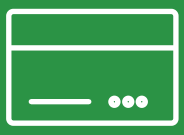
Dataguard™

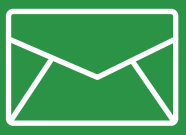
We provide digital and operational security solutions dealing with resilience and risk

ePay datasheet

Secure, encrypted payslips, easily



Dataguard ePay
Encrypted Payslips



Dataguard eMail
Encrypted eMail

Dataguard eBox
Encrypted Storage

How do you manage your company's payslip distribution?

- Do you still manually print payslips and send them through the mail to your employees?
- Or do you email digital versions to them?
- Do you email them to your employees and password protect the documents?
- Do you you upload them to a portal for your employees to access and download?

Did you know...

- Your processes may be in breach of GDPR
- The confidential data of your business and that of your employees may be vulnerable
- You may be placing unnecessary burdens on your IT response mechanisms
- You may be contributing to a high business-wide carbon footprint
- You may be holding back the aspirations of your business to become fully digital

Problems associated with payslip distribution

	Payroll	Payslip transit	Employee
a Payslips printed and mailed	Expensive printing Purchase of payslips Postage costs	Vulnerable to interception anywhere from payroll desk to employee's letterbox Vulnerable to physical theft	Filing and archive burden
b Payslips emailed directly		Vulnerable to interception PDF passwords require user entry for each payslip opened which rules out high-strength passwords	Passwords liable to be forgotten or inaccurate entry, causing user difficulty and upstream admin workloads to reset. Password-protected PDFs use one-time passwords*see below
c Payslips uploaded to portal		Portals are potential targets for attack. Worst case scenario is if portal itself stores payslips in unencrypted form. Employer owned portals require maintenance and security.**see below Vulnerable to interception during email transit from portal to employee	Passwords liable to be forgotten or inaccurate entry, causing user difficulty and upstream admin workloads to reset

* A PDF which is password protected will always require the same password to open it. Should the end user forget or mislay the password, it is incumbent upon the sender to know and record the password in order to resend it, adding in new layers of admin pressure and security vulnerability. If the sender does not keep records of all historic payslip passwords, then the payslips become unopenable to those users who forget or mislay their passwords.

** If portal is run by employer, then responsibility for backup and security applies as it would for any employer controlled data

The ePay solution

FOR THE EMPLOYER

Easy add-on

Dataguard ePay gives you the ability to seamlessly add-on secure digital functionality to your existing payroll infrastructure.

The uniqueness of this platform is that it is designed to work with **all** payroll solutions - it does not matter which software you have now, it will work with it and anything that you might want to install in the future.

Wide range of benefits

You can reap all the benefits (cost, time, efficiency, environmental, regulatory compliance all within a high grade security environment) with the minimum of business disruption, staff training or systems development costs associated with taking such a significant step.

Payslips. By Email. Securely.

- Fast to adopt
- Integration with any payroll solution
- Very cost efficient
- Increased productivity
- Flexibility to include non-digital employees
- Highly secure end to end
- Reduced carbon footprint and environmentally friendly

FOR THE EMPLOYEE

Receive your electronic payslip immediately

Dataguard ePay gives you the option to receive and archive your payslips electronically, now and into the future, whatever that may bring.

Simple app on any of your devices

Download either a smartphone or desktop app (or both) and whenever your payslip is sent you have access to it immediately. You do not need to login to a portal and retrieve it. Like a traditional payslip it is 'pushed' to you but receipt is through your choice of device (or devices).

Your payslip. By Email. Securely.

- Accessible 24/7
- Maintains confidentiality
- Flexibility to view, print or store local
- Payslips accessible regardless of current employer
- Multi device - smartphone, tablet or computer - iOS, OSX, Windows, Android
- Reduced carbon footprint and environmentally friendly

How it works

Register and download the Dataguard software. In your existing payroll system simply add your employees' chosen email addresses to their payroll details and add an email field to your print template.

Invite employees to use the service and, thereafter, instead of printing the payslips you simply email the batch to all those who have chosen to receive their payslips in this manner.

The software and platform then takes over and manages all the stages of the message encryption and transmission through to recipient authentication and decryption.

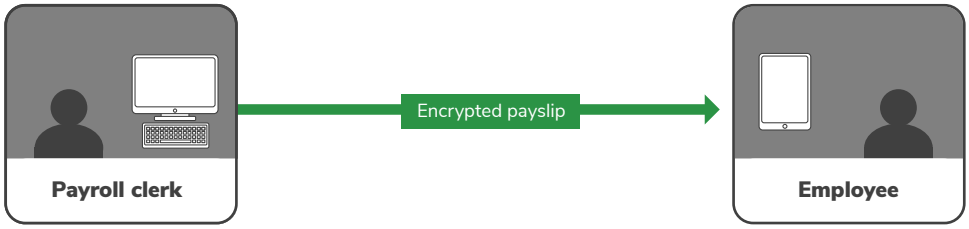
At all stages the email containing the payslip is secure, and can only be accessed by the intended recipient.

If an employee does not have an email address you can offer them a choice between receiving a payslip mailer or to continue with the way they currently receive their payslip.

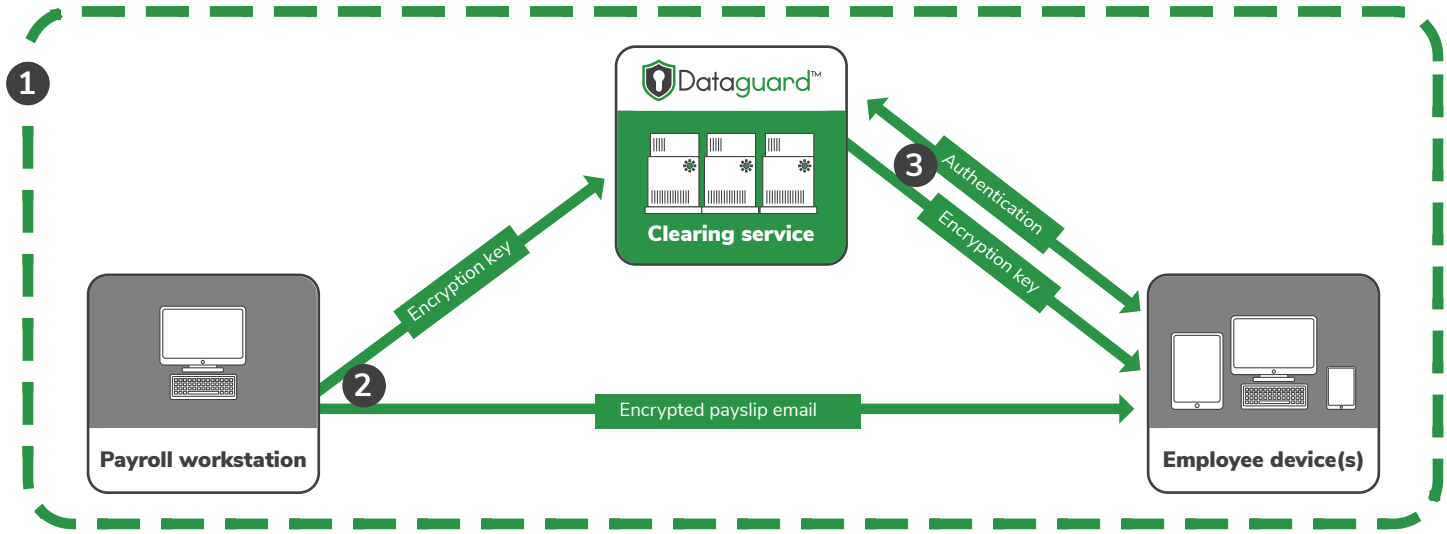
Employees accept the invitation to receive digital payslips from their payroll department. They can then download and install the client software.

With the secure delivery of the payslip to the employee's choice/choices of device, the attachment can be opened with a double click (like a PDF document) through a custom user interface. It can then saved or printed as required by the employee.

How the system looks to users



Behind the scenes encryption and authentication



1. Fully encrypted AES 256 capability established between payroll, employee and Dataguard
2. Encrypted payslip sent by email to recipient, encryption key sent to Dataguard clearing service
3. Recipient authenticated, encryption key passed on, message decrypted and read

Why is ePay so safe?

To open the encrypted message you need to have the recipient's email address, the hash code and the message key. None of which are sent together.

The email is sent encrypted without the hash code & message key so if it is intercepted on its journey the message and its attachment would be unreadable. The hash code and message key are sent to the clearing service without the email address details of the sender and the recipient or the message content.

Only the recipient who is registered with the client software is able to read the message. For added security the recipient can choose to add a password on to the email which needs to be confirmed before the message will open.

What is regify®?

The Dataguard ePay service is powered by regify® technology. regify® enables the only network solution for secure and binding e-mail-communication and electronic post. Whereas many vendors narrowly define "secure e-mail" as encrypted e-mail, regify®'s comprehensive solution includes features such as confirmation of receipt and an auditable web-based tracking log of the transactions. regify® elevates ordinary e-mail to the level of a registered electronic letter. Regify®'s secure digital transaction service is globally recognised and trusted . It has been approved by Mastercard to underpin its encryption key technology for its virtual credit cards. Uniquely, these keys are only ever used once and only for each individual transaction.

How does Incert fit in?

Incert Luxumbourg is the equivalent to BACS or UKPAY and is a security clearing house and is used by regify® for managing its Public and Private Encryption Keys. Incert is a public agency under the Luxembourg Ministry of Economy and a recognised centre of expertise. It is based at one of the most secure Tier 4 Data Centres in the world. Tier 4 is the highest level of data storage and is built to be completely fault tolerant and has redundancy for every component. It has an expected uptime of 99.995%. This datacentre is used by regify® as the secure base for its platform

Security standards and algorithms in more detail

A data security process is only as strong as its weakest link. Deploying high level security to only one part of your process, does not, by definition mean your entire process meets that standard. Dataguard is powered by regify® which is based on established standards and proven algorithms which complement each other's strengths right across the data communication process.

regify® uses the following:

SSL encryption
For the connection between the employee and the sender, a SSL connection is used. If you are an authenticated masterEpay member and you are using your identity-file, the complete data transfer will get encrypted in addition to SSL.

AES encryption
The message and attachment (*.rgf file) are encrypted using AES256. A new key is generated for each message. Compared to traditional PKI technology, certificate-based hybrid encryption is not required. As a result, the security of the message does not depend on the security of an RSA key.

RSA encryption
RSA encryption is used for the secure transfer of the message-key to the clearing service.

Dataguard ePay does not have access to the message key. The provider communicates on the basis of an identity-file useing RSA encryption. The information secured by using RSA needs to be secure for just one moment. A secure keylength is not needed by the regify process, as the message-encryption does not rely on RSA keys.

SHA-2 hashcodes
The message integrity is achieved by using SHA hashcodes with a length of 256 bit.

Random number generators, that qualify for cryptography
The random number generator is based on the strict NIST SP 800-90 standard. This is compliant with FIPS PUB 140-2. They are used for generating the key for the regify® message, for

Dataguard Security Ltd
Bloxham Mill | Bloxham | Banbury | Oxfordshire | OX15 4FF
+44 1295 724 101 | dataguard-uk.com