Dataguard™

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

eBox datasheet

Dataguard ePay
Encrypted Payslips

Dataguard eMail
Encrypted eMail

Dataguard eBox
Encrypted Storage

How do you manage the sharing of confidential files?

- Q Do you restrict the sharing of confidential documents due to security concerns?
- Q Do these restrictions hinder idealised workflows?
- Q Does the maintenance of user rights for shared access of confidential files cause significant workload issues?
- Q Are you confident that your cloud storage is fully secure?
- Q Do you struggle to maintain version control with your shared files?

Did you know...

- ⚠ Your processes may be in breach of GDPR
- ⚠ The intellectual property of your business and the confidential data held by key projects may be vulnerable
- ⚠ Cloud storage users are reliant on the security the host implements

Comparison between confidential document and data sharing solutions

Dataguard™

	a **Local storage** of confidential documents & data	b **Server storage** of confidential documents & data	c **Cloud storage** of confidential documents & data	d **Dataguard** Encrypted storage
Transit	Regardless of the security of the storage of your confidential files, the files and data held by these files will still need to be transmitted between users. This makes the data vulnerable to hacking and man-in-the-middle attacks. Not every server or cloud solution provides in-transit encryption.			✓ All files in transit encrypted to AES 256 standard
Synchrony	Manual management of access, simultaneous document use and version control becomes exponentially more difficult as the number of users, documents and amends climbs.	Server and cloud storage can only provide synchronisation whilst the data is within its domain. As soon as a user copies or sends that file to a new domain (a new user or a mobile device for instance) then all the synchronisation ties are broken.		✓ All files remain within Dataguard domain. Impossible to not be synchronised across all users
Security	Manual password management of documents creates inherent vulnerabilities. Low strength passwords and unencrypted password transmission between users is a feature of this form of management.	Not all server and cloud solutions provide encryption for their files at rest. And of those do, only one provides encryption on a per-file basis - meaning if the security key is breached and the encryption is compromised malicious actors can only access the data for that single file, rather than the whole store		✓ All files at rest encrypted to AES 256 standard
Auditability	There is no method of automatically generating an audit trail of users, permissions and amendments. Least of all where amendments have been simultaneously created.	None of the current server or cloud storage facilities can provide full audit trails of users, permissions and amendments		✓ Full auditability of users, permissions and amendments, regardless of numbers of users, files or versions

The eBox solution

Easy add-on and use

Dataguard eBox gives you the ability to seamlessly add-on secure digital functionality to your existing document workflow. It provides user friendly administration and intuitive control.

End to end security

You can enjoy high levels of confidence in your confidential data processes, knowing that data and files are encrypted at every transmission, and in shared storage, and that encryption keys are only ever held by registered users.

Electronic File Sharing System – Encrypted

- Dataguard eBox has the highest levels of data security and data protection
- User-friendly administration with minimal effort
- Anonymised key management via a trusted, independent third party
- Only registered users have access to data
- Registration information deposited with a trusted, independent third party
- Verification of registration data on demand at any time
- One Dataguard eBox for an organisation or one per group or task
- Operational flexibility with options for public and private cloud
- Integration into business applications via Application Programming Interface (API)
- Available for all major software platforms Mobile (Android, iOS) and desktop

Who would benefit from Dataguard eBox

Everyone needs the ability to share and store files securely!

You do not need extensive software knowledge in order to set up the solution. Dataguard eBox works as an add-on to your existing software, no software integration is required.

ALL organisations have sensitive date that they need to share and examples of the most important ones who share PII data regulated by GDPR are:

Dataguard eBox makes the secure sharing of data easy and intuitive so whether you are in HR, Accounts, IT, C-Suite or indeed any department that shares sensitive data then we can ensure it remains safe always!

- Accountants
- Technology
- Solicitors
- Pharmaceutical
- Healthcare
- Finance

How it works

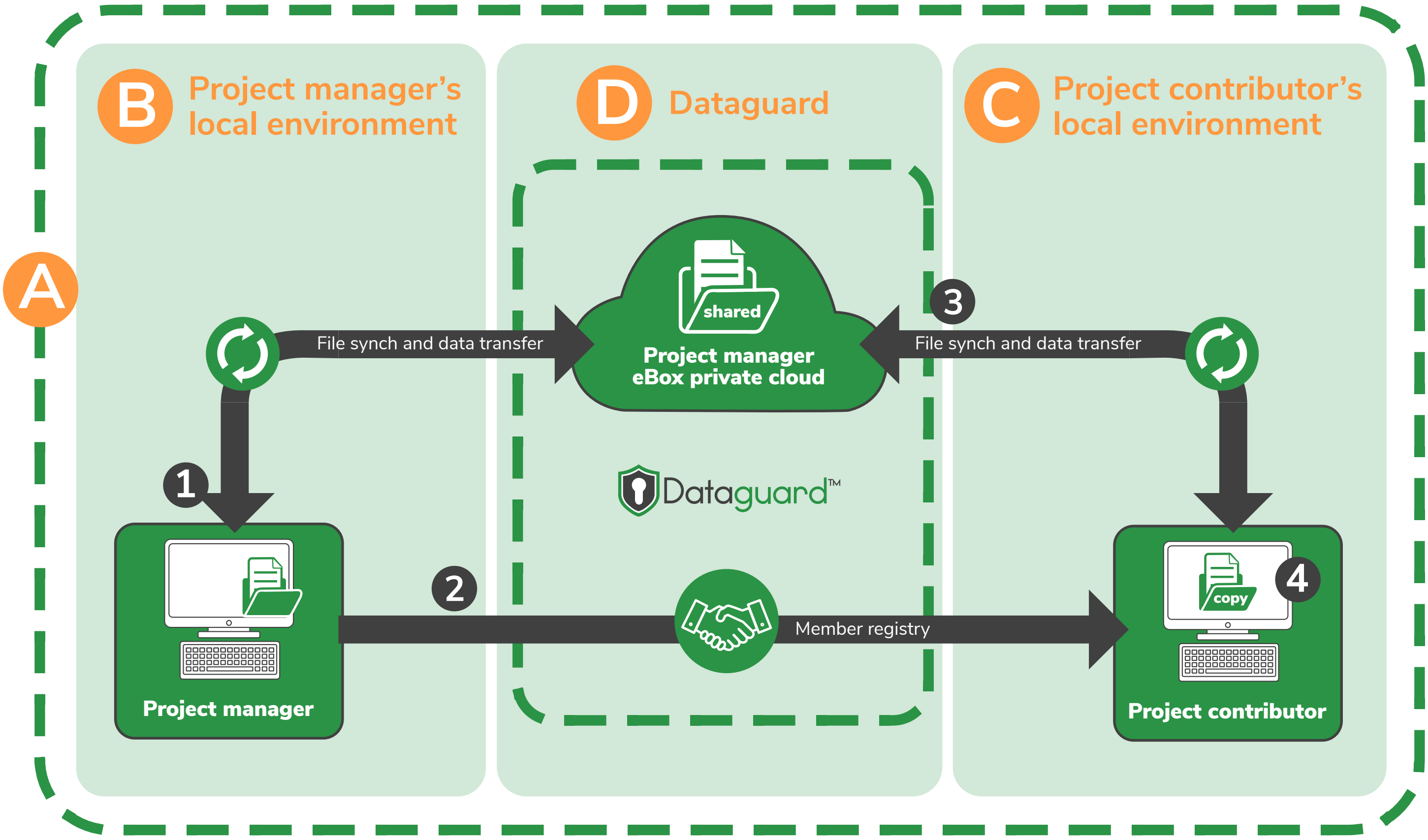
The creator of an individual eBox creates it by push of a button, then electronically invites the members and assigns user rights.

Upon acceptance of the invitation, the user will be admitted to this eBox and in addition to receiving online web access, the user may also choose to automatically replicate parts of the eBox or the eBox as a whole onto his own infrastructure, from smartphone to server.

Every eBox will be automatically registered by a trusted, independent third party in an auditable manner as is required.

The software creates an eBox folder inside your standard "Documents" folder. Everything inside is part of your eBox(es). You can do all those regular tasks like create, copy, paste, move, change and delete your files and sub-folders, as part of your normal workflow.

All eBox related tasks such as invitations, restoring files and versions, can be done using your eBox manager .



A
B
Project manager's local environment
D
Dataguard
C
Project contributor's local environment
shared
Project manager eBox private cloud
File synch and data transfer
File synch and data transfer
3
1
Dataguard™
2
Member registry
copy
4
Project manager
Project contributor

Security structure

A Fully encrypted AES 256 capability established between project manager, Dataguard and project contributors

B C **Encrypted project files** only exist locally in project members' devices. **Encryption keys** only exist locally in project members' devices.

Files are encrypted on the fly by users' devices. Everything that leaves a project member's device is encrypted.

D Dataguard manages the project member identities and the passing through of encrypted data to permitted devices. Data is unreadable at any point other than permitted users devices.

Set-up and user process

1. eBox **private cloud** created at touch of a button on project manager's device
2. Invitations, acceptances, user rights assignments and web access for contributors initiated by project manager and managed by Dataguard
3. Project contributors access/create/amend documents through eBox software all within local replica of original file structure
4. Partial or complete 'copies' of eBox can be created locally by contributors

Why is eBox so safe?

In order to make sure that your eBox data is always secured, the encryption and decryption is done on the fly so that the eBox provider, who hosts the data, is not even able to peek into your files.

All data stored by Dataguard is encrypted with a unique eBox-key. Dataguard cannot access the contents and does not even know the file names.

What is regify®?

The Dataguard eBox 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