

## [Digital Signature and Encryption – central and transparent for the User]

### [SecurE-Mail Gateway]

Sending e-mails proves to be the most commonly used internet application. E-mails are firmly established within daily business connections.

Nevertheless it is not possible yet to represent electronically the whole related company specific workflow. Thus, the release of workflow in form of binding instructions via email is strictly to be realised via digital signed e-mails, but therefore additional software (encrypting plug-in) are required at these particular workstations.

Consequence: each user has to take the corresponding steps for each e-mail. These individual solutions are inasmuch critical for the company security policy as the implementation is always bound to the right command of the application and employee's self-discipline.

### [The Challenge]

The aim of the project consists in representing organisational processes, e.g. representatives arrangements, assignment of activities within a team, archiving of email communication or centralized issue of receipts of delivery. Previous available systems were limited to the sheer transport of e-mails without representing the workflow.

The workflow particularly with regard to cryptographic operations becomes complicated due to its dependency on individual workstations respectively persons. Not to mention the content and virus filtering procedure which is hard to realise in terms of encrypted end-to-end communication.

### [Central Post Office]

The SecurE-Mail Gateway from Utimaco Safeware integrates cryptographic processes (en- and decryption, signature, verification) in a central place within the company network. Existing workflow processes have been in a safe and easy manner enhanced with confidentiality, authenticity and integrity. Already existing decentralised e-mail solutions and encryption components can be integrated into the workflow via centralised representation of the security policy. SecurE-Mail Gateway uses the internet standard SMTP/ESMTP for e-mail communication and is for this reason able of being integrated into any e-mail internet infrastructure (e.g. Lotus Notes, Microsoft Exchange etc.).

Both for e-mail en- and decryption and Digital Signature the SecurE-Mail Gateway uses the well established internet standards S/MIME, OpenPGP and PrivateCrypto. Incoming and outgoing e-mails can automatically be decrypted for the addressee within one's own network, respectively encrypted for those external. Essential secret keys can be discarded into a Hardware Security Module. This process is absolutely transparent for the user.

### [Secure Key Memory]

An essential component of the SecurE-Mail Gateways consists in the Hardware Security Module. This security processor stores data trustworthy in a secure environment by intelligent protecting mechanisms. Any physical attempt to acquire secret keys is reliably detected and defended.

### Core Features and Advantages:

- Common Point of Trust
- Integration of e-mail security into the workflow process
- Consistent realisation of Security policy
- E-mail standard SMTP compatible
- S/MIME, OpenPGP and PrivateCrypto support
- Transparent Security for the users
- Independent from mail servers e.g. Lotus Notes, Microsoft Exchange etc.
- Central content and virus filtering possible
- Integrating TimeStamp
- Secure Key Memory: Hardware Security Module
- Customisation possible

### [Specifications]

#### Special Feature

**Operating system** Secure hardened system environment including operating system

**CD-ROM** Complete installation on CD-ROM

**Management** Web management

#### Expansions

##### Utimaco Safeware Products

- SafeGuard® PKI
- SafeGuard® Sign&Crypt
- SafeGuard® PrivateCrypto
- CryptoServer® Hardware Security Module
- CryptoTimeStamp

**Note** All other trademarks mentioned belong to the corresponding holders

### [Extensions]

#### Central TimeStamp

For business issues such as orders and auction offers is the point of time at which the information comes in of great importance. Additional to Utimaco Safeware SecurE-Mail Gateway the CryptoTimestamp certificates data authenticity and integrity at a particular time. The TimeStamp is a unique data identifier in a given form at a given time. Possible changes at the original data are clearly detectable.

#### Central archiving system

Central archival storage of the company communication is possible without burdening the e-mail communication. An easy and effective security facility– optional even signed or encrypted –due to the connection with the CryptoTimestamp.

## Contact eB2Bcom

**Sydney:** +61-2-9779-1597  
**Melbourne:** +61-3 -9896-7800  
**email:** sales@eb2bcom.com  
**Web:** [www.eb2bcom.com](http://www.eb2bcom.com)