

PersonalSign ePKI

Secure E-mail for the Enterprise

Industry, education and government alike at some point must confront the need to securely correspond with employees, customers, partners, and constituents who reside both and outside the trusted organisation network. Often these correspondences involve sensitive information including patient data, customer records, intellectual property, or confidential business agreements. Sensitive information aside, senders of even the most public information may wish to assure recipients that the message did indeed originate from them, especially during these times when so many unsuspecting victims have been widely fooled into providing credit card or similar compromising information to the dishonest entities masquerading as reputable organisations.

What is secure email?

To address the concerns highlighted above, many organisations have turned to secure email as a method to correspond safely using their favorite email client like Outlook, Outlook Express, Mozilla Thunderbird and Apple Safari. These popular email clients among others support the Secure/Multipurpose Internet Mail Extensions (S/MIME) standard for encrypting and digitally signing e-mail. Please see GlobalSign Secure Email whitepaper for further details surrounding this standard. Putting aside the technical implementation, S/MIME provides two main benefits that all types of organisations can benefit from:

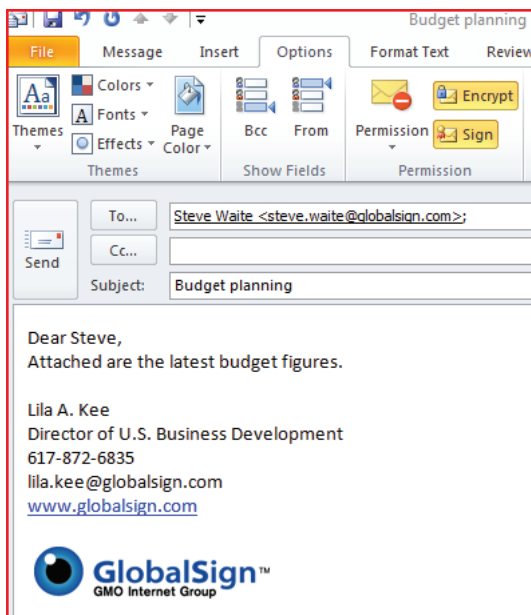
Encryption

Messages encrypted with the recipient(s) public key can be transported over unsecure networks e.g. the Internet, in a way that assures data confidentiality. Privacy is maintained since only the holder of the corresponding private key can "unlock" the message and view the content in clear text.

Digital Signatures

Encrypted messages aren't a whole lot of good if recipients can't trust that the message originated from the person identified in the message. Email addresses are often issued with a wide degree of security, ranging from in-depth verification of the individual to virtually no control. Therefore, true secure messaging requires the implementation of digital signatures that are verifiable by a trusted source like GlobalSign.

Illustration of message being prepared for digital signing and encryption:



WebTrust audited

Because of GlobalSign's strict adherence to accepted Certificate Practice Statements (CPS), most popular email clients inherently trust messages secured by Digital IDs issued from the GlobalSign trusted hierarchy. This inherent trust provides easy to understand user interfaces and show that the message can be trusted because the origins have been authenticated and the message hasn't been altered. GlobalSign's roots are widely trusted and therefore also produce an easy and fast method for all parties involved in a trusted message exchange to verify the message is legitimate.

For more information about GlobalSign solutions, please call Belgium +32 16 8991900 or UK +44 1622 766766.

Visit www.globalsign.eu or www.globalsign.co.uk for more information

Enterprise PKI

Assuring both senders and recipients of secure email that the original message was received unaltered only addresses a fraction of organisations concerns. Like "wet-ink" signatures, senders of messages written in association with company, school, or government agency must bind the message to both a subject (either individual or role e.g. Marketing Department) and an organisation. GlobalSign's ePKI provides this capability by issuing S/MIME compliant Digital IDs to individuals and roles affiliated with a verified organisation. GlobalSign will not allow certificates to be issued without an initial verification of the organisation's legal status (e.g. Dun & Bradstreet check) as well as authorisation via an independent check that the request is legitimate (e.g. inbound phone check).

Issuing Digital IDs should be likened to issuing company ID badges, network user name and passwords, laptops or any resource that requires strict tracking. Stringent records of whom which credentials have been issued, how user rights match current assignments and which administrator was associated with a particular transaction should be followed. This is especially true given the fluid nature of today's workforce that has replaced the static nature of human resources in the past. ePKI is a zero foot print, managed service that provides administrators an easy method to issue PersonalSign Digital IDs used for secure email.

Flexibility

GlobalSign recognises that organisations wrestle with planning on the right amount of Digital IDs to take advantage of volume discounts. Additionally, like any technology mistakes happen, computers crash, end users lose track of credentials and need replacement credentials "yesterday". ePKI addresses both concerns head-on by offering:

- **10% extra IDs are added to your inventory to address employee, partner and contractor attrition. For example purchase a 100-pack of PersonalSign Digital IDs and 110 will be added to your inventory**
- **Free replacement certificate! Lost or deleted IDs can be reissued free of charge by the ePKI administrator at any time during the day or night**

Connecting with your users

GlobalSign also recognises your end users are most likely to respond to invitations to apply for Digital IDs from a known entity. Therefore ePKI has been built to allow significant organisation branding – from customised emails originating from an organisation appointed address to company logos and specific subscriber agreements that capture additional terms and conditions organisations may wish to present to their end users.

Tailored to fit your IT environment

Whether you wish to standardise on a particular browser or method of enrolling for a Digital ID, ePKI provides a flexible no-cost option to allow the ePKI administrator an optimal method to certificate provisioning. Furthermore, secure email often entails encryption and ePKI is equipped with features to make managing encryption easier:

- **Multi-year validity to reduce life-cycle management of renewals and reduce likelihood of deleting expired certificate needed for later decryption**
- **Access to all public certificates issued from organisation's ePKI managed service for easy directory posting**
- **Bulk enrollment via bulk upload of a comma separate file that auto-generates invitation emails**
- **Microsoft Internet Explorer and Firefox based browser support**
- **GlobalSign server-generated key generation where a PKCS12 public/private key and certificate "package" is delivered to the user for easy back-up**
- **LDAP Data Interchange Format (LDIF) reporting, for easy uploading of fielded digital certificates to your LDAP directory**

Case Study

A large U.S. Mid-western University often performing often government funded research, needed to comply with privacy regulations surrounding the electronic transmission of sensitive information. Microsoft Outlook's secure email capabilities, already used as standard on the University's professional desktops was an easy choice to meet the data integrity, user authentication and data confidentiality requirements. By implementing a GlobalSign ePKI 50-pack PersonalSign certificate license, members of the organisation are now able to easily digitally sign and encrypt sensitive correspondence. The University's ePKI administrator is also able to issue, renew, re-issue and revoke Digital IDs to a dynamic workforce without requiring GlobalSign to get involved in each transaction. Implementing security into their electronic correspondence has significantly increased productivity, while at the same time fully complying with government and industry regulations and best practices.