TALLINN UNIVERSITY OF TECHNOLOGY

Faculty of Information Technology

Department of Computer Science

TUT Centre for Digital Forensics and Cyber Security

ITC70LT

Artur Tychina 132242IVCMM

IMPLEMENTATION OF CORPORATE DATA LEAKAGE PREVENTION IN ESTONIA

Master's Thesis

Supervisor: Truls Ringkjob

Supervisor's degree: TUT master's degree

Supervisor's position: IT college and visiting TUT lecturer

Tallinn 2015

Author’s declaration of originality

Author’s declaration of originality is an essential and compulsory part of every thesis. It always follows the title page. The statement of author’s declaration of originality is presented as follows:

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Artur Tychina

20.05.15

Abstract

In current work, author is going to propose a system, which will prevent leakage of corporate data. The system will be based on full encryption of user devices, with a strong system of user's file exchange control within the organization and outside it. An encryption system is widely uses hardware solutions for key storage, such as ID-cards, TPM (chip on motherboard) and USB-tokens.

File exchange will be based on a flexible system of public keys exchange and strong element of control. Author suggests various options for data recovery, in case of keys loss or damage, and also have reviewed the possible scenarios for the theft of information from encrypted devices.

Author tested the speed of the encrypted devices and concluded that the performance will not reduce dramatically. Author also has analyzed the ability of the system and found that author's system can be easily applied especially in Estonia, is due to the deep integration of the e-state. As a result, this system represents a reliable way to protect corporate data against leaks, even implemented by insiders, offering an entirely new approach of control, monitoring and data protection.

Author's project is intended to serve to large organizations such as ministries, multinational corporations, the military departments within NATO, large financial companies and the various secret services.

The thesis is in English and contains 65 pages of text, 7 chapters, 30 figures, 2 tables.

Annotatsioon

Äriteabe lekete ennetamise lahendused Eestis

Käesolevas lõputöös pakub autor välja süsteemi, mis aitab vältida äriteabe leket. Süsteem põhineb kasutajate seadmete täielikus krüpteerimises, range kasutajate failivahetuse kontrollisüsteemiga organisatsiooni sees ja väljaspool. Krüpteerimise süsteem kasutab laialdaselt krüpteerimise võtmete hoidmiseks riistvara lahendusi, nagu ID-kaardid, TPM (kiip emaplaadil) ja USB-mälupulgad.

Failide vahetus põhineb avalike võtmete paindlikul süsteemil ning on range kontrolli all. Autor pakub mitmeid valikuvõimalusi andmete taastamiseks võtmete kaotamise või kahjustamise korral, samuti on üle vaadanud võimalikud stsenaariumid info vargusel krüpteeritud seadmetest.

Autor testis krüpteeritud seadmete kiirust ning järeldas, et nende suutlikkus ei vähene radikaalselt. Samuti analüüsis autor süsteemi töövõimet ning leidis, et tema süsteemi on võimalik vaevata rakendada Eestis tänu e-riigi eriti sügavale integreeritusele. Selle tulemusena esindab süsteem usaldusväärset viisi, kuidas kaitsta äriteavet lekkimise eest, mis oleks teostatud isegi organisatsiooni liikmete poolt, pakkudes täiesti uue lähenemise kontrolli, jälgimisse ning info kaitsmisse.

Autori projekt on mõeldud kasutamiseks suurtele organisatsioonidele, näiteks ministeeriumitele, rahvusvahelistele organisatsioonidele, NATO sõjalistele ametitele, suurtele finantsvaldkonna ettevõttetele, ning mitmetele salateenistustele.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 65 leheküljel, 7 peatükki, 30 joonist, 2 tabelit.

List of Abbreviations

Abbreviation	Definition
TPM	Trusted Platform Module
AES	Advanced Encryption Standard
GPO	Group Policy
FVEK	Full Volume Encryption Key
AD	Active Directory
VMK	Volume Master Key
UEFI	Unified Extensible Firmware Interface
MBAM	Microsoft BitLocker Administration
FTP	File Transfer Protocol
HDD	Hard disk drive
SRK	Storage Root Key

List of Figures

List of Tables

Contents

1. Intro

In the modern world, the problem of data protection against the leaks – costs sharply as never. Such resources as WikiLeaks or Snowden-case shows, that data are not protected properly today from losses, even in government institutions and at the secret services. It results in catastrophic consequences for the state. The state is not able to protect their sensitive data – is vulnerable, its army and power can turn into nothing if the enemy will know all the secrets of this army. Future wars will begin, most likely, not with the artillery preparation, but with cyber-attacks. Thus, the data protection of state structures – the primary task for Cyber Security specialists.

1.1. Motivation

There are many ways to obtain sensitive data – from different ways of hacking to the banal theft of data carriers, such as laptops, flash drives, etc. The most banal way, however, is not the rarest. Quite often, we hear from mass media that a next official or worker of the special services forgot the suitcase or notebook in a public place from what become a public great number of secret documents. This problem continues to be actual – the loss of data carriers – is a headache for risk managers around the world. One way of such solutions to solve this problem, can be encrypted media. Encryption can provide a good level of data protection at minimal cost, so that no one can read data from stolen or accidentally found media, except their owners. However, this scheme is good in theory, in practice, users ignore security requirements and do not encrypt their data, even if the company policy requires them to do so. As a result, a huge amount of information falls into the wrong hands, that endangers many companies and government institutions.

1.2. Aim

Author is going to propose a new approach to the problem of data encryption in an enterprise environment. This approach will allow to not only effectively interchange the encrypted data within the company, but also will allow to avoid a situation, when data remain not encrypted. The user simply will not have such a choice – to encrypt or not. Any data that is copied from his computer or flash drive will be in the encrypted state and it will be able to open by person, to whom a user gave access beforehand.

1.3. Scope

Author is going to propose a system that will use BitLocker encryption, TPM-chip or ID-card key storage for them, ID-card authentication, public key servers to provide access to other users for certain files, system of control for files send outside of organization and Master-device for the read-out of encrypted data from the damaged devices. All of these technologies already exist separately, but author proposes to combine them into one powerful tool to ensure reliable protection of all data on portable devices.

Application of this method:

- rule out the possibility of transmitting a unencrypted data to third parties
- exclude data acquisition by message interception
- data are always in an encrypted state, another state is excluded
- monitors the data exchange (what, who, whom, when)
- provides full control and centralized access management to data sharing

1.4. Outline

This thesis is organized as follows. Chapter 1 gives introduction to thesis and gives motivation, scope and aim of the use of encryption and protection against data loss in the state and the corporate sector. In Chapter 2, author will give statistical data and results of researches on the losses of data and financial losses of companies that neglected the encryption. In Chapter 3, author will discuss the currently existing software solutions for data encryption in the corporate segment. Chapter 4 in details will tell about proposed by author encryption system, protection and control of data within organizations, will describe the procedure for locking and recovery of compromised devices and other details. In Chapter 5, author conducted a row of tests to find out – how much will decrease the performance of encrypted system compared to unencrypted. Chapter 6 will offer a few scenarios with attempts to steal data, and similarly what author's system can answer on these attempts, will demonstrate how it protects the data. In Chapter 7, author will sum up of this thesis.

2. Statistics

2.1. Data Leakage

Corporate espionage and cases of unpremeditated loss of data present a serious threat to any business, but in spite of this, many companies are still not in a hurry to implement some means to protect confidential information. According to the study, "Kaspersky Lab" and B2B International, only slightly more than half of the companies around the world use data encryption technologies at the files level, securely protecting sensitive files and folders, as well as at the level of full-disk encryption.

Meantime, only in the airports of the USA 12 thousand notebooks are lost every week. The total cost of the devices lost for a year is estimated in 987 million dollars. At the same time there are more considerable unobvious financial losses, is the cost of loss of corporate data, estimated in 25 billions of dollars of losses in a year. And this – the data only for one country. Not hard to imagine what could be the numbers for the whole world.

From data of the international research of “Kaspersky Lab", conducted in partnership with B2B International in late 2012, much of the companies pays insufficient attention to the protection of corporate information. In particular, 35% of companies worldwide do not use such important technology as data encryption. [1]

The research from Kingston – which was carried out in partnership with the Ponemon Institute – found that 72% of UK companies admit to having lost confidential data through missing USB sticks, with 72% mentioning loss without notification.

Researchers also found that 49% of organizations admit that the losses relate to customer data. Interesting, researchers discovered that staff are also negligent of the potential USB stick security issues, so putting sensitive company data at risk.

Kingston say that the analysis – which took in responses from 2,942 IT professionals in Denmark, Finland, France, Germany, Netherlands, Norway, Sweden, Switzerland, Poland and the UK – reveals there are marked differences in the approach and implementation of USB drive security from country to country.

In the UK, only 23% of respondents confirmed that their companies have the technologies to prevent or quickly detect the download of confidential data onto USB drives by unauthorized individuals.

The statistic, says Kingston, shows most organizations in the UK are ignoring the risks of using unencrypted USB drives, resulting in 72% of those questioned having suffered a loss of confidential or sensitive data because of missing USB drives in the last two years.

When comparing individual European countries, perceptions and practices about the importance of USB security is highest in Germany – with 62% agreeing that their business has an adequate USB security policy in place to prevent employee misuse.

On the contrary, the UK, France and Poland are most at risk as a result of employees' practices – 73% in the UK, 85% of respondents in France and 83% in Poland said that employees use USB drives without obtaining advance permission to do so. [2]

In the last three years, cases publicized by Britain's Information Commissioner's Office (ICO) [3] show that lost USB drives – very few of which ever employ encryption despite containing sensitive data – have become a major bane of the public sector. [4]

Kingston recommends that organizations provide all employees handling sensitive data with encrypted drives, create policies for acceptable use, and employ asset tracking and recovery to manage their deployment. [5]

The research also showed the following:

Employees are negligent when using USB drives and this is putting organizations' sensitive data at risk. Bar Chart 2 reveals what employees are doing all the time or frequently: using USB drives without obtaining advance permission to do so (75%); losing USB drives without notifying appropriate authorities about this incident (63%) and using generic USB drives such as those received free at conferences, trade events and business meetings (38%).

In many cases, USB security policies are meaningless because 37 percent of respondents say their organizations do not enforce compliance and 13 percent are unsure. As shown in Figure 1, the primary reason for not enforcing these policies is that organizations are relying upon employee integrity and trusting they will not violate the policy.

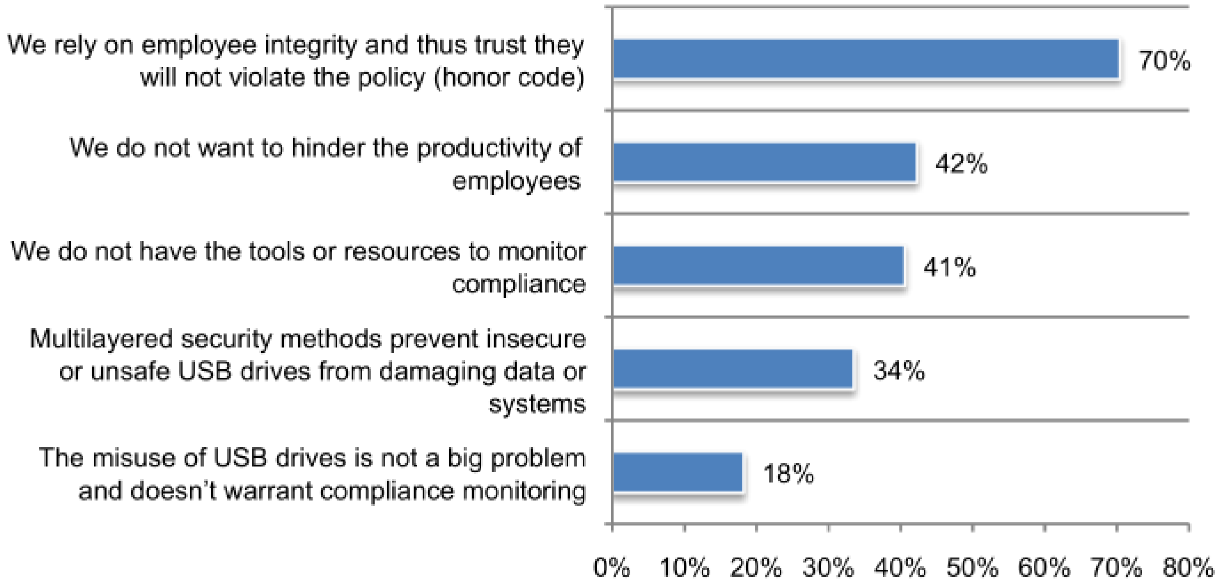


Figure 1: Why policies are not enforced. More than one response permitted

Most USB devices in the workplace are not secure and contain confidential business information. USB drives are prevalent and popular with employees. Figure 2 shows that on average, organizations in study report the use of more than 43,457 USB drives in the workplace. On average, 46 percent of these drives are not considered secure. Typically, employees download and store sensitive information about customers, confidential non-financial documents and other intellectual properties.

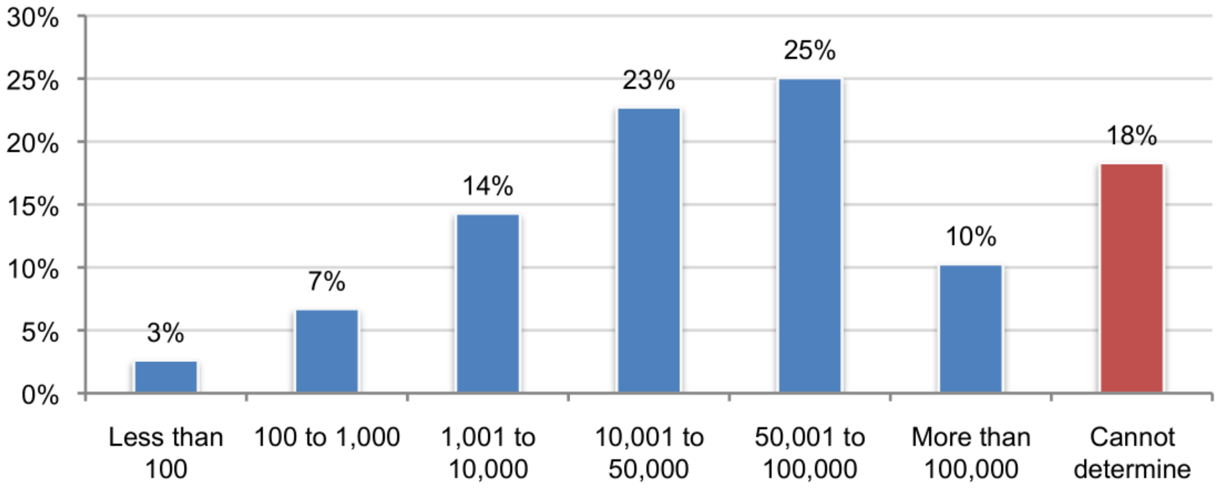


Figure 2: How many USB drives are used by employees (end-users) in organization today? Extrapolated average value is 43,457 USB drives.

According to Figure 3, approximately one-third (34 percent) report that they do not encrypt data stored on USB drives. Customer data and employee records are the two types of data most often encrypted. If they do encrypt, 49 percent of respondents say it is to be in compliance with regulations/EU and nation-specific privacy laws and 38 percent say it is to comply with self-regulatory programs.

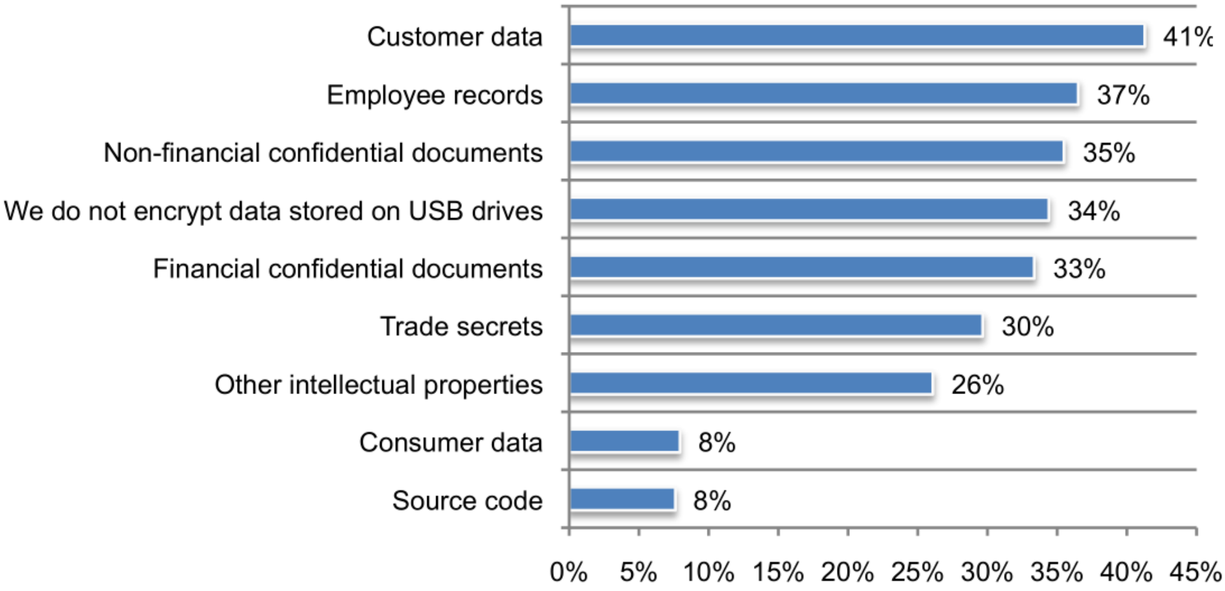


Figure 3: What types of sensitive or confidential information are normally encrypted when stored on a USB drive? More than one response permitted.

As shown in Figure 4, on average organizations in study have lost more than 34,188 records about customers, consumers and employees as a result of missing USBs. Respondents believe that on average 66 percent of these lost or stolen records could have been protected from abuse, if the USB drive was encrypted.

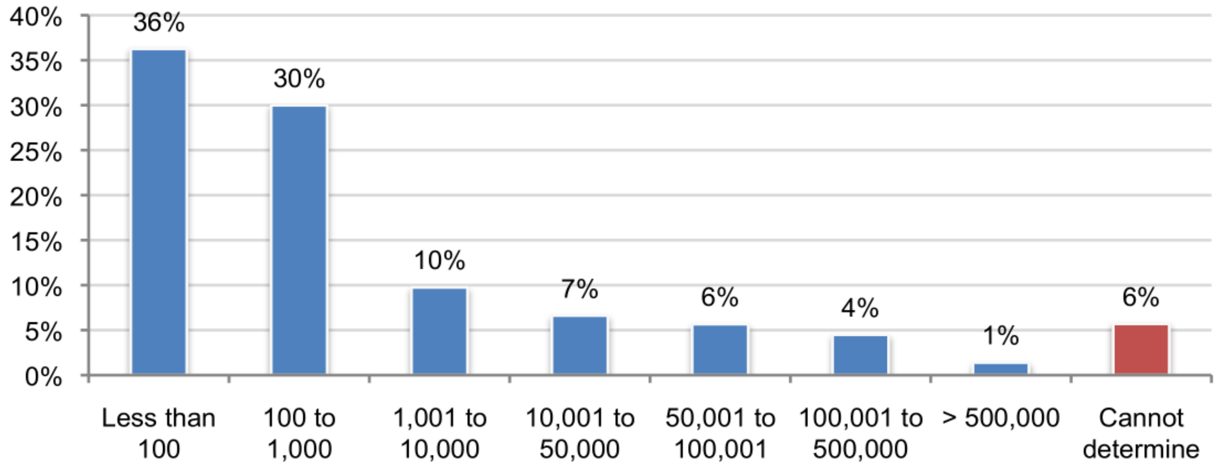


Figure 4: How many records were lost or stolen or as a result of missing USB drives over the past 24 months. Extrapolated average value is 34,188 records.

The research given above is an alarm signal and shows the level of unpreparedness of companies in a fight against data loss. Research establishes the lack of seriousness of attitudes toward defense of USB-devices in a corporate segment that results in the scale data leakage. Such an attitude can also talk about that it touches not only USB-devices, but also other portable technique, such as tablets or laptops. Even if a company has a policy that requires users to encrypt media – many of them do not, because of inadequate control over the implementation of the existing security policies. As a result, users ignore any security requirements and confidential data flow away in the total, which inflicts losses to the companies.

According to the database of Privacy Rights Clearinghouse [6] from 2005 to 2015 it was officially registered 187,543,303 Records, that leaked from Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, stationary electronic device such as a computer or server not designed for mobility. 1,847 published cases of loss of data were fixed overall, however it is needed to not forget, about those cases that were not made public. Overall, a picture does not suggest optimism.

2.2. Money

Is it a serious risk – the loss of data? How much money will lose companies if their data will be stolen. In fact, not all data are important for companies and, moreover, not all data cost money. However, research of company IBM and Ponemon in 2014 revealed the following:

The most and least expensive breaches. German and US companies had the most costly data breaches ($201 and $195 per record, respectively). These countries also experienced the highest total cost (US at $5.85 million and Germany at $4.74 million). The least costly breaches occurred in Brazil and India ($70 and $51, respectively). In Brazil, the average total cost for a company was $1.61 million and in India it was $1.37 million

Size of data breaches. On average, U.S. and Arabian region companies had data breaches that resulted in the greatest number of exposed or compromised records (29,087 and 28,690 records, respectively). On average, Japanese and Italian companies had the smallest number of breached records (18,615 and 19,034 records, respectively).

Countries that lost the most customers following a data breach. France and Italy had the highest rate of abnormal customer turnover or churn following a data breach. In contrast, the Arabian region and India had the lowest rate of abnormal churn.

Countries that spent the most and least on detection and escalation. On average, German and French organizations spent the most on detection and escalation activities such as investigating and assessing the data breach ($1.3 million and $1.1 million, respectively). Organizations in India and the Arabian region spent the least on detection and escalation at $320,763 and $353,735 respectively.

Figure 5 presents the costs associated with detection and escalation of data breach incidents in 10 countries. Such costs typically include forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors. As noted, German companies experienced the highest detection and escalation costs and India and the Arabian region experienced the lowest.

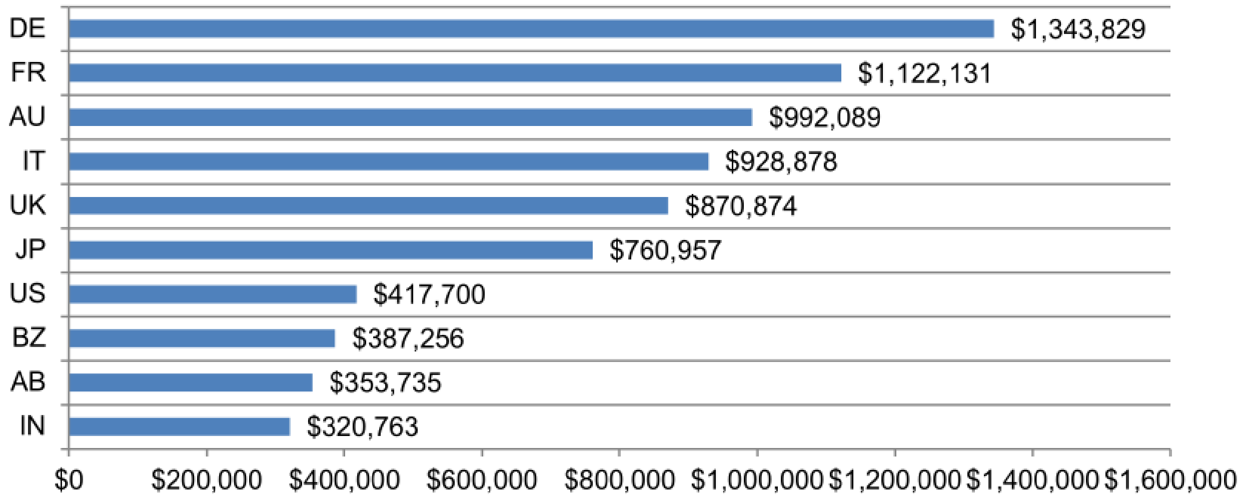


Figure 5: Average detection and escalation costs. Measured in US$

Countries that spent the most and least on notification. Typical notification costs include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts and other efforts to make sure victims are alerted to the fact that their personal information has been compromised. U.S. and German organizations on average spent the most ($509,237 and $317,635 respectively). Brazil and India spent the least amount on notification ($53,772 and $19,841, respectively).

The more records lost, the higher the cost of the data breach. Figure 6 shows the relationship between the total cost of data breach and the size of the incident for 314 organizations in ascending order by the size of the breach incident. The regression line clearly indicates that the size of the data breach incident and total costs are linearly related. In this year’s study, the cost ranged from $135,603 to $23,143,454

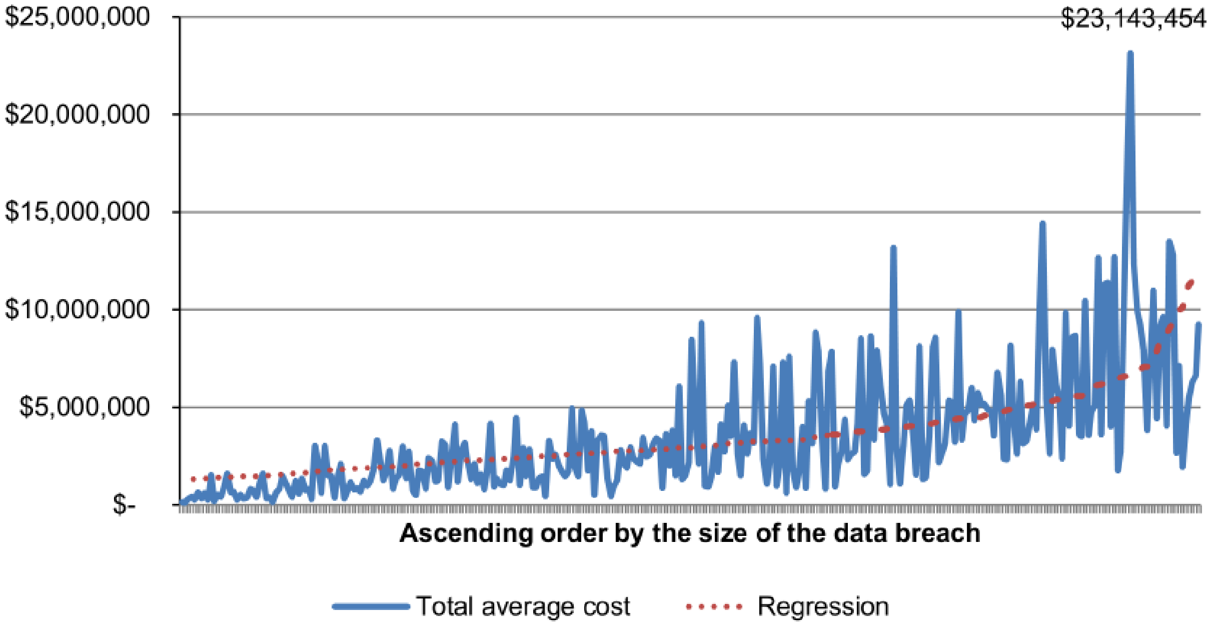


Figure 6: Total cost of data breach by size of the data breach. Regression = Intercept + {Size of Breach Event} x β, where β denotes the slope. Measured in US$.

Post data breach costs are highest in the U.S. and Germany. Figure 7 shows the distribution of costs associated with ex-post (after-the-fact) activities for 10 countries. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services and regulatory interventions. The lowest costs were in Brazil and India.

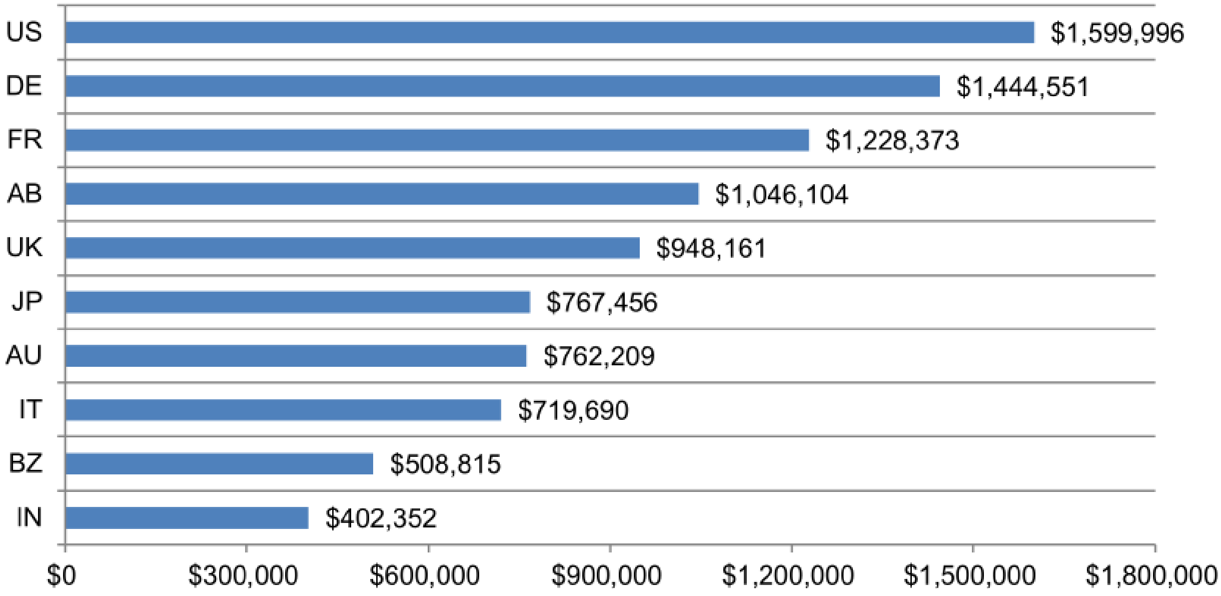


Figure 7: Average post data breach costs. Measured in US$

Lost business costs. Lost business costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. The highest lost business cost was an average of $3.3 million and the lowest was $252,876 in India.

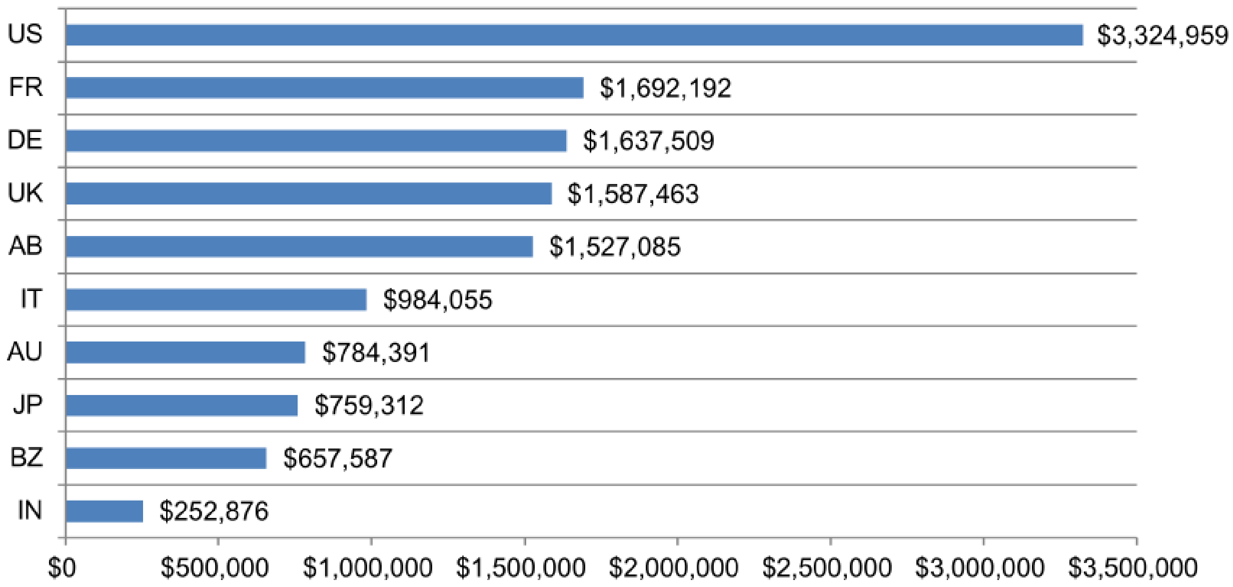


Figure 8: Average lost business costs. Measured in US$.

These studies shows that the costs for companies, that have experienced the data loss, arrive at unbelievable scales. Companies have to spend imposing facilities not only on the damage inflicted by the theft of data, but also on the consequences of event, which typically include help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services and regulatory interventions. Besides a company runs into the loss of clients and their loyalty, which is not surprising.

In general, data loss is a serious financial and reputational shock for the company, which can lead to the death of business. If the loss of private companies can be measured in money, the loss of state-owned companies do not have money measurements. How much can cost loss of secret military or reconnaissance information, if the question is about human lives – such cannot be measured by money, however clear that it is frightful losses and it will be heavily to get well from that.

3. Statement of the Problem

As it is possible to see from the researches given above – a situation deplorable. The companies do not want to spend funds for safety and control over the implementation of the existing security policies. As a result, users can casually refer to the data that are stored on portable carriers and neglected encryption, which leads to essential losses and harms to business what not to be compared to the minimum costs of tools that could prevent data leakages or data use by malefactors if leak nevertheless happened.

It is obvious that there is a question of solving a single problem – how to force users to comply with the requirements of security policy, how to force user to encrypt all files on all devices. The answer is obvious – it is necessary to deny users the ability to use unencrypted files. In other words, to create an environment in which any file, if he got in this environment, will be encrypted and a user will have no opportunities and no tools to keep the file or device unencrypted. A method and instruments, that author gathers to offer, provide such environment, moreover, they yet provide control of files exchange between users so, that not a single file will be passed to the colleague or third person without registration of this event. I.e. the transfer of each file will be registered in a common database on the server. How will it work author will tell later in the public-key-server chapter.

3.1. What we have today

Today in the IT world, there are many products that are similar and offer similar encryption features. However, all of them have a row of defects as compared to a decision that author gathers to offer. For comparison, author will lead a few of them and will describe their advantages and main defects that do them weaker than author's solution.

3.1.1. Kaspersky Endpoint Security

The most successful and close variant is Kaspersky Endpoint Security 10. This product uses AES encryption of whole physical disk or file-based encryption. Main advantages of product is support of UEFI, TPM, Smart Card, physical disk and file-based encryption are supported. There is a centralized management of encryption – all encryption keys are stored in the Security Center and are available only to the security administrator. This means, that if password is lost or TPM-chip is damaged, all data can be restored, as the Private Key is stored centrally on a server. It's kind of vulnerability, since leakage of keys from the server may cause leakage files from user devices. As well has a function of secure files sending to outside of encrypted space. Users can create self-extracting password-protected archives of encrypted files and folders. The recipient can open the received file and access the files, just after will enter a password, which is known only to him. This is comfortable technology, that, however, requires from the users of "superfluous movements", that, as is generally known from the research given above, does technology small applicable – users are too lazy and impatient, to do such movements.

On the whole the product of company Kaspersky turned out successful enough, and he is maximally near to the that idea, which author gathers to suggest. A year ago, many functions were not presented in the Kaspersky Endpoint Security (UEFI / TPM, Smart Card, Private Key Server support), however now these useful functions are. That did author’s idea not so original, however that does not mean that the product fully corresponds to that author gathers to suggest – there is a part of significant deficiencies, about which author will talk in resume of this chapter. [7]

3.1.2. Symantec PGP Whole Disk Encryption

Symantec's PGP Whole Disk Encryption supports AES-NI when available. Users can authenticate using Smart-Card, Trusted Platform Module (TPM), or passphrase. Protected systems can be centrally managed by Symantec's PGP Universal Server – simplifying deployment, policy creation, key management, and reporting. Passphrase and machine recovery options include local self-recovery with question and answer authentication, and one-time-use tokens, is also available through the restoration of Public Certificate, but only for external storage media. Unlike Kaspersky encryption keys are not stored on a shared server, but Symantec provides a system for files exchange on removable media, by creating a workgroup key. This idea is the cornerstone of the system, which author represents. It is nice to see, that someone else has already decided to apply it in a practice. In the rest, products of Kaspersky and Symantec are similar. [8]

3.1.3. McAfee Endpoint Encryption

McAfee Endpoint Encryption is very similar to the product from Kaspersky and Symantec: there are used Self-extracting archives for file sharing and the ability to use public key sharing for exchanging data within the company using the McAfee ePO technology. However, this product does not support the centralized recovery of passwords and access to the system.

Forgotten passwords can be restored using the Recovery disk. As well, product is able to manage and interact with embedded encryption technology of operating systems – FileVault for Mac OS and BitLocker for Windows. There is also a support of TPM, Smart-Cards and tokens. [9]

3.1.4. Microsoft BitLocker Management and Administration (MBAM) server

Simplified BitLocker Deployment: Microsoft BitLocker Administration and Monitoring let's to choose the deployment scenario. Administrator can provision BitLocker as part of Windows 7, Windows 8, or Windows ToGo deployment or Administrator can configure BitLocker encryption to be provisioned after the operating system is installed, by using the additional Group Policy controls in MBAM. The controls are checked periodically and if a device is detected as non-compliant, MBAM will help put it back into the desired state.

With out-of-box reports, managers can get a better view of compliance status, enabling them to easily determine if lost or stolen devices were encrypted. IT staff can also create custom compliance reports using built-in SQL Server Reporting Services tools to show them just the information that they need to see. MBAM also provides the ability to store BitLocker recovery keys in an encrypted database with granular access controls and creates an audit trail of who has accessed recovery key information, keeping this information protected and only accessible to the right people in the organization.

Using the Self Service and Helpdesk recovery portal, users and authorized help-desk staff will find it easy to support recovery scenarios if they run into issues. Main advantages of product is support of UEFI, TPM, Smart-Cards and tokens. [10]

3.1.5. Summary

Each of these systems in their own way good. And each has a number of advantages and disadvantages. The system of Kaspersky is unable to create shared encrypted files and stores Private key on the server, what is unsafe. The system from Symantec does not support the centralized variant of hard drive restore, there is only support for removable media. The system of McAfee does not have a centralized system for password recovery and system access. It should also be noted, that all these systems are designed for corporate use and imply serious costs of their implementation and enforcement, as well as a competent IT staff. With proper setup and use, those systems are capable to provide reliable data protection from accidental loss or theft of the device containing the media. However, there are a few basic defects at these systems – they require from the user to manipulate some, such as data transfer. That, as we know, reduces the user's desire to use these tools – is take users time, is too complex and simple too lazy to do it. Moreover, the main disadvantage – none of these systems do not protect from intentional data leakage. Yes, they will protect the data if the media was accidentally left in a public place or stolen. However, imagine a situation where a user deliberately trying to "leak" the information to a third party. User can sent by e-mail, FTP, Cloud technology, or simply copy the self-extracting archive to unencrypted memory stick and transmit it, together with a password to a third party. Alternatively, user can simply copy the archive to his personal e-mail to subsequently "leak" secret documents to the press, Internet, or to competitors, because he knows the password of the archive. In addition, there is no registration of the archive creation events, making it impossible to follow the detection of the source of information leakage. Overall, the transmission of the unencrypted files outside the system in any way is not regulated and possible, from here a main lack of such systems is possibility of information leak, that will result in catastrophic consequences. Mainly, it will be impossible to find out a source of leakage, which means that similar leaks will occur repeatedly, while the system of file exchange, outside of encrypted environment, will not be revised. Whoever wants to get the endless train of catastrophic losses, will forced to think about the monitoring, control and reporting of file exchange.

The verdict is dire: the system securely protects files from being stolen by outsiders – are not able to provide protection against leakage, as the result, even the most secret structures and divisions will have their Snowden and will frequently quoted on WikiLeaks. The main task of modern security departments – prevent such leakages and to ensure the highest data security level of companies and the state. Author is ready to offer complex solution that is able to provide not only the reliable protection of data in case of theft of device, but also protection from the losses of data in case of their intentional "leak". If a "mole" was led in organization, then author’s system will complicate his life so, that he will force to give up an idea to "leak" out some data by the methods are known today – e-mail, FTP, Flash Drive, Cloud etc. The conception offered by author will allow avoid wrecking on working places, subornation of employees and penetration of spies in organization or, at least, greatly complicate their lives, as the transmission of data in unencrypted form will actually be eliminated or extremely difficult.

4. System Concept

The system concept is based on different technologies, most of them are exist today and are implemented in a variety of commercial products. Some of the products listed above in Section 3.1 of this paper. Whole conception will be presented in this head, short description that gives common presentation will be given in the beginning; after will be detailed all points presented in short description.

4.1. Short description

The system, which author represents, is based on BitLocker data encryption technologies. By activating the system, all user data on the HDD will be encrypted by AES-key, private key will be stored on the TPM chip on computer motherboard or on Smart-card. Since ID-card has its own private key, that eliminates the need to maintain key on TPM chip, and provides greater fault tolerance in case of damage or failure of the computer motherboard. Authentication occurs by Smart-card, USB-token and PIN-code. Once authenticated, the user will be allowed to boot the system and work with it. At the time of working with files – they are decrypted, but only when user call to them, at other times files are in an encrypted state, which does not allow them to copy or read quietly. When sending files outside the system or when copying to an external device – they are copied and sent in encrypted form. This will prevent accidental or intentional data leak from the computer.

However, file sharing is relevant today than ever before, one day it may be necessary to send a file to a colleague within the organization or collaborating organizations. For this purpose, there are special servers of public keys exchange. The whole process of public key encryption is automatic. If file gets in attachment in e-mail client – e-mail client will check the names of recipients and make a request to the public key server. After the receipt of the public key, an e-mail client encrypts a file and sends it to recipients. At the receipt of file, a recipient will be able easily to open it on the encrypted system, because he is authorized and has an access to all files that are encrypted with his public key. Approximately the same scheme will be implemented during file sharing on the shared resources: FTP, Mapped Network Drives, Flash Drives etc. System, determining that the file is laid out in the share, immediately prompted to select from a drop down menu of employees, who will be given access to that file. After that, the system performs encryption using the received public keys from the server of the chosen employees.

Thus, even not necessarily to differentiate rights for access to the different files into the network of company. Paradigm of Read/Write rights stops to play a decision value. A value has only – whose public key is in encrypted file, others will not be able even to open file and read it. Thus, the problem of preservation of confidential information within the company solved. However, it does not solve the problem of sharing files outside the company or organization. Author suggests two ways to solve it.

The first method consists in creation of the general trusted servers of the public keys between different organizations, and then file sharing between the companies will be as easy, as sharing within companies. However, this involves the use of the same encryption system in different organizations such a method is not possible otherwise. For Estonia, this method can be easily realized on all levels for all organizations, because practically all users have ID-card and they can decrypt with it help every encrypted file sent to them. The second method is sending a password-protected encrypted self-extracting archive with additional audits and inspections by superior officers.

The system offered by author is able to encrypt entire hard drives as well as external media. However, often there is a situation, when an employee cannot decrypt his data because of damage of Smart-card, damage of TPM-chip or forgotten password. For this case is provides Master-device, which is kind of a NAS, where can be inserted any type of media - HDD, Flash Drive, CD, microSD etc. This Master-device is able to decrypt any employees devices within a company. As well as the system of Master-cards, which will allow to unlock encrypted device. It becomes possible due to that all devices are always encrypted not only by means of user's public keys, but also by means of administrator public key (Master-device). This device is not connected to the Internet in order to prevent leakage, it is located in a physically well-protected room, to which should have access only a few employees. In the case of storing of private key on the ID-card, the device can be decrypted by the system administrator who owns the card. However, this method should be excluded because it is vulnerable.

The system author proposes should also have the ability to disable or block compromised devices. This feature avoids any attempts to decrypt the information and its leakage from stolen devices. It is also should be implemented system of OS locking every n-long period of time without communication with the server, so it will be implemented to protect against theft of the device in an active state.

Thanks to the presence of file sending servers and key exchange is implemented a system of total control and monitoring of all file sharing - who, to whom, when and what was sent. These logs are useful for further analysis and case study related to issues of confidentiality. Security department, who will use this system, will be able to get operative and filtered information on actions with the files of all employees of organization.

In general, the whole procedure of encryption and file sharing will be unnoticed to the user. Only, on what the user will be necessary to distract is the choice of employees with whom it is needed to share files and that only if a file exchange goes not by e-mail. This approach completely eliminates the factor of laziness, forgetfulness or fear inexperienced employees to extra clicks to create encrypted files, that always provides secure file transfer. The user cannot send an unencrypted file to an unauthorized recipient - the system simply will not allow it to happen. In addition, the monitoring system of sending outside of organization will not allow to the user intentionally to "leak" out confidential files to the third person, which will provide the reliable protection of company’s data from such phenomena as Snowden and WikiLeaks. Detailed scheme of work of each system instruments will be described below.

4.2. Encryption and Authentication

4.2.1. BitLocker

As the encryption system was chosen BitLocker. BitLocker has several advantages over other products. First of all, the encryption tool is integrated into an assembly Windows 8 Pro, which makes it available "out of the box". This means that organizations do not have to further invest in the acquisition of third-party applications, as well as spend system administrator’s time for installation and solving compatibility problems of third-party applications. This also means that the tool can be easily tested on any machine with Windows 8 Pro, without the need to find a trial version or purchase third-party applications. This is a big advantage of this tool, that the adoption of this instrument will be easily justifiable to the management of a company, as well, they are usually care primarily about price.

The following are the requirements for a successful launch BitLocker on the computer.

Table 1: BitLocker system requirements

Requirement	Description
Hardware configuration	The computer must meet the minimum requirements for Windows 8.
Operating system	Windows 8 or Windows Server 2012
Hardware TPM	TPM version 1.2 or 2.0 A TPM is not required for BitLocker; however, only a computer with a TPM can provide the additional security of pre-startup system integrity verification and multifactor authentication.
BIOS configuration	• A Trusted Computing Group (TCG)-compliant BIOS or UEFI firmware. • The boot order must be set to start first from the hard disk and not the USB or CD drives. • The firmware must be able to read from a USB flash drive during startup.
File system	For computers that boot natively with UEFI firmware at least one FAT32 partition for the system drive and one NTFS partition for the operating system drive. For computers with legacy BIOS firmware, at least two NTFS disk partitions, one for the system drive and one for the operating system drive. For either firmware, the system drive partition must be at least 350 megabytes (MB) and set as the active partition.
Hardware encrypted drive prerequisites (optional)	To use a hardware encrypted drive as the boot drive, the drive must be in the uninitialized state and in the security inactive state. In addition, the system must always boot with native UEFI version 2.3.1 or higher and the CSM (if any) disabled.

As encryption, BitLocker uses Advanced Encryption Standard (AES) as its encryption algorithm with configurable key lengths of 128 or 256 bits. The default encryption setting is AES-128, but the options are configurable by using Group Policy. Everything is standard here, a competition solutions are used the same algorithms of encryption. However, BitLocker is good yet, that his mechanisms are deeply integrated in the ecosystem of Windows. It is standardly can be controlled using the Windows Group Policy, BitLocker key management may be associated with Active Directory, which, while not as secure, but increases fault tolerance in case of lost passwords or keys. The recovery key can be stored in the Active Directory user account. If necessary, the encrypted drive can be inserted into another computer with Windows 8 Pro, and then can be launched key recovery procedure. What is absolutely not safe and should be avoided. In general, the system BitLocker is convenient and easy to use, but it has some significant drawbacks and is far from the level of security that author is willing to offer. Nevertheless, nothing prevents to take it as a basis and bring to the desired level of excellence.

4.2.2. Encryption

Author’s system takes the best of BitLocker and offers a high level of protection. The system will encrypt the entire physical disk with key AES-256, drive can be as removable (Flash Drive, microSD etc), as well as a built-in. All data on the drive will be encrypted with randomly generated symmetric key, the symmetric key is encrypted with two or more asymmetric public keys:

- public key of the user (Owner)
- public key of Master-device
- public key of a user, who have access to data

Public Key of Master-device is needed to recover data in case of loss of user’s private key.

The sectors of HDD are encrypted by the key of encryption of all volume (full-volume encryption key, FVEK). Users, however, this key will not operate and do not have access to it. FVEK key is encrypted by the main key of volume (volume master key, VMK). This level of abstraction provides unique advantages, but makes the whole process more difficult for understanding. FVEK key is kept in the strictest secrecy, because at his disclosure would be required to re-encrypt all sectors. Since the re-encryption takes considerable time, it is necessary to prevent the disclosure of the key. Therefore, the system works with a VMK key. [11]

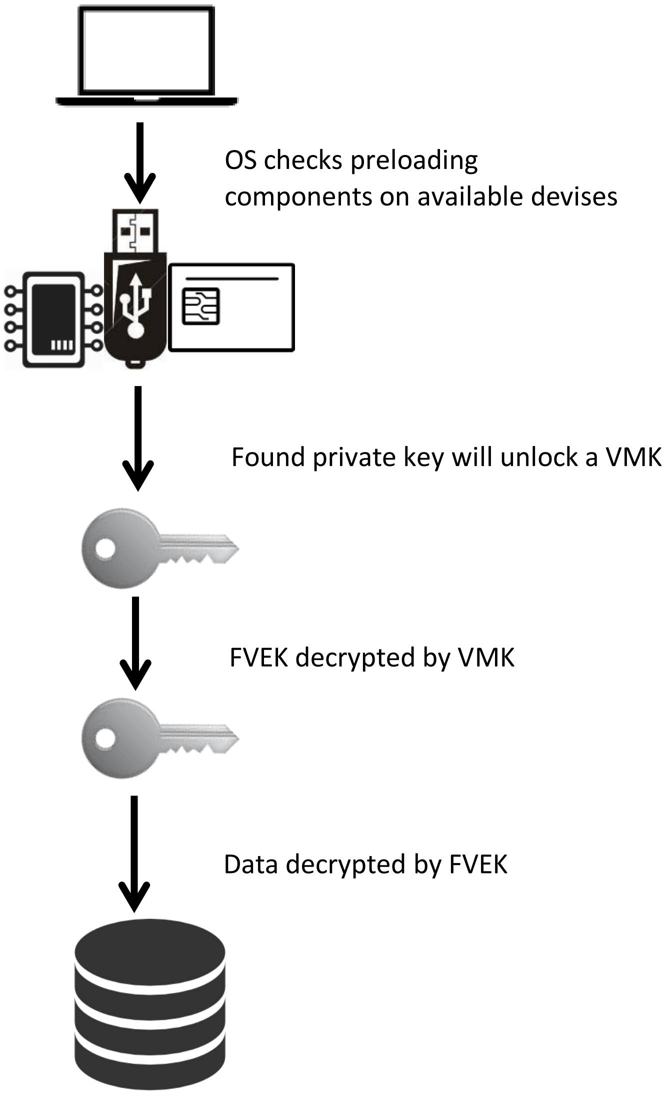

OS checks preloading
components on available devises
Found private key will unlock a VMK
FVEK decrypted by VMK
Data decrypted by FVEK

Figure 9: Data decryption procedure

FVEK key (encrypted with VMK key) is stored on the disc among the volume metadata. Thus, he never gets on drive in a decrypted form. The key VMK is also encrypted and "protected" by a private key, which is stored in the ID-card, TPM-chip or USB-token. In our case, the VMK - is a public key that can only be decrypted by the private key of a user or Master-device.

4.2.3. Keys

User’s Private Keys can be stored in different places and in different media, but author’s system involves only two such places:

- TPM-chip on the motherboard
- Users ID-card

Trusted Platform Module (TPM) - a chip is intended for realization of the basic functions related to security, mostly using of encryption keys. [12] The TPM is usually installed on the motherboard desktop or laptop computer, and cooperates with the other system components via the system bus. Computers equipped with a module TPM, have the ability to create cryptographic keys and encrypt them that way, that they can only be decrypted by the TPM. This process often named the "concealment" of the key ("wrapping" key) or "attachment" of the key ("binding" key) helps to protect the key from opening. Each TPM module have the main hidden key, called the storage root key (Storage Root Key, SRK), which is stored in the TPM.

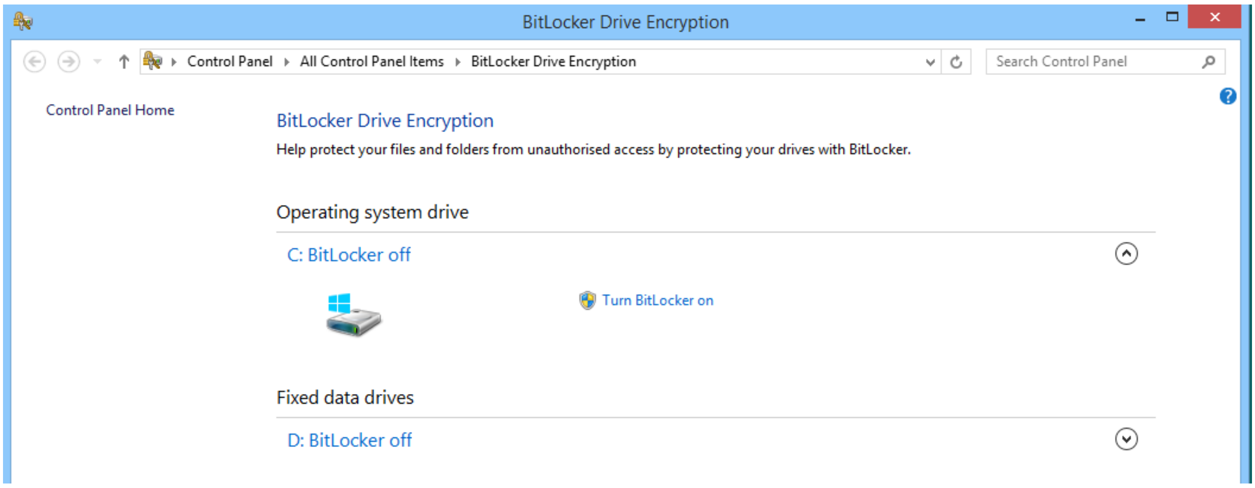
Author’s system is constructed in such a way that any encrypted disk or removable device can only be decrypted on the same motherboard, on which they had been encrypted or in a Master-device, in case of TPM encryption. It will allow to avoid possibility of decryption of stolen removable media or hard drives.

The second variant implies wide distribution of ID-cards in a country, where this method will be used. For example, in Estonia will be no problems with it there, because ID-card has every resident - in the middle of 2015 recorded 1,243,367 active ID-cards, which is 95% of the Estonian population. [13] The private key is stored on the ID-card is unique to each cardholder and the public key is available to anyone who will ask for it. Thus, the key is stored on the card can be used to decrypt and access the disk and file system. Before encryption, the user inserts the card into the reader, and indicates a configuration that the key is located on the card should be taken as a basis for encryption.

A method of using the ID-card is very simple for users and administrators, as facilitates recovery of the system in place, without the need to use the Master-device. However, this method is more vulnerable and easier way for attackers, which will be considered in the Chapter 6, dedicated to the possible scenarios of data theft. In general, the method is designed to facilitate the use of the proposed system by author and do not annoy users.

Procedure of encryption will be looks like the following (as it happens in the standard BitLocker):

The system administrator enables encryption on a computer:


BitLocker Drive Encryption
Control Panel ▸ All Control Panel Items ▸ BitLocker Drive Encryption
Search Control Panel
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorised access by protecting your drives with BitLocker.

Operating system drive

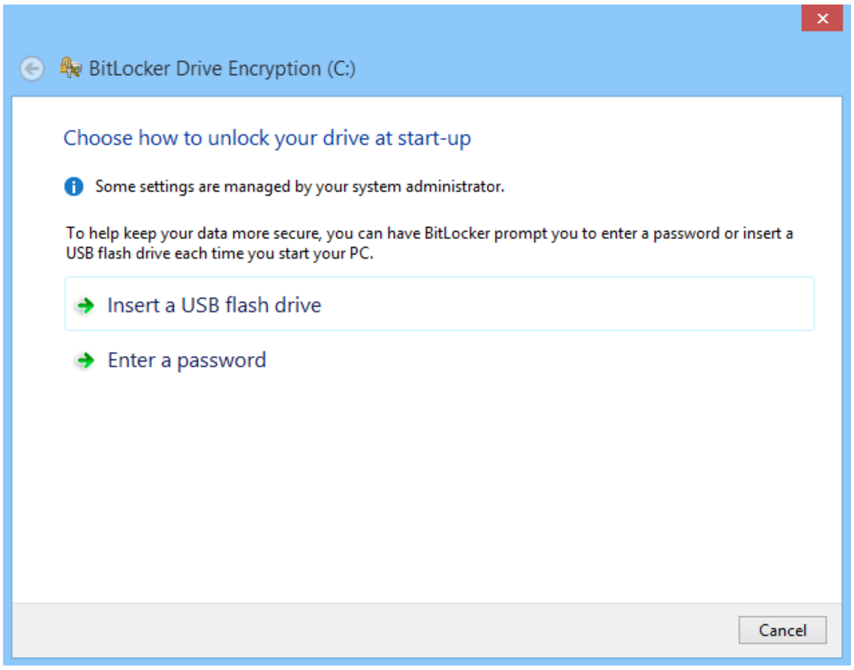
C: BitLocker off

Turn BitLocker on

Fixed data drives

D: BitLocker off

Figure 10. Windows BitLocker



Choose how to unlock your drive at start-up

Some settings are managed by your system administrator.

To help keep your data more secure, you can have BitLocker prompt you to enter a password or insert a USB flash drive each time you start your PC.

Insert a USB flash drive

Enter a password

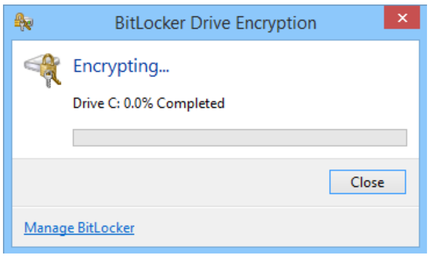
Figure 11. Windows BitLocker wizard

A wizard is started, where it will be possible to choose the method of authentication.

In such kind, the choice of authentication takes place in BitLocker. Author's system will additionally offer to choose the storage location of the private key: TPM or ID-card. As authentication variants will be offered:

- PIN-code + Smart-card + token (in the case of ID-card)
- PIN-code + Smart-card (in the case of ID-card), this function will be marked as not recommended, because of the lack of security.
- PIN-code + Smart-card (in the case of TPM)
- PIN-code + token (in the case of TPM)

As soon as an administrator will choose the suitable method of authentication and will enter a password, the system will suggest to define a server with public key of Master-device. This option can be set through GPO. Alternatively, offer to enter the server address manually. After the public key of Master-device is downloaded, the system will go into a reboot and begin the encryption process.



BitLocker Drive Encryption

Encrypting...

Drive C: 0.0% Completed

Figure 12. Windows BitLocker encryption process

As a result, the user's public key and the public key of Master-device will encrypt the entire disk.

4.2.4. Authentication

Authentication is produced for system unlock, that a user was able to get access to OS and work files. The system will support the following types of authentication:

- PIN-code + Smart-card + token (in the case of ID-card)

At operating system booting, or awoken from sleep mode and hibernation, the system will require that the ID-card has been inserted into the reader, and USB-token, with a partial key is inserted into the USB connector on a computer, and then system will prompt to enter a password (PIN-code). Additional protection is provided in the form of a token to complicate the process of stealing information carrier. If we exclude the USB-token, then will be enough for attacker to take over user’s ID-card and carrier of information, which an attacker wants to crack. However, the token is greatly complicates the operational work and takes a USB-port on the PC, which is not too many, for example, on laptops. This method of authentication is safe enough, but not quite convenient, when it comes to laptops.

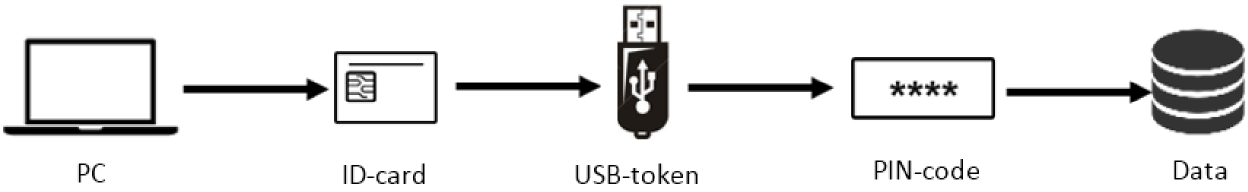


Figure 13. Authentication process. PIN-code + Smart-card + token (in the case of ID-card)

- PIN-code + Smart-card (in the case of ID-card)

At operating system booting, or awoken from sleep mode and hibernation, the system will require that the ID-card has been inserted into the reader and then system will prompt to enter a password (PIN-code). Since this option is inferior to the previous one by security reason, it will be noted in the Configuration Wizard, as not recommended for use. However, it is very comfortable for users work, because does not require superfluous actions and carrying superfluous devices. Nevertheless, in the case of theft of a laptop (or encrypted disk), and an ID-card, the attacker will only have to “guess” a password for authentication, which greatly simplifies the task of breaking the system.

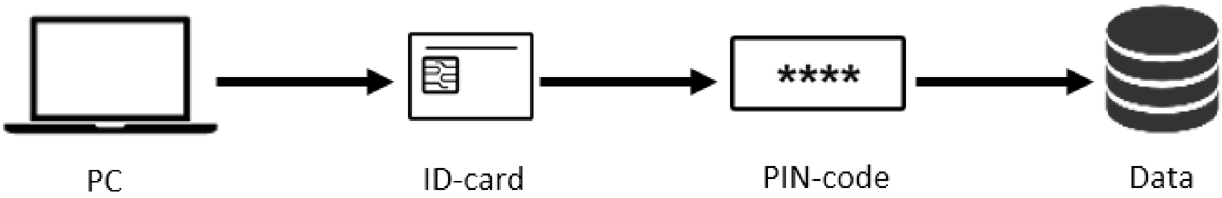


Figure 14. Authentication process. PIN-code + Smart-card (in the case of ID-card)

- PIN-code + Smart-card (in the case of TPM)

At operating system booting, or awoken from sleep mode and hibernation, the system will require that the Smart-card has been inserted into the reader and then system will prompt to enter a password (PIN-code). This method is equal with previous by simplicity of use, with the only difference, that this method is more secure, in case if the attacker will get only removable disk, or encrypted files. To decrypt files or disk, attacker needs not only a Smart-card, as in the previous case, but also a computer on which they were encrypted.

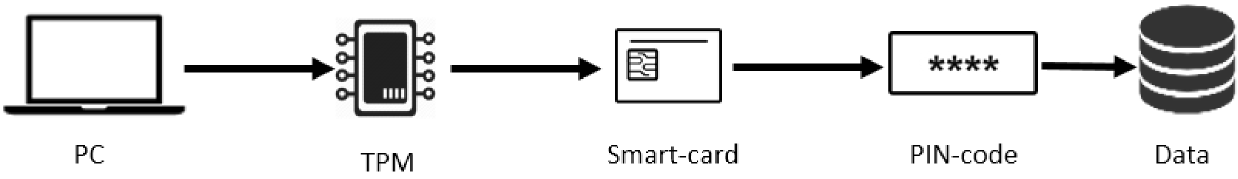


Figure 15. Authentication process. PIN-code + Smart-card (in the case of TPM)

- PIN-code + token (in the case of TPM)

At operating system booting, or awoken from sleep mode and hibernation, the system will require that USB-token, with a partial key is inserted into the USB connector on a computer, and then system will prompt to enter a password (PIN-code). This method is equal with previous by simplicity of use, with the only difference that instead of a Smart-card will be used USB-token with keys stored on it.

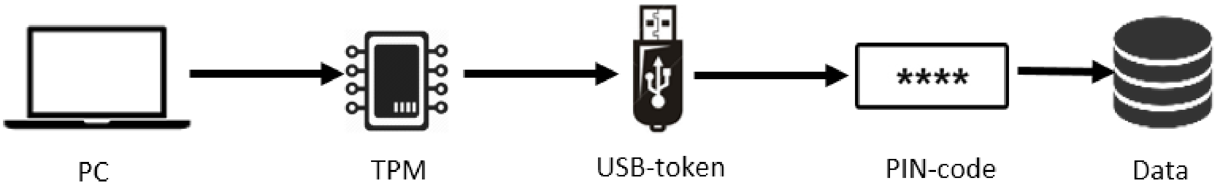


Figure 16. Authentication process. PIN-code + token (in the case of TPM)

At startup, the system searches for a suitable device with the private key by querying TPM, checking the USB-ports. Finding out a device with the key allows to the system to extract the private key from device, which decrypt a VMK key, which decrypt a FVEK key, which decrypt data on a disk. In that way happens decrypting data on the disk, in case of a successful authentication.

All listed authentication methods are designed to unlock the system for work. Each of these methods in his own good, but, as usual, for greater security is required to sacrifice ease of use and vice versa.

4.3. Public key Servers and File exchange

4.3.1. Public key Servers

For effective file exchange should be established a system of servers, with user's public key located on them. Such servers can be created on SQL-Server base, which contain a database and operate by a request-response scheme. The most effective version is represented, when such servers are tightly connected with Active Directory. This means that each user registered in the AD will have an entry, which describes his public key. This occurs through the binding of a specific device to the user account. For example, the company gets a new laptop, administrator installs the OS on it, enters to a domain, and enables encryption. Private keys are stored by one of the above methods, and public keys are entered into AD, where a device is registered. For that purpose, one of the attribute fields of AD will be selected. Once a user is logged on to device - his account will associate with account of the computer, on which the user has to work. Moreover, in the users account attributes registers public key of device, then it is called a user's public key, but in fact is the key of device.

A situation is possible, when for two users there can be the identical public key. This can occur, if two or more employees share a computer, as is often happens in financial institutions or structures, who offer 24/7 service. In this case, users have a common token and known to them PIN-code. However, this situation is not desirable, since generates a set of vulnerabilities that can easily lead to data leakage, and most importantly, to further complication of investigation of leakage incidents. Similar scenarios will be considered in Chapter 6.

4.3.2. File Exchange

Creating of a public key server will allow in further to implement multiple scenarios for file exchange within the company. The whole exchange procedure will often be invisible to the user or take a matter of seconds. This should not cause users annoyance, significantly slow down, or complicate business processes.

Procedure of file exchange will look like the following:

- User intends to send a file by e-mail with help of mail client.
- User creates a new e-mail and puts in the necessary file to attachment and clicks "Send" button
- System (in this case e-mail client software module) determines the recipients in the "To" field and makes a request for this name in the AD (or any other public key server).

- AD (or any other public key server) receives the request and finds accounts of recipients, and their public keys (or more precisely, the key of devices on which they work).
- AD (or any other public key server) sends the public key to the client.
- Client encrypts the file with public key of users specified in "To" field.
- File is encrypted with the sender's, recipients, and Master-device public keys.
- File is sent to the recipients.
- Action is recorded in the log on the server.

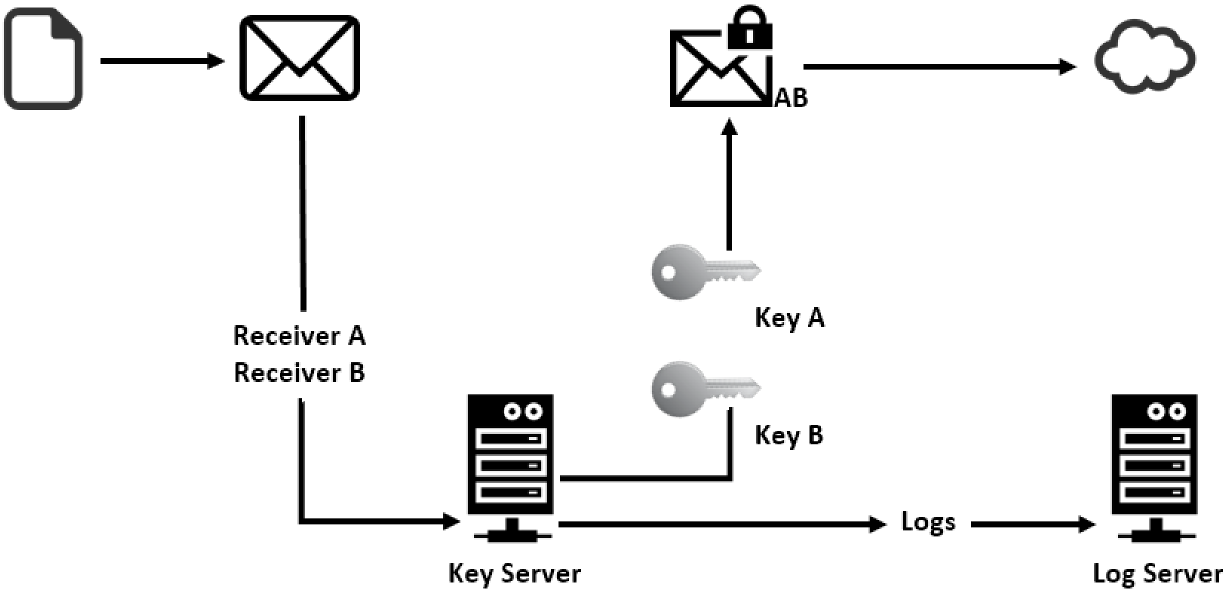


Figure 17. E-mail sending procedure

E-mail text is encrypted in the same way. As a result, an intercepted message could not be read also in the future, used by third parties as well as a fully encrypted and even other members of the organization cannot read it or use this file, as long as their public keys will not be added to the file. Similarly, should take place a file sharing within the network. It may be necessary to put the files in the share, such as internal portal, a network drive, FTP or external media. Then, there can be realized two access scenario.

First scenario:

- User copies the file to a network share or an external drive.
- System detects, that a copy of the file, or a file itself, leave the hard drive.
- System immediately displays a window, asking the user to add employees, who should have access to this file.

- User selects from a list of those employees, who need access to this file.
- System sends a request to AD (or any other public key server) to obtain users public keys.
- AD (or any other public key server) receives the request and locates a user’s accounts and their public keys (or more precisely, the key of devices on which they work).
- AD (or any other public key server) sends the public key to the client.
- System encrypts the file with public keys.
- The file is encrypted with owner of a file, recipients, and Master-device public keys.
- The file is copied to the target.
- The action is recorded in to a log on the server.

Second scenario:

- User clicks the right mouse button on the file he want to share with other users.
- Appears pop-up menu, with “Share” option
- By selecting this option, the user enters to a Share window
- User selects from a list of employees those, who need access to this file.
- The system sends a request to the AD (or any other public key server) to obtain public keys of those users.
- AD (or any other public key server) receives the request and locates at user accounts, and their public keys (or more precisely, the devices on which they work).
- AD (or any other public key server) sends the public key to a client.
- System encrypts the file of public keys.
- Action is recorded in to a log on the server.
- After that, user can transfer file to any shared resources within an organization.

Both scenarios can be represented by the scheme:

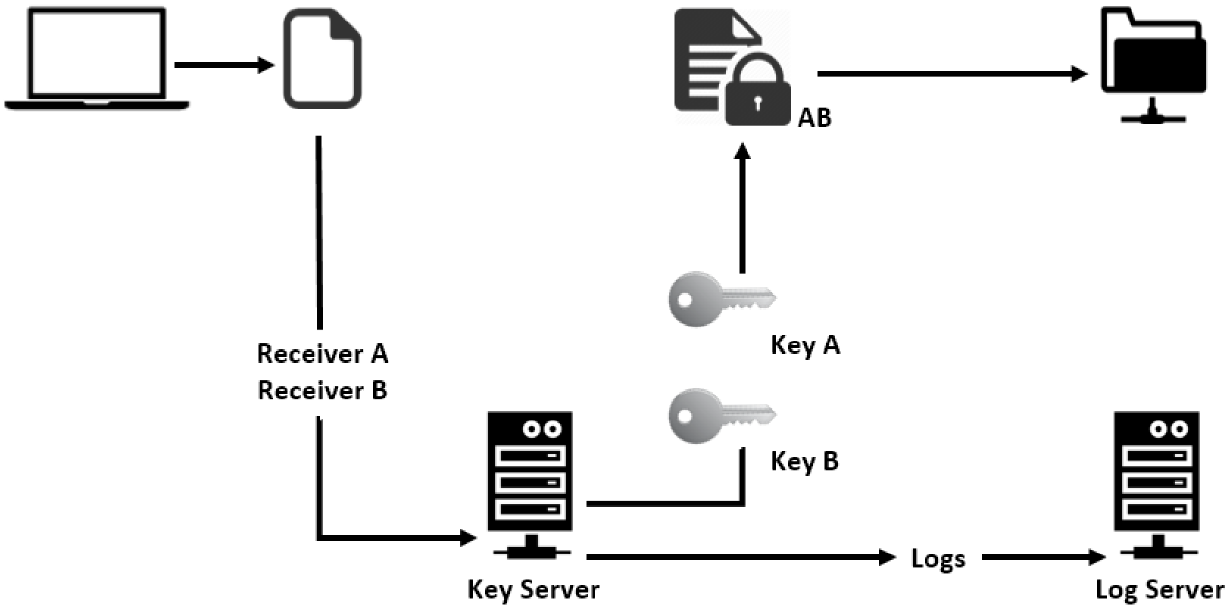


Figure 18. File exchange procedure

Both methods provide a high level of confidentiality, as ensure that none of the file will be read or used by random person, as they will not be able to decrypt it. The difference between these two methods is only in the fact that in the first case, the system forces a forgetful user to select to whom share a files and in the second, user himself, manually perform all access granting procedures and then share the file. The second method is preferable, because it helps to avoid errors, when the system will not give out a forced window of granting access, or a system failure may occur. As a result, the recipients will not be able to open the file. The second method gives a guarantee, that the recipients will be able to open the file, because it was encrypted before being sent.

4.3.3. File Exchange outside of organization

File exchange outside the organization does not look so simple. However, he does not have to be simple, when the task is to make an information "leak" difficult as possible to third parties. Any such attempt must meet on the way a whole series of barriers and inconveniences, however, this should not prevent of file exchange between authorized persons in different organizations. At least, has to be found the balance between security and usability of the system, which is not always done ideally in existing solutions. Is always sacrificed either security or usability. Data leakages are not eliminated in one case, and in other, we get angry users, who dislikes a badly working "paranoid" security system. Author will try to propose a system where been respected, in author’s opinion, the balance and security will be at a high level, and users will not be so angry.

The first way of such a solution may be a consolidation of public key servers of various departments and organizations, which are authorized for each other. This method implies that there are several organizations, which uses similar methods of encryption, with the use of public key servers. These organizations want to realize the exchange of files between themselves in the same way, as it is implemented within organizations - with the request of the public key from servers. The issue can be resolved by combining of servers or dedicated servers to the trusted zone. This would mean that the public key server can search for keys not only in his database, but also to send a corresponding request to other trusted server, which is located outside of the organization.

Here is how it might look like in the case of sending e-mail:

- User intends to send a file by e-mail with help of mail client
- User creates a new e-mail and puts in the necessary file to attachment and clicks "Send" button
- System (in this case e-mail client software module) determines the recipients in the "To" field and makes a request for this name in the AD (or any other public key server)
- AD (or any other public key server) receives the request and looks recipients accounts, and their public keys on own database
- Not having found the desired account, the server sends a request to a trusted server known to him
- Trusted server receives a request, looks at accounts of recipients and their public keys
- A trusted server finds public keys and sends them back to the server that sent the request
- AD (or any other public key server), receives public keys from the trusted server and sends the public key to the client.
- AD (or any other public key server) sends the public key to the client.
- Client encrypts the file with a public key of users specified in "To" field.
- File is encrypted with the sender's, recipients, and Master-device public keys.
- File is sent to the recipients.
- Action is recorded in the log on the server.

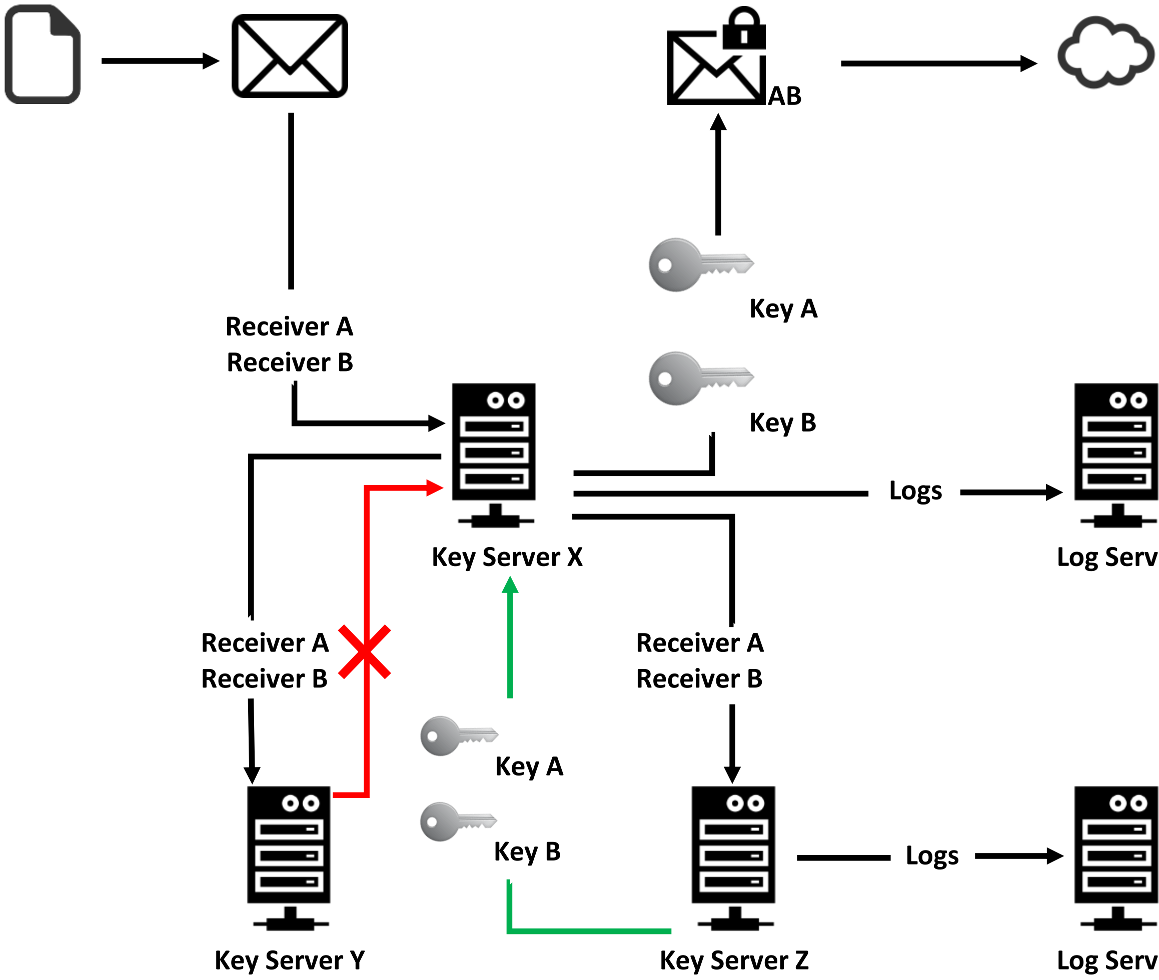


Figure 19. E-mail sending procedure with trusted public key servers

Such scheme allows organizations to quickly and securely share own files. Also, is allowed chain of servers, when servers start query their trusted servers, and those, in turn, begin to query their own. However, this method is not safe as in the end of the chain may be a public key server of the attacker, which was added to the chain by incompetent employees of third-party companies.

However, there can be a situation, when the public keys of recipient are not present neither on the server of organization, nor on the trusted servers. In this case, the recipient can receive an encrypted message with an encrypted file, and will not be able to read it. For this case is provided option to send a self-extracting archive that will be encrypted and protected with a password. This option presented today in a number of commercial solutions, described above.

However, this is not an escape from the information leaks – a user may thus send to a third party or his personal e-mail a lot of confidential information and it will not be controlled. Later, this information can be published in the media, sold to competitors and foreign intelligence services.

Author suggests complicating this procedure, by adding a control element in to it. There is control system of money transfers in financial institutions, when accountants make a lot of transfers per day, and at the end of the day a chief accountant checks them and confirms, as a result all transfers are performed at the end of the day after chief accountant confirmation. The same principle can be implemented in the system of files exchange among the unauthorized recipients.

It will look like this:

- User intends to send a file by e-mail with help of mail client
- User creates a new e-mail and puts in the necessary file to attachment and clicks "Send" button
- System (in this case e-mail client software module) determines the recipients in the "To" field and makes a request for this name in the AD (or any other public key server)
- AD (or any other public key server) receives the request and looks recipients accounts, and their public keys on own database
- Not having found the desired account, the server sends a request to a trusted server known to him
- Trusted server receives a request, looks at accounts of recipients and their public keys
- A trusted server cannot find public keys and sends this response to the server that sent the request.
- AD (or any other public key server), receives a response that the key is not found and sends the response to the client.
- The client sends an e-mail with a file in to the buffer zone.
- Head of the Department or the security officer will receive a notification, when e-mail enters the buffer zone.
- Head of the Department or the security officer checks the file and recipients, whether they are permitted to receive such files.

- If the recipient is authorized to receive such e-mails, the message is marked as allowed for sending.
- If a recipient is not permitted to receive such e-mails, the e-mail will be blocked.
- Permitted e-mail goes to the sending server, where attachments is packed to the archive, and sets a password on it.
- System sends an email with the archive.
- System sends a separate email with the password for the archive.
- Event is recorded to the log on the servers.

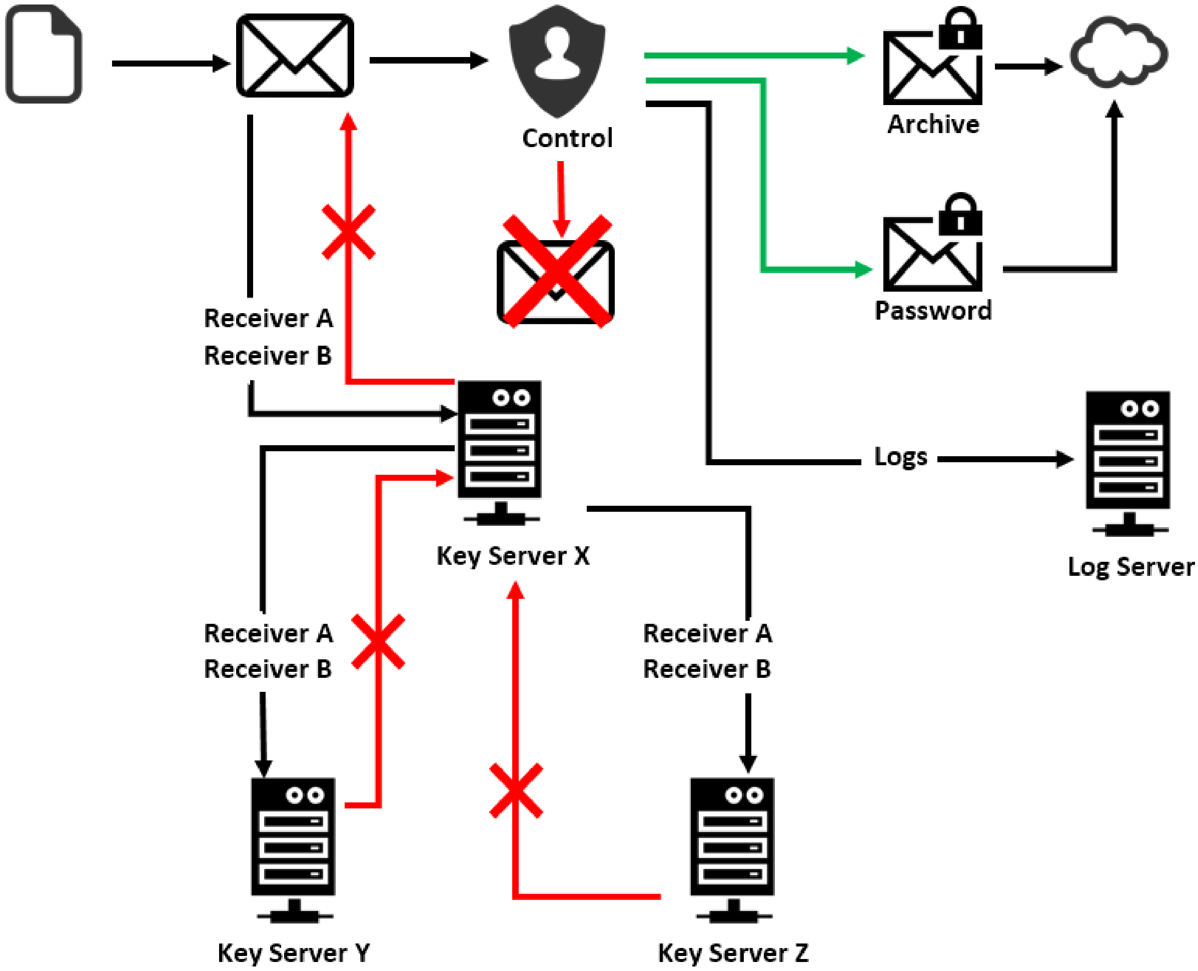


Figure 20. E-mail exchange procedure with controllers

Thus, there is a control of sending confidential files outside the organization. Monitoring is carried out by authorized persons, who will be able to allow file sending or deny it. It's extra work, maybe even will need to create a special department for this procedure, however, it will ensure a high level of security and the possibility of information leakage dramatically reduced, as for this purpose, attacker should have to enter into an agreement with a whole department, what is unlikely. Reduces the speed of e-mail delivery, it is also possible that increases the number of blocking of safe e-mails, which can lead to some users dissatisfaction. However, in this case, this approach is justified by security requirements.

The role of the buffer zone is intended to perform a server that operates on the principle of reverse spam-filter, the filter performed not by e-mails receiving, but e-mails sending. Since there is a separate filter-server of outgoing mail, then rules can be created there. For example, if the organization conducts frequent correspondence with another organization, that does not have a public key server, some of its recipients, with whom conducted the most intensive file exchange, can be added as an authorized. In that case, the system will automatically pack the file in to archive and send it to the recipient, without checking it by controlling person. Thus, procedure of files exchange will be speed-up among the authorized persons, though significantly reduces the element of control. If a person or an entire organization will be compromised, they will immediately be blocked on the server, and sending emails to be held by standard procedures with a controlling entity.

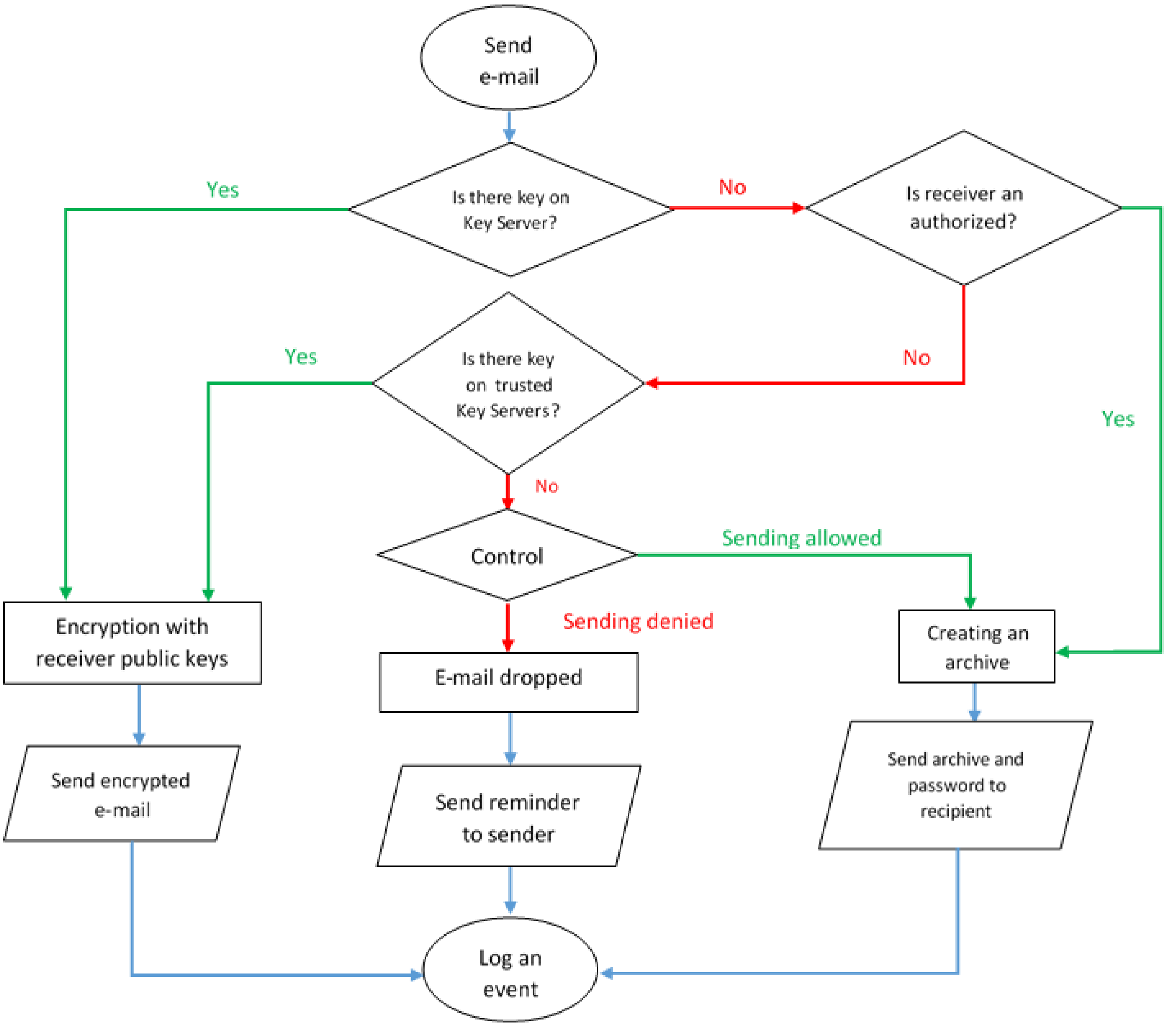

Send e-mail
Is there key on Key Server?
Yes
No
Is receiver an authorized?
Yes
No
Is there key on trusted Key Servers?
Yes
No
Control
Sending allowed
Sending denied
Encryption with receiver public keys
E-mail dropped
Creating an archive
Send encrypted e-mail
Send reminder to sender
Send archive and password to recipient
Log an event

Figure 21. Logical schema of e-mail exchange control

In the same way could be realized procedure of writing files to external media, but it is too vulnerable and even the existence of a controlling person is not able to solve this problem, since the decrypted file can then be used to transfer for bad purposes.

4.3.4. Solution for Estonia

The great advantage for Estonia is the presence of the system of ID-cards. Every Internet user has the opportunity to use a security system offered by the state. A symbiosis of encryption system, proposed by author, and the ID-card, is able to simplify the procedure of files exchange between unauthorized organizations, since any recipient who has the ID-card also has a public key and can receive encrypted files without having to unpack an archive and get the passwords to them. However, this does not eliminate necessity of presence of controlling staff. Because a file still can be sent away to the unauthorized person or malefactor, controllers should check up every such file sent. However, it eliminates the need to create archives and send passwords to the recipient, which makes file transfers more secure and resistant to interception.

In the whole, system of ID-cards and the public key servers, removes the need for organizations to take care of the presence of such equipment for them self. Public keys search and files exchange are considerably simplified. This means that the system that author proposes is most applicable in Estonia and in the countries, where such technologies are implemented already. Therefore, the use of the ID-card is the most convenient and acceptable way in the selection procedure of encryption and private keys storage.

4.4. Logs and Control

One of the main advantages of the system proposed by author, is a complete monitoring and logging of all activities related with the files exchange. As was mention above, any attempt to send a file to authorized person within or outside of the organization - will be recorded. Any attempt to send information to an unauthorized person would be subject to control and will be recorded. Here author want to describe in more detail, how controllers and system of logs should work in the organization.

4.4.1. Control

Controllers can be different members of the organization, it can be as heads of departments, as well as whole security department. The second option is preferable, because it allows the load off heads of departments, as in the case of large file exchange - this role can lead to a high load of one person, which is unacceptable. Also, the second option is more secure. Head of Department may have a personal attachment to their employees and more trust them, therefore will not be able to adequately assess the risk of file sent and wrongly take decisions, by giving more freedom to the employees. In addition, the attacker can enter into a criminal conspiracy with a Head of Department, to arrange intentional data leaks, what make it much more difficult, when it deals with the whole department. Thus, a presence of security department is the most acceptable variant and embodies the scenario of reliable control in a life. Each time a user's e-mail enters the buffer zone for assessing, they begin to engage by controllers. Which Controller will deal with this e-mail is not known beforehand - it removes the possibility of collusion, because the probability of an agreement with the whole department is negligible. After receiving the request, the controller begins a process of checking an e-mail contents and its recipient. If the supervisor is not able to make a decision or issue of access is too controversial, he sends it to three (or more) higher employees. These employees must be the immediate superiors of the sender and from now, they should to make a decision about sending permission. If at least one of the chiefs will be not agree to give permissions for sending, the message will be blocked, and the sender receives a notification, that his e-mail is blocked and cannot be sent.

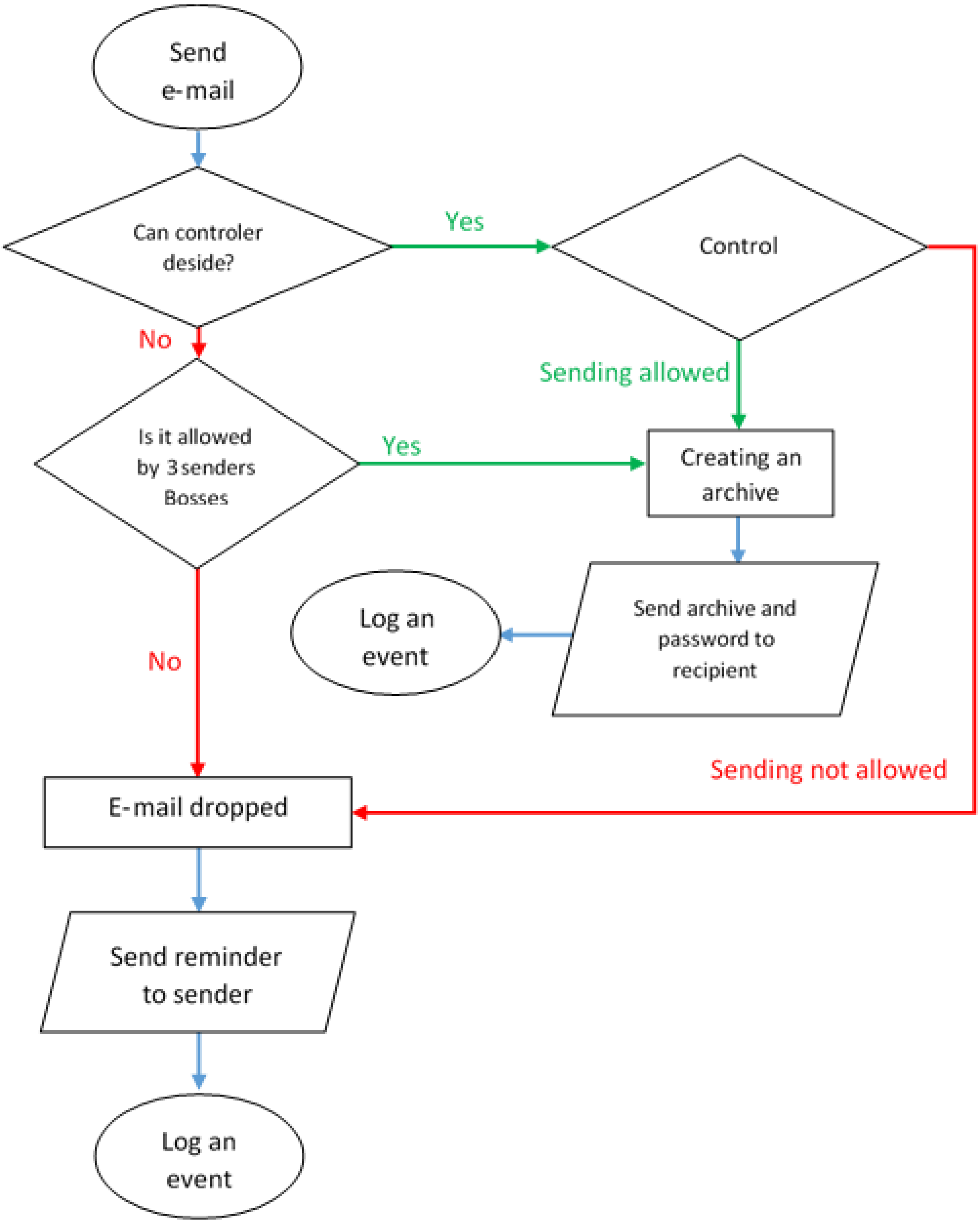


Figure 22. Logical schema of detailed control procedure

Thus might look control procedure, but each organization is in a right to decide, how it will be done concretely in their case. Author merely suggested the most appropriate scenario for the implementation, as author sees it.

4.4.2. Logs

As it is often impossible to avoid leaks and almost impossible to build a perfect security system, that can prevent leakage for 100%, then any such system should provide an opportunity to quickly investigate of occurred leakage incidents. Author’s system records every action in the log on the server, so to make it clear who, to whom, when and what was sent.

The logs are recorded at least during the following events:

- User sent a file within the organization
- User sent a file outside the organization to an authorized recipient
- User sent a file outside the organization to an unauthorized recipient
- User uploaded a file on a company’s network resource
- User uploaded a file on a removable disk
- User was not permitted to send a file outside the organization
- User is allowed to send a file outside of the organization

In case of a situation, where there will information leak occur, investigators will be able to retrieve logs and check, where the leak could occur and to whom was sent the information. In case of detection of a source of leak, it must be blocked in the system and deprive his rights of an authorized recipient. If we are talking about company employees, his public keys will be removed, and all e-mails that was sent to him will eventually settle in the buffer zone, where it will be blocked by the controllers, since the system will not be able to find a keys on the server.

Also, by the server of the keys control will be sent a request to a user device, that the private keys of a user became expired and a device will be blocked. User’s private keys will get status Expired, and as soon as the user tries to unlock his device, nothing will go out for him. The further user attempts to "leak" out information will be stopped thus, and a device will have status of compromised. Unlocking such a device will be possible in a different ways. That can decide every organization for themselves – either by entering a special key from the keyboard that will be generated by key server, or will have to be authorized, for example, an administrator with his ID-card, whose public key encrypts all devices in organization. Or HDD of devices should be placed in a Master-device to extract the necessary information from it, if such information presented on HDD. It will provide high-rate of reaction on incidents and isolation of the compromised devices, to avoid further losses. The only condition should be a permanent connection to the Internet, about possible ways to protect data without the Internet connection, author will tell in Chapter 6.

In general, thanks to the strong system of control, logs and blocking of compromised devices - a high level of reliability and data security is provided, with minimal impact on users work. Such approach certainly will make happy not all employees. Users do not like frequently, when superfluous control intrudes in their work and it is not possible to totally avoid complaints and dissatisfaction from the user's side, however it is a force paying for strong data security. What is more important for the organization – security or usability, each decides for themselves. Author's task is only to offer acceptable balance to solve this paradigm.

4.5. Breakdowns, blocking and recovery

In any work, even of the most reliable system, a human factor and degree of reliability of hardware are always inscribed. Hardware can break down, and people can make mistakes. Errors will cause system to operate improperly and breakdown of hardware to the stop of whole system. Author's system is not an exception, below will be considered the possible system problems caused by human errors and hardware failure on the client side.

4.5.1. Loss or damage of token or ID-card

Can be a situation, when the user has lost or broken one of fuses with the keys. For example, a token or ID-card. In that case, he will not be able to unlock the device and the work will be interrupted. In that case, should be provided recovery procedures, there may be several different variants. The first variant implies the presence of system administrator or any other person, who is responsible for Master-Card, which will be able to unlock the device and start the reconfiguring procedure of entire system. This procedure involves the use of a new token or ID-card, recording a new user private key, creating a new public key, re-encryption of entire system. This is possible because whole system is encrypted not only by user key, but also by public key of Master-device. This procedure is vulnerable to some extent, because the possession of a Master-Card allows to access any company device, the only thing it will need – is to take over the device, to take over the Master-Card and to find out Master-Card PIN-code.

4.5.2. This user has forgotten PIN-code

The device can also be unlocked by administrator’s Master-Card or responsible person, because for each card there is the own PIN-code. For Master-Card PIN-code must be more secure and stronger. After device unlocking the procedure for changing PIN-code will start, that does not require re-encryption of entire HDD. If a user is on a business trip or not in the office, then recovery of lost PIN-code is not possible.

4.5.3. Damaged motherboard with TPM-chip

If the whole computer crashes, than recovery of user’s private key from TPM-chip is not possible. However, all the data can be recovered, if to connect a hard drive to the Master-Device, on which TPM-chip stores its private key, and as HDD was encrypted by public key of this Master-Device, then it will be not too difficult to recovery it. The hard drive will be decrypted and all the data will be read, encryption will be disabled, after that, the unencrypted data can be overwritten on another hard drive. A new hard drive may be inserted into another computer and process of encryption may be started over. Master-Device is not connected to the Internet in order to prevent information leakage, while the disk is decrypted. This device is priority in the use, because appears most safe as compared to Master-Cards.

As a result, any damage or loss of tokens and cards can be resolved by the presence of Master-Device or Master-Card. However, most secure is to use a Master-Device, and most comfortable is a Master-Card. Which from two variants will decide to use an organization, depends on aims that organization sets before itself. In general, the problem of the human or "hardware" factor is fully presented.

4.6. Locking of devices

4.6.1. Compromised user

In addition to the damage and forgetful users, there may be a number of problems still to be resolved by a key server. One of such problem can be compromised user, for example, he may disappear, or becomes aware that he is a source of information leakage, or he may lose the management’s trust. On this case, is envisaged procedure of blocking of user keys. It looks as follows:

- Comes reports about compromised user
- A command is given, to block the user keys

- Key Server removes a user's public key from a database
- Key Server assigns to the user’s private key a status «Expired»
- Key Server enters this status in the database
- Next time user connects to the server, the device will obtain data about user's key
- Device immediately enters to the locked state, and refuses to accept user keys as they are "Expired"
- Now device can be unblocked only with Master-Card or in the Master-device

4.6.2. Compromised device

If a request comes about the theft of device or about its loss, then there is procedure of blocking of device. It looks approximately similarly as was described above, when will blocked not only a device, but also all user’s keys. It is done in order to avoid a situation, when a user forgets to report about the loss of token and Smart-cards together with a device, and similarly on a case, when token was copied without the user consent.

4.6.3. Offline device locking

However, what to do if the device is stolen, and it cannot contact the server, since it is not connected to the network. As a result, it cannot be blocked, and the attackers may try to break it using all the means available to them. Is known a case, when “attackers” got access to unlocked encrypted laptop and 3 hours collecting the information, preventing laptop from lock or going in sleep mode and thus get data from it:

“Two plainclothes FBI agents, one male and one female, walked up behind Ulbricht and began arguing loudly. This staged lovers' tiff caught Ulbricht's attention long enough to distract him from his laptop. As soon as Ulbricht looked up, the male agent reached down and slid the computer over to his female colleague, who quickly snatched it up and handed it over to Kiernan for further investigation.

Understandably alarmed, Ulbricht stood up sharply, Kiernan told the jury. But he did not resist arrest, and Kiernan was able to access the computer — a Samsung 700z — to collect evidence almost immediately. Kiernan recalled taking his "brand new USB" and extracting all of the files from Ulbricht's laptop before taking photos of the computer with his FBI-issued Blackberry.

Kiernan estimated he spent about three hours collecting evidence from Ulbricht's computer that day. But this was far from the end of the government's investigation". [14]

To avoid such method of breaking or alike, is envisaged a procedure of blocking offline devices. Attackers, who stole the laptop, can know that the key server will immediately block the computer. To avoid this, they can disconnect the computer from the network. And then, there are several possible scenarios.

First scenario: a system, which is in offline more than one day (or any other time selected by administrator) will be locked automatically and require access to the Internet, to connect with a server.

The second scenario: a system in offline more than one day (or any other time selected by administrator) will be locked automatically and require to enter a verification code that will be generated by key server, based on a special algorithm associated with the device ID and user's public key. To find out this code, user can contact the system administrator and identify himself.

The third scenario – the strongest, when the system will completely blocked, status "Expired" will be assigned to a user's key and unlocking with a Master-Card will be required.

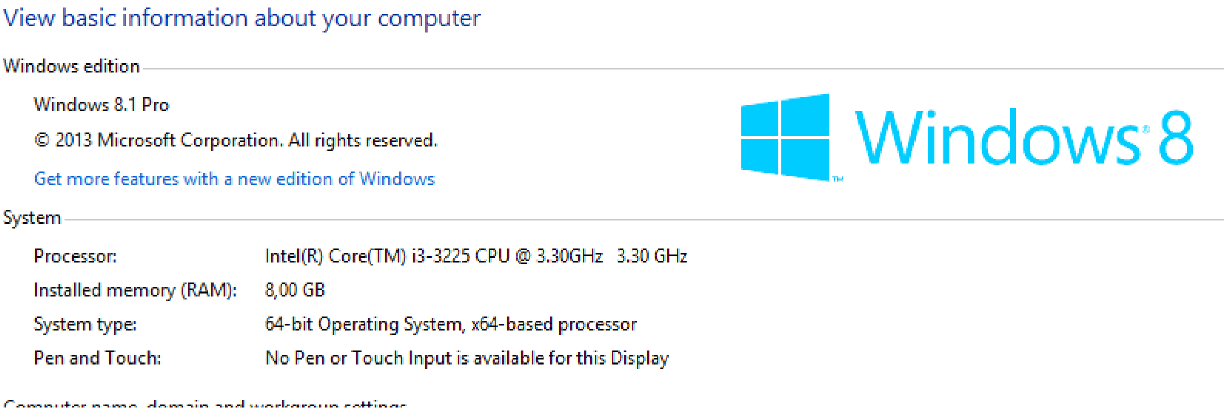
All of these methods are designed to protect data on the computer from offline attacks, and each organization can choose the most suitable version.

5. Performance

As is well known, the main problem of implementation of any security system - is user’s dissatisfaction. People will always complain that they are too lazy to enter a password each time during login procedure, it is uncomfortable to encrypt files, as it is too long and difficult to do, and so on. Another complaint is often the complaints about performance degradation of encrypted system, which, they say, it runs slower and longer handles the requests.

To test this theory, were conducted a performance tests on encrypted with help of BitLocker system. For a basis, the following configuration has been chosen of a standard office computer with ordinary SATA drive:

- Processor: Intel Core i3-3225 CPU 3.3 GHz
- RAM: 8Gb
- OS: Windows 8.1 Pro 64-bit
- HDD: Western Digital Blue 500Gb; SATA 6 Gb/s; 7,200 RPM; 126 MB/s
- TPM: No



View basic information about your computer

Windows edition

Windows 8.1 Pro

© 2013 Microsoft Corporation. All rights reserved.

Get more features with a new edition of Windows

System

Processor: Intel(R) Core(TM) i3-3225 CPU @ 3.30GHz 3.30 GHz

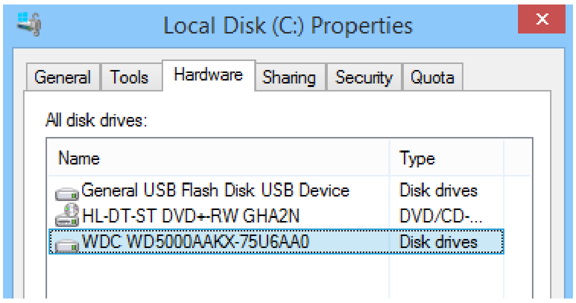
Installed memory (RAM): 8,00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain and workgroup settings

Figure 23. Tested platform specification



All disk drives:

Name	Type
General USB Flash Disk USB Device	Disk drives
HL-DT-ST DVD+-RW GHA2N	DVD/CD-...
WDC WD5000AAKX-75U6AA0	Disk drives

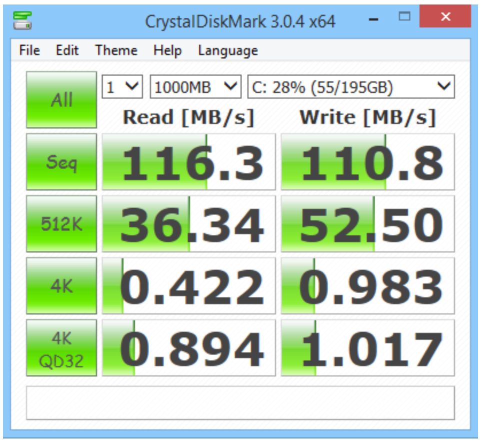
Figure 24. HDD specification

We will conduct the tests of read/write speed on a disk with help of CrystalDiskMark 3.04. [15]

The program performs the following tests:

- Seq: Sequential (Block Size=1MiB) Read/Write with single Thread
- 512K - random Read/Write (block size = 512KB)
- 4K: Random 4KiB Read/Write with single Queue & Thread
- 4K QD32: Random 4KiB Read/Write with multi Queues & Threads

Here what result was after a single run:



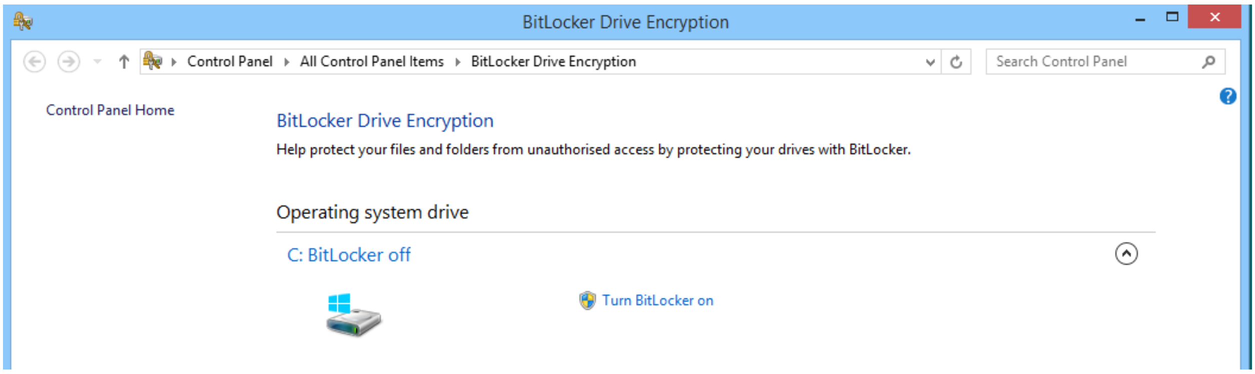
1 | 1000MB | C: 28% (55/195GB)

All	Read [MB/s]	Write [MB/s]
Seq	116.3	110.8
512K	36.34	52.50
4K	0.422	0.983
4K QD32	0.894	1.017

Figure 25. HDD speed before encryption

The manufacturer claimed a read speed was 128 MB/s in ideal conditions. Author gets 116 MB/s.

Let’s run the built-in encryption procedure on a disk without TPM:



BitLocker Drive Encryption

Control Panel ▸ All Control Panel Items ▸ BitLocker Drive Encryption

Search Control Panel

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorised access by protecting your drives with BitLocker.

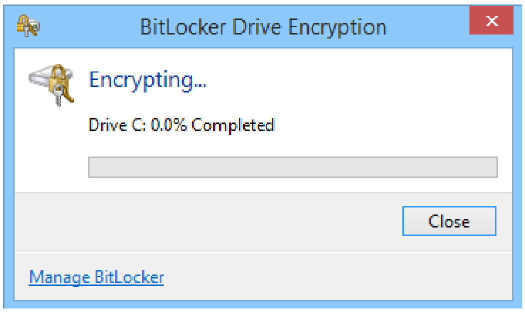
Operating system drive

C: BitLocker off

Turn BitLocker on

Figure 26. Enabling Windows BitLocker

Encryption procedure has begun:



BitLocker Drive Encryption

Encrypting...

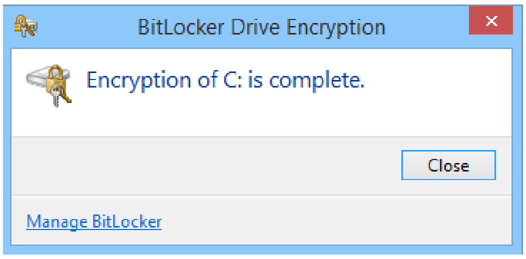
Drive C: 0.0% Completed

Close

Manage BitLocker

Figure 27. Encryption procedure

Encryption procedure is completed:



BitLocker Drive Encryption

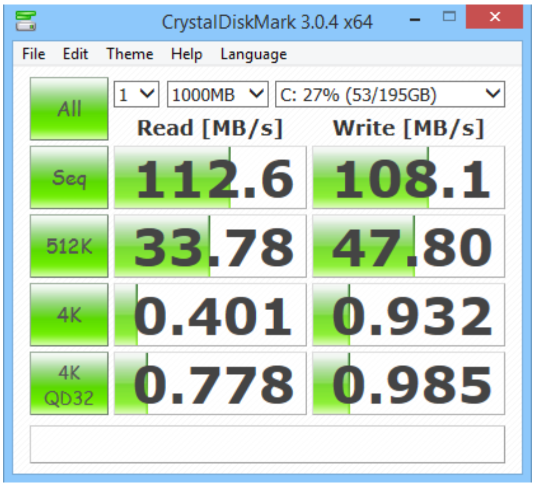
Encryption of C: is complete.

Close

Manage BitLocker

Figure 28. Encryption completed

Author has tested a HDD speed with a CrystalDiskMark one more time, here is what author gets:



```
1   1000MB   C: 27% (53/195GB)
            Read [MB/s]   Write [MB/s]
Seq           112.6         108.1
512K          33.78         47.80
4K            0.401         0.932
4K QD32       0.778         0.985
```

Figure 29. HDD speed after encryption

All output data can be presented in a table:

Table 2. HDD performance

	BitLocker On		**BitLocker Off**		**Performance degradation**	
	Read (Mb/s)	Write (Mb/s)	Read (Mb/s)	Write (Mb/s)	Read (Mb/s)	Write (Mb/s)
Seq	112.6	108.1	116.3	110.8	3.18%	2.44%
512K	33.78	47.80	36.34	52.50	7.04%	8.95%
4K	0.401	0.932	0.422	0.983	4.98%	5.19%
4K QD32	0.778	0.985	0.894	1.017	12.98%	3.15%

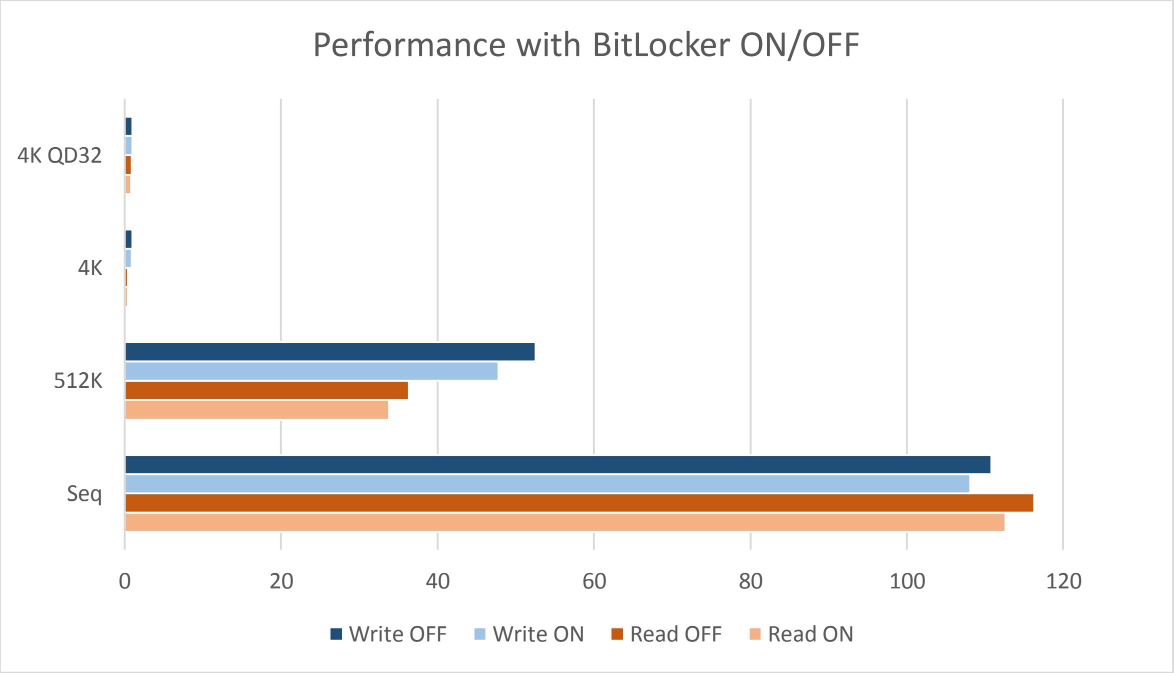


Figure 30. HDD performance

As can be seen from the above tests, performance actually fell an average of 7% when reading and 5% when writing data to the HDD. This cannot be considered as a significant performance degradation, this numbers are not critical and is hardly will be noticeable during users work. It is possible to draw conclusion from here, that we should not afraid the system performance degradation because of encryption, such fears are strongly exaggerated. This test is a positive signal for the encryption systems and opens a clear way for their wider application.

6. Scenarios

In this chapter, author will consider a few scenarios that could happen in real life, there will be included various attempts to break-in and theft of information, and will demonstrate how the system is protected against them.

6.1. Stealing from external media

We will simulate a situation, when a user decides to copy some data from his working computer to USB-drive: he inserts USB-drive in to a computer and copies some documents on it. At this very moment, the system will find that the data is moved to the USB-flash drive displays a menu with the request – who of employees needs to give access to this file, with whom a user wanted to share this information. A user can just close a window – to choose none of colleagues and then a file will be copied simply as he is. Coming home user inserts the USB-flash drive into his home computer and found an encrypted file, open and use that he will not be able. Thus, the system is protected from evil-minded copying of files to external media.

6.2. Data leakage via e-mail

Imagine a situation when a user tries to steal confidential documents by sending them to his personal e-mail, or e-mail of a third party. User creates a new mail, attaches files to it, enters the recipient’s address and sends a mail. Since the recipient is not an authorized, mail arrives into the buffer zone, and exposes to control. Controller finds out that this recipient has no authority to get such documents, blocks a mail and reports to management about an incident of attempt to "leak" of confidential information. Management takes actions. Thus, any attempt to "leak" the information by e-mail will be stopped.

6.3. Data leakage from laptop

Consider a situation in which the attacker steals a laptop with confidential information. When he tries to gain access to the operating system, he will be prompted to insert a token or Smart-card. Since attacker does not have them, the system will not be loaded. Then the attacker will try to remove the hard drive and read information from it, however, will fail, because all information will be presented in an encrypted state. The more time an attacker will be busy with a laptop, the more likely that the laptop will be blocked and to access it will be possible only by the administrator or with help of Master-device.

6.4. Data leakage from clipboard

Imagine a situation when working with classified documents a user copies the information to the clipboard. Inserts own USB-flash drive, which is not encrypted. Creates a new document on it and pastes a copied text from the clipboard. Saves the document and removes the USB-flash drive from PC. Later, at home, user inserts a USB-flash drive into his home computer and detects a single encrypted file, which he cannot read or use. It happened because the system encrypts any content created inside of it. Since the system creates a file on the flash drive – it was created in encrypted form, since system cannot create any content, which is not encrypted. Even if to insert the information from the clipboard into already created file on USB-drive – system will encrypt the content of that file. Because after pressing SAVE button and closing it, user "releases" this document and a system will immediately encrypt it.

From the above scenarios, it is clear, that to steal information even being into organization very difficult, certainly, there is a method to do it, however, he is not so obvious. With its main task – to protect against data leakage, the system can handle perfectly.

7. Conclusions and Future Research

As mentioned above, during of conducted research it was found out that the organizations as a whole and the organizations staff in particular, do not care about safety of confidential information and with criminal negligence related to the requirements of security policies. Users lightly perceive requirements to encrypt data, and companies does not monitor an implementation of own security policies. All these factors lead to enormous financial losses, because of multiple data leaks. Knowing such fact, that companies are often reluctant to share information about real financial losses, it is possible to suppose, that these losses are much greater. Meanwhile, there are many commercially solutions available on the software market, designed to protect users data by providing encryption and recovery tools. It, certainly, will save large amount of organizations from leaks of confidential data in case of theft of media, however, until now, not a single instrument was presented, which would be able to protect the organization from information leaks, which is carried out by company's employees.

In this work, author offers a tool that can solve the problem of leakage from the inside and close the issue of the existence of "Snowdens" in the organizations. Author supplies the project with a wide range of encryption tools, emergency recovery tools, control and monitoring tools. Author's project is intended to serve to large organizations such as ministries, multinational corporations, the military departments within NATO, large financial companies and the various secret services. Obviously, this project involves close cooperation with the developers of BitLocker software by Microsoft and require serious financial resources for its implementation. This product is not intended for use by individuals, since it implies a serious server capacity, such as a key server, domain controllers, and the Master-Device.

Implementation of this product will also be accompanied by early dissatisfaction of users, to whom will be unusual to work in encrypted and strictly controlled system, however, an adaptation period is always accompanied by nervousness and complaints of users, no matter what product would be implemented. Encryption and control is always complicates the work and involve the acquisition of new skills by users, which makes them not always welcome. However, the task of specialists of Cyber Security is to find a delicate balance between comfort and security, and to provide a balanced solution where security is at a high level, and system usage will be as comfortable as possible within a given system.

The tests conducted by author showed, that during use of author’s system the performance of computers falls quite insignificantly, what would be quite unnoticeable for a user, who will be unhappy with anything, but not with the speed of the system, since it will remain almost unchanged.

In the future, during of the development and improvement of a project, author thinks that a system of controllers deserves special attention, which can be thought out in detail and improved. Should also pay attention to the trusted servers of public keys, to their interaction and synchronization. A more profound consideration should be given to use of the private key of ID-card in system encryption.

Summary

Every organization need to make a choice for themselves, what is more important a user’s comfort or safety of confidential data, which constantly appears on WikiLeaks. In general, system, author has proposed is a powerful and sophisticated mechanism to protect data from accidental and especially from intentional leaks. Widespread use of the physical custodians keys such as USB-tokens, TPM-chips, especially the use of Smart-cards makes this system reliable and increases its cracking resistance. The ability to use, during encryption process, of regional ID-cards makes the system easy to deploy and convenient to use it in Estonia, as removes from organizations a load associated with the adjustment and maintenance of key servers, as well as provides simple way of encrypted files exchange, among different organizations, thanks to a common server keys. Thus, Estonia is at the forefront of data protection of its organizations and provides a complete platform for implementing of a complex control mechanisms and data encryption, within large organizations. This once again proves the advantage of building of e-state and opens the shortest way for whole state in the world’s future of reliability and data security.

References

[1] "The Number of the Week: 38% of Companies Do Not Care about Encryption of Corporate Data." Kaspersky Lab. April 3, 2013. Accessed March 4, 2015. http://www.kaspersky.ru/news?id=207733979.

[2] Ponemon Institute. "The State of USB Drive Security in Europe." Independently Conducted by Ponemon Institute. November 1, 2011. http://media.kingston.com/pdfs/Ponemon/Ponemon_research_EMEA_summary_UK_1111.pdf.

[3] Dunn, John. "Hospital Lost Unencrypted USB Stick despite Strict Security Policy." Computerworld UK. October 3, 2011. Accessed April 2, 2015. http://www.computerworlduk.com/news/security/3307842/hospital-lost-unencrypted-usb-stick-despite-strict-security-policy/.

[4] Dunn, John. "Lost USB Stick Earns Rochdale Council ICO Rebuke." Computerworld UK. November 7, 2011. Accessed April 2, 2015. http://www.computerworlduk.com/news/public-sector/3316000/lost-usb-stick-earns-rochdale-council-ico-rebuke/.

[5] Dunn, John. "USB Sticks Still Being Used Insecurely, Ponemon Study Finds." ITworld. November 26, 2011. Accessed April 2, 2015. http://www.itworld.com/article/2734875/security/usb-sticks-still-being-used-insecurely--ponemon-study-finds.html.

[6] "Chronology of Data Breaches." Privacy Rights Clearinghouse. February 15, 2015. Accessed May 8, 2015. http://www.privacyrights.org/data-breach.

[7] "KASPERSKY ENDPOINT SECURITY for Bussiness Extended." Kaspersky Lab. February 26, 2015. Accessed March 19, 2015. http://www.kaspersky.ru/business-security/endpoint-advanced#tab=frame-2.

[8] "How Endpoint Encryption Works." Symantec. 2015. Accessed March 19, 2015. http://www.symantec.com/content/en/us/enterprise/white_papers/how-endpoint-encryption-works_WP_21275920.pdf.

[9] "McAfee Endpoint Encryption Solution." McAfee. February 15, 2015. Accessed March 20, 2015. http://www.mcafee.com/ru/resources/solution-briefs/sb-endpoint-encryption-keeps-data-safe.pdf.

[10] "Microsoft BitLocker Administration and Monitoring (MBAM)." Microsoft. Accessed May 8, 2015. http://www.microsoft.com/en-us/windows/enterprise/products-and-technologies/mdop/mbam.aspx.

[11] Hynes, Byron. "Data Protection with BitLocker Drive Encryption." SecurityLab. June 1, 2007. Accessed March 8, 2015. http://www.securitylab.ru/analytics/296866.php.

[12] "Trusted Computing Group." TPM Main Specification. March 1, 2011. Accessed May 8, 2015. http://www.trustedcomputinggroup.org/resources/tpm_main_specification.

[13] "Avaleht ID.ee." Avaleht ID.ee. April 15, 2015. Accessed April 15, 2015. http://www.id.ee.

[14] Bertrand, Natasha. "The FBI Staged A Lovers' Fight To Catch The Alleged Kingpin Of The Web's Biggest Illegal Drug Marketplace." Business Insider. January 22, 2015. Accessed April 13, 2015. http://www.businessinsider.com/the-arrest-of-silk-road-mastermind-ross-ulbricht-2015-1#ixzz3YELTvNkW.

[15] "Crystal Dew World." Crystalmark.info. February 13, 2015. Accessed March 8, 2015. http://crystalmark.info/download/index-e.html.