From : Marlon Domingus

Date : December 08 2017

Subject : EUR document vault / BlackBerry Workspaces - security

**EUR Document Vault**

***in short***

Scientific integrity and safeguarding privacy in scientific research are important values for Erasmus University Rotterdam. With regard to taking the appropriate organisational and technical measures, the EUR acts compliant to the General Data Protection Regulation (GDPR). To this end, it applies the principles of privacy by design and privacy by default in the research design. A data protection impact assessment (DPIA) takes place under the supervision of the data protection officer of the EUR. For online collaboration during research the EUR Document Vault is used; an end-to-date end-encrypted and ISO 27001 certified secure environment. This document vault runs on BlackBerry Workspaces (see also: https://www.youtube.com/watch?v=WiTZAvegfS0) a system also used by the AIVD, the General Intelligence and Security Service of the Netherlands. In this document vault, EUR researchers are able to work safely with data of the highest data classification. In the document vault, the lead researcher has access to a wide range of advanced file protection measures, logging and monitoring of use and controlled access.

***detailed***

All documents stored on the EUR document vault are kept in encrypted form using individual, strong, randomly generated 256-bit AES encryption keys. These keys are part of a key-chain hierarchy, which includes a top-level 256-bit AES master key. Decrypting a document requires access to all elements of the key-chain.

The EUR document vault runs on BlackBerry Workspaces

**Network and Remote Access Security**

*Secure network architecture*

Firewalls monitor and control communications at the external boundary of the network and at key internal boundaries within the network.

*Role Based Access*

BlackBerry Workspaces web applications employ a Role Based Access Control security methodology. The security layer of the software restricts the user according to security permissions, with no ability to move across unauthorised boundaries.

*Two-Factor Authentication*

Administrative access to production systems requires strong two-factor authentication.

**Data Privacy**

*Data Encryption*

BlackBerry Workspaces uses the FIPS 140-2 compliant 256-bit AES encryption, which is a modern and very strong cryptography system used by businesses and governments to protect sensitive information.

All key data fields that contain data from user input, registration, content, and policies are encrypted at rest. The storing of the documents and meta-data in encrypted form ensures that even if intruders obtain the actual physical disks on which they reside, they will not be able to read or modify them.

*Communication Security*

All user data transmissions over the Internet to and from the BlackBerry Workspaces servers are sent using HTTPS (Secure HTTP connections), and are encrypted via SSL/TLS (Secure Sockets Layer/Transport Layer Security) employing strong keys (128-256 bit, depending on the browser capabilities).

*Secure Storage*

Once documents are uploaded to the BlackBerry Workspaces servers, they are immediately encrypted and stored on a secure volume, accessible only to the BlackBerry Workspaces application server. Direct access to this volume from outside is impossible, as this volume is not accessible to the Internet in any way other than through the mediation of the BlackBerry Workspaces application servers. The application servers moderate the access of users to content based on their assigned permissions within the policy set by the content authors.

*Secure Key Management*

Each document is stored encrypted using its own unique cryptographic key. Thus, gaining access to one key does not invalidate the security of the rest of the documents in the system.

*Secure API Access*

The application server does not expose any les (documents, executables, or configuration). The only way to access les on the system is by providing the server with a valid security token tied to both the verified user and to the user’s physical machine, and transmitted in encrypted form (using HTTPS) to prevent interception.

*Data De-identification*

Encrypted documents are stored in a manner that prevents association between the document itself and meta-data information such as the document’s owner, its recipients, or its original file name.

**Secure Online Viewer**

The secure online viewer allows high fidelity online viewing of secure documents without requiring the recipient to install any software or plug-ins. The secure online viewer uses various methods for protecting the content of documents presented in it:

• The document is streamed over SSL

• Documents are encrypted using AES 256-bit and RSA-2048 encryption.

• The viewer’s browser does not cache the document locally.

• Code is obfuscated using various techniques, making its protection logic very difficult to analyse

• Various protection measures are taken to prevent viewers from copying the document’s text or images.

• Watermarks unique to the recipient can be added to the document.

• The administrator can customise a watermark’s position, text, structure, and color.

• The operating system’s print screen function is hampered (for more advanced protection users can always use Spotlight feature).

• The document owner or administrator can deny print permissions, but the recipient can always request print permission. The browser’s print function is always disabled (a print job will result in blank pages).

• The owner can set an expiration date or revoke the document at any time.

• The owner can track the viewer’s actions (such as opening and printing the document). Log attributes include the time and date of the action, the user’s IP address and geographical location (based on IP geo-location technology), and the viewing machine’s ID.

• The document owner can modify all user rights easily at all times.

**App**

The BlackBerry Workspaces app provides many security features, including:

• 256-bit AES encryption at rest (for documents synchronised to the device or cached)

• Optional user passcode required for access to the documents (centrally provisioned)

• Document watermarks

• Document expiration

• Disabling of iTunes and iCloud sync and backup

• Secure key storage

• Document tracking and remote document kill

• Jailbreak detection

• Anti-clock tampering measures

**Qualifications**

**FIPS 140-2**

BlackBerry Workspaces encrypts files while they’re in use, at rest or in transit using FIPS 140-2 validated cryptographic library and 256- bit AES encryption.

**HIPAA**

BlackBerry Workspaces is able to support the HIPAA and HITECH regulations, as well as sign HIPAA Business Associate Agreements (BAAs) with customers.

**AICPA / SOC 2**

BlackBerry Workspaces has completed a AICPA / SOC 2 certification of its internal processes.

**Certificates**

BlackBerry is ISO 9001 certified:

<https://global.blackberry.com/content/dam/blackberry-com/PDF/enterprise/company/certificates-qnx-iso-9001-v2.pdf> [valid - September 15 2018]

ISO 9001 is the most widely adopted international quality standard with over 1.1 million certificates issued worldwide. BlackBerry has been certified to ISO 9001 since 2005. The standard is based on a number of quality management principles which include having a strong customer focus, organisational leadership driving quality engagement, using the process approach and continual improvement.

ISO 27001:2013 certified

<https://global.blackberry.com/content/dam/blackberry-com/PDF/enterprise/company/certificate-blackberry-iso-27001.pdf> [valid - May 31 2019]

ISO/IEC 27001 provides a model for establishing an information security management system (ISMS), which aligns people, resources, and controls, to create a series of measurable security practices to protect information assets. BlackBerry has an established record of integrating secure practices. In 2002, BlackBerry was one of the first organisations in North America to receive accreditation against the BS7799 Security Standard. This standard was later adopted by the International Standards Organisation as ISO/IEC 27001:2005 and, most recently, ISO/IEC 27001:2013