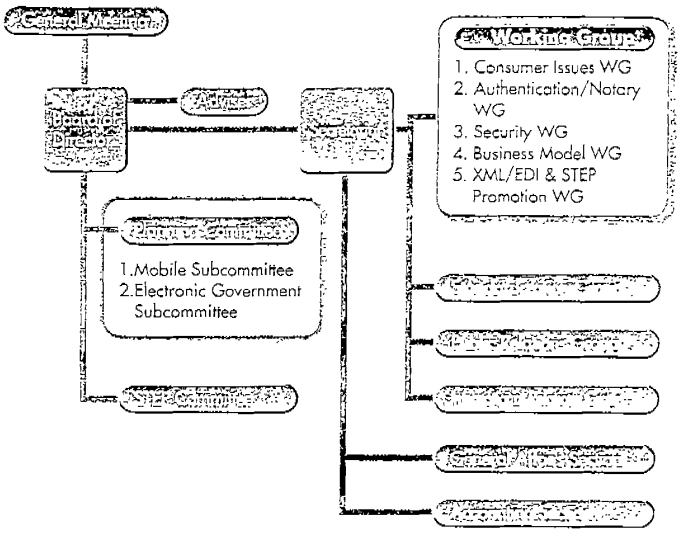
The Japan EC/CALS Organization (JECALS) has been active in BtoB electronic commerce, the Electronic Commerce Promotion Council of Japan (ECOM) in BtoC, and the Center for the Informatization of Industry (CII) has been active in electronic data exchange. Having accomplished much to make EC work, however, JECALS and ECOM were dissolved in March 2000.

With the success and growth of EC, more and more issues cut across what have been regarded as BtoB and BtoC frameworks; if we want be a primary source of EC-related information, for the world as well as Japan, we must collect the results of research conducted in these organizations and, with the ingenuity of industry, continue to work on new problems.

Industry has therefore assembled to establish a new organization, the Electronic Commerce Promotion Council of Japan, to facilitate close cooperation in promoting electronic commerce and standardization such as XML/EDI and STEP (standards concerning expression and exchange of product model data), an effort which had been carried out separately in the earlier organizations.

The council expects, considering the remarkable technological development of EC, to be active over the next four to five years. It will, over that period, make rules and recommendations to the government to achieve secure EC in both BtoB and BtoC, establish, maintain, and manage international standards based on user needs, and conduct activities to further promote EC and make international contributions in this field.

ECOM Organizational Chart



Secretariat: Japan Information Processing Development Center- Electronic Commerce Promotion Center

Main Activities

1 General Meetings, Board of Directors Meetings, and Committee Activities

(1) General Meetings

General meetings are held annually, in principle within three months of the end of the business year. General meetings are comprised of the Board of Directors, A regular members, B regular members, and special members. The General Meeting passes resolutions on items determined by Council regulations (election of directors and advisors, changes in regulations, and other policy issues) and receives reports on activity conditions.

(2) Board of Directors Meetings

Board of Directors meetings are held semiannually, prior to the beginning and after the end of the business year.

The Board of Directors and advisors are elected at the General Meeting by Board members (company representatives) and special members. The Board of Directors passes resolutions on important items concerning operation of the Council determined by Council regulations (operating budget, operating plan, settlement of accounts, and operating report).

(3) Planning Committee

The Planning Committee coordinates and considers study themes, activity policies, and other issues related to the operations of the working groups. Additionally, the Planning Committee also establishes subcommittees within the committee for study of important new themes and proposes establishment of new working groups as necessary.

In principle, the participating members of the Planning Committee and its subcommittees are limited to Board members and intelligent people.

(4) STEP Committee

The STEP Committee studies specific issues related to STEP activities. In principle, only Board members representing companies with an interest in STEP can participate in this committee. (Expenses for the STEP

activities are seprately needed.)

2 Working Group Activities

Working Groups have been formed for the following major themes to consider issues concerning electronic commerce (including operations and systems). Working group activities include consideration of issues and formulation of standards and agreements, guidelines, operating procedures, and other specifications. (Working groups are also established on an ad hoc basis as deemed necessary.)

- Consumer Issues Working Group (consumer's privacy protection, personal data protection, electronic settlement, and other consumer issues)
- Authentication/Notary Working Group (implementation of guidelines, upgrading of versions, systemic infrastructure, and other authentication issues)
- Security Working Group (security seal support and other security issues)
- Business Model Working Group (Web business model, SCM business model, and other business model research)
- Diffusion and Promotion Working Groups (XML/EDI: Diffusion of standards; STEP Implementation Working Group: Promotion of practical application)

3 Standardization Activities

The results of working group activities are collated to formulate and disseminate standards for electronic commerce. Specific activities include collaboration with international standardization promotion organizations, deliberation of standardization proposals, including Japan's proposals, and active promotion of practical application support activities for domestic standardization.

- Maintenance and administration of CII standards
- XML/EDI standardization
- Participation in and cooperation with ISO/TC154
- Participation in and cooperation with ISO/TC184/SC4
- JIS standardization (CII, EDIFACT, STEP)
- STEP (ISO domestic committee, response to international committee, formulation of standards, diffusion activities geared to small and medium-sized companies)

4 Diffusion and Publicity Activities

ECOM engages in a wide variety of activities for diffusion and publicity of electronic commerce to the largest possible audience. These activities include information dissemination via the Web, symposiums, seminars, training workshops, exhibitions, electronic commerce experience seminars, and introductory seminars for electronic commerce held in areas throughout Japan.

5 International Cooperation Activities

ECOM promotes close relationship with many overseas EC-related organizations through information dissemination via the Web, survey of overseas EC trends, international cooperation for EC activities with the Japan-South Korea ECOM, participation in and cooperation with UN/CEFACT, and international support by the Consumer Issues WG.

6 Research Activities

ECOM also conducts market research in Japan and trends research of conditions in foreign countries through collection of materials.

Membership and Benefits

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	3,000	700	200	10	—	—

[illegible]	[illegible]						
[illegible]	[illegible]	○	○	○	×	○	×
[illegible]	[illegible]	○	×	×	×	○	×
[illegible]	[illegible]	○	×	×	×	○	×
[illegible]	[illegible]	△(Note 1)	×	×	×	○	×

WG [illegible] (Note 2)		No limit	Up to 2 WG	×	×	No Limit	×
WWW	Page for members (Note 3)	○	○	○	×	○	×
	Page for the public	○	○	○	○	○	○

[illegible]		○	○	○	Paid (10% off)	○	paid
[illegible]		○	○	○	Push info/paid (10% off)	○	paid
[illegible]	[illegible]	○	○	○	○	○	×
	[illegible]	○	○	○	×	○	×

Notes

1) Expenses for the STEP activities are separately needed.

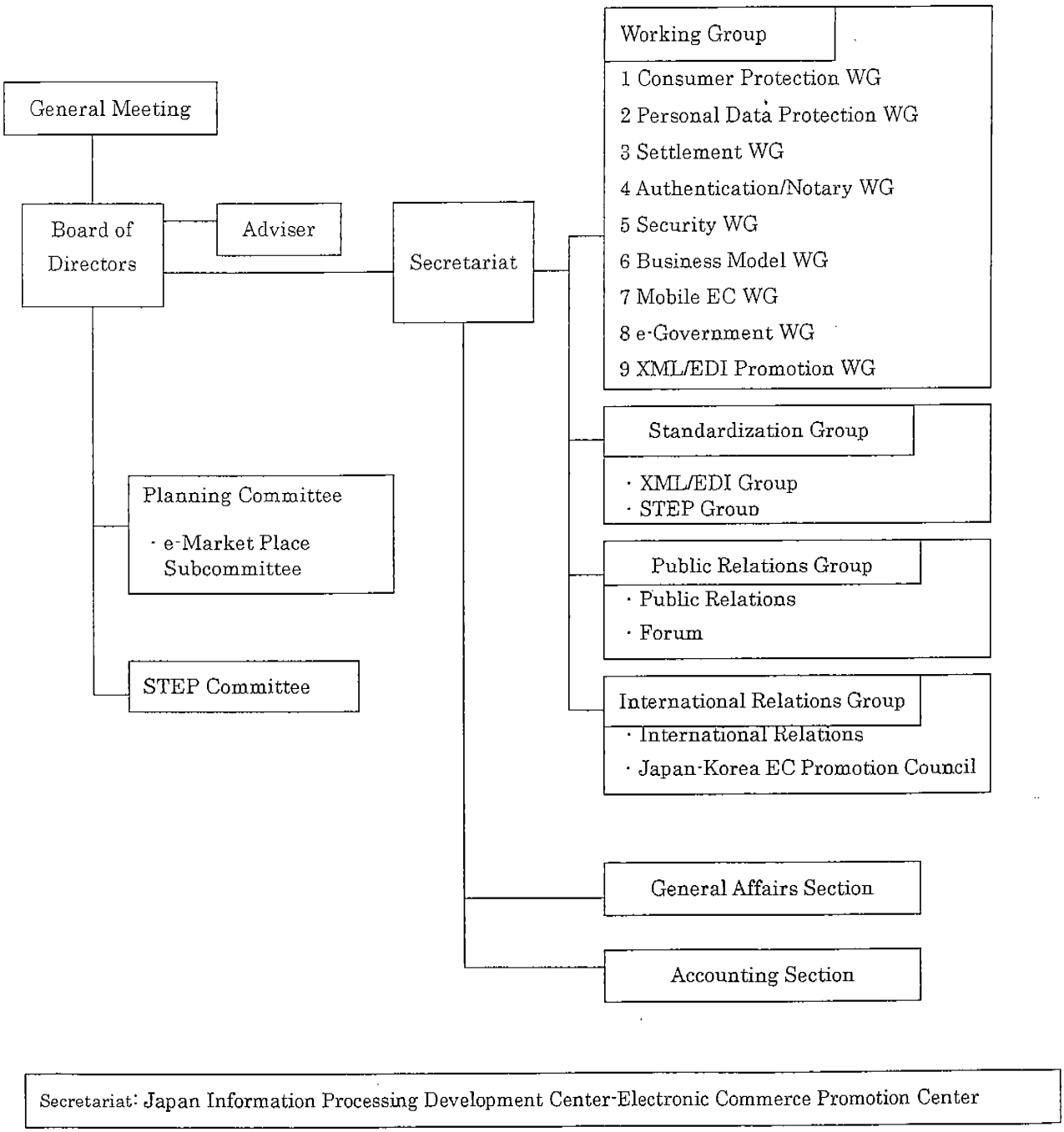
2) In addition to member passwords, separate Web member page passwords are issued to members participating in working group activities, and these members receive newsletters, the bulletin, and reports of results. Additionally, each working group holds seminars concerning its specialized themes when necessary.

3) Pages for members provide information limited to members, priority dissemination of information to members, invitations and priority registration for conferences sponsored by ECOM and related organizations, and other information concerning electronic commerce.

4) In principle, seminars are held ten times a year. Symposiums for announcement of results are held annually, and other special symposiums are held during computerization month and on other appropriate occasions. Periodic seminars are open to the public. Associate members are granted a ten percent discount, and Board members and A and B regular members can participate free of charge.

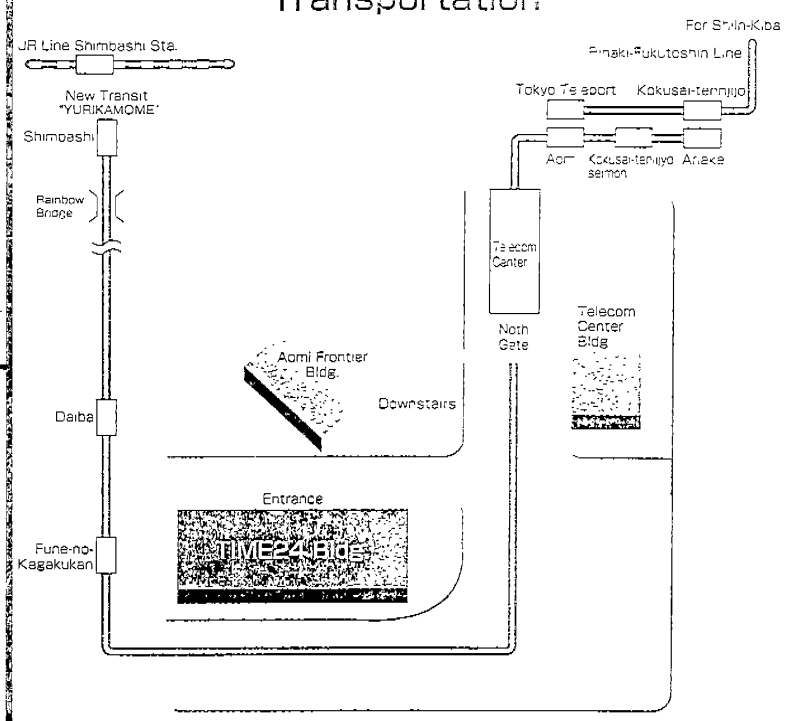
ECOM Organization Chart

April 2, 2001



Secretariat: Japan Information Processing Development Center-Electronic Commerce Promotion Center

Transportation



■Take the Yurikamome from JR Shimbashi Station to Telecom Center for 17 minutes. 2 minutes walk from there.

Electronic Commerce Promotion Council of Japan

TIME 24 BLDG. 10FL., 2-45 AOMI/KOHTOKU,TOKYO 135-8073 JAPAN
TEL:+81-3-5500-3600 FAX:+81-3-5500-3660
URL http://www.ecom.or.jp/ecom_e

[illegible]

Non-profit private sector

To Promote EC in Japan

- Preparation of Rule
- Standardization
- Diffusion
- Publicity

1

Mission

✓Establishing a new business environment
All businesses and consumers can participate with confidence

✓Establishment, maintenance and spread of standards for conducing EC

✓Proposals to government
Playing a part of activities between government and private sector

✓Expanding the use of results by other countries
(especially to Asian countries)

2

ECOM started its activities

Electronic Commerce Promotion Council of Japan
(ECOM)

3

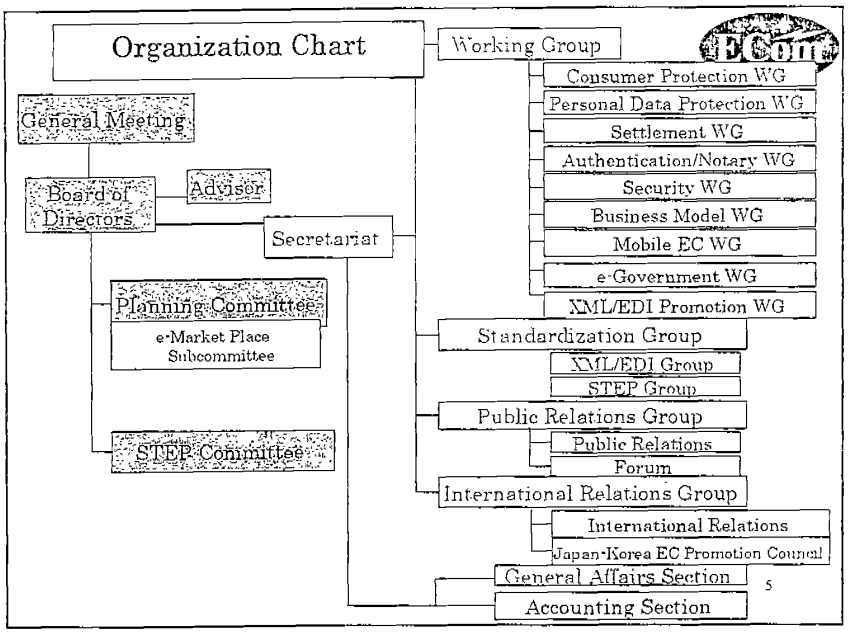
Number of Members

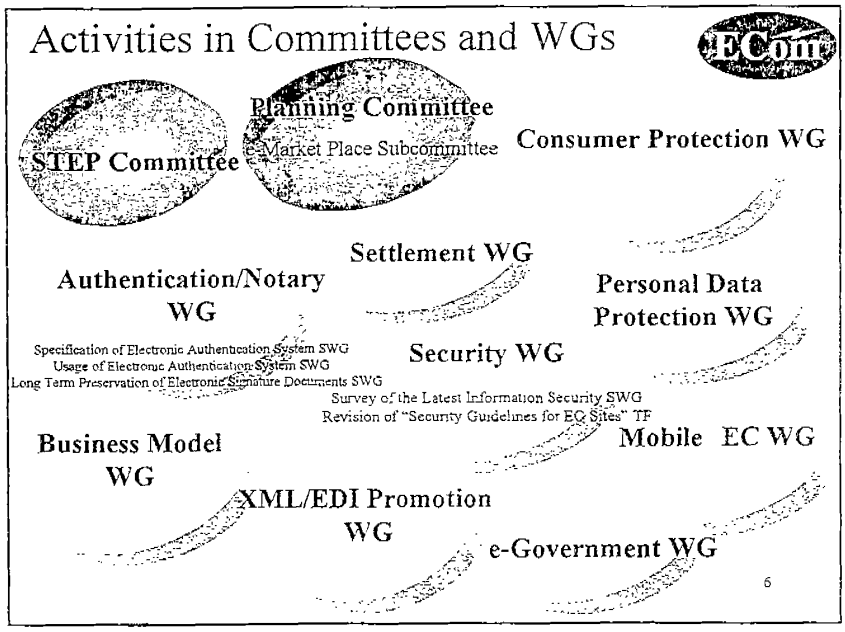
(As of April 27, 2001)

• Board Member	39
• Regular Member A	105
• Regular Member B	168
• Special Member	1
Total	313

Besides there is the associate membership for an individual.

4


Organization Chart
General Meeting
Board of Directors
Adviser
Secretariat
Planning Committee
e-Market Place Subcommittee
STEP Committee
Working Group
Consumer Protection WG
Personal Data Protection WG
Settlement WG
Authentication/Notary WG
Security WG
Business Model WG
Mobile EC WG
e-Government WG
XML/EDI Promotion WG
Standardization Group
XML/EDI Group
STEP Group
Public Relations Group
Public Relations
Forum
International Relations Group
International Relations
Japan-Korea EC Promotion Council
General Affairs Section
Accounting Section
5


Activities in Committees and WGs
STEP Committee
Planning Committee
e-Market Place Subcommittee
Consumer Protection WG
Settlement WG
Authentication/Notary WG
Personal Data Protection WG
Specification of Electronic Authentication System SWG
Usage of Electronic Authentication System SWG
Long Term Preservation of Electronic Signature Documents SWG
Security WG
Survey of the Latest Information Security SWG
Revision of "Security Guidelines for EC Sites" TF
Business Model WG
Mobile EC WG
XML/EDI Promotion WG
e-Government WG
6

Other Activities

Standardization Group

Formulation and Dissemination for Standard of EDI, XML, STEP, etc

International Relations Group

Information Dissemination via the Web
Survey of Overseas EC Trends
International Cooperation for EC Activities

Public Relations Group

Information Dissemination via the Web
Symposium, Seminars, Training Workshops,
Exhibitions, EC Experience Seminars

7

Deliverables

- ECOM Guidelines for Transactions between Virtual Merchants Consumers
- Proposal Concerning Level of Certification and Confirmation of Applicant's Identity
- Proposal for Liability of Certification Authority
- Proposal Concerning Diffusion of Electronic Settlement in the B-to-C Market
- Guidelines for Building IC Card Terminal Infrastructures
- Proposal for Seal Program for "Shop on Secure System"
- Business Model Research on Consumer-Oriented Electronic Commerce Sites
- Current Status of Business-to-Business Electronic Commerce in Japan
- Model Contract for SCM Electronic Commerce: Comments

etc.

8

Guidelines for end entity facility of electronic signature creation and verification

2001. 6. 14

YONEKURA Tokio

Electronic Commerce Promotion Council of JAPAN
(ECOM)

CONTENTS

1. Objectives of ECOM activities(1/2)

Electronic Authentication system is composed of

- Certification Organization and
- End entity facilities

Electronic Authentication system should be

- More trustworthy
- Easy to introduce
- Highly interoperable

1. Objectives of ECOM activities(2/2)

The Law

Certification organizations:
- Confirmation of Identity of Subscriber
- Secure Certification operations

The Guidelines

Hardware and Software of End entity:
- Guarantee the validity of Electronic Signatures

consumers, Internet shop, company employees, etc.

Reliable Electronic Authentication and Electronic Signatures

2. Structure of "Guidelines for end entity facility"

(1) Purposes

(2) Guidelines

(3) Readers

(4) Relationship between Readers and Parts of Guidelines

(5) Guideline for users in homes

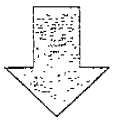
(6) Guideline for users in companies

(7) Guideline for developers

 5

(1) Purposes

Consideration of requirements for user systems that use electronic authentication systems from secure and useful points of view



Guidelines for the users and developers of end entity system and Applications

 6

(2) Guidelines

(i)Guidelines for users
to maintain security・・・・・・
・Which we should pay attention to?
・How to prevent accidents?

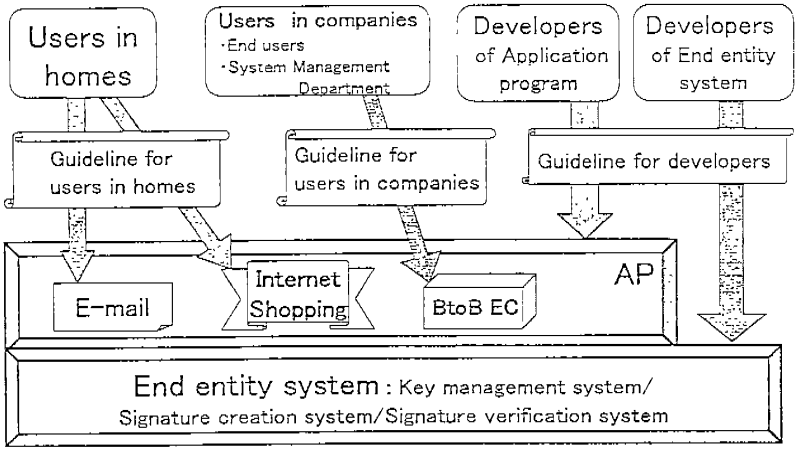
(ii)Guidelines for developers
・Which we should pay attention to?
・How to prevent accidents?
・How to improve the usability ?

(3) Supposed Readers

(i)Users
a. Users in homes
b. Users in companies
– End users
– System management department

(ii)Developers
a. Developers of Application program
b. Developers of End entity system
(Key management system/
Signature creation system/Signature verification system)

(4) Relationship between Readers and Parts of Guidelines



 9

(5) Guideline for users in homes

(i) Application for users in homes

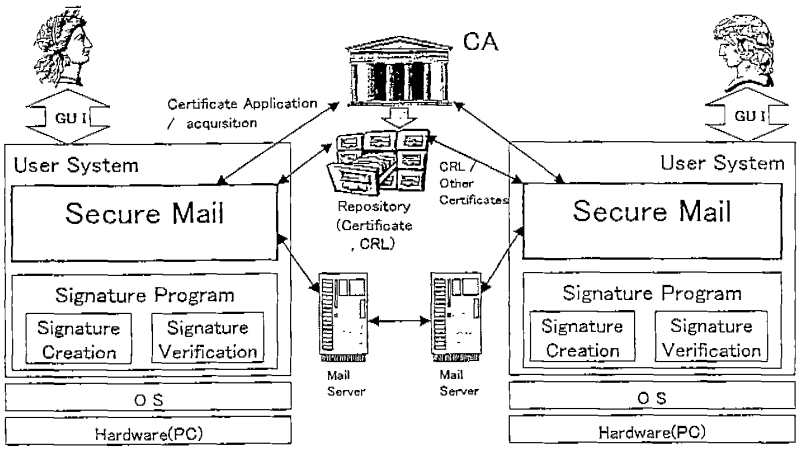
- E-Mail
- Internet shopping

(ii) Recommendation / Requirement

 10

(i) E-mail

a. Secure E-mail



 11

(i) E-mail

b. Steps

Key Creation and Certificate Acquisition

- Key Creation
- CRL Acquisition
- Certificate Application/Acquisition /Registration

Signature Creation and Verification

- Signature Creation / Mail Send
- Receive Mail / Signature Verification
- Key / Certificate Update
- Password Management
- Revocation Requirement

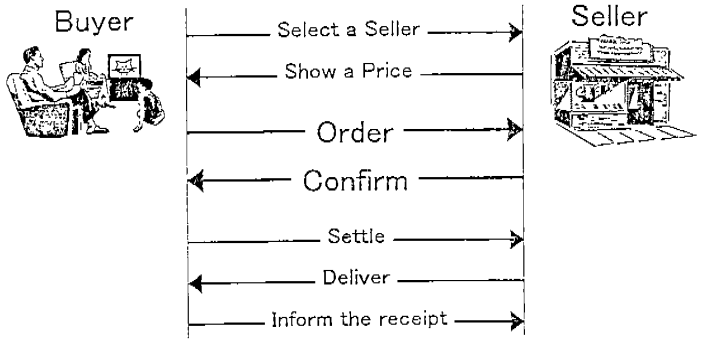
Cancellation

- Certificate: Revocation/ Elimination
- Key: Cancellation

 12

(ii) Internet shopping

a. Order (Buyer) and Confirmation (Seller)



b. Steps

Key Creation and Certificate Acquisition — Buyer, Seller

- Key Creation
- CRL Acquisition
- Certificate Application / Acquisition / Registration

Signature Creation and Verification

- Seller Selection (Buyer) / Price Presentment (Seller)
- Signature Creation / Order (Buyer)
- Signature Verification / Signature Creation / Confirmation (Seller)
- Signature Verification (Buyer)

- Key/Certificate Update
- Record Management of PKC
- Password Management
- Revocation Requirement

Cancellation — Buyer, Seller

- Certificate Revocation/Elimination
- Key Cancellation

(iii) Recommendation / Requirement

a. Preparation
: Software, Virus check, CA selection, Certificate Application /Acquisition / Confirmation, System clock

b. Key/Password Management

c. Signature Creation

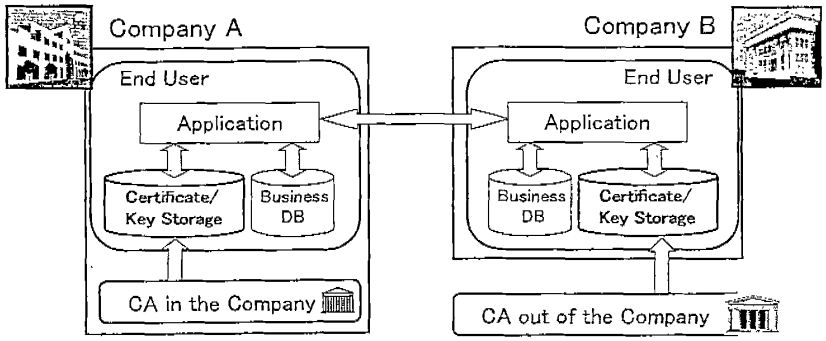
d. Update/Cancellation of Key/Certificate

e. Signature Verification

(6) Guideline for users in companies

(i) BtoB EC system

a. EDI System for Procurement



(i) BtoB EC system
b. Steps

Key Creation and Certificate Acquisition

- Key Creation
- CRL Acquisition
- Certificate Application / Acquisition / Registration

Signature Creation and Verification

End Users — System Manager

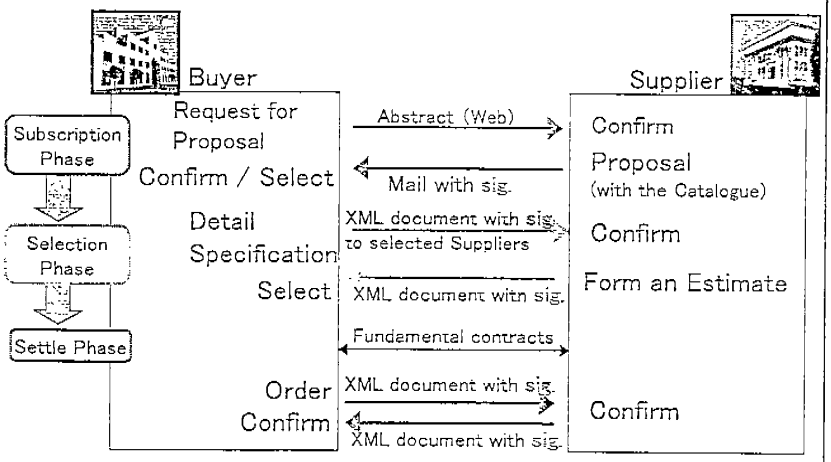
Next Page

- Key/Certificate Update
- Record Management of PKC
- Password Management
- Revocation Requirement

Cancellation

- Certificate Revocation/Elimination
- Key Cancellation

Work Flow of EDI System for Procurement



(ii) Recommendation / Requirement

・End Users・・・ Understanding, Practice

・System Manager・・・ + Guidance

a. Preparation

: Software, Virus check, CA selection, Certificate Application /Acquisition / Confirmation, System clock

b. Key/Password Management

c. Signature Creation

d. Update/Cancellation of Key/Certificate

e. Signature Verification

(7) Guideline for developers

(i) How to improve the Usability ?

a. Intelligible display of certificates

b. Easy acquisition of CA information

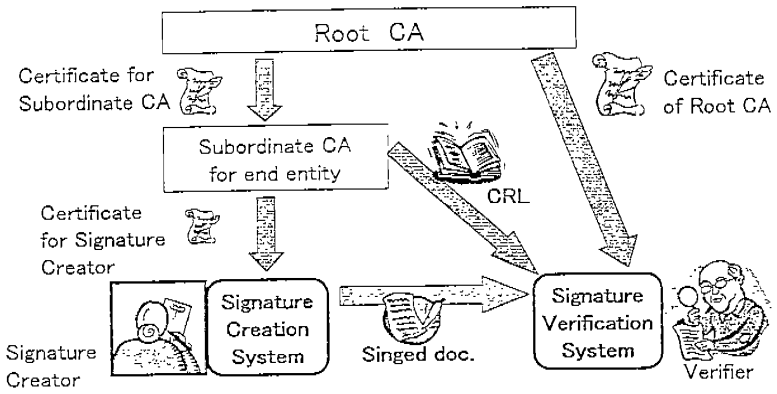
c. Concise display of verification results

d. Friendly error messages

e. Support for selection of private keys and certificates etc.

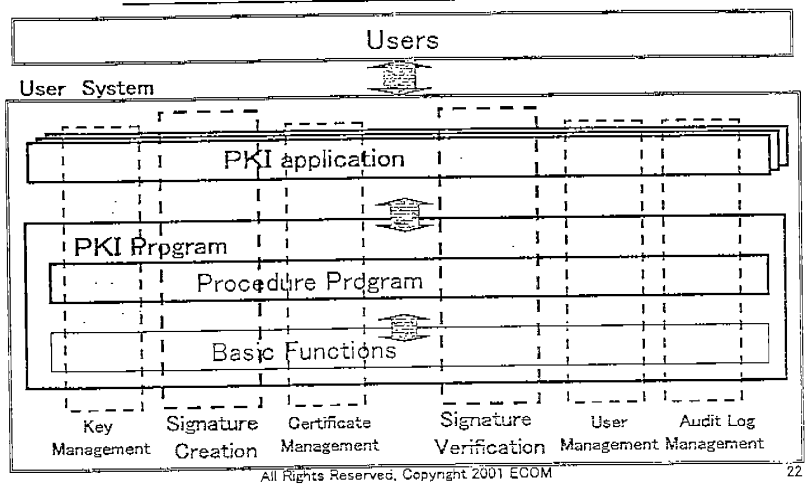
(ii) How to improve Security ?

Environment



a. Logical model

Structure of the user system



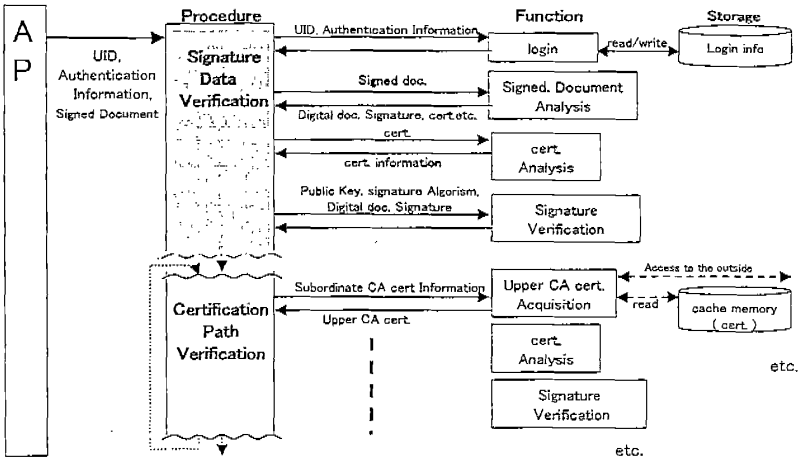
a. Logical model of the user system

- Procedures of signature creation / verification
- AP–Procedure Interface

1. Key Management
2. Signature Creation
3. Certificate Management
4. Signature Verification
5. User Management

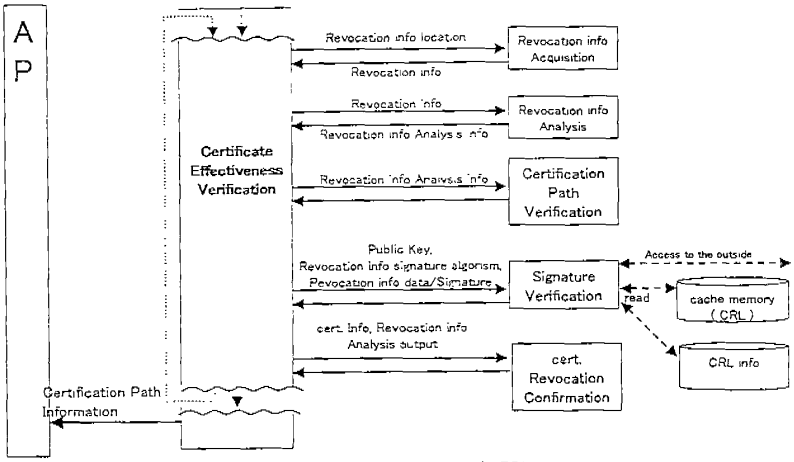
a. Logical model of the user system

Signature Verification Interface (1/2)



a. Logical model of the user system

Signature Verification Interface (2/2)



b. Threat Analysis

- Property to be Protected
  1. Private Key of Users
  2. Authentication Information
  3. Data for Signature Creation and Verification
  4. Audit Log
  5. End entity Program itself
- Threat

  Which Property is supposed to be Attacked ?
  by Whom and How ?

b. Threat Analysis

・Security Countermeasures in End entity Program

1. User Authentication
2. Audit Logging
3. Encryption of Private Key / Authentication Information
4. Detection of malicious changing
5. Elimination of Canceled Private Key and eliminated user's Authentication Information
6. Use of Strong Crypto System (Algorism and Key Length)
7. Management of Logging Device

b. Threat Analysis

・Security Countermeasures in Application Software

- Reconfirming Interface to avoid miss operations
- Confirmation of User Access Right

3. Next Step

From this Spring・・・

We have started describing the security requirements as Protection Profile based on ISO/IEC 15408.

ECOM Web Site

Please visit ECOM web site below.

http://www.ecom.or.jp/ecom_e/

Thank you so much
for your kind attention.

Annex A

Law Concerning Electronic Signature and Certification Services

(Date of enforcement : April 1, 2001)

(i)Presumption of the genuine establishment of electromagnetic records

(ii)Provisions for voluntary accreditation of designated certification services

(iii)Other necessary items

Annex B

Other activities of this year

B.1 Issues of electronic authentication systems from the point of user's view

B.2 Guidelines for long-term storage of electronic signed documents

B.1 Issues of electronic authentication systems from the point of user's view

(i)Model agreements for use of electronic authentication systems

(ii)Proposal for advanced use of electronic authentication systems

B.2 Guidelines for long-term storage of electronic signed documents

(i)Verification after the expiration of the term

(ii)Time stamp of signature creation

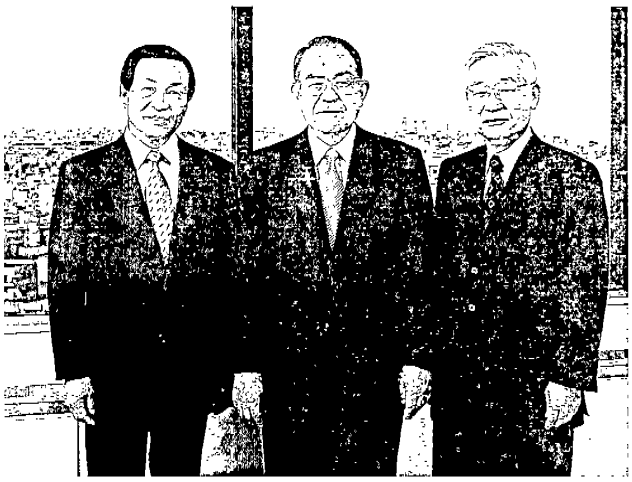
etc.

HITACHI
Inspire the Next

Outline of Hitachi

Contents

Message



Tsutomu Kanai, Chairman of the Board and Director (middle); Hiroshi Kuwahara, Vice Chairman of the Board and Director (left); Etsuhiko Shoyama, President and Director

This year marks the 90th anniversary of Hitachi, Ltd., and we are determined to make a great leap forward into the 21st century. To meet the challenges of this generation, our motto for the coming century is "reliability and speed."

Last year, Hitachi, Ltd. announced a new strategy for growth called "i.e. HITACHI," a medium-term consolidated business plan. Through implementation of this plan, Hitachi will strive to meet the expectations of our customers, stockholders, and investors.

With our wealth of knowledge and information technology, Hitachi will supply customers with new value added, becoming the "Best Solutions Partner" by utilizing the Internet in each and every industrial field with which Hitachi is involved. Our activities will span many departments: information electronics including information and communication, semiconductors and displays, power generation systems, industrial plants and equipment, as well as home electric appliances, digital media, automobiles, and measuring instruments.

In order to achieve our goal to become "the brand of choice Hitachi," a new corporate statement entitled "Inspire the Next" has been created, which concisely expresses Hitachi's promise to society. The title means to invigorate the next era and our corporate philosophy is firmly dedicated to enriching human life and making the world a better place by offering new products, systems and services.

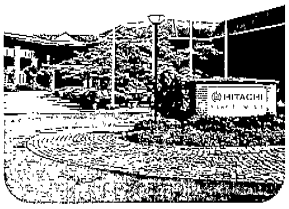
With this statement as a guide, Hitachi will deploy all its corporate activities in such a way that it becomes the most trusted company in the world.

Hitachi is most grateful for your continuing support.

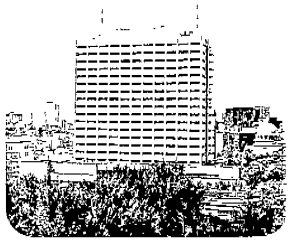
Corporate Information

Corporate name: .....Hitachi, Ltd.
Address: .....6, Kanda-Surugadai 4-chome, Chiyoda-ku, Tokyo, 101-8010 Japan
Founded: .....1910 (Incorporated in 1920)
Capital: .....¥281,738 million (US$2,658 million)
Net sales: .....¥8,001,203 million (US$75,483 million)*
Net income: .....¥16,922 million (US$160 million)*
Number of employees: 337,911


Hitachi (China), Ltd.'s Headquarters



Hitachi Europe Ltd.'s Headquarters


Hitachi, Ltd.'s Headquarters

Hitachi Asia Ltd.'s Headquarters

Information Systems & Electronics
Mainframe Computers
Software
Computer Terminals and Peripherals
Systems Integration
PCs
Magnetic Disks
Telephone Exchanges
DVD Drives
Semiconductors
Display Tubes
LCDs
Semiconductor Manufacturing Equipment
Test and Measurement Equipment
Medical Electronics Equipment

Power & Industrial Systems
Nuclear Power Plants
Hydroelectric Power Plants
Thermal Power Plants
Control Equipment
Compressors
Rolling Mill Equipment
Plant Engineering and Construction
Elevators
Escalators
Air-Conditioning Equipment
Industrial Robots
Rolling Stock
Automotive Equipment
Construction Machinery

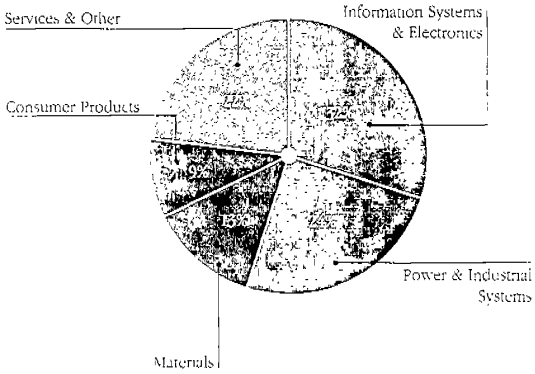
Consumer Products
Room Air Conditioners
Refrigerators
Washing Machines
Microwave Ovens
Vacuum Cleaners
Heating Appliances
Kitchen Appliances
Lighting Fixtures
TVs
VCRs
Mobile Phones
Audiotapes
Videotapes
Batteries
Optical Storage Media
Floppy Disks

Materials
Synthetic Resin Materials and Products
Printed Circuit Boards
Ceramic Materials
Special Steels
Rolls for Rolling Mills
Malleable Cast-Iron Products
Forged and Cast-Steel Products
Pipe Fittings
Wire and Cable
Copper Products
Rubber Products

Services & Other
General Trading
Financial Services
Transportation
Property Management
Printing

Hitachi America, Ltd.'s Headquarters

1999 Net Sales



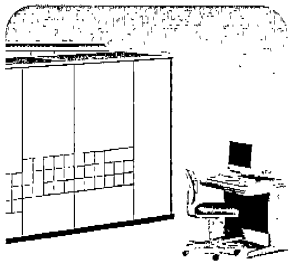
Notes:
1. Figures are as of March 31, 2000.
2. Financial statements are originally expressed in yen and converted to U.S dollars for the convenience of the reader at the rate of ¥106=US$1.
3. Figures denoted by an asterisk (*), including the results in the diagram above are consolidated figures for the fiscal year ending March 31, 2000

Australia
Hitachi Australia Ltd
Brazil
Industrias Hitachi S.A.
Canada
Hitachi Canadian Industries Ltd
China
Fujian Hitachi Television Co., Ltd
Shenzhen SEG Hitachi Color Display Devices Co., Ltd
Beijing Hitachi Huasun Information Systems Co., Ltd
Beijing Hitachi Elevator Service Co., Ltd
Shanghai Hitachi Electrical Appliances Co., Ltd.
Beijing Hitachi Huasun Control System Co., Ltd
Hainan Hitachi Elevator Co., Ltd.
HEMW Hitachi Electric Power Equipment Advanced Technology Development Co., Ltd
Shanghai Hitachi Household Appliances Co., Ltd
Hitachi (China) Ltd
Xian Hitachi Northwest Power Generation Advanced Technology Development Co., Ltd
Changsha Hitachi Automotive Products Ltd
Shanghai Hitachi Electric Home Appliances Co., Ltd
Shengyang Northeast Electrical-Hitachi Power System Ltd
Dalian Hitachi Baoyuan Machinery & Equipment Co., Ltd
Hitachi Semiconductor (Suzhou) Co., Ltd
Shanghai Yungtay Engineering Co., Ltd
Shanghai Hitachi Shuanglu Freezer Co., Ltd.
Hitachi Elevator Engineering Co. (Hong Kong) Ltd
Hitachi Instrument (Suzhou) Ltd
Hitachi Air-conditioning & Refrigerating Product (Guangzhou) Co., Ltd.
Guangzhou Hitachi Elevator Co., Ltd
Xuji Hitachi Electric Co., Ltd.
Hitachi Technology (Taiwan) Ltd.
Kaohsiung Hitachi Electronics Co., Ltd
Taiwan Hitachi Co., Ltd.
Yungtay Engineering Co., Ltd
Power EPC Co., Ltd.
France
Hitachi Computer Products (Europe) S.A.
Germany
Hitachi Semiconductor (Europe) GmbH
India
Dass Hitachi Pte. Ltd
Transformers and Electricals Kerala Ltd.
Hitachi CG Motor Engineering Pvt. Ltd
Amtrex Hitachi Appliances Ltd
Indonesia
P.T Hitachi Consumer Products Indonesia
P.T Hitachi Power Systems Indonesia
Korea
LG Hitachi Ltd
Hyosung Data Systems, Ltd
Malaysia
Hitachi Consumer Products (Malaysia) Sdn. Bhd
Hitachi Semiconductor (Malaysia) Sdn. Bhd.
Hitachi Electronic Products (Malaysia) Sdn. Bhd
Hitachi Air Conditioning Products (M) Sdn. Bhd
Philippines
Hi Eles Industrial Corp
Hitachi Computer Products (Asia) Corp
Hitachi Industrial Machinery Philippines Corp
Russia
Zao-Hitachi Svetlana Power Electronics
Singapore
Hitachi Consumer Products (S) Pte. Ltd
Hitachi Electronic Devices (Singapore) Pte. Ltd
Hitachi Elevator Engineering (Singapore) Pte Ltd
Hitachi Asia Ltd
Hitachi Micro Systems Asia Pte. Ltd.
Hitachi Nippon Steel Semiconductor Singapore Pte. Ltd.
Spain
Hitachi Air Conditioning Products (Europe) S.A
Thailand
Hitachi Consumer Products (Thailand), Ltd
Hitachi Industrial Technology (Thailand), Ltd
Siam-Hitachi Elevator Co., Ltd
Bangkok-Hitachi Elevator Service Co., Ltd
Hitachi Compressor (Thailand), Ltd
Siam Hitachi Automotive Products Ltd
U.K.
Hitachi Home Electronics (Europe) Ltd
Hitachi Europe Ltd
Hitachi Micro Systems Europe Ltd
Hitachi Automotive Products Europe, Ltd
U.S.A.
Hitachi America, Ltd
Hitachi Home Electronics (America), Inc
Hitachi Instruments Inc.
Hitachi Semiconductor (America) Inc
GE-HITACHI HVB, Inc
Hitachi Automotive Products (USA), Inc
Hitachi Computer Products (America), Inc
Hitachi Telecom (USA), Inc
Hitachi Data Systems Corporation
Hitachi Electronic Devices (USA) Inc.

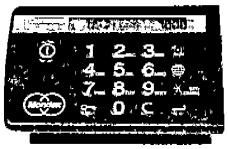
Information Systems & Electronics

The rapid growth of the Internet combined with a rise in electronic commerce has considerably boosted investment in information technology (IT), and steady growth worldwide is anticipated. In Japan, deregulation in the financial and other industrial sectors has led to an increased demand for information systems. Hitachi's experience in systems construction and operation, state-of-the-art networks, open systems and information security technologies will allow us to achieve our goal of being a leader in the information services market worldwide.

Providing systems integration (SI), disk array systems, online transaction processing software, supply chain management and enterprise resource planning (ERP) software, healthcare-related systems, as well as telecommunications, digital media and services, such as electronic commerce, content delivery and outsourcing, Hitachi continues to develop superior products and sophisticated technologies that meet the demands of an increasingly connected global marketplace.

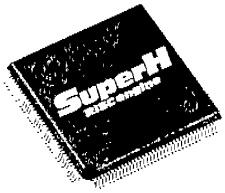


Hitachi's market-leading enterprise server.



The cutting edge of technology: electronic cash systems and devices are transforming monetary transactions around the world.

Note. Mondex is a registered trademark of Mondex International Ltd



Hitachi is a major manufacturer of semiconductors such as this high performance RISC processor.

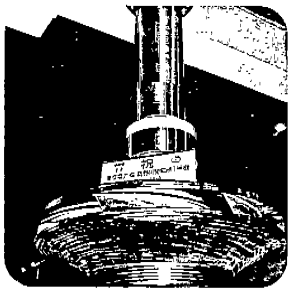
Flexible and efficient, Hitachi's advanced module assembly type contributes to advanced medical systems technology.

Power & Industrial Systems

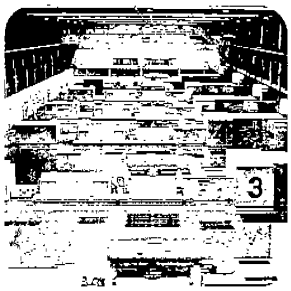
Power Systems and Equipment

Energy is the driving force behind the industrial world, and identifying safer, more efficient resources is vital to our future. Hitachi's cutting-edge technologies and innovations, including the development and manufacture of fuel for use in nuclear-power generation, have led the way in the energy industry.

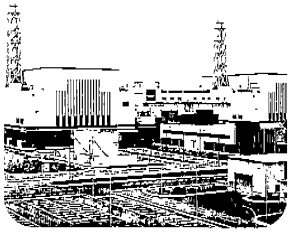
Hitachi is one of only a few companies worldwide that can provide the expertise and total systems needed to cover a whole spectrum of energy needs: nuclear, thermal and hydroelectric power plant systems, as well as the speedy, efficient information system infrastructures needed to compete in a global marketplace. By developing new technologies and streamlining various installation processes, Hitachi will continue to provide new, highly efficient generating systems that meet the energy needs of tomorrow



The runner of a 412,000kW, 728m/778m (world's highest head), 500r/min Francis type pump-turbine for the Kazunogawa Power Station, the Tokyo Electric Power Co., Inc.



The Kawagoe Power Station Unit No. 3 of the Chubu Electric Power Co., Inc. This efficient combined-cycle power generating plant offers advanced thermal capacity to meet the energy demands of the future.



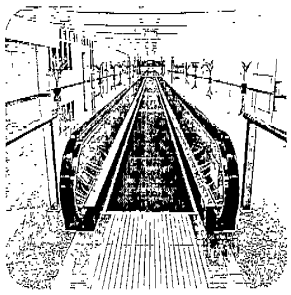
The first ABWR units, Nos. 6 and 7, of the Kashiwazaki Kariwa Nuclear Power Station, the Tokyo Electric Power Co., Inc.

Power & Industrial Systems

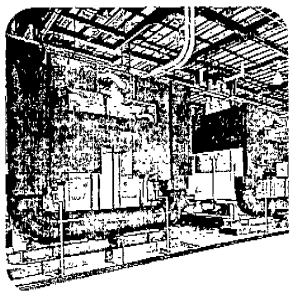
Industrial and Infrastructure Equipment

Supporting the world's infrastructure through advanced technology that maintains and controls transportation, air conditioning, elevators and escalators is one way Hitachi enhances the quality of daily life. In addition, Hitachi technology helps safeguard public health with water treatment facilities and pollution control systems, as well as with the engineering of food processing facilities.

Hitachi's wide range of experience in manufacturing has brought technological advances and greater efficiency to industry as well, in the form of factory automation, computer-integrated manufacturing systems and robots. By applying our far-reaching expertise and environment-friendly technology, we are helping to make the world a safer, more comfortable and efficient place.

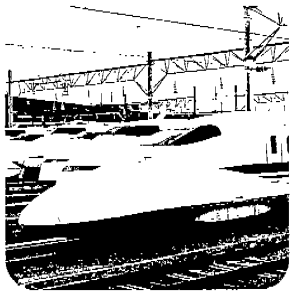


Beijing Capital International Airport (Beijing, China)

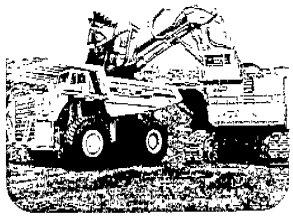


The large-capacity 2,500 USRT (8,790 kW) absorption chiller for the district heating/cooling system in the New Haneda Airport Terminal Building, Tokyo.

Power tools manufactured by Hitachi Koki Co., Ltd., for professionals as well as do-it-yourselfers.



Series 700 Shinkansen train with a 25kV AC electric multiple unit for the Central Japan Railway Company.

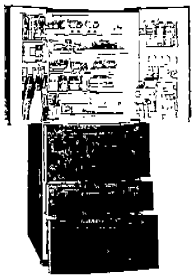


Hydraulic excavator (loading shovel) boasts an operating weight of 515,000 kg (1,140,000 lbs.).

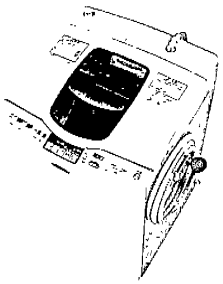
Consumer Products

Hitachi is committed to providing consumers with the best in high-quality, energy-efficient and easy-to-use products. Our expertise in electronics technology enables us to manufacture a wide variety of consumer products with advanced functions and enhanced convenience to suit today's diverse and changing lifestyles. To meet the varied demands and desires of our customers worldwide, Hitachi's designers stay well informed and well aware of consumer preferences and market trends, tailoring a wide array of convenient, energy-saving products that have made total reliability the hallmark of every Hitachi technology.

DVD player and CD recorder



Fast cooling refrigerator-freezer with wide range PAM control system



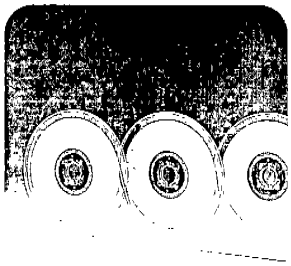
Extra-large capacity washer with PAM control system and water softener

Materials

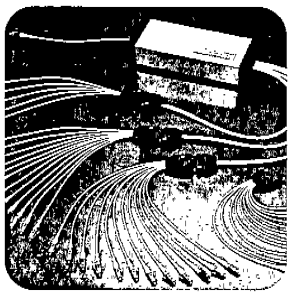
From office equipment and household appliances to heavy machinery and power cables, Hitachi's materials can be found in every facet of society. We also contribute to the service sector in such fields as trading and transport, including international freight shipments and domestic passenger services.

Hitachi is sharpening its competitive edge by expanding in such high-value-added and emerging growth areas as information technology, electronics, telecommunications, the environment and energy. Our industrial proficiency has made us the leader in the specialty steel market. To succeed in an era of global competition, our aim is to continue the development of pioneering materials and components for a wide range of products and services, including semiconductors, computers, automobiles, aircraft, optical fibers and fiber-optic systems.

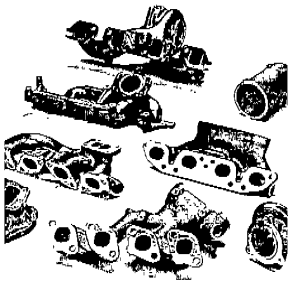
As part of Hitachi's commitment to respond to strong social and environmental needs, we are developing power cables with environment-friendly features. Hitachi will continue to invest in globally strategic products and work to create a cleaner, safer, more efficient world.



Anisotropic conductive film ANISOLM series



AWG (Arrayed Waveguide Grating Filter) is a key component for constructing cost-effective wavelength division multi/demultiplexing systems.



Heat resisting steel and iron castings for exhaust gas related parts

Services & Other

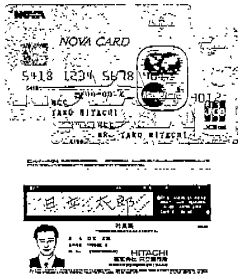
Following are several examples of Hitachi group companies that are active in services and other areas.

Nissei Sangyo, a trading company, utilizes its marketing skills to provide technological solutions and internal management systems. With demonstration centers in Europe, the United States and Asia, the company provides sales support for scientific and industrial systems, aiming to become a "global business creator" in the areas of semiconductors, information and communication technologies, digital media, life sciences, environmental technologies, public-sector operations and import operations.

Hitachi Credit Corporation's traditional core business is in installment credit and leasing arranged through consumer and corporate product vendors. With the establishment of Hitachi Credit Securities Co., Ltd., the company can now offer a full range of services, having expanded into the unique and increasingly specialized business of securitized asset sales. Hitachi Credit Securities Co., Ltd., also handles investment trusts and money management funds

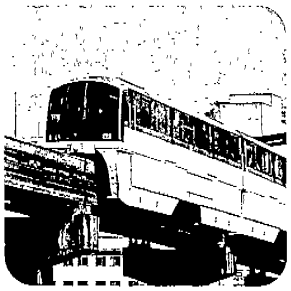
Hitachi Transport System, Ltd., owner of the Tokyo Monorail Co., Ltd., is expert in corporate logistics—freight, outsourced distribution and third-party logistics. The company is now focusing on new growth areas, such as convenience stores and healthcare networks.

Nissei Sangyo's San Francisco office facility with a fully-equipped electron microscope demonstration laboratory.



Hitachi ID Project – using Mondex on MULTOS.

Note: MasterCard is a registered trademark of MasterCard International Incorporated. JCB is a registered trademark of JCB Co.,Ltd.



Straddle-type series 2000 monorail train for the Tokyo Monorail Co., Ltd.

For a Better World

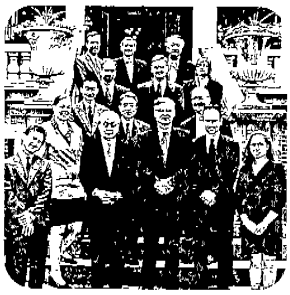
Hitachi believes that a company has a responsibility to serve and enrich society. It has initiated a number of social activities, with six Hitachi-endowed foundations supporting scientific and technological research, education, environmental protection, international cooperation and other worthy causes.

At the Hitachi Young Leaders Initiative (HYLI), an international student forum, potential young Asian leaders gather together to strengthen networks and promote understanding of global issues. The Hitachi International School Teachers' Exchange Program (HISTEP) has been encouraging mutual understanding among teachers at schools in the vicinity of Hitachi facilities in the U.S., Europe and Japan. In Europe, the Hitachi Science and Technology Forum is held to discuss how science and technology contribute to society. Each subsidiary overseas, as a corporate citizen, carries out local grassroots philanthropic activities.

In fiscal year 1999, Hitachi introduced an environmental accounting system designed to promote ecological efficiency and contribute to society by striking a harmonious balance between corporate growth and environmental protection.

Through its continuing support of various projects, Hitachi is helping to weave the fabric of international harmony.

Hitachi brings American and European teachers to Japan on HISTEP to promote international understanding.



Hitachi and the U.S. Council on Foreign Relations (CFR) jointly invite a select group of outstanding young Americans to Japan for an extended period of research or related professional activities.

The 3rd HYLI was held in Malaysia in June 1999, attended by 24 Asian students, with Datin Paduka Zaleha binte Ismail, Malaysian Minister of National Unity and Social Development, as the guest of honor.

The 3rd Hitachi Science and Technology Forum held in Ireland in May 2000 focused on "Electronic Commerce and Its Impact on Society."

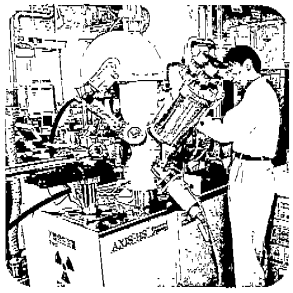
Research & Development

Creativity and innovation provide the foundation for all of Hitachi's research and development activities. We have always focused on R&D as a driving force for ensuring our business competitiveness.

Hitachi researchers are engaged in a wide range of ongoing studies in the fields of electronics, telecommunications, software, energy and new materials. In 1999 alone, we allocated some US$4,079 million for R&D, representing 5.4% of our total sales.

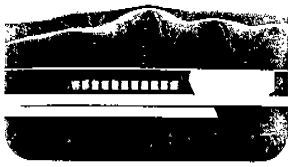
Hitachi has established R&D centers in Europe and the United States, which are geared to developing products best suited to local needs and that create seeds for the future.

By establishing Hitachi Research Visit Programs and hosting international conferences, we have also demonstrated our strong support for international collaboration in R&D. In addition to cooperating with other nations, Hitachi has enthusiastically pursued R&D alliances with the world's leading companies.



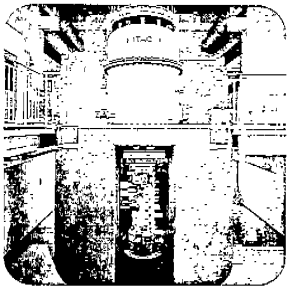
Hitachi's advanced lithium battery has been developed for various products, including dispersed type battery energy storage systems and electric vehicles.

Note: This work has been supported by New Energy and Industrial Technology Development Organization (NEDO)



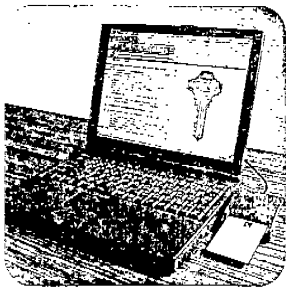
Perpendicular magnetic recording system with areal recording density of 52.5 Gbits/in² (8.14 Gbits/cm²).

Note: This work has been supported by New Energy and Industrial Technology Development Organization (NEDO)



World's most powerful 1-MV field-emission transmission electron microscope reveals rows of gold atoms just 49.8 pm apart—the world record for resolution.

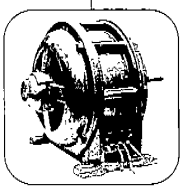
Note: This work has been supported by Japan Science and Technology Corporation (JST)



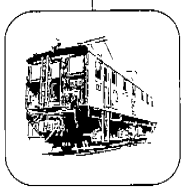
Hitachi's advanced technology ensures security in e-commerce, digital satellite broadcasting, IEEE home networks, etc.

History

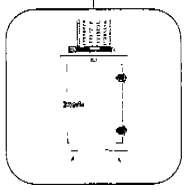
1910



1924



1932



1958

1970

1910
- Founded by Namihei Odaira as an electrical repair shop
- Succeeded in first domestic manufacture of three 5hp (3.6775 kW) electric motors as the company's first products

1911
- Completed 2 kVA transformer

1914
- Began manufacture of alternating current galvanometers and voltmeters

1915
- Completed 10,000hp (7,355kW) water turbine

1916
- Began manufacture of electric fans

1924
- Completed the first large-scale DC electric locomotives to be manufactured in Japan

1930
- Began the manufacture of pole-mounted transformer

1931
- Completed 10,000 A hydraulic electrolytic cell

1932
- Began the manufacture of elevators
- Completed Hitachi's first electric refrigerator

1933
- Completed 23,600hp Ilgner set

1940
- Completed an automatic telephone exchange with 5,000 lines

1943
- Completed 85,000 kW Francis water turbine and 70,000 kVA alternating current generator

1949
- Completed Hitachi's first power shovel

1951
- Completed 6,500 kW Kaplan turbine and 7,000 kVA alternating current generator

1952
- Completed 21,000 kW two-stage pump-turbine

1953
- Completed low-pressure 300m³/h air separator

1954
- Completed the first large-scale cold strip mill to be produced in Japan

1955
- Completed 100,000kW Francis water turbine and 93,000 kVA alternating current generator

1956
- Hitachi Cable, Ltd and Hitachi Metals, Ltd established
- Completed Japan's first diesel electric locomotive

1958
- Electron microscopes awarded the grand prix at the World Exposition in Brussels
- Completed 6-transistor portable radio

1959
- Completed electronic computers based on transistors
- Hitachi America, Ltd established

1961
- Developed fully automated washer
- Completed experimental nuclear reactor

1962
- Hitachi Chemical Co., Ltd established

1963
- Completed 265,000 kW impulse reheating-type, cross-compound turbine
- Released the first large-scale computer developed exclusively with Hitachi's own domestic technology

1964
- Completed the first cars for the Shinkansen (Bullet Train)
- Developed train seat reservation system
- Manufactured monorail running between Haneda Airport and Hamamatsu-cho, Tokyo

1965
- Began mass production of color television tubes using rare earth phosphor material

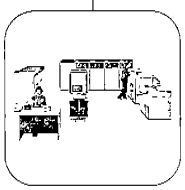
1966
- Developed LTP processing of a silicon transistor

1967
- Developed dry-type room air conditioner

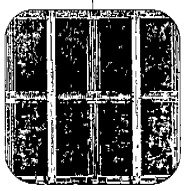
1968
- Developed hybrid LSI
- Developed computer for controller's use
- Developed 300m/min elevators for high-rise buildings

1969
- Completed on-line banking system
- Developed and mass-produced all-transistor color televisions
- Developed audio system with two-way speakers

1974

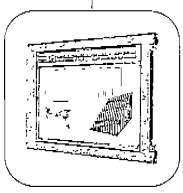


1984

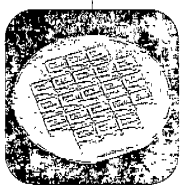


1991

1995



1998



1970
- Developed computer-aided traffic control system for the Shinkansen (Bullet Train)
- Completed prototype of visual information processing robot

1971
- Completed file storage device with 1GB capacity

1972
- Developed ionized semiconductor element

1973
- Developed new heat-resistant insulating materials
- Developed new-type image pickup tube

1974
- Commercial operation began at Japan's first 460,000 kW nuclear power station
- Completed automated semiconductor assembly (LSI, transistor wire bonding)
- Released the first series of general-purpose large-scale computers

1975
- Developed high-performance heat transfer tube
- Hitachi High Crown Control Mill developed

1976
- Succeeded in the world's first experiment of fiber optic communication systems

1977
- Developed high-speed amino-acids analyzer
- Construction of "FUGEN," the prototype of a new converter reactor

1978
- Completed world's first field emission electron microscope with record-high resolution
- Experimental color camera with solid-state miniature image device developed
- Released the world's largest and fastest computer at that time

1979
- Completed world's first puffer type, 1-cycle gas circuit breaker prototype

1980
- Completed 300 MW high-voltage direct current transmission between Hokkaido and Honshu
- Completed nuclear fusion equipment

1981
- Developed magnetic recording video camera
- Established color picture tube dry process technology

1982
- Hitachi Europe Ltd. established
- Succeeded in world's first micro-level observation of magnetic field by the use of electron beam holography
- Hitachi's first supercomputer announced
- Listed on New York Stock Exchange

1983
- Hitachi Australia Ltd. established
- Manufactured 1-megabit high-speed CMOS mask ROM
- Developed air conditioners with scroll compressors

1984
- Completed Japan's first model of improved standard-type boiling water reactor
- Started mass production of 256-kilobit DRAMs

1985
- Completed the "JT-60" large-scale Tokamak device for break-even plasma experiments
- Developed CAD/CAE systems with high-definition color displays
- The Hitachi Foundation was established to promote cultural, educational and scientific exchanges between Japan and the U.S.
- Released the first large-scale computer with fully applied LSI

1986
- Completed scanning electron microscope that can record electron spin

1987
- Put fuzzy control to a practical use
- Completed rear-projection large liquid crystal color display

1988
- Developed basic technology of neural network
- Developed 4-legged robot
- Design Center upgrade brings corporate laboratory count to nine
- Hitachi Asia Pte. Ltd. established

1989
- Developed world's fastest superconductive computer
- Developed superconductive MR imaging equipment
- Established two R&D centers in the U.S. and two laboratories in Europe

1990
- Developed high-definition TFT color liquid crystal display
- Developed an experimental 64-megabit DRAM
- Released very large-scale computer with the world's fastest processing speed at that time

1991
- Developed inverter-controlled electric locomotive with the world's largest control capacity
- Developed highly sensitive image pickup tubes

1992
- Completed system for 500kV transformer substation
- Developed personal facsimile
- Developed atomic observation and manipulation technology using scanning tunneling microscope

1993
- Completed high efficiency nuclear power plant with reheating system
- Developed Shinkansen (Bullet Train) with new maximum service speed of 270 km/h
- Succeeded in observation of single-electron memory motion at room temperature

1994
- Hitachi (China), Ltd. established
- Developed the original 32-bit RISC processor SuperH family
- Developed the brand new ATM which enables bills to be pressed and disinfected

1995
- Developed the experimental 1-gigabit DRAM chip
- Developed Super TFT LCD module featuring ultra-wide viewing angles
- Developed 10 Gbit/s fiber optic transmission equipment

1996
- Developed electronic commerce-related products
- Developed MPEG camera

1997
- Developed contactless IC card system
- Developed rewritable, large capacity DVD-RAM drive

1998
- Developed 320 Gbit/s optical data transmission system
- Developed the experimental 128-megabit single-electron memory
- Developed PAM control refrigerator/air conditioner

1999
- Developed phase-state low electron-number drive memory
- Put manganese secondary lithium battery to a practical use
- Established dependable autonomous hard real-time management technology

HITACHI
Inspire the Next

Printed in August 2000
Printed in Japan (H) **GM-E131** 0800