TTFN Associates

An Update on the SECG

Standards for Efficient Cryptography Group

- Formed by Certicom in 1999

International industry & academic consortium for the development of standards specifically designed to promote interoperability of ECC cryptosystem implementations

SECG has produced public ECC standards which have been widely referenced in both research and government publications

Approximately 50 organizations worldwide

Participants include:

TTFN Associates

First standards

- SEC 1: Elliptic Curve Cryptography
- SEC 2: Recommended Elliptic Curve Domain Parameters

New work

- Updating SEC 1 & 2 to incorporate NIST curves, AES, SHA-2 family
- Signature standards for ECNR, ECPVS (proposed)
- Implicit certificate standard (proposed)
- Reference implementations (proposed)

For More Information

Visit www.secg.org

- Site currently being updated

Contact me:

William Lattin
SECG Chair
TTFN Associates
wlattin@earthlink.net
T: +1.650.947.4863

Please join this project for ECC cryptosystem interoperability!