# GlobalSign – KeyTalk Secure Email Service

## Background

With the new GDPR legislation active since the 25th of May 2018, more and more companies start to realise that a lot of their privacy relevant information is send by normal unencrypted internal and external email. Especially the external email is vulnerable to 'data-leakage' because an external email can pass multiple mail servers, where everyone with enough access to these servers can read the content of these mails.

You could even say that sending digital mail the way we do today is comparable with sending a classic letter in an open transparent envelope or even sending a postcard with privacy relevant text on it.

Since 1996 the technology and the global trust framework is available to send secure encrypted email with the use of personal S/MIME certificates. S/MIME stands for Secure/Multipurpose Internet Mail Extensions. An S/MIME certificate is a sort of digital passport which you can use to digitally sign your email or even encrypt your email so no one can read your email other than the one receiving it.

The substantial cost for an S/MIME certificate, the very technical installation procedure and the need for the sender to acquire the public key of the receiver of the email, to send an encrypted email are the reasons that sending encrypted mail did not raise to be the standard.

Talking to our customers we found out that they would really like to use digitally signed and encrypted email if the extra cost weren't that high and the installation and use would be very simple. So together with our Certificate and Key Management partner KeyTalk, we developed the GlobalSign 'Secure Email Service'.

## Description of the Secure Email Service

To fulfill the need to use encrypted email in an affordable and easy to use way, GlobalSign, as a Qualified Trust Service Provider (QTSP) and KeyTalk as a Certificate and Key Management partner, jointly developed this Secure Email service.

This Secure Email Service consists of a number of components all relevant for the proper way of working;

- A personal S/MIME certificate issued by GlobalSign a globally trusted CA.
- A Secure Email client app, this is an end-user app developed by KeyTalk, available for Windows, OS X, Android and iOS. The app handles the request, installation and configuration of the S/MIME certificate for the mail program of the user. (mostly MS Outlook)
- LDAP directory service, is a specific service configured as a public Directory Service in which every user of the Secure Email Service will be registered and where the public keys for these users will be stored. The Directory Service will be

hosted across multiple Datacentres of GlobalSign and therefore accessible for everyone with an internet connection.
- CKMS, a Certificate and Key Management System, in this case the CKMS of KeyTalk. The CKMS is needed to securely manage the crypto key pairs used for the encryption and decryption of email messages and for the enrolment and management of the certificates at various endpoints (workstations, laptops, tablets and smartphones)
- The possibility for users of the service to request a GlobalSign PS1 S/MIME certificate for their external contacts without additional cost.

The Secure Email Service is intended for those companies who want to be ready for the new GDPR legislation and because of that they want to tackle their most vulnerable source for data leakage, the internal and external email traffic. With this service they can provide all their employees and even their customers with the possibility to digitally sign their emails and optionally encrypt them without any hassle.

## How easy is this Secure Email Service for the end-user?

With the design of the Secure Email Service, one of the most important features was the ease of use for the end-user. So the following steps are a description of the configuration process of the Service:

- The user must have the GlobalSign Secure Email app available on his user device (laptop, tablet or smartphone)
- After starting the app, the user will be asked only once to authenticate using his corporate credentials to start the process.
- After a successful authentication, an automated request for a personal S/MIME certificate will be send to GlobalSign.
- The GlobalSign issuing platform will then generate an S/MIME certificate for this specific user and the KeyTalk CKMS will generate the associated key pair.
- The user will be automatically entered in the Public GlobalSign LDAP Directory Service and the public key of the user will be published in the Directory Service.
- The Secure Email app will then configure the email program of the user so it can make full use of the installed S/MIME certificate for digital signing and encryption.
- Finally the Secure Email app will publish the necessary user data in the GlobalSign Public S/MIME directory service and will configure this Service as an address book for the email program to use (MS Outlook / Mac Mail).
- The email program of the user is now capable of sending and receiving digitally signed emails with the option to encrypt each single email or decrypt an email coming from another user registered by the GlobalSign Secure Email Service.

## The final hurdle

The final hurdle in the process of sending an encrypted email is if you want to send an encrypted email to someone without an S/MIME certificate and therefor you will not have the public key of this person available to encrypt the message.

The Secure Email app will have the ability to request for a GlobalSign PS1 S/MIME certificate with a validity of a year, for the contact you want to send an encrypted email without additional cost. The KeyTalk CKMS, triggered by the request in the app will than issue an automated request to GlobalSign for a PS1 S/MIME certificate and the GlobalSign issuing platform will offer the requested certificate to the receiver of the PS1 certificate with a small explanation and installation instruction of the PS1 S/MIME certificate and inform the KeyTalk CKMS.

KeyTalk will than generate an automated email to the requester and to the receiver of the PS1 certificate and the encrypted correspondence between the two contacts can start. Next to the small installation instruction the receiver will get additional information on the benefits of the Secure Email Service.