

NSA's Elliptic Curve Licensing Agreement



Mr. John Stasak
Cryptography Office
Information Assurance Research
National Security Agency



Why Elliptic Curve Cryptography Is Important to NSA



- *The next generation cryptography to protect USG information will use elliptic curve cryptography*
- *Increased security obtained with reduced bandwidth over conventional methods*



Overview of License Agreement



- *Field of Use*
- *NSA Approved Product*
- *Licensed Patents and Patent Applications*
- *Sublicensing Rights*



Field Of Use

- *The Licensed Patents and Patent Applications with elliptic curves over $GF(p)$, where p is a prime number greater than 2^{255} and*
- *Either NSA Approved Product or a product for national security compliant with FIPS 140-2 or its successors*



NSA Approved Product



- *A product that is approved by NSA for use by either:*
 - *Federal, State or Local government agencies protecting classified or mission critical national security information, or*



NSA Approved Product



- Foreign government agencies for protecting classified or mission critical national security information where interoperability with US entities is a possibility or for protecting classified or mission critical national security information that originated in the U.S. Federal, State or Local Government*



Licensed Patents and Patent Applications



- *Key Agreement and Transport Protocol*
 - *with Implicit Signatures*
 - *With Implicit Signature and Reduced Bandwidth*
- *Digital Signatures on a Smartcard*
- *Strengthened Public Key Protocol*
- *Elliptic Curve Encryption Systems*
- *Authenticated Key Agreement*



Sublicensing Rights



- *NSA has a perpetual nonexclusive, nontransferable, worldwide, royalty free, fee-bearing license under the Licensed Patents and Patent Applications within the Field of Use to make, have made, use, sell, offer for sale, and import Licensed Products for use by End Users and to practice the Licensed Processes in the Field of Use, as well as to sublicense to others*



What is Really Covered



- *The use of elliptic curves defined over $GF(p)$ where p is a prime number greater than 2^{255} when the product satisfies the Field of Use conditions*
- *Both compressed and uncompressed point implementations*
- *Use of elliptic curve MQV and ECDSA under the above conditions*



Who to Contact to Get a NSA License



- **NSA's Information Assurance Business Affairs Office**
 - **National Security Agency**
Attn: IAD Business Affairs Office
9800 Savage Road, Suite 6740
Fort Meade, MD 20755-6740
 - **410-854-6091**
 - **BAO@nsa.gov**