

## Utimaco Supports Elliptic Curve Cryptography Algorithms in Hardware Security Module

- **EU and US cryptographic guidelines call for ECC algorithms**
- **Shorter key length allow for faster processing time**
- **SafeGuard CryptoServer support ECC-based public key protocols and end-to-end key management**

**Oberursel, 8th January, 2006** / Utimaco – The Data Security Company supports Elliptic Curve Cryptography (ECC) algorithms. Utimaco's support for ECC follows the unveiling of cryptographic guidelines from the European Union and the U.S. government in independent security compliance initiatives. New features in the SafeGuard CryptoServer include ECC with 8000 plus signatures.

SafeGuard CryptoServer is a tamperproof hardware security module (HSM). ECC support in SafeGuard CryptoServer provides enterprises as well as government agencies with a certified, efficient and high-performing HSM in accordance with Suite B, the National Security Administration's (NSA) cryptographic recommendations for protecting the U.S. Government's classified and unclassified communications. SafeGuard CryptoServer also meets Restriction of Hazardous Substances (RoHS) compliance requirements as outlined in the directive of the European Parliament which restricts the use of hazardous substances for electrical and electronic equipment within the European Union.

SafeGuard CryptoServer ensures the secure and reliable introduction of electronic processes in business processes, payments and government solutions because of its high security standard and certification according to FIPS 140-2 Level 3 criteria, and the support of ECC-based public key protocols, coupled with end-to-end key management. SafeGuard CryptoServer with ECC-based public key protocols are available with the new cost efficient SafeGuard CryptoServer S-Platform and in the FIPS 140-2 Level 3 certified SafeGuard CryptoServer CS-Platform.

"Information technology is the backbone of every business process," said Malte Pollmann, Vice President of Utimaco. "With upcoming compliance requirements and privacy initiatives, the use of hardware-based security in electronic business processes is mandatory. It is vital that companies use security products to be in line with international security regulations and to make sure their data processes are not interrupted by using poor and unstable security implementations."

Hardware security modules ensure secure generation, storage and application of cryptographic keys and certificates in encryption and signature processes. From electronic payment and banking processes to processing digital certificates, the highly flexible SafeGuard CryptoServer products protect applications and keys across a broad range of business and administrative processes. These include transaction security, secure PKI environments, document management and archiving, database security and authentication, secure toll-collection systems, electronic billing, and more.

Die National Security Agency (NSA) has announced the „Suite B“ Algorithm catalogue for the protection for classified and unclassified data. This catalogue does not contain RSA anymore, but several ECC-Algorithms. For more information visit: [http://www.nsa.gov/ia/industry/crypto\\_suite\\_b.cfm](http://www.nsa.gov/ia/industry/crypto_suite_b.cfm).

For comparison of algorithm length visit:  
[http://www.nsa.gov/ia/industry/crypto\\_elliptic\\_curve.cfm](http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm)

## Note to the editor

### Utimaco Solution Portfolio

The comprehensive SafeGuard Solution Portfolio from Utimaco provides the full spectrum of data confidentiality and integrity wherever you are, whatever you do.

#### **SafeGuard Shield protects data on end devices and in networks (data at rest)**

**SafeGuard Easy:** Hard disk encryption and pre-boot authentication

**SafeGuard PDA:** Secure authentication and data encryption on PDAs and smartphones

**SafeGuard PrivateDisk:** Easy-to-use and powerful encryption of files and folders in virtual drives

**SafeGuard LAN Crypt:** Group-based, transparent multi-user encryption

**SafeGuard CryptoServer:** Hardware Security Module for master key protection and electronic processes

#### **SafeGuard Transit secures data during transmission (data in motion)**

**SafeGuard Mail Gateway:** Encryption appliance for central e-mail security

**SafeGuard PushMail:** E-mail security for push mail services

**SafeGuard RemovableMedia:** Security-to-go protection for all removable media (*shipping Q2*)

**SafeGuard PrivateCrypto:** Easy encryption of e-mail attachments and other files

**SafeGuard SignatureServer:** Security solution for generating qualified digital signatures

#### **SafeGuard Process secures data during processing (data in use)**

**SafeGuard CryptoServer:** Hardware Security Module for master key protection and electronic processes

**SafeGuard SignatureServer:** Security solution for generating qualified digital signatures

### Utimaco Safeware – The Data Security Company.

Utimaco is the leading provider for data security solutions. The Data Security Company enables mid-sized to large organizations to safeguard their data assets against attacks and to comply with privacy laws by protecting their confidentiality and integrity. In response to twenty-first century threats – the new world of Data Security 2.0 – Utimaco's complete range of solutions provide full 360° protection unlike free, end-point or built into encryption solutions which only cover specific security needs. Its advanced SafeGuard Solutions help to manage and secure data in what ever conditions: during storage (data at rest), during transmission (data in motion) and during processing (data in use). Utimaco offers its customers comprehensive on site support via a worldwide network of partners and subsidiaries in Europe, the USA and Asia. Utimaco Safeware AG, with headquarters in Oberursel, near Frankfurt, Germany, is listed on the Frankfurt Stock Exchange (ISIN DE0007572406). For more information, visit our website at [www.utimaco.com](http://www.utimaco.com)

#### Additional information:

Utimaco Safeware AG

<http://www.utimaco.com>

Rieke Bönisch

Tel: +49 (0)6171 88 - 12 10

E-Mail: [rieke.boenisch@utimaco.de](mailto:rieke.boenisch@utimaco.de)