CRYPTREC: the cryptography evaluation project for e-governance by MPHPT (Ministry of Public Management, Home Affairs, Posts and Telecommunications) and METI (Ministry of Economy, Trade and Industry).

Since the late 1990's, the U.S. and Japanese governments, the EU, and ISO have actively promoted these encryption algorithm validation, selection, and standardization activities. They are now almost reaching completion, and the cryptographic algorithms that will be widely used in the first half of the 21st century are being chosen. The above Japanese cryptographic algorithms were highly regarded throughout these activities for their excellent efficiency and high commercial viability (LSI implementation), and it is likely that one or more of them will be widely used. Currently, ISO and CRYPTREC recognize that they need to emphasize secure implementation, and they plan to establish the corresponding validation criteria and validation standards.

As concern over secure implementation of cryptosystems increases, CRESERC is expected to be applied in various situations that require information security (for example, e-governance and ubiquitous communication systems) as the world's leading implementation technology in the field.

Roles of the three companies

In this joint R&D, Hitachi provided secure implementation technology for elliptic curve operations, Mitsubishi Electric provided efficient implementation technology for elliptic curve operations, and NTT provided efficient and secure implementation technology for the basic arithmetic.

Future plans

All three companies plan to launch products incorporating each others' technology in e-governance systems and ubiquitous-related security products based on their joint R&D results, namely CRESERC.

For further information, please contact
NTT Information Sharing Laboratory Group
Musashino-shi, 180-8585, Japan
E-mail: koho@mail.rdc.ntt.co.jp

Most Advanced Wireless Technology in Scotland Launched at EICC

An exhibition of the most advanced wireless technology ever to be seen in Scotland was launched at the Edinburgh International Conference Centre (EICC) on August 5, 2003 and will run until March 2004. Scottish Enterprise has been instrumental in bringing this technology to Scotland with assistance from NTT in partnership with the EICC and BT. The exhibition will give visitors to the EICC the opportunity to experience data-transfer and connection speeds of more than 50 times faster than normal dial-up speeds—without the need for wires.

Users who have a wireless-enabled laptop or PDA (personal digital assistant) will be able to send and receive e-mail, browse the web, and securely access their own company intranet sites if available—demonstrating the benefits of broadband and wireless technology.

EICC visitors will have the opportunity to experience the most widely used wireless technologies (802.11b*1), provided and installed by BT. This will be contrasted with the wireless technology of the

*1 802.11 standards: 802.11 is a family of specifications for wireless local area networks (WLANs) developed by a working group of IEEE. There are currently four specifications in the family: 802.11, 802.11a, 802.11b, and 802.11g. All four use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing.

future, in the form of 802.11a and HiperLAN2[*2] solutions, being supplied and installed by NTT, which can send information at speeds of up to 54 Mbit/s. The exhibition will demonstrate in a hot spot area the difference in data transfer and connection speeds between the three technologies. This demonstration is part of the Scottish Enterprise Broadband for Business Program, which aims to educate and raise awareness about the business benefits achievable with broadband technology.

Charlie Watt, senior director of e-business at Scottish Enterprise, spoke at the launch. He said: "This exhibition capitalises on Scotland's growing expertise in wireless technology and recognises Scotland as a centre of excellence in this field. It is extremely pleasing that such a major player in the world's telecoms industry, NTT, has chosen Scotland for this exhibition—it is a welcome opportunity to showcase Scotland's wireless expertise on a world stage."

NTT has provided some of the world's most forward thinking wireless equipment and the technical expertise and back-up to support the installation of this equipment. Kazuyoshi Tateishi, Executive Director, NTT Information Sharing Laboratory Group, said: "This exhibition is of great significance since it is the first time for 5-GHz-band wireless LAN systems to be demonstrated in a practical environment in Europe. In Japan, the broadband population exceeds 10 million, and hot spot services using wireless LAN technology have been deployed on a commercial basis. Intercarrier roaming and content delivery services are now growing rapidly. Our main purpose is to promote the 5-GHz-band wireless LAN technology developed by NTT Laboratories, especially the HiperLAN2 technology that is a common standard in both Europe and Japan. We expect that a great number of visitors to the EICC will experience wireless broadband and become aware of the benefit."

EICC Chief Executive Hans Rissmann commented: "The introduction of cutting-edge wireless technology is extremely important to the EICC. The Centre has forged a reputation over the last eight years of being at the forefront of new developments and this is one of the most important to date. Our delegates will be able to move seamlessly around the building and stay in touch with their office via wireless access to the Internet. However, more importantly, they will have a glimpse of the future with two additional demonstration networks. These new networks will mean greater numbers of delegates will be able to access more information—more complex information—faster. When this facility is linked to our award-winning customer service, I believe that we will have a very powerful mix and a unique offering. Ultimately we are always trying to improve our efficiency and effectiveness and provide the best possible service for our clients. I am confident that this will be another step towards that ultimate goal."

BT has been working with the EICC on a range of technical projects to make it one of the most advanced facilities of its kind. Wireless networks have been installed to provide fast, flexible platforms for voice, data, video, and multimedia functions. Brendan Dick, BT Scotland's general manager, said: "Wireless technologies are recognised as being part of the broadband jigsaw as we work to create a fully connected Scotland. Wireless has the potential to bring fast Internet access to areas currently outside the reach of existing networks and BT plans to test a wide-range wireless solution in Scotland this winter. As well as leading the way for its own customers, the EICC's innovative project has allowed us to provide a platform for an acknowledged world leader to showcase its hyper-speed wireless networks and enable people to glimpse the future at first hand. We believe partnerships are essential to ensure everyone has fast Internet access—north, east, south and west!"

For further information, please contact

NTT Information Sharing Laboratory Group
Musashino-shi, 180-8585, Japan
E-mail: koho@mail.rdc.ntt.co.jp

*2 HiperLAN: A set of WLAN communication standards primarily used in European countries. There are two specifications: HiperLAN/1 and HiperLAN/2. Both have been adopted by the European Telecommunications Standards Institute (ETSI).