



DATASHEET

OX Guard

PGP for email and files

The privacy and integrity of our communications is becoming more and more important and relevant. Particularly in the light of revelations about pervasive monitoring by governments and intelligence agencies. Many instant messaging services offer message encryption by default as a response to this. However, even though the capability to offer encryption for email exists, many people are not aware of it, or think that it's too complex or hard to setup.

Provide a simple solution

OX Guard is designed to let our customers offer a secure encrypted email solution that is usable by anyone. A solution that is, for the average user, as easy as a single click, but also lets knowledgeable users take advantage of advanced encryption options.

OX Guard is designed to work seamlessly with other users, whether or not they are aware of email encryption.

Within the OX environment

OX Guard delivers user-friendly security that is completely transparent. Users, who have subscribed to the service, simply create an email as usual, hit the

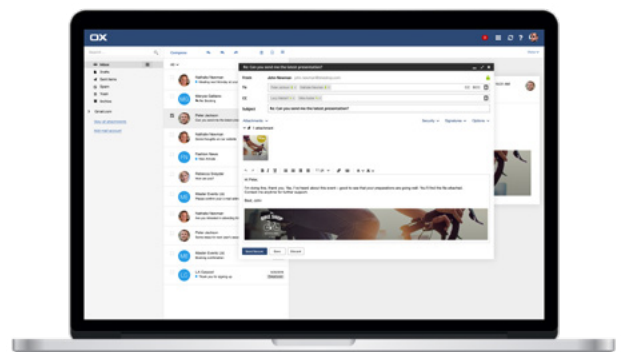
'Send Encrypted' button and OX Guard handles the rest. The message, together with all its attachments, is instantly encrypted and sent. At the other end, it is automatically decrypted and presented to the recipient as normal. If the recipient has not setup OX Guard, they are offered a simple tour of its capabilities, and then they just have to choose a password.

Outside the OX environment

So what happens if the recipient uses a different email service? OX Guard will lookup the encryption keys for any users who have published them, including automatic lookup for users who are using Open-Xchange via another service provider.

If OX Guard cannot lookup an encryption key, then instead of receiving the sent email, the recipient receives a special notification email. This email contains a one-time link to a specially generated OX App Suite Guest Account. From within this account the recipient can read, and reply to, the encrypted content. The Guest account remains active as long as emails continue to be received.

The guest account also provides the opportunity to acquire new customers. Additional marketing, messaging and advertising can be added to the guest account to attract new users.



Secure because it is simple

Simple to use OpenPGP

OX Guard is OpenPGP made simple. It makes this highly secure system easy and fast enough for all your users to use.

One of the hardest things for most users to understand is key management. OX Guard handles all this for the user. The user simply supplies a password and OX Guard does the rest. All keys are created and managed, and all PGP Public keys are automatically retrieved for email recipients.

Note that the OX Guard servers can also act as public key servers for the primary email accounts.

Recovery

If a user forgets their security password it can still be recovered. The user simply enters password recovery and OX Guard retrieves access to the private keys, resets things and the user gets access to their emails again. Advanced users can turn this feature off for maximum security.

Combatting bad habits

Two bad security habits are: receiving unencrypted, but sensitive, emails and leaving them in your inbox; leaving encrypted emails open while you do other things. To help OX Guard provides mail filter rules that lets users automatically encrypt selected incoming emails. It also provides a click-off feature that automatically re-encrypt open emails when clicked away from.

Advanced users

Some users will understand, and want to manage their own PGP keys, and OX Guard lets them. In advanced mode users can export keys, upload public keys, upload private keys, set the PGP mode (inline/mime etc.) and more.

OX Guard interoperates seamlessly with any other PGP-based client, including Thunderbird Enigmail and Mac GPGTools.

Extended features

OX Guard supports the verification and sending of PGP signed emails. When an email is sent it is signed, and when received the user is visually informed if the email has been tampered with. Advanced users also have the option to send their public key along with emails.

OX Guard with OX Documents

Traditionally it is a pain to work with encryption, but OX Guard makes everything simple. When editing an encrypted document, with OX Documents, the user simply edits it as usual. In the background OX Guard handles the complexity of decrypting the document, passing it to the editor, handling the edits and automatically encrypting it again when finished.

OX Guard at a glance:

Guest mode

Public key management available for non-OX Guard users. Access via auto-generated OX App Suite web account.

Proven OpenPGP security

OX Guard uses OpenPGP, one of the world's most secure encryption technologies, together with Elliptical Curve to send and receive secure emails and encrypt files.

Simple email security

Single click email security: Just press 'Send Encrypted' to send an encrypted email.

External secure email delivery

Send secure emails to users who do not usually use encryption. Recipients get access to a secure auto-generated guest account.

PGP key management

OX Guard seamlessly allows users with existing OpenPGP keys to import, export and share their keys.

Offline support

OX Guard lets users import and export their personal encryption keys. This enables the use of other OpenPGP clients such as GPG Mac Mail, Thunderbird, etc.

Signing and verification

OX Guard supports OpenPGP signing and verification of emails and files.

Encrypted file storage

Secure files when uploading to OX Drive (Drag and Drop) or manually after uploading.

Seamless use of OX Documents

Transparent and seamless handling of OX Documents with encrypted files in OX Drive.

