ELLIPTIC CURVE CRYPTOSYSTEM (ECC)

[redacted] PES41

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Background:

Elliptic curves are being used in algorithms for factoring integers, primality proving, and public-key cryptography. They provide relatively small block sizes, high-speed software and hardware implementations and offer the highest strength-per-key-bit of any known public-key scheme. The Ellipitic curve systems are being drafted in two work items by the American National Standards Institute (ANSI) ASC X9 (Financial Services): ANSI X9.62, The Elliptic Curve Digtal Signature Algorithm (ECDSA); and ANSI X9.63, Elliptic Curve Key Agreement and Transport Protocols. Elliptic curves are in the draft IEEE P1363 standard (Standard for Public Key Cryptography) which includes encryption, signature, and key agreement mechanism.

(U//~~FOUO~~) In August 1998, ECC became an American National Standards Institute (ANSI) draft standard aimed at providing developers with guidelines for creating these "faster" digital signatures for applications in the financial services industry. The IEEE and IETF are also examining ECC.

(U//~~FOUO~~) ADVANTAGES:

ECC has gained widespread acceptance as the technology that has revolutionized the field of cryptography, in many instances performing orders of magnitude faster than existing cryptosystems at equivalent security levels. ECC is enabling digital security for every kind of computing device today. ECC offers the highest strength-per-bit of any known public-key system; it provides the same valuable security benefits as other public-key systems, while needing only a fraction of the overhead.

(U//~~FOUO~~) LEADING ECC COMPANIES:

RSA was founded in 1982 by the inventors of the RSA Public Key Cryptosystem (RSA is named after their surnames' first letters; Rivest,

Shamir, and Adleman.). RSA Data Security, Inc. is the world's brand name for cryptography, with more than 300 million copies of RSA encryption and authentication technologies installed and in use worldwide. RSA's encryption technology is embedded in Microsoft Windows, Netscape Navigator, Intuit's Quicken, Lotus Notes, and hundreds of other products.

(U//FOUO) Comtron, Inc. was founded in 1985 with the debut of the Portable Data Terminal product (PDT), which was widely used by Japan's distribution industries. In 1992, Comtron introduced infrared wireless LAN technology to the Japanese market; and, in 1995, introduced wireless products based on 2.4GHz radio frequency technology, establishing itself as a pioneer in the wireless networking business and capturing 45 percent market share. To respond to its OEM customer needs, Comtron also offers software and hardware development, localizing, porting, and installation.

(U//FOUO) NTT Electronics Corporation (NEL), founded in 1982 as a subsidiary of Nippon Telegraph & Telephone Corporation, is an advanced electronics vendor which provides key devices for information & communication systems such as high-speed LSI or low-power LSI and network products implemented with those LSI based on the successful fruits of NTT's R&D.

(U//FOUO) Diversinet Corp. (NASDAQ: DVNTF, CDN: DVNT) is a leading developer of products based on public-key infrastructures and technologies required for corporate networks, Intranets and the Internet for electronic commerce. Its proprietary PKI technology offers customers ease-of-use, efficient operation and flexible implementation for diverse security authentication applications.

(U//FOUO) ECC Licensees and Partners:

Certicom: 3Com/Palm, Cylink, Diebold, Infowave, Motorola, NTT Electronics, Pitney Bowes, Schlumberger, Siemens, Sterling Commerce, and VeriFone
Comtron, Inc.
Sapher Servers
Xcert International Inc.
Baltimore Technologies
NTT Electronics Corporation (NEL)

Internet Security Systems, Inc. ISS
Diversinet Corp. (NASDAQ: DVNTF, CDN: DVNT)
Diebold, Incorporated, (NYSE: DBD)
Infowave
Rainbow Technologies
Entrust Technologies
SurfinGate
GTE CyberTrust
RPK Public Key Cryptography
RSA Products

(U//~~FOUO~~) CONCLUSIONS:

Elliptic curve cryptosystems offer the highest strength-per-key-bit of any known public-key system. With a 160-bit modulus, an elliptic curve system offers the sam elevel of cryptographic security as DSA or RSA with 1024-bit moduli. The smaller key sizes result in smaller system parameters, smaller public-key certificates, bandwidth savings, faster implementations, lower power requirements, and smaller hardware processors.