



# Open Systems Standards Tracking Report

Newsletter on Information Technology and Telecommunications Standardization  
Volume 8, Number 3, March 1999

## *A Wearable Computer MAC and PHY Layer Standard*

# *Progress Report: IEEE 802.11 Wireless Personal Area Network Study Group*

by Dick Braley and Ian Gifford

[Dick Braley is Chairman of the IEEE 802.11 Wireless Personal Area Network (WPAN) Study Group, and Manager of Systems Design and Development in the Courier Technology Department at FedEx in Memphis, Tennessee, U.S.A. He initiated the WPAN standards development activity within the IEEE in 1997 and has played a key role in championing the WPAN efforts within the 802.11 Working Group. At FedEx, his primary responsibilities are in the wireless systems development area, developing wearable computing system networking for support of courier technologies and providing a wide range of wireless technologies to help differentiate FedEx from its competitors. Dick may be reached via e-mail at [rcbraley@fedex.com](mailto:rcbraley@fedex.com). Ian Gifford is Technical Editor and Secretary of the IEEE 802.11 WPAN Study Group and Manager of Standards at M/A-COM, an AMP Division, in Lowell, Massachusetts, U.S.A. He has played a key role in driving the WPAN efforts within the 802.11 Working Group. At AMP, Ian's primary responsibilities are in the M/A-COM Business Development and Technical Marketing Group with a primary focus in the Wireless Systems area on Wireless LANs and Wireless WANs. Additionally, he is active in the IEEE and other organizations such as TIA, Committee T1, and ITU-R. Ian may be reached via e-mail at [giffordi@amp.com](mailto:giffordi@amp.com).]

This article provides an update on the development of standards for wireless personal area networks (WPANs), which provide interconnectivity between devices that constitute "wearable computing" systems as well as access to gateways for wider area networks. For background information on the wearable computer environment, including a historical overview of the IT industry and wearable computers, see the September, 1997, *Open Systems Standards Tracking Report* article "Paradigm Shift in Computing: Wearable Computers," authored by Dr. Dan Siewiorek, and available at <http://www.digital.com/info/osstr/tr0997.htm#A2>.

## History of IEEE 802.11 WPAN

The IEEE Ad Hoc "Wearables" Standards Committee was initiated by Dick Braley in June 1997 during an IEEE Standards Activities Board (SAB) meeting. According to Braley, the purpose of the Committee is to "encourage development of standards for wearable computing and solicit IEEE support to develop standards." The consensus recommendation to Braley from those that attended the SAB meeting was that he bring his request to encourage such standards development to the IEEE PA.

During the IEEE Portable Applications Standards Committee (PASC) Plenary in July 1997, an IEEE Ad Hoc Committee was assembled (17 attendees) to discuss "Wearables" Standards. The Committee identified several areas that could be considered for standardization, including:

- Personal area networks [PANs] (zero-range to micro [~5 meters] – capacitive, IR, RF)
- Peripherals
- Nomadicity (5 meters+)
- Wearable computers (CPUs, operating systems, related systems)
- Power/battery (power-saving in other systems/communications)

The committee determined that the best area of focus was the PAN area or Wireless PAN. The IEEE Ad Hoc "Wearables" Standards Committee met twice more – once in December 1997 and again in January 1998. During the January 1998 meeting, it was decided to send two delegates to the IEEE 802.11 Interim Meeting that was taking place that same month. During the IEEE 802.11 Interim

## In This Issue ...

In this issue of the *Open Systems Standards Tracking Report*:

- Progress Report: IEEE 802.11 Wireless Personal Area Network Study Group
- JTC 1 Update
- The Global Standards Mandate: What Global Businesses Are Doing About It
- The Key Recovery Alliance: Building on Past Successes

Meeting, the idea of presenting a Tutorial at the March 1998 802 Plenary was confirmed. Forming a Study Group was the next step, and in March 1998, the "Wearables" Standards Ad Hoc Committee became the IEEE 802.11 Wireless Personal Area Network (WPAN) Study Group.

## The WPAN Study Group

The *scope* of the IEEE 802.11 Wireless Personal Area Network (WPAN) Study Group is to define derivative versions of the 802.11 physical (PHY) layer and medium access control (MAC) layer specifications for wireless connectivity with fixed, portable, and moving devices within or entering a personal operating space (POS). A personal operating space (POS) is the space about a person that typically extends up to 10 meters in all directions and envelops the person whether they are stationary or in motion.

The Group's *purpose* is to provide a supplemental standard for low complexity, low power consumption wireless connectivity to support interoperability among devices within or entering the POS. This includes devices that can be networked, such as computers, personal digital assistants (PDAs)/handheld personal computers (HPCs), printers, microphones, speakers, headsets, bar code readers, sensors, displays, pagers, and cellular and personal communications service (PCS) phones that are carried, worn, or located near the body.

A goal of the WPAN Group is to achieve a level of interoperability sufficient to transfer data between a WPAN device and an 802.11 device. The 802.11 PHY and MAC have been reviewed to determine their suitability to meet the functional requirements of the WPAN applications.

The IEEE 802.11 WPAN activities are focused on standards that will be derivative versions of the 802.11 PHY and MAC layer specifications for wireless local area networks (WLANs).

## WPAN Model

The WPAN usage model is still being defined. To establish the WPAN Functional Requirements through group consensus, the Study Group continuously edited a single document – 98/160r2 – over the course of several meetings. The following is a list of functional requirements, broken down into three groups, sorted in order of importance A through C. The fourth group is a group of miscellaneous requirements that were considered, but not prioritized into a specific level of importance.

### Group A Functional Requirements:

- Worldwide spectrum allocations for unlicensed bands such as 2.4GHz
- Low cost, that is, relative to target device
- Small size, for example, ~.5 cubic inches, excluding antenna and battery
- Very low current consumption, for example, average 20mW @ 10/90 or less
- Data
- Allow coexistence of multiple wireless PANs in the same area (20 within 400 square feet)
- Allow coexistence of multiple wireless systems, such as P802.11, in the same area
- WPAN Network Access Control

### Group B Functional Requirements:

- Delivered data throughput at the MAC SAP: (19.2 - 100) kbit/s (actual 1 device to 1 device)
- Ability for all devices within a WPAN to communicate with each other
- Networking support for a minimum of 16 devices
- Voice
- Range of 0-10 meters
- Attach within one (1) second, once within range
- Bridge or gateway connectivity to other data networks

### Group C Functional Requirements:

- No single element of failure
- Video
- Roaming ability to hand-off to another PAN

### Miscellaneous Functional Requirements:

- WPAN density: One WPAN in 2 square meters, average density at acceptable [TBD] performance levels
- Power Consumption: Each WPAN device consumes less than 20 mW long term average [TBD] given a 10% TxRx load in the WPAN

## IEEE 802.11 WPAN Activities

Since its formation in March 1998, the IEEE 802.11 Wireless Personal Area Network Study Group has met during all 802.11 Working Group meetings, as well as three times in an independent session. Although the Study Group was originally chartered from March 1998 to July 1998, it has been rechartered twice, from July 1998 to November 1998 and November 1998 to March 1999.

One of the Study Group's goals is to seek industry input on market requirements and technical solutions for a WPAN with 0 to 10 meter range, data rates of less than 1 Mbit/s, low power consumption, small size less than 0.5 cubic inches, and low cost relative to target device. To assist in meeting this goal, Study Group members identified a number of groups with whom they felt they should establish a liaison relationship. The following were some of the groups contacted in early June 1998:

- ATM Forum, Wireless ATM (WATM) Working Group
- Bluetooth Special Interest Group (SIG)
- ETSI, Broadband Radio Access Networks (BRAN) Project
- Home Radio Frequency Working Group (HRFWG)
- Infrared Data Association (IrDA)
- Internet Engineering Task Force (IETF), MobileIP Working Group
- Wireless LAN Alliance (WLANA)

To date, the two liaisons that have produced the most Study Group submissions and discussions are Bluetooth and HomeRF.

- **HomeRF Working Group** - The Study Group has recently received information that the HomeRF Lite (HRF-Lite) Subcommittee Marketing Requirements Document (MRD) rev. 0.3 will be revised at the February 1999 HRF-Lite Meeting. The current plan is to have the HRF-Lite specification v1.0 be available at the end of 1999. It is generally believed that the HRF-Lite activity will result in a WPAN specification.
- **Bluetooth Special Interest Group** - The Study Group is assisting the SIG to prepare an IEEE 802 Tutorial for the March 1999 Plenary in Austin, Texas, U.S.A. It is generally believed that the Bluetooth activity will result in a WPAN specification.

## Current Status of the WPAN Study Group

Within the IEEE, a standards project does not officially exist until a Project Authorization Request (PAR) is approved. The WPAN PAR is the official document that will authorize work on the PAN standard project in the IEEE. PARs are approved by the IEEE Standards Board based on a review and recommendation from the New Standards Committee (NesCom), one of several Board committees.

The WPAN PAR and another document called the Five Criteria are in process and will be submitted to the March 1999 802 LMSC Plenary for review and disposition.

The IEEE 802.11 Working Group circulated Letter Ballot 16 between the November 1998 Plenary and the January 1999 Interim Meeting. Motion 3 of this ballot, which was submitted by the WPAN Study Group, read: "To submit the contents of documents IEEE 802.11-98/161-r4 and -98/162-r7 to Executive Committee. Motion 3 was passed with 60/14/4 or 81%. WPAN's PAR and 5 Criteria."

Therefore, during the January 1999 Study Group session, the group agreed to submit the WPAN's 5 Criteria -98/161-r4 and PAR -98/162-r7 documents to the Executive Committee on or before the February 8, 1999 deadline. During the session, the WPAN Study Group agreed to provide Executive Committee and 802.11 Working Group with the following recommendation:

"The WPAN Study Group recommends that it become a Task Group of 802.11 with the understanding that this will likely require a change in the 802.11 charter and a rule change within 802 to allow multiple MAC Layers within a Working Group. The motivation for becoming a Task Group within 802.11 is to ensure the best use of a shared media. If this is not feasible, the SG recommends the formation of a separate Working Group under 802 that would include all PAN related activity including Bluetooth, HomeRF, and others, should they also submit PARs."

Finally, during the January 1999 IEEE 802.11 Interim Meeting in Orlando, Florida, U.S.A., the Working Group approved a motion to recirculate a revised Project Authorization Request and Five Criteria document, via a WG Letter Ballot, to try and resolve all of the No comments. The results of this recirculation ballot will be made available after March 3, 1999.

## Additional Information is Available

More information and complete background on the IEEE 802.11 Wireless Personal Area Network Study Group can be found at <ftp://ftp.flexipc.com/wearablesgroup/Index.htm>.

Additionally, there are numerous advances being made on wearable computers, nomadicity, and other related areas. Information on these advances, such as the standards (higher layers) work being done in the Internet Engineering Task Force (IETF) Mobile IP Working Group, may be of interest, specifically the recently received Cellular IP draft, which can be viewed on the Web at <http://www.ctr.columbia.edu/~andras/cellularip/draft-valko-ellularip-00.txt>. A second draft that may be of interest is the UMTS/IMT-2000 and Mobile IP/DIAMETER Harmonization draft that may be readily found at <http://search.ietf.org/internet-drafts/draft-gustafsson-mobileip-imt-2000-00.txt>.

These drafts both indicate wide area gateway issues that may be of interest to networked WPANs with data and voice traffic for the PSTN and/or Internet. Finally, the Second International Symposium on Wearable Computers (ISWC98) held in October 1998 provided those interested in "Wearables" a chance to learn about the progress being made in Industry. The Third ISWC (ISWC99) is scheduled for October 18-19, 1999 in San Francisco, California, U.S.A. General information about ISWC99 may be found at <http://iswc.gatech.edu/>.

## Conclusion

Dr. Siewiorek stated in his September 1997 article that one of "...the goals of wearable computing is to provide 'the right information to the right person at the right place at the right time.' The average person should be able to take advantage of the information on or off the job. Mobile access is the gating technology required to make the World Wide Web available to anybody at anyplace at any time."

The WPAN Study Group generally agrees with Dr. Siewiorek, however, the IEEE 802.11 Wireless Personal Area Network Study Group is trying to identify a new mobility domain. We agree that Wearable computers will need a "wireless internet" for WWW access; but there is also a need for a "wireless intranet" for wearable and handheld computing and communicating devices to network, unobtrusively, the growing number of peripheral devices we carry with us on a day to day basis.

The Study Group started out trying to identify an existing standard that would meet the WPAN application. As of this writing, the group has not found a standards-based MAC and PHY Layer to use as-is. Therefore, we look forward to PAR approval and our derivative work as well as reviewing the Bluetooth Specification v1.0 during the Spring of 1999 and the HRF-Lite Specification that is likely to be ready in the winter of 1999.

---

---

# JTC 1 Update

by Scott Jameson

*[Scott Jameson represents Compaq Computer Corporation in the U.S. Technical Advisory Group for JTC 1, where he serves as Chairman. He was the Head of Delegation from the United States to the recent ISO/IEC JTC 1 Plenary meeting. Scott also represents the corporation in NCITS, the National Committee for Information Technology Standardization, and several of its management committees. He may be reached by e-mail at [scott.jameson@compaq.com](mailto:scott.jameson@compaq.com).]*

JTC 1, the Joint Technical Committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) for Information Technology standardization, held its thirteenth Plenary meeting in Rio de Janeiro, Brazil, in mid-February. This was the first meeting under the leadership of Thomas Frost of AT&T, who was recently approved as Chairman by the ISO Council.

JTC 1 has traditionally met approximately every nine months to review the progress of work within its Subcommittees (SCs) and to consider issues that affect broad areas of international standardization. The primary focus of this meeting was the review of two processes that had been undergoing trial use: the PAS process and the Business Team concept.

## Review of the PAS Process

The trial period for the Publicly Available Specification (PAS) process concluded at the end of 1998. To date, the trial period has resulted in eight authorized PAS Submitters, one successful transposition of a PAS into an International Standard (IS), and one PAS submission currently being balloted for approval as an IS. While this initial PAS activity was less than expected, JTC 1 felt that it had sufficient experience to evaluate the results. A JTC 1 ad hoc meeting was held in October 1998 to consider the comments on the process and make recommendations for JTC1's consideration at this Plenary.

The ad hoc meeting's recommendations addressed several areas. First, the PAS process, as described in the PAS Management Guide, was revised to make the timing of certain events and the criteria for approvals more explicit. In particular, a newly recognized PAS Submitter must make its first submission within 6 months after the recognition is granted. Other recommendations dealt with how the new process would be applied to the currently recognized Submitters. While they are encouraged to follow the revised process with any new submissions, their current status is unaffected. When existing submitters requalify, they must do so according to the new rules. Other recommendations dealt with enhancing the process and better integrating it into JTC 1. They include devoting more Plenary time for the submitters to report to JTC 1 and share their experiences among themselves and with JTC 1. Finally, it was recommended that JTC 1 more actively promote its PAS process and its successes.

JTC 1 agreed with these recommendations and resolved to conclude the PAS trial period and make the PAS process, as revised, an integral part of JTC 1 operations.

## Business Teams

JTC 1 had also been conducting a trial on the use of Business Teams, a mechanism that could be used to rapidly identify standardization needs in a particular technology area. At its June 1998 Plenary, JTC 1 accepted the report of its Electronic Commerce Business Team. The second Business Team, on Imaging and Graphics, reported at this meeting. Following these reports, JTC 1 reviewed the effectiveness of the Business Teams and observed they had, to at least a limited extent, met their objectives and identified areas where further standardization was required. The attendees at the Brazil meeting did

express some frustration that the recommendations had not yet been picked up by the Subcommittees, where the standards would actually be developed, but concluded this was not the fault of the Business Teams. Given these results, JTC 1 affirmed the use of Business Teams as a tool to identify areas of new work.

## New Directions for JTC 1

JTC 1 made a number of operational changes at this meeting. These were largely driven by the Chairman's initiatives to maintain JTC 1's relevance to the market. One mechanism intended to accomplish this is to keep the participants at the JTC 1 management level, the National Bodies present at the Plenary, better apprised of the technical work under development within the JTC 1 structure. To this end, significantly more time at future meetings will be devoted to discussions with SC Chairpersons. It is envisioned this extended dialogue will allow JTC 1 to have a better understanding of the standards being written in the SCs, the anticipated users of the standard, and the expected impacts on the marketplace. It is hoped that JTC 1 can provide insights to the SCs, based on its broad view of its program of work, and this improved interaction will be beneficial to all.

JTC 1 also agreed it needed to better understand some trends that reflected the overall health of the organization. It looked at some statistics that indicate that while the number of published standards has been increasing on an annual basis, the number of new projects has not. If this trend continues, eventually JTC 1 would complete all of its projects and have no new development activities. This analysis led to a determination to monitor these statistics on a regular basis, as well as the initiation of some activities intended to promote JTC 1 to attempt to attract new development work.

These new operational methods will be put into place at the next JTC 1 Plenary, taking place in Seoul, Korea, in November 1999.

## Summary

The 13<sup>th</sup> annual plenary of JTC 1 concluded with the resolution that the revised PAS process will be an integral part of JTC 1 operations. JTC 1 also affirmed the use of Business Teams as a tool to identify areas of new work. New operational methods that are designed to encourage additional JTC 1 development activities will be implemented in at JTC 1's next plenary in November.

---

## *Industry Cooperation for Standards and Conformity Assessment (ICSCA) Shares A Vision*

# *The Global Standards Mandate:*

# *What Global Businesses Are Doing About It*

by Henry Line

[Henry Line has been involved with various aspects of standards development for more than fifteen years. He recently completed 22 years with AMP, Incorporated, in Harrisburg, Pennsylvania, U.S.A., where he served as Vice President of Global Product Standards. Henry has authored several papers on the importance of standards and strategic standards management, many of which have been presented at conferences and have been published in standards journals, as well as in *Focus* and *Fortune* magazines. He is an advocate of the positive role that the U.S. voluntary consensus standards system can play in improving the educational preparedness of our nation's workforce. Henry is an active member and Co-Chairman of the Industry Cooperation for Standards and Conformity Assessment (ICSCA). He also serves as a vice chairman and a member of the board of directors for the American National Standards Institute (ANSI) and is on the Board of Directors of the American Society for Testing and Materials (ASTM).]

In free societies, the mainspring of human progress has been the indomitable ability of man to turn his creativity and energies into better ways of accommodating the needs and wants of society. We owe our standard of living solely to the unfettered

development and implementation of technology. Nothing drives the point home better than studying the timeline of basic technology. From the discovery several thousands of years ago that the addition of straw makes bricks stronger to mankind's astounding successes to

tame space or dramatically improve his condition by advancing the front of medical science, it is fascinating to trace mankind's advances over time.

Under any circumstances these milestones would be noteworthy, but to a capitalist society they are especially important. Each major new advance of technology brings with it answers to the questions of how the many needs of the current and future generations will be satisfied – of how the next round of wealth will be created. As the basis for economic (and, therefore, societal?) progress, the impact of technology on mankind has likely been far more profoundly felt in recent years (it is not important to choose a date) than by those of just a few generations ago. A good measure, were such statistics ever developed, would be the longevity of these advances in technology and of the businesses they create. To this point, it has been reported that the average life expectancy of Fortune 500 companies, from birth to death, is between 40 and 50 years. It follows that in a high-tech, highly competitive environment, companies failing to make this list may well be even more short lived. Accordingly, the companies that best take advantage of the opportunities to participate in industry standards development have distinct advantages over those that leave the work to others.

The key factors for the success of a manufacturing company can be distilled down to a very few basic requirements – produce a product that satisfies market requirements, deliver it in a timely fashion at a competitive price, and provide it with a level of quality that satisfies customer requirements. Companies have many (usually too many) criteria to which they measure themselves on how well they do these things.

Most often these measures take the form of some ratio, return on assets, return on equity, sales per employee, and the like. Most are some measure of revenue divided by some investment or cost. In most cases, the measure is improved by increasing the numerator of the ratio (revenue), and reducing the denominator (cost). The point to this all-too brief discussion is that standards have a profound influence upon both elements of these measures.

Those with only a cursory knowledge of standards will understand that if a company can successfully introduce its technology into new industry product standards, the state-of-the-art documents defining the requirements for today's high-tech products, it will enjoy a first-to-market advantage in the marketplace. Up goes the numerator. Similarly, those companies that successfully use standards to reduce their costs of operation will find an edge, or at the very least, achieve parity with an equally cost-conscious competitor. Down goes the denominator, and up goes the performance of the ratio. Standards professionals recognize these two attributes of standards – their ability to both enhance revenues and lower operating costs – as absolutes. It is also generally accepted among most standards professionals that their greatest inadequacy is their inability to make CEO America aware of the fundamental importance of standards to the success of their companies. Upper management is disengaged from the process and remains so at their own peril.

## Impact of Globalization and Market Convergence

The challenges to business of the past several years aggravate the matter of standards significantly. Two hugely important phenomena are taking place that have dramatically altered how companies transact business and where they must transact it. Both are grounded in new implementations of technology, in particular, semiconductor, computing software, communications, and transportation.

The first of these is the globalization of business and the second is the convergence of previously disparate markets – both technologically

and economically. No longer is it possible for companies to assure their survival by confining their operations solely within their own borders. And no longer is it possible to assume that the demographics of the company's market are the same as they were just a few years ago. For example, who today can clearly differentiate among the computer, telecommunications, desktop publishing, or even the consumer products marketplaces? Most critical to the market convergence phenomenon is the need for an ongoing, thorough understanding of the competitors participating in the company's market, with emphasis upon how they are changing, especially with regard to new offshore entrants. The emergence of huge global companies, marked especially by dramatic increases in global mergers and acquisitions, is another clear response to these global urgencies.

## Standards: Their Role in Assuring Corporate Survival

In the final analysis, the new global competitive dynamics do not change the company's most basic mandates for addressing them. Perhaps the margin for error has been reduced. It remains true that the key factors for success are those that we have mentioned previously – understand and address customer requirements more effectively than the competitor and rid the enterprise of all nonvalue-adding costs. What is different, however, is the role that standards now play in corporate survival. There is no better vehicle than standards for accommodating the needs of converging global markets, for enabling the rapid implementation of technology, and for reducing nonvalue-adding costs.

Only through the use of standards can the requirements of interconnectivity and interoperability be assured and the credibility of new products and new markets verified. Two examples outside the area of information technology help illustrate the point:

Automobile manufacturers that produce cars in one country for sale (and service) in another, or that produce engines in one country for use in automobiles in another country, need standards. These standards are necessary to ensure that *all* the components meet *all* the requirements of *all* the countries that are involved with the production and use of these automobiles. Likewise, the Boeing Aircraft Company in Seattle, Washington, U.S.A., which assembles aircraft from components produced all over the world, depends on standards to ensure that these components meet international requirements. It goes without saying in both of these examples that another critical purpose of standards is to ensure the components fit together properly.

These examples, and countless others that could be cited, prove the point and also highlight the importance for companies to get involved with standards setting at both the national and international levels.

## Some Standards-driven Requirements May Not Add Value

It is also very important for companies to understand that they have been, or could be, confronted with standards-driven requirements that might not add value to their products, their operations, or to their customers. Very often the problems are not with the standards themselves, but with the requirements that so often accompany them for demonstrating conformance to those standards. These include such things as nonvalue-adding marking requirements, lack of transparency among laboratories requiring duplicate testing, mandatory third-party certification, and the like. Mandatory third-party certification is particularly nettlesome to global businesses. The most troublesome of these requirements are those that advanced the management system certification schemes such as ISO 9000 (Quality Management),

ISO 14000 (Environmental Management), and several others that have been proposed.

While many companies point to the value they have received from implementing these standards, many more are just as adamant in their belief that no external certifier can better demonstrate compliance to these standards than the companies themselves. While these companies encourage the use of third-party certification by those who choose to use it, they resent having it imposed upon their operations when they can demonstrate that doing so adds no value. Companies have the same reaction to unnecessary marking requirements, duplicate product testing, or to any imposition of unnecessary costs that could threaten their ability to compete effectively. As before, the solution is the same. Companies must be a part of the standards process where these requirements are articulated or they risk being a casualty of it.

## The Industry Cooperation for Standards and Conformity Assessment (ICSCA)

It is against this backdrop of the rapid implementation of technology and the implementation of standards requirements that provide questionable value that the ICSCA was formed. Founded in 1996 in Geneva, Switzerland, this global body comprises industry standards executives and other high level professionals who share a vision of increased trade and commerce through the appropriate application of global standards. Fundamental to the group, now over 50 companies strong and including leaders in global standards development, is the principle that all standards should add value to the products and processes affected by them, and, especially, to customers. The ICSCA is a forum to coordinate industry viewpoints on behalf of strengthening international standardization and its relevance to the facilitation of global trade and business. There is no charter, nor are there bylaws or dues. The only prerequisites for membership are that members must be product producing companies, or industry associations of such companies, who agree to promote the resolutions of the group.

### ICSCA's Resolutions

ICSCA held its fourth annual meeting in January 1999 in Boca Raton, Florida, U.S.A.. Among the many resolutions adopted or reaffirmed at this meeting by the ICSCA members were the following:

- To promote the use of global standards.
- To oppose mandatory third-party certification requirements and management system certification standards that are not customer driven or that would otherwise add no value.
- To affirm the supplier's declaration of conformance as the preferred method of demonstrating conformity while preserving third-party certification for those suppliers who choose to use it.
- To promote voluntary private sector standards as preferred alternatives to government agency developed standards or regulations.
- To support efforts at all levels, including the IEC, ISO, and ITU, to develop standards faster, better, and at lower cost.
- To populate the standards developing committees with the right technical experts.
- To encourage participation by the company's executive management in the process.

## Conclusion

As never before, standards are influencing the success of companies – both as determinants in the ability of companies to penetrate new markets and as tools to control (or, add to) costs in company operations. To advance their interests, companies, including those at the executive level, must get involved in the standards developing process. Not doing so abdicates decisions regarding new product requirements and operating costs to the competition, more and more of which is coming from abroad. The standards fora exist wherein companies can make their voices heard. These include the standard developing committees, industry associations, the ICSCA, the American National Standards Association, and the many hundreds of technical committees of the IEC, ISO, and ITU.

There is no question that appropriate participation comes at a cost that is not inconsequential. However, a never-ending stream of company case studies, many of them describing lessons learned the hard way, demonstrates that these costs pale in comparison to the costs that are a consequence of not being at the standards table when the decisions are made.

---

# The Key Recovery Alliance: Building on Past Successes

by Bob Frith

*[Bob Frith is the President of the Key Recovery Alliance. He is the Manager of Standards Strategy and Development for the Information Security Systems and Products Division (ISSPD) of Motorola, Incorporated, in Scottsdale, Arizona, U.S.A., where he has held a number of marketing positions within this division. Before joining ISSPD, Bob's previous assignments were within Motorola's IT organization. Bob may be reached via email at bfrith@mot.com.]*

Comprised of over thirty leading international companies that are involved in information security, both as suppliers and major users, the Key Recovery Alliance (KRA) is working together to facilitate the worldwide use of strong encryption. Since its formation in October 1996, the Alliance has provided value to industry by focusing on the identification of major barriers to the development of marketable key recovery products and services and, as appropriate, proposing solutions.

## KRA Background

The KRA came about in response to several market events. Companies in the United States, Europe, and Japan that were beginning to deploy strong cryptography began to recognize their information was subject to risk in the event that decryption keys were lost, damaged, or unavailable. Additionally, some governments were considering regulations that would have made key recovery a requirement for the use, import, or export of strong cryptography.

During its two and a half year history, the KRA has provided a forum for industry-led design of key recovery that meets the needs of the marketplace. An alliance of companies who are working together to facilitate the worldwide use of strong encryption, the KRA is focused on identifying major barriers to the development of marketable key recovery products and services and, as appropriate, proposing solutions for industry.

One such effort in which the KRA has been involved has been the production of a number of technical specifications and papers that discuss the requirements of businesses and the proper role of government in cryptography regulation. These papers, which include perspectives that focus on topics such as "Business Requirements for Key Recovery" and a "Public Policy Requirements for a Global Key Recovery Infrastructure" may be found at the KRA's web site at <http://www.kra.org>. Another effort in which KRA has been active has been presentations at a number of conferences that have helped to educate the marketplace and policy makers on various issues that need to be considered in the development and deployment of key recovery products. These issues include development of company policies for their internal use of cryptography, the need to design key recovery systems that will preserve interoperability, and the importance of customer control over de-encryption keys.

The KRA has also met with representatives of various governments to advise them on policy issues that will promote the use of strong cryptography in electronic business (e-business). Meetings with the governments of countries have afforded the governments the opportunity to better understand the impact of policies and regulations of strong cryptography on businesses.

In fulfilling its mission, the KRA has addressed the appropriate role of key recovery and has developed technical solutions that would meet business requirements. In doing so, the KRA has produced a number of papers in which the KRA has described business scenarios for key recovery and developed a number of interoperability specifications.

## Technical Specifications to Become Available

The KRA is preparing to release additional technical specifications that will support interoperability among key recovery-enabled products. These specifications will assist companies that wish to implement key recovery capabilities in their products to meet customers' requirements. Information as to how to obtain these specifications may be obtained from the KRA web site. However, documents in preparation stage are only available to member companies.

These technical specifications will provide guidance to companies that wish to implement or acquire key recovery capabilities within their security products. In addition, these specifications will promote interoperability between products, provide architectural guidance for design, and help ensure implementations that will be acceptable to the market.

## The KRA's Current Directions

At its January 1999 meeting in San Francisco, California, U.S.A., the KRA accomplished three key tasks:

1. The technical specifications that were near completion were reviewed in preparation for their release in the coming months.
2. The Board of Directors reviewed the current status of key recovery. It looked at the needs of customers and the concerns

and uncertainties of governments that are changing their policies regarding encryption. Based on these facts, the KRA developed plans for the coming year.

3. Officers and directors were elected for the coming year.

One highlight of the January meeting was the discussion that focused on one Asian government's proposed policy for the testing and conformance of encryption products. The presentation, made before the entire KRA membership present, communicated to the Alliance that this government was revising their policy to allow for the acceptance of certification by a "mutually recognized" testing program as a result of guidance from the KRA. This acceptance of certification will significantly reduce the cost of and delays in marketing products in this important country.

Following the conclusion of the meeting, KRA members began to prepare customer trials of key recovery to demonstrate the capabilities of products that implement KRA specifications.

## KRA Meets Again in April

The next meeting of the KRA will take place during the week of April 12th in Ft. Lauderdale, Florida, U.S.A., with several key goals slated for accomplishment. The technical specifications now in progress will be substantially completed and readied for acceptance by the members. KRA members will also consider several additional goals for 1999 to address deployment issues. The April meeting is one to which all companies interested in developing or using products with key recovery capabilities are invited to attend. It is also anticipated that KRA members will consider additional projects not related to key recovery for acceptance. Information about the April meeting is available on the KRA web page.

## Membership is Encouraged

Membership in the KRA is valuable to all companies. Those companies that are specifically involved in information security, both as suppliers and major users, are particularly encouraged to consider becoming members. As members, product suppliers of all sizes have the opportunity to develop common specifications that will ensure interoperability, thus allowing customers to select products that best meet their requirements. Those companies that are implementing strong encryption within their enterprises and that are members of the KRA have the opportunity to better understand the issues concerning the management of encryption systems.

## Conclusion

The KRA serves a valuable role for industry. While the public debate surrounding key recovery is sometimes quite passionate, the KRA maintains its position of offering exceptional value to industry with thorough analysis of industry's encryption needs complemented by careful technical analysis. This results in a work process that produces a solid base of information and specifications. These same processes that the KRA utilizes may also be used to address other critical industry issues and it is anticipated that the April meeting in Florida will provide a forum for discussion of additional such projects.

For further information about the KRA, its papers and technical specifications, upcoming meetings and the benefits of membership, visit the KRA web site at <http://www.kra.org>.

**Compaq Computer Corporation**  
Industry Standards and Consortia (ISAC)  
LKG1-2/W10  
550 King Street  
Littleton, MA 01460-1289  
U. S. A.

FIRST CLASS  
U.S. POSTAGE  
PAID  
COMPAQ COMPUTER  
CORPORATION

ADDRESS CORRECTION REQUESTED.

Printed in U.S.A. © 1999 Compaq Computer Corporation. All rights reserved.

The *Open Systems Standards Tracking Report* delivers news and views to the industry at large about standardization and related issues such as, but not limited to, regulation, legislation, and legal decisions. The opinions expressed herein are solely those of the individual authors and not those of Compaq Computer Corporation.

*Compaq, the Compaq logo, Registered in U.S. Patent and Trademark Office. HomeRF is a trademark of the HomeRF Working Group Association. AT&T is a registered trademark of American Telephone & Telegraph Company.*

## Here's How To Subscribe!

The *Open Systems Standards Tracking Report* is published monthly and is sponsored by Compaq Computer Corporation. To submit information or to receive a FREE subscription, please fill out the form below and send it to Compaq Computer Corporation, 550 King Street, Littleton, MA 01460-1289, United States. Mailstop: LKG1-2/W10, Attention: Bob Schaumann. Or send e-mail to: bob.schaumann@compaq.com.

### *Open Systems Standards Tracking Report - Staff*

**Publisher:** Bob Schaumann  
**Production:** Gloria Chao  
Maureen Bishop-Elfring  
**Circulation:** Jan Litchfield

Name \_\_\_\_\_

Company \_\_\_\_\_ Telephone No. \_\_\_\_\_

Title \_\_\_\_\_ Mailstop \_\_\_\_\_

Street Address \_\_\_\_\_

City, State, Country, Postal Code \_\_\_\_\_

E-mail Address \_\_\_\_\_

-----  
**Compaq Computer Corporation believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. Compaq Computer Corporation is not responsible for any inadvertent errors.**

The *Open Systems Standards Tracking Report*, including back issues, may be viewed on the World Wide Web at <http://www.digital.com/info/osstr/>.