AV-LAB

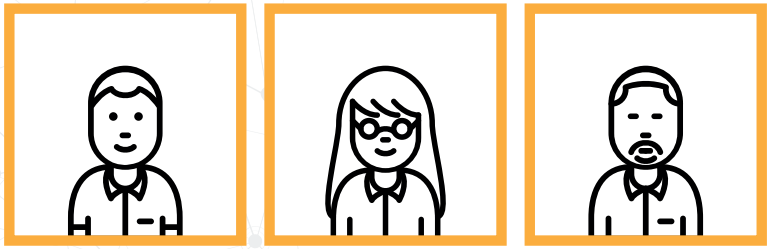
THE INDEPENDENT ANTIVIRUS TESTS

Date: June 2020

"Made in Poland": a comparison of solutions to encrypt documents and sensitive information

Experts are unanimous

Encryption is one of a few recommended ways to protect digital information against an untrusted third party. Documents converted into unreadable form will be useless to hackers. Thanks to cryptography and mathematical computing, it is possible to adapt computer data to worthless digital noise, providing protection and confidentiality of files being processed.



The concept of integrity and confidentiality [1] is explained in Polish law of 10th May 2018 on personal data protection to the regulation of the European Parliament and the Council of 27th April 2016. These terms determine the way of handling personal data – they must be processed using technical and organizational measures in order to ensure safety in the event of inadvertent loss, physical destruction, or partial damage. The organizational measures may be pseudonymization and minimalization. The technical measures may be encryption which is a technically irrefutable method, meeting data integrity and confidentiality requirements.

In the context of RODO, anyone who processes personal data must comply with the rules. This applies to the biggest private and public organizations, from banks and public services businesses to websites which are managed by individuals conducting small businesses. It can therefore be conducted that it is necessary to provide the protection of personal data wherever they occur.

The weakest link in encryption is to edit unlocked documents. Experts agree that insufficient security may lead to a loss of information. As a result of successful cyberattack or malware activity, a person who controls an attack chain will be able to capture decrypted data. Additionally, experts believe encryption should be one of a few steps to digitally protect data from disclosure, as it guarantees the protection of stored backups, and also allows to share documents, meeting high security standards..

Encryption provides the highest level of protection of information, although the recipient's credibility is a weak link when it comes to deliver encoded files. A sender must be sure, and at the same time aware of the risk that a recipient who is about to receive confidential documents has not lost control of its device, and he is who he claims to be. Experts agree that no one other than the sender and the recipient should be able to read encrypted data. This problematic aspect is important for those who expect the highest standards of privacy.

Entrepreneurs and individuals who would like to try out the encryption software mentioned in this report do not have to meet such stringent requirements about technical knowledge on cryptography. Solutions developed by Polish engineers provide an authenticity, secrecy, and functionality of group file sharing through easy to use graphical interfaces. From organizational point of view, the opportunity to choose where to store encrypted files, or manage employee accounts is another advantage. This means that small and big companies do not have to choose between security and privacy because these areas have been managed well by developers of the solutions being compared.

Cypherdog, Specfile, and Netia Data Safe are ready to meet strict requirements set by the General Data Protection Regulation. They have additional features that help organize and manage work, and at the same time guarantee uncompromised security of access to files including user privacy, and secrecy of information being sent.

[1] http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001000/U/D20181000Lj.pdf

Why it is worth to encrypt?

- Encryption hides information from untrusted people.
- Encryption protects data against an unauthorized access from the outside and the inside of a company.
- Encryption is an additional protection of a company laptop and a smartphone.
- Encryption does not create an additional risk of data leak.
- Encryption is independent of other security layers.
- Stolen encrypted documents are not valuable to criminals.

Who is encryption important for?

There are professional groups or industries which security is essential for. These include people responsible for company finance, accounting offices, lawyers, doctor, judges, attorneys. Personal data processed by emergency services, police and bank should be particularly protected. Private companies and state institutions should benefit from encryption because of the confidentiality of tender and information documents, research and development projects, offers, and trade agreements. Information security also applies to people who do not agree to share contacts and metadata with companies such as Google, Apple, Facebook.

When encryption is not effective?

- Confidential documents must be encrypted in edit mode.
- Encryption does not protect against all threats.
- Ransomware can overwrite already encrypted files.
- Encryption does not provide security in case of drive failure.

Remember!

The encryption key is the only form of securing file and directories. You have to protect application password as best you can.

Store sensitive data in encrypted directories or encrypted external drives.

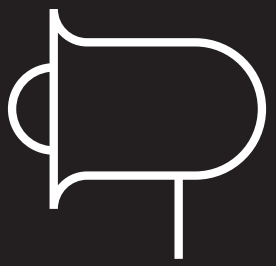
Connect an encrypted drive to your computer only when you are working with importantdocuments, and disconnect it right after the job is finished.

Unlocked files can be stolen by a hacker or destroyed by malicious software.

Besides encryption, use a solution to protect against Trojans and keyloggers. An active keylogger reduces the protection effectiveness of private key password.

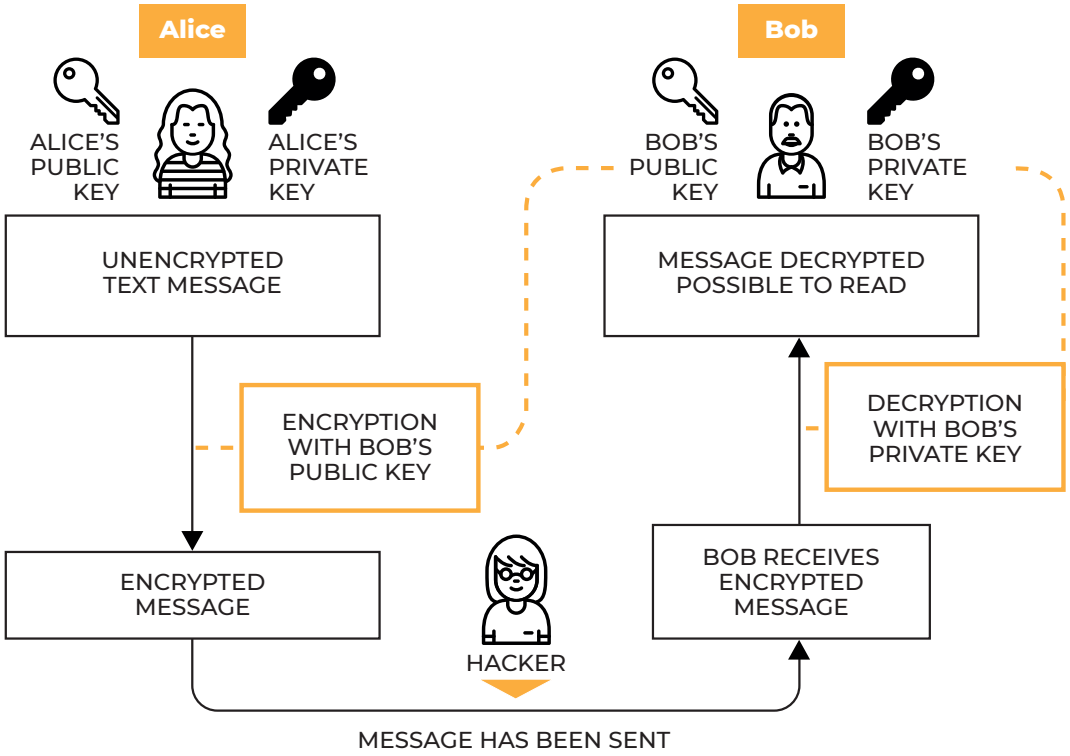
Data breach is not always the result of a cyberat-tack from the outside. Someone inside your company can steal data through a web browser, email, instant messenger, or photos taken with a smartphone.

Implement the DLP (Data Leak Prevention) solution in your business to protect against uncontrolled data breach.



Encryption based on asymmetric cryptography

The public key cryptography allows establishing a secure communication even when it is not possible to agree on a secret key in advance. This is important for secure online transactions. The public key cryptography provides a mechanism of “signing” files digitally. This ensures that contacts are authentic. But it has one disadvantage: it does not guarantee that a message definitely comes from the sender. Someone who has already come into possession of a device may pretend to be the caller. For this reason alone, it is important to remember to protect computers, laptops, and smartphones against theft.



In the asymmetric cryptography both sides that communicate have two own keys: four keys in total. The magic of the public key cryptography lies in the fact that a message encrypted with a public key can be decrypted just with the private key belonging to the same key pair. Therefore, in order to send an encrypted message to a sender you must have the public key which files are encrypted with.

As an example:
If Alice encrypts a message with Bob’s public key, and even though a hacker knows that Alice used Bob’s public key, and that a hacker knows Bob’s public key, he is not able to decrypt a message. Only Bob can decrypt a message from Alice using his secret private key.

Public keys may be disclosed and exchanged, for example, via email, instant messenger, on website, or deliver on a flash drive in person, but it is not recommended to disclose a public key to third parties. Indeed, there are graphic applications used to generate keys, but they can be difficult to operate, and exchange between interlocutors without the technical expertise at the appropriate level.

The private key and application password protection

A private key should be kept as secure as possible and stored out of the reach of other people because it should only by possible for the owner of this key to decrypt data. If you disclose a private key, encrypted data can be decoded (but not always).

Developers of the Cypherdog, Specfile, and Netia Data Safe solutions use additional protection in case of theft of login and password of application. It can be, for example, so-called “trusted devices”: only those indicated by a user or an administrator allow an owner of an account to authorize access.

The obligation to import a copy of a private key or create a rescue configuration may be an additional control. Only then it will be possible to log in to another device. Solution providers have taken care to ensure that control mechanisms that are independent of encryption secure data against unauthorized access with one more protection layer.

How to encrypt files with Cypherdog, Specfile, or Netia Data Safe?

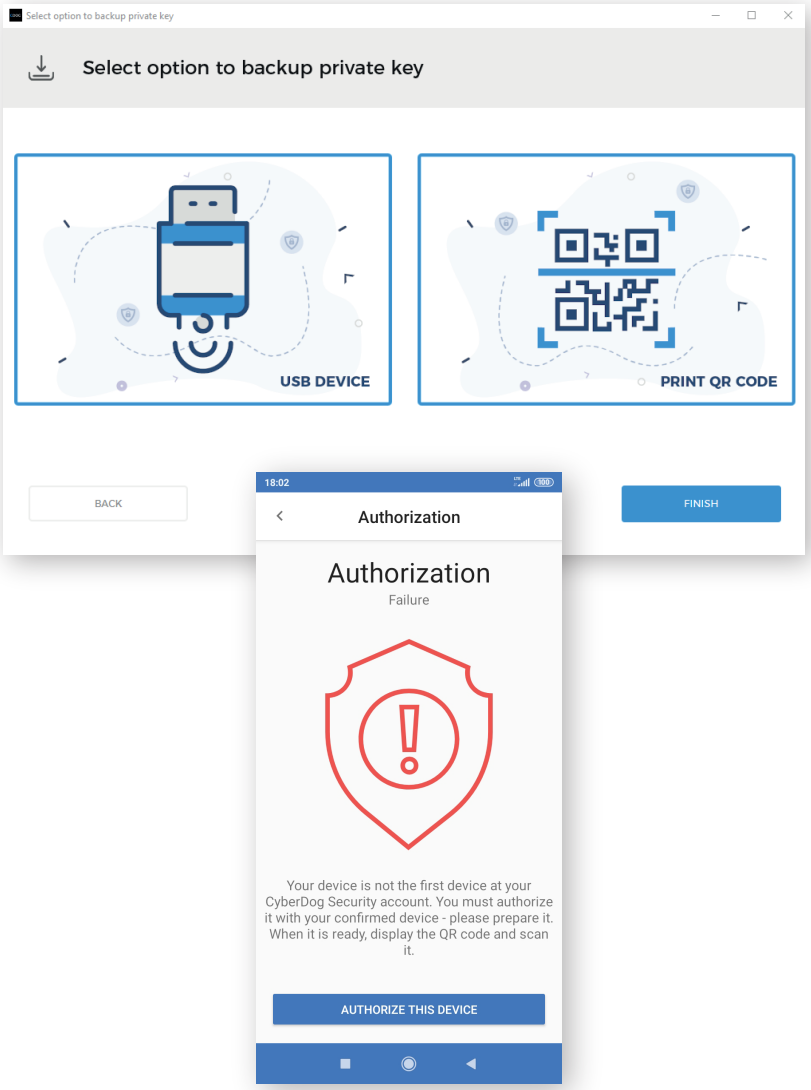
The solutions described in this report do not require technical knowledge of encryption. In addition to automatic exchange of keys, they add subsequent layers of security that are not available in the asymmetric cryptography.

User does not need to know anything about generating keys and using the public key cryptography. The Cypherdog, Specfile, Netia Data Safe software are recommended to all entrepreneurs as well as private individuals because of the possibility of group work, and additional security enclosed in the graphic application that is not more difficult to use than a web browser. Technically, the aspects needed to generate and exchange keys shall be implemented by the application that is as simple to use as possible.

CYPHER.DOG™ specfile.pl NETIA Data Safe

Presentation of tested solution

CYPHER.DOG™



The application allows to securely send files in any formats and size. All transfers are encrypted in the end-to-end mode. Developed technology and method of encryption ensure that no one except the specified recipient is able to decrypt a transferred file. All you need to do is add a recipient to your address book, and start a secure file transfer.

Data cannot be read by anyone, neither by a developer nor by any other “third party”. At the same time by confirming the identity of contacts in blockchain registry, user can be confident that no one is pretending to be the person who he communicates with.

Cypherdog, in addition to encryption in the same application, offers a text chat with added contacts. The developer has implemented the highest level of privacy, so that the solution applies to any organization, and individual consumers who value anonymity and confidentiality. It is particularly useful in the legal, financial, sales, medical, industrial sectors, and research and development organizations.

Questions to the expert

Expert's name: **Przemysław Kucharzewski**

Post held: **VP Sales, Cypherdog Sp. z o.o.**

? In what situations does encryption not affect data security? Things to bear in mind when encrypting files.

Encryption does not affect data security in the event of deliberate or unwitting violation by their owner of basic principles of keeping secrets needed for authentication in a system that stores this data. Secondly, the use of weak methods of encryption also significantly reduces security of encrypted data. Unique and strong passwords should be used to secure encryption. Select encryption method that provides a high level of security, with relevant keys that are stored in a way that unauthorized users cannot obtain them. Plus, remember to permanently delete unencrypted original file (a simple "delete" command does not mean at the same time that it is impossible to recover a file using tools to recover deleted files).

? Does working with decrypted files pose a threat to a company? What to avoid, and how to protect sensitive data when editing file?

Working with decrypted file should take place on secure computers that belong to a company in properly protected local or virtual network. Data encryption is a necessity in case of sending data between users using public networks, or storing on external servers and platforms. Operating systems provide sufficiently high level of security for files stored locally such as drives encrypted with the BitLocker technology for Windows, or FileVault for MacOS. The weakest link in disk security regardless of their location (computer or cloud) is always the user that does not respect basic principles of security policy of storing authentication data.

How companies should allow employees to share files to do so in accordance with a security culture and current legislation.

In corporate local network, operating systems, network directory services, and centralized authentication and authorization services are sufficient resources to build well-managed environments for work groups. However, a security culture requires strictly to use solutions to encrypt both communication channels and data themselves when transferring data outside a corporate local network.

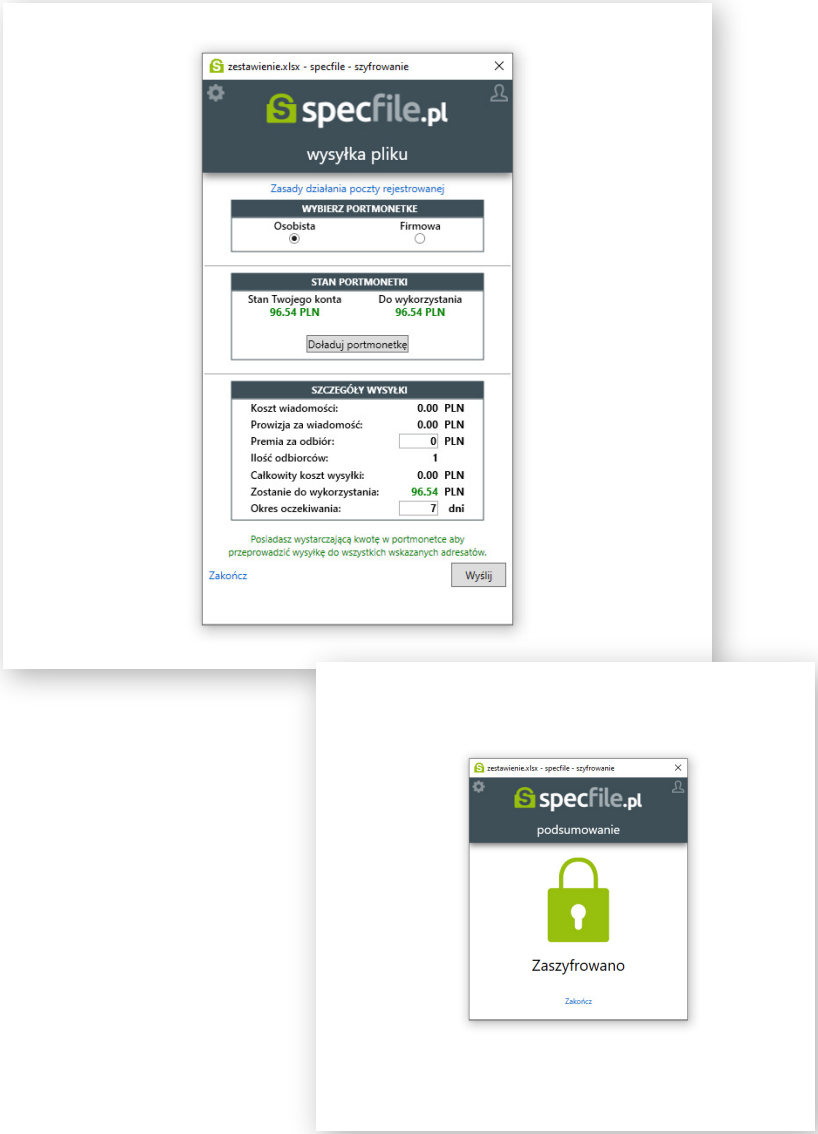
Can encryption help eliminate the problem of mixing files and business data with private ones?

The idea of “mixing” personal and business data is a denial of the basic principles related to the confidentiality of company data. Encryption in this case does not solve the basic problem of the lack of control of the company over its data. Only when an employee is provided with the environment that absolutely separates corporate data from private data, we can start building additional layers of information security such as “encryption in transit”.

Is encryption sufficient to meet many requirements posed by so-called RODO in the context of processing and retention of personal data?

Encryption helps meet many requirements, but not all. Encryption is particularly helpful in the field of compliance with the obligations of storing backups under the regulations related to running business activities as well as law on processing confidential information. The second very important issue associated with encryption is to ensure a consistent system for an authorization and audit of access t o these data. Even the best methods of encrypting data in situations when everyone has access to the encryption key are only to create the appearance of information confidentiality, accessibility, and integrity.

Presentation of tested solution



Specfile allows one-click data encryption, and send so-called “Electronic Registered Mails”, equivalent to traditional registered letters. If a recipient receives and decrypts a file sent, a sender will receive an email with acknowledgement of a receipt. This kind of exchange of information ensures that any confidential file is protected against unauthorized access. The application allows secure exchange of confidential documents between partners and colleagues over the Internet.

Specfile uses cryptographic algorithm with 256-bit key to encrypt files. The key is encrypted using the RSA algorithm with the use of a pair of 4096-bit private and public keys. Currently, there are not known decryption methods of such encrypted files without the knowledge of keys which ensure the confidentiality and security of all directories.

Specfile will have applications in patent protection, know-how plans, tax settlements, company documents, and file archiving. Non-technical users will find themselves in this application who work in accounting offices and law firms. The solution of this developer can protect patients results, and their records in clinics and hospitals.

The product meets all expectations wherever the staff want the application to be easy to use and intuitive to encrypt.

Questions to the expert

Expert's name: **Katarzyna Abramowicz**
Post held: **President of Specfile Project**

? In what situations does encryption not affect data security? Things to bear in mind when encrypting files.

Encryption does not affect data security in many situations: when encryption occurs in the infected system, when we encrypt data that is publicly available, when encryption has been carried out the wrong way, or when encryption is not combined with data integrity verification and mechanisms to ensure that the origin of data is undeniable, for example, digital signature. In addition, encryption has been carried out in a system with a fairly predictable state at the time of encryption what can result in poor quality of pseudorandom data used to encrypt and generate secrets, and also that encryption occurs in an untrusted environment which configuration is not fully controlled by a user. Encryption security is at risk when it is based solely on a single factor, for example, on user's password which as we know most often has a low safety index. I think it is worth knowing.

? Does work with decrypted files poses a threat to a company? What to avoid, and how to protect sensitive data when editing?

From the perspective of software allowing to work with .pdf, docxitp files, this application must see file data so it would be non-confidential. This means that the work eventually is carried out on public data. There is no need to remember to encrypt a file after finishing work in our application.
Instead of calculating whether something is safe or not, it is better to confine yourself to calculation of potentially known bad practices, threats to encryption and elements of a system that can compromise this process, and then ensure that all threats are eliminated.
It can therefore list situations such as: a weak policy of access control to confidential and even worse its execution. When another person has an access to our computer or we encrypt data in an environment that we do not control. This list should be much longer and cover many purely technical aspects.

How companies should enable employees to share files to do so in accordance with a security culture and current legislation.

In general, a user is usually a weak element of a system. The more users can access a file, the more potential inflammatory links to compromise distributed data.
No matter how secure policy of data protection we create – too much depends on the end user and his practices when handling data. More investment is needed here in education, rather than in infrastructure.

Can encryption help eliminate the problem of mixing files and business data with private ones?

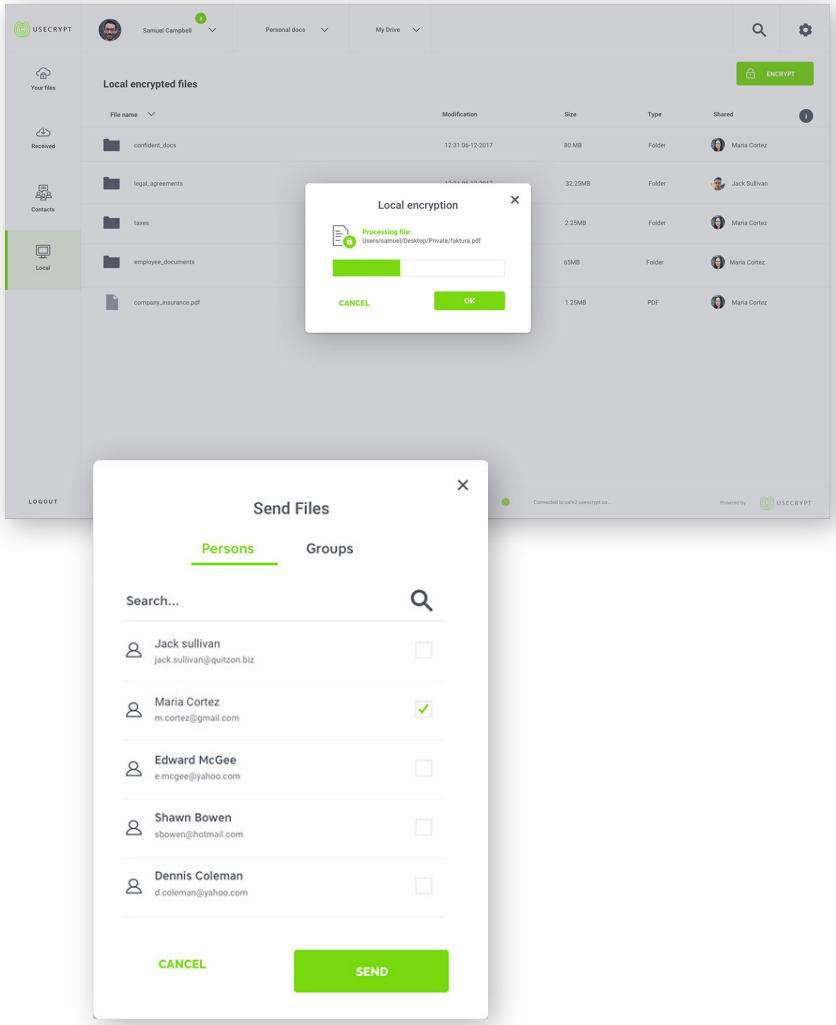
It depends what role we give to encryption. The goal is to secure documents. In our opinion, encryption can even increase the mixing of files. A lot depends on the established file and directory hierarchy. Remember, we are talking about software that only encrypts files. Of course, you can somehow aid a user in this regard by creating a dedicated work mode of the application, for example, private or corporate, and impose or allow him to select directories intended for this data. Applications do not know if they encrypt a private or corporate file. In most cases, users prefer freedom to create a document structure on their computer.

Is encryption sufficient to meet many requirements posed by so-called RODO in the context of processing and retention of personal data?

It definitely helps eliminate the risk of document content being leaked. Remember that encryption is just one of the requirements of RODO. However, it is a significant safety enhancement and an effective tool to prevent data loss and harm to users.

Presentation of tested solution

NETIA Data Safe



Netia Data Safe is a service that ensures a secure storing and sharing of company data through the use of innovative and polish cryptographic technologies that guarantee the confidentiality even from a service provider and a developer of encryption software.

The solution is based on the innovative encryption technology called HVKM (Hybrid Virtual Key Management) which consists in the division of a private encryption key into two separated and stored separately parts. The first is on a computer, and the second is stored securely on a server.

In practice this means that no one other than the owner of a file or recipients indicated by him cannot decrypt data. The software developer or IT administrator also does not have this possibility, because they do not have a unique key half.

The service is addressed to a wide range of entities, among others hospitals, medical institutions, law firms, notarial offices, accounting offices, property managers, audit firms, employment agencies, and headhunting companies. The solution can be applied to wherever we are dealing with the need to secure sensitive data requiring special protection.

Questions to the expert

Expert's name: **Jakub Sawicki**

Post held: **Product Manager of Cybersecurity**

? In what situations does encryption not affect data security? Things to bear in mind when encrypting files.

When we are talking about data security, encryption is one of the primary and essential areas. To this question. I can answer you with conviction that we should not have a situation when files remain unencrypted. Let us remember that most of the documents which we work on are sensitive or even strategic part for our employer. If they were to get into the wrong hands, we would have had a personal data leakage (RODO and penalties associated with it), and a critical breach of credibility or even future of a company (in case of leakage of projects or scheme unpatented inventions).
Things to bear in mind. First of all, examine what encryption and decryption mechanics are used. You can also study a scenario where our login and password would be acquired (for example as a result of a phishing attack or keylogger), and a criminal gains access to data, and decrypts them effortlessly.

? Does work with decrypted files poses a threat to a company? What to avoid, and how to protect sensitive data when editing?

Cybersecurity is one big restricting the possibilities. Maybe it is a strong term, however making cybercriminals life difficult is the most effective way to secure our business. Unfortunately, this often results in inconvenience and limitation for our users.
This is why all additional verifications, passwords, applications, or filters are applied here.
How to assess the usefulness of encryption? Let us imagine that our office computer is stolen. Tragedy? That is part of it, but if we use backups, cloud encryption, and file-based platforms, we do not lose what is essential – sensitive or strategic data to our company. Cybercriminals can recover data even from computers destroyed by an analysis of, for example, only a hard drive. Unencrypted data will be recovered without any problems. Well-encrypted data without a decrypting key, a verified device, and a password?
If they have all computers in the world, and a few billion year to decrypt...

? How companies should enable employees to share files to do so in accordance with a security culture and current legislation.

First of all, use platforms that enable entrepreneur (that is the actual owner responsible for data) to manage (movement, privileges) files, and in the event of loss – with no fear of them being read by unauthorized people.
From the perspective of the users, systems that enable collaborative work, versioning and mutual notification of new changes are very convenient and effective.
Let us recall the last project in which we had to prepare a document, and changes were made by several people. Many versions, everyone works on different one. Finally, a project manager spends hours to merge changes and create a final version. Not to mention even spamming mailboxes and blocking a mail server which for each email and recipient must process and keep additional unnecessary copies of a file.
Using a collaboration platform for many users simultaneously and versioning files is a great job optimization. If everything is encrypted and managed – we are good.
When it comes to regulations and security policy, let us always have legislation in mind, and in particular a short, but very significant abbreviation – "RODO" that is General Data Protection Regulation which more than one publication has been already written for, but for us "ordinary citizens", there are two key messages: "data must be encrypted" (this is probably one of the few technical words that appear in the content of the Regulation), and "personal data leakage means trouble and serious penalties".

? Can encryption help eliminate the problem of mixing files and business data with private ones?

Absolutely! There are several ways to discuss personal data. One of them is containerization that means separation of the work area even on a private device (BYOD – Bring Your Own Device) that will be managed and monitored without any intervention in the private sphere. This can be achieved on both a mobile device and a personal computer.
In the Netia Data Safe service, such container can be automatically created and maintained, that is create a folder which will be automatically encrypted (even on the "drag & drop" principle). Additional tools of security and management of end devices (EDR class: Endpoint Detection & Response, Endpoint Management & Security) allow to force and maintain all security policies, for example, "between the hours of 8 a.m. and 5 p.m., save all .docx, .xlsx, .pptx files in the encrypted folder".
With a proper internal communication, we will avoid the situation when employee's private documents encrypt spontaneously.
On the other hand, this is not a hopeless situation because no one (even Netia) will access the data without the appropriate authority.

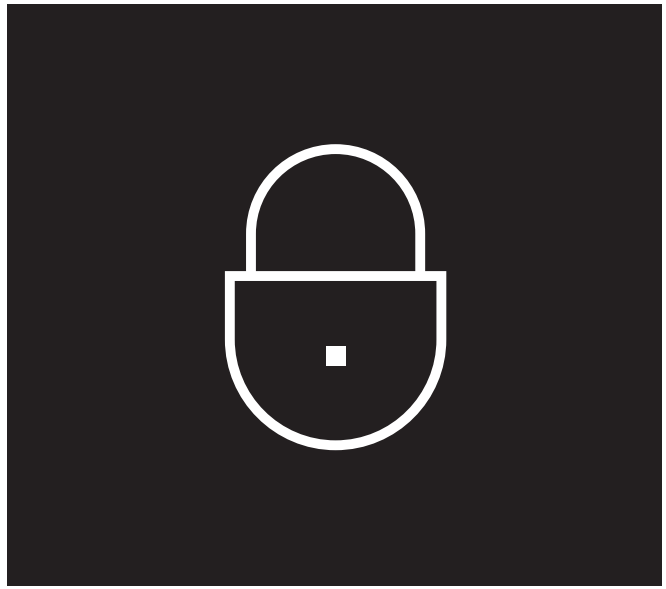
? Is encryption sufficient to meet many requirements posed by so-called RODO in the context of processing and retention of personal data?

It will certainly be one of the most important elements. Entrepreneur who implements a data encryption system may claim that it complies with the requirements of RODO. There mere storing and processing of data will be secured “with due diligence”, and “the right to be forgotten” that customers have toward all entrepreneurs (delete all copies of their personal data) will be possible to fill up which is not fully possible when we use public tools, for example, Google Drive, Facebook, WhatsApp because we are not sure about the final deletion of data. With Netia Data Safe, each entrepreneur is data owner in the full sense of the word, and he is confident about the primacy of managing them.

However, we should not forget the continuous process of training users and improving a security policy. None of the systems will provide 100% safety, so some responsibility (even so small) lies with users. We constantly work on the development and quality of our solution, but we will not be successful without cooperation. When it comes to cybersecurity, we do not stop even for a moment, so I encourage to follow our publications and information because this dynamic and constantly evolving world requires us to be ready. Take care of your business, and keeping our mutual security leave to us. We are here!

security by design

privacy by default



Comparison of solutions to encrypt and group work

SECURITY OF APPLICATION AND DATA

Function or feature	Cypherdog	Specfile	Netia Data Safe
PLACE OF STORAGE OF THE CRYPTOGRAPHIC KEY	A private key is located on an employee's device. A public key is sent to the developer's server and the blockchain network	A public-private key pair when generated on a user's device is placed on the developer's server where the private part is password protected. The secured key pair is then downloaded when logging in. The developer does not have access to the user's private key.	In the standard version, ½ key is located on the local computer, and ½ in the developer's cloud. The version for companies with their own server, ½ key is located on the local computer, and ½ on the company server.
ENCRYPTION METHOD	AES + RSA + end-to-end	AES + RSA	HVKM + end-to-end + UST + AES + RSA + KDF + DH + MAC + KEM
DOES THE DEVELOPER HAVE ACCESS TO EMPLOYEE'S FILES?	No	No	No
DOES A COMPANY ADMINISTRATOR HAVE ACCESS TO EMPLOYEE'S FILES?	No	No	No

Function or feature	Cypherdog	Specfile	Netia Data Safe
IS THERE A WAY TO RECOVER ACCOUNT PASSWORD?	**Yes.** When registering a user, a private key backup is generated in the form of four QR codes. These codes can be printed or placed on the user's removable disk. The "Enterprise" version also provides the option to archive private keys on a service that is run by an administrator on your corporate local network.	**No**	**Yes.** When registering, a rescue configuration is created to recover access to an account if the configuration or password is lost.
IS THERE A RISK OF LOSING FILES IF I DISCLOSE MY LOGIN AND PASSWORD?	**No.** Only the loss of both a profile's login and a password, and a private key password along with a device or a file with key backup or an encrypted key presents a risk of file loss.	**Yes.** You must ensure that your account password is protected.	**No.** Additional controls are required to log on to another computer (see description below).
HAS THE APPLICATION BEEN SUBJECTED TO A SECURITY AUDIT?	**Yes.** An internal audit has been carried out. An external security audit is scheduled for the third quarter 2020.	**Yes.** The application has been subjected to an external audit of a cryptographic system by the cryptography department of Military University of Technology, and twice a usability audit.	**Yes.** Both an internal audit (engines of susceptibility testing used by Netia Security Operations Center), and an external audit by Deloitte consisting in an cyberattack have been carried out.

Function or feature	Cypherdog	Specfile	Netia Data Safe
IS IT POSSIBLE TO LOG IN TO ANOTHER COMPUTER WITH THE SAME LOGIN AND PASSWORD?	**Yes.** However, the migration of a private key is required. The migration of a private key to a new computer is possible using a backup key recovery procedure. In the Enterprise version, the key can optionally be recovered from a dedicated service that is controlled by an administrator on the local corporate network, if the service is configured and started.	**Yes.** However, it is absolutely crucial to take care of the account password because there are no additional mechanisms to prevent from logging into another device.	**Yes.** To log in, a configuration file is required related to an account and an additional authorization. Without authorization of a new device, it is not possible to log into another computer.
HAVE YOU AUDITED AN INFRASTRUCTURE, A SERVER, A STORAGE LOCATION OF DATA AND KEYS?	**Yes.** An internal audit has been carried out. An external security audit is scheduled for the third quarter 2020.	**Yes.** No detailed information.	**Yes.** Data and half of the RSA key (see section 1 covering division of the key) is located in Netia Data Center which uses a range of technologies and security (Data Center level – Tier III).

Comparison of solutions to encrypt and group work

FEATURES THAT HELP FACILITATE AN APPLICATION

Function or feature	Cypherdog	Specfile	Netia Data Safe
IS INTERNET ACCESS REQUIRED WHEN ENCRYPTING OR DECRYPTING A FILE?	**Yes.** You must log into the application. Internet access is needed, among others to confirm compliance of sender's public key with all available repositories.	**No.** No Internet access is required to encrypt and decrypt files on a computer. However, some features will be limited without a connection.	**Yes.** The Internet is absolutely necessary (both for encryption and decryption) because ½ decryption key is located on employee's computer and ½ on corporate server (in the on-premise version) or a developer (in the cloud version)
DOES AN ACCOUNT ADMINISTRATOR OR OWNER HAVE THE POSSIBILITY TO REVOKE ACCESS TO A SHARED ENCRYPTED FILE?	**No.** An administrator can disable an account for an employee in the Cypherdog Enterprise version.	**No**	**Yes.** It is possible to manage users account by an administrator. An administrator can manage files if he has permission to do so.
HOW TO DECRYPT OR ENCRYPT FILES?	Using the Cypherdog application.	Using the Specfile application or the developer's website.	Using the Netia Data Safe application.

Function or feature	Cypherdog	Specfile	Netia Data Safe
LOCATION OF ENCRYPTING AND DECRYPTING FILES	In the application on an employee's computer using a graphical interface or command line.	On an employee's computer using the right mouse button or application on the developer's website.	In the application on an employee's computer or in the cloud environment in case of group work.

Comparison of solutions to encrypt and group work

PLANNING GROUP WORK

Function or feature	Cypherdog	Specfile	Netia Data Safe
SHARING ENCRYPTED FILE WITH EMPLOYEES	**Yes.** The system only supports strong end-2-end encryption without exception. It is possible to send encrypted file between two Cypherdog users. A file can only be decrypted by one recipient. No collective access within the "working groups".	**Yes.** When encrypting a document, it is possible to specify who will have access to a file. It is sufficient to provide an email address. An unregistered recipient will receive an invitation, and he will have to create an account to read a file. Automatic access to a file is granted to administrators in a company.	**Yes.** Sharing data is as secure as possible within created groups with colleagues. Only authorized users have access to files. If permissions are revoked, file access will not be possible.

Function or feature	Cypherdog	Specfile	Netia Data Safe
CHAT WITH EMPLOYEES	**Yes.** Secure communicator is available in the Cypherdog Premium and Enterprise versions (desktop and mobile). The developer does not have access to messages and interlocutors identify information. The product guarantees maximum security.	**No**	**Yes.** Secure communicator is available as a separate application from the same developer.
IMPORTING CONTACTS FROM AN ENCRYPTION APPLICATION TO A COMMUNICATOR AND VICE VERSA	Not required. Contacts synchronize automatically. The system backend stores an encrypted copy of an address book. The developer does not see a user's contact list.	**No**	As standard, a communicator is a mobile application, and Netia Data Safe is a desktop application, so without integration with, for example, Active Directory it will not be possible.
PLACE OF STORAGE OF ENCRYPTED FILES	Encrypted files or entire directories can be stored on an employee's drive, the developer's cloud, or on corporate servers.	After encryption, files are ona user's computer. A customer can then move or copy them to any location.	Encrypted files or entire directories can be stored on an employee's drive, the developer's cloud, or on corporate servers.
USER MANAGEMENT	**Yes.** This feature is available in the Cypherdog Enterprise version.	**Yes.** This feature is available for companies.	**Yes.** This feature is available for companies.

Function or feature	Cypherdog	Specfile	Netia Data Safe
THE AMOUNT OF SPACE FOR AN EMPLOYEE'S FILES	By default, each user of the Cypherdog applicationwill receive 5GB of storage for files. It is possible to expand an available space in the AWS cloud. Unlimited storage on a user's device	Files are stored on a computer. The amount of storage available for data is conditioned by a free disk space. In addition, the application includes synchronization features with, for example, the cloud. A user can specify a directory or cloud which an encrypted document should be sent to, and then the application will send an encrypted document to this location. The document will be automatically backed up.	Each user receives 150 GB in the basic version. Additionally, depending on the variant from 500 GB to 2 TB of file sharing storage for custom deployments. Netia can offer more storage for data upon request. Disk capacity on the client side is a limitation when installing the product on corporate servers.

Comparison of solutions to encrypt and group work

ADDITIONAL INFORMATION

Function or feature	Cypherdog	Specfile	Netia Data Safe
SUPPORTED OPERATION SYSTEMS	Cypherdog: Windows, macOS, Linux. Cypherdog Messenger: Android, iOS.	pecfile: Windows. Encrypting and decrypting without the application: via any browser in all systems.	Netia Data Safe: Windows, macOS. Messenger: iOS, Android.

Function or feature	Cypherdog	Specfile	Netia Data Safe
SERVICE LEVEL AGREEMENT (SLA)	The developer offers SLA of 99,9%. The system is based on a high availability architecture on 6 continents.	**No**	The developer offers SLA of 99,9%. SLA in the on-premise version depends on business infrastructur.
PRICE PER LICENSE (MONTHLY)	16 dollars* for the Premium version 8 dollars* for the Enterprise version *Individual calculations possible	11 zlotys	Prices start from 60 PLN for: • Storage space in the Netia cloud (from 150 GB for each user or 2 TB shared storage) • Technical support Prices are set individually with more users
LANGUAGES AVAILABLE IN THE APPLICATION	Polish, English, Ukrainian, and Russian	Polish	Polish and English
IN WHICH LANGUAGES TECHNICAL AND COMMERCIAL SUPPORT ARE AVAILABLE?	Dedicated technical support team of Cypherdog is available in English and Polish.	Polish	Dedicated technical support team of Netia is available in Polish and English.
CAN THE SOLUTION BE USED BY NON-BUSINESS USERS?	**Yes**	**Yes**	As part of the non-standard offer, Netia may perform such implementation.

Function or feature	Cypherdog	Specfile	Netia Data Safe
IS IT POSSIBLE TO ENCRYPT FILES FOR FREE, BUT WITHOUT ADDITIONAL FEATURES?	**No.** The encryption application is paid. It is possible to decrypt uploaded file only in the free version.	**Yes.** The application for personal use allows free and unlimited file encryption but does not have any additional features.	**No.** It is possible to read files only under a free license
DEVELOPER'S WEBSITE	**https://cypher.dog**	**https://specfile.pl**	**https://www.netia.pl**

Recommendation granted

Cypherdog

Ultimate privacy protection.
Very strong encryption.
Chat available in the application and dedicated communicator.
Thoughtful features for convenience of group work.
Support for all operating systems including Linux.
The use of blockchain technology.
That is how we should design modern solution for confidential group work.

Specfile

Encryption and decryption functionality, independent of the operating system, including through a browser.
Confirmation of mailing and receipt of registered mail.
Notification of a pending list for people without an account.
Sharing encrypted documents with corporate and private individuals.
It is probable the best data encryption service for people and businesses that want a easy-to-use solution.

Netia Data Safe

The solution allows to store everything on corporate servers without anyone on the outside having access, even the developer.
The unique technology of division of encryption key HVKM (Hybrid Virtual Key Management).
Advanced functionality of group work. These are the product identification marks which allows to secure data that require special protection.

Summary

Name: **Adrian Ścibor**

Position: **Leading editor of AVLab.pl**

In 2015, scientists estimated that the quantum computer at that time would need a billion qubits to break encryption based on the RSA algorithm with 2048-bit key length. That is much more than 50-80 qubits that state-of-the-art quantum computers have now.
And mathematics has once again proved that it is the queen of science: experts from Cornell University have developed a quantum computer model [2] that can do such calculations within 8 hours, and not using a billion of qubits, but “only” 20 million qubits.
This interesting technical work, very important, and shows that in the near future, there may be further quantum computers that will reduce by a whole order of magnitude the number of qubits needed to perform factoring activities. Will this type of device be developed in the coming decades?

In a decade or so, security of the RSA-2048 algorithm may be undermined. Currently, a stronger than the RSA-2048 encryption is often used, for example, in online banking, internet communicators, encryption of email and files. There are larger issues at play between countries. If the RSA-2048 encryption has been used so far to secure data and communication, in twenty years, there may be problems in keeping secrets from the past.

Encryption is one of the basic security standards. It is widely available and easy to use. For this reason, we wanted to present the Polish engineering solutions in the area of encryption without having to access the software from abroad.

The information in our study has been discussed in cooperation with engineers of each developer. At this difficult time, it is worth supporting Polish entrepreneurs and promoting local, and most importantly, good solutions that enable secure and confidential group work for a wide range of economic activities.

[2] https://arxiv.org/abs/1905.09749

THE INDEPENDENT ANTIVIRUS TESTS

AVLab as an independent Polish organization that acts as the guardian of security on the Internet provides information through articles, trainings, and conferences. Professional reviews and security tests are our distinctive feature.

In tests, we use malicious software, tools, and techniques of bypassing security that are used in real attacks. For more information on our offer, please visit the websites:

https://avlab.pl/o-nas **https://avlab.pl/wspolpraca**