



# GraffitiMail

## GraffitiMail Security Features

Your documents are processed in a secure mailing facility. Accredited to ISO 27001 and fully compliant to the Data Protection Act, you can rest assured that your mail is being processed in a professional and confidential environment currently processing thousands of documents every day for blue chip clients as well as SME organisations.

### GRAFFITIMAIL PRINTER DRIVER

#### **DOCUMENT INTEGRITY**

Documents are stored in the PDF/A file format. This ensures that all the resources which are required to produce the document, such as fonts and graphics, are stored with the document data at all times.

In addition to this, fulfilment metadata is also embedded into the document. This means that all the information which is needed to know how to fulfil the document is also carried with the document itself. Fulfilment information can include envelope type, stationery, inserts, colour print requirements and much more.

#### **DOCUMENT SECURITY**

The document, resources and metadata are encrypted to 192bit Triple DES. This ensures that regardless of the transmission method, the document remains secure. The document is then transmitted from the GraffitiMail Mail Printer Driver at the user's site to the Mail-Management site. To add an additional layer of security, this transmission is carried out using a secure communication channel such as SFTP (FTP & local file copy are also available if transmission security is not a concern).

#### **APPLICATION INTEGRITY**

To prevent malicious behaviour within the client infrastructure, the GraffitiMail Mail Printer Driver is digitally signed & obfuscated. This protects against application disassembly and allows system administrators to ensure only trusted applications are used.

### GRAFFITIMAIL MAIL MANAGEMENT SITE

#### **DOCUMENT SECURITY**

Even when documents arrive at the Mail Management site, they remain stored in their encrypted form. Documents are only decrypted for Web Portal viewing and Production Print purposes. This helps to ensure that the strict ISO 27001 security levels are met.

### WEB PORTAL

#### **SYSTEM SECURITY**

The Web Portal is a web facing application, as such security is of paramount importance and so has significant investment in ensuring that the Web Portal is as secure as possible. A 3rd party security firm has been employed to perform penetration and security testing on the Web Portal. Following this activity, security accreditation for the Web Portal was awarded.



#### **KEY THREATS & SECURITY MEASURES WHICH WERE TESTED:**

- Support for secure communication (HTTPS)
- Open Web Application Security Project (OWASP) Top 10 threats
- The Web Application Security Consortium Top threats
- The Open Source Security Testing Methodology Manual Top threats
- SANS Common Weakness Enumeration TOP 25 threats



Graffiti Group Ltd • Caswell Science & Technology Park  
Towcester • Northamptonshire • NN12 8EQ  
Co Reg. No 4887340 • VAT No: GB 832 1166 58

0330 024 3001  
www.GraffitiGroup.co.uk  
info@GraffitiGroup.co.uk