aepd agencia española protección datos

isms forum

apep Asociación Profesional Española de Privacidad

Guidelines for the validation of cryptographic systems in data protection processing

v. May 2023

EXECUTIVE SUMMARY

The widespread use of information and communication technologies and services has made encryption one of the most important measures to protect data security. Properly implemented cryptographic mechanisms provide robust measures for the protection of personal data in automated processing to ensure confidentiality, integrity, and authenticity.

The strength and robustness of an encryption system, i.e. its ability to withstand attacks aimed at breaking the protection it provides, depends on its behaviour as a system, not just on each individual component. In order to provide an adequate level of protection, encryption systems must be efficient and effective in the context of each particular processing, as well as being operational.

The GDPR explicitly mentions encryption as a measure for the mitigation of security risks in the protection of personal data:

- In order to ensure a level of security appropriate to the risk to the rights and freedoms of personal data subjects,
- It is a safeguard, among others, to fulfil compliance with the GDPR,
- It is a safeguard that decreases the likelihood of an impact on data subjects in the context of a personal data breach.

Therefore, as a protection measure, encryption will not have the same impact on all processing activities and will necessarily be complemented by other privacy safeguards and security measures.

For encryption to be an effective measure in a processing operation, the controller, or the processor, has to verify, evaluate and assess all elements involved in the encryption process, going beyond the selection of an algorithm or a specific implementation. On the one hand, it is necessary to determine the requirements to be met by the encryption system in the context of the processing of personal data. And on the other hand, it is necessary to validate that these requirements are met, as well as to monitor that they are kept over time. In any case, it should be borne in mind that the protection of personal data implies considering the lifetime of such data, which can be as long as the lifetime of the data subject, and it will be necessary to take into account the context of technological changes that occur over long periods of time. It is important to note that encryption does not entail anonymisation, although it could be used as a pseudonymisation tool.

These guidelines outline the elements that it is recommendable to assess in the design and validation of an encryption system used in the processing of personal data, taking into account the importance of that system in such processing, and especially focused on those cases in which encryption is used to preserve confidentiality. In addition, a non-exhaustive and non-enforceable list of controls is proposed to facilitate the GDPR controller or processor, the CISO, the DPO, data protection advisors and internal and external auditors in the selection, validation and monitoring of encryption systems in the context of a specific processing operation, as part of the implementation of data protection by design and accountability principles.

Key words: cryptography, encryption, keys, algorithm, mitigation, risk, GDPR, audit, data protection.

This document has been developed by the Agencia Española de Protección de Datos (Spanish Data Protection Agency) in collaboration con la Asociación Profesional Española de Privacidad (APEP) and the Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum) and reviewed by Carlos Bachmaier, DPO of Sociedad Estatal, María Isabel González Vasco, Professor at the Department of Applied Mathematics, materials Science and Engineering and Electronic Technology (MACIMTE, by its initials in Spanish) of the Universidad Rey Juan Carlos and Isabel Barberá, Privacy Engineer at Rhite.

CONTENTS

1 INTRODUCTION

Encryption is a procedure by which information (which will be referred to as clear information) is transformed into a seemingly unintelligible set of data (or encrypted information). To achieve this goal, modern cryptography combines transformations based on mathematical algorithms, "secure" implementations of these algorithms and the use of keys. The main characteristic of encryption is that, without access to the appropriate key, it should be unfeasible (at least in a time and resource frame) to access or alter the content of the encrypted information undetected.

Encryption as a measure appears explicitly in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), and in Organic Law 7/2021 of 26 May on the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties (LO 7/2021). n the GDPR it appears among the measures that can be applied for the mitigation of security risks in the protection of personal data (Recital 83 and Article 32), as a safeguard that helps to establish the compatibility of the processing (Article 6(4)) or as a safeguard that reduces the likelihood of an impact on data subjects in the context of a personal data breach and makes communication to data subjects optional (Article 34).

Encryption is an appropriate security measure as long as its implementation and operation are in line with the characteristics and impact of the processing. Otherwise, it becomes a measure that generates a false sense of security that relaxes the application of other complementary measures in the processing, in particular privacy safeguards by design.

Limiting the issue of encryption to the mere selection of an algorithm is a simplistic view that neglects essential aspects that may render such a measure useless. An encryption system or cryptosystem is much more complex, and can be understood as all the elements that make up the encryption and decryption processes involved in the processing of personal data: the algorithm, its implementation, the creation and management of the lifecycle of the keys, the tools that make up its suite, the communication, the devices used, the governance model, etc. The application of the principle of proactive responsibility (art. 5.2 and art. 24.1 of the GDPR) requires validation[1] of the cryptographic system in the processing of personal data in the context of the nature, scope, context and specific purposes of each processing operation.

The level of detail in the design, validation and monitoring of the cryptographic system must be appropriate to the importance and relevance of encryption in data processing and the impact of such processing on the rights and freedoms of data subjects.

The role of encryption in a processing operation could be that of an additional safeguard among the many that are implemented in a particular processing activity, or even a data protection by default measure[2]. It could also be a decisive measure in a processing activity to manage a high risk or even one of the measures on the basis of which it is established that there are sufficient safeguards to protect the rights of data subjects. In the latter case, we could refer to different articles of the GDPR in which measures are an important part of determining compliance with the requirements of the data protection regulation:

- Weighting of legitimate interest (art. 6.1.f)

[1] The documented act of proving that any procedure, process, equipment, material, activity, or system actually leads to the expected results. The process of confirming that an item (a system, a work product or a part thereof) matches the needs of its stakeholders.

[2] Article 25 states for the establishment of appropriate technical and organisational measures to manage both "risks of varying likelihood and severity posed by the processing to the rights and freedoms of natural persons" as well as depending on "the nature, scope, context and purposes of the processing" even if there is no risk to the rights and freedoms of data subjects.

- Determination of compatible processing operations (art. 6.4.e)
- Limitations to rights established by law (art. 23)
- Choice of a processor (art. 28)
- Reduction of a high risk of processing (art. 32) and (art. 33.7.d)
- Duty to communicate a personal data breach to data subjects. (art. 34.3.a)
- Passing the proportionality assessment of the processing (art. 35.7.b)
- Codes of conduct and certification (art. 40, 41 and 42)
- Compliance with the GDPR on international data transfers (art. 46, 47, 49 and 50)
- Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (art. 89)

The strength of an encryption system is an objective assessment of the likelihood of it being compromised in a given period of time. This possibility should be very low, in the case of data protection, for the entire lifetime of the personal data. This strength does not depend exclusively on the algorithm used or the length of the key, and not all systems have the same strength. Using a very strong encryption system may entail a high cost, both in the implementation and in the operation of the processing, and may also conflict with the fulfilment of other requirements (non-data protection) regarding with latency, energy, resources, performance, portability, usability, cost, return on investment in security, etc.

However, from the point of view of the GDPR, it is not acceptable lowering security levels below those needed for personal data protection, and to put at risk the rights and freedoms of data subjects, on the basis of criteria other than the protection of rights and freedoms.

In particular, in the event that the main guarantee on which a processing operation is based is the encryption of personal data, it is necessary to carry out an exhaustive validation of the strength of the cryptosystem[3]. This validation must be carried out "by design" and the use of the encryption system must be integrated into the processing as established in the A Guide to Privacy by Design published by the AEPD.

In any case, the personal data protection policies, which would form part of the controller's governance framework or data protection policy, referred to in Article 24 of the GDPR, should reflect the controller's strategies in relation to cryptographic systems from a data protection perspective, and be integrated into the information systems security management procedures.

This guideline does not go into the detail of all the specific cases of actual implementations, nor it address the assignment of staff roles in the whole process, but is a starting point for an initial framework of analysis and, a help to controllers and processors in the selection of the controls deemed relevant to check. Of course, controllers and processors should add additional controls when they are needed in the validation of a cryptosytem in a specificity processing activity.

[3] OWASP has identified encryption flaws as the second most important web security risk factor in 2021.

2 INITIAL CONSIDERATIONS

2.1 Recipients

This guidance is aimed at controllers and processors/sub-processors to whom the GDPR or the LO 7/2021 applies, who implement cryptography in their processing of personal data. Therefore, it is also aimed at data protection officers, personal data protection advisors, data protection auditors, security specialists, and managers of processes in controllers or processors. Developers of encryption solutions that are intended to process personal data and, in general, developers of ICT system products and services are also advised to use this guide.

2.2 Obligations

The controller and any processor/sub-processors (Art. 32.1 GDPR) are obliged to ensure that the security measures implemented for the purpose of managing risks to rights and freedoms are effective and are subject to regular verification, evaluation and assessment (Art. 32.1.d)

It should be underlined that measures established under Article 32 have to be assessed on a regular basis, unlike other appropriate technical and organisational measures, in order to ensure and be able to demonstrate that the processing is in compliance with Article 24(1) of the GDPR which provides that they shall be reviewed and updated as necessary.

The actual implementation of a processing activity (which defines the nature of the processing) will involve the acquisition of components, the use of services, possibly the hiring of processors, sub-processors and the communication of data, which will also affect the cryptosystem as part of the security measures.

The controller has to define the allocation of duties in the security management with the processors, in particular in relation to the encryption system, taking into account that part of the direct management will normally remain in its hands. In the case of components and use of third-party services for the implementation of the cryptosystem, controllers and processors/sub-processors will have to be diligent in requiring performance certifications in line with the requirements of the specific processing and the regulations in force.

2.3 The role of the DPO

In those cases where a DPO is appointed, the DPO has, among other duties, to inform and advise the controller or processor, and their employees, of the obligations arising from the GDPR (art. 39.1.a), to supervise compliance with data protection regulations, staff awareness and training, audits, (art. 39.1.b) and, in the case of a Data Protection Impact Assessment, to advise and supervise its implementation (art. 39.1.e).

This advisory and supervisory role could take the form of general data protection audits and regular audits with regard to the correct implementation of security measures. In particular, the DPO has to be informed of any kind of internal incidents and contextual changes regarding with the encryption system. On the basis of this information and taking into account the characteristics of the processing as a whole, the DPO may submit its conclusions and recommendations to the highest management bodies of controllers and processors.

With regard to the purpose of these guidelines, the DPO must be familiar with the processing and the requirements of the cryptosystems to be implemented in the processing. He/she will have to advise and, as part of his/her duties of supervising compliance with the provisions of the GDPR, supervise the regular process of verification, validation and assessment of the proper functioning of the encryption system.

In short, the DPO must:

- Know the nature or how the processing implementation.
- Know the level of risk to rights and freedoms of such processing.
- Know the impact of the cryptosystem in the set of security measures that determine the viability of the processing from the point of view of rights and freedoms.
- Advise of the needed requirements for the encryption system(s), which elements of the system are most critical and what checks should be carried out.
- Supervise the regular process of verification, evaluation and assessment of controls.
- Report to the organisation's management.

Within a process of continuous improvement, the audit is one of the best management tools that can be used by the DPO to define the recommendations to be noticed to the controller and to ensure the strength of the cryptosystem regarding with the protection of personal data.

It is also good practice to regularly monitor how the organisations' processors/sub-processors and suppliers maintain their encryption system, starting, for example, with a vendor assessment[4].

2.4 Beyond confidentiality

Encryption can be used both to protect the confidentiality of personal data and to determine the integrity of information, as well as in authentication, non-repudiation and pseudonymisation processes.

Although this document focuses on encryption as a measure to preserve confidentiality, it may be of help where encryption systems are used in processing for the purposes outlined above, and where the failure of such measures could affect fundamental rights in relation to data protection.

2.5 Security by design and validation

The controller, before including an encryption system in the processing, has to carry out two tasks:

- Determine from the design the requirements for cryptosystem robustness that are necessary in processing and
- Validate that these requirements are being effectively achieved in the implementation of information systems and their operation.

Art. 24.1 of the GDPR provides that the controller shall implement appropriate technical and organisational measures for processing. In order to be appropriate, the measures must be established on the basis of, on the one hand, the nature, context, scope and purposes[5] of the processing and, on the other hand, the risk to the fundamental rights and freedoms of individuals posed by the processing itself. In relation to the risk to fundamental rights and security, Art. 32 establishes that the measures put in place must be appropriate to ensure an adequate level of security. As the Spanish Supreme Court has already established, security

[4] Process of evaluating and approving potential suppliers through objective assessment.

[5] Therefore, default measures have to be put in place, regardless of the risk of the processing.

measures are an obligation of means, not of result[6]. Measures must have three objectives: first, to ensure the protection of rights and freedoms; second, to ensure compliance; and third, to be able to demonstrate compliance. Moreover, protection and compliance are not one-time actions, but require regular review and updating, in the case of security measures.

The requirements established in the previous paragraph (to guarantee, to demonstrate and adequacy of the measures) require setting up from the design stage of the processing the strength and robustness requirements of the cryptosystem that are necessary in the processing. The strength and robustness requirements must be established objectively and must be proportional to the potential impact of the processing in the rights and freedoms and, in this case, to the importance of the encryption system within the set of security measures in the processing. For this reason, these guidelines propose four scenarios for auditing a cryptographic system according to the role of cryptography in the processing. These scenarios, ordered from least to most demanding in terms of guarantee, are as follows:

- Encryption is a default data protection measure.
- The encryption system is a measure that manages medium and low risks in processing.
- Encryption is a complementary measure to manage the high risk to rights and freedoms in processing.
- Encryption is the main or most important measure to manage a high risk to rights and freedoms in the processing, or even to legitimize the processing.

On the other hand, both Art. 24 and Art. 32 of the GDPR oblige the controller to carry out a periodic objective evaluation and review of the measures. One instrument for reviewing and updating the measures is the audit, where the effectiveness of the policies, procedures and technical and organisational measures should be validated for the current processing activity. An audit of the encryption system, its configuration, implementation and use, conducted from a data protection perspective, may be a part of a more general data protection audit of the processing.

An encryption system that is not regularly evaluated, verified and validated in the context of processing, would be a system that does not offer objective/factual guarantees. Note that a validation, or audit, is not a "reverse engineering" process[7]". In other words, the system has to be designed and implemented in an accountable manner[8] (Art. 5.2 of the GDPR), which implies that an objective/formal development methodology must be used, guided by specific requirements, with verification and validation processes, and documented. Verification of compliance with the principle of accountability is the first step in the validation and/or audit process. Validation or audit do not replace the obligation of accountability, but complement it.

2.6 REQUIREMENTS AND LIFETIME OF PERSONAL DATA

Each processing will have particular requirements in relation to the encryption system (latency, memory limitations, performance, HW/SW resourcesHW/SW[9], power consumption, cost, etc.), in addition to strength and robustness requirements. These are all interrelated

[6] Comunicación Poder Judicial: The Supreme Court states that the obligation of companies to take the necessary measures to ensure the security of personal data cannot be considered an obligation of result

[7] A process or method by which one attempts to understand through deductive reasoning how a previously created device, process, system or piece of software performs a task with little (if any) idea of exactly how it does so).

[8] A processing cannot comply with the principle of proactive accountability if its component parts, or the means by which it is implemented, do not comply with it.

[9] Hardware/Software

requirements, e.g., lower latency will certainly require higher power consumption and perhaps increases cost. Similarly, higher robustness will depend on and impact the other requirements.

The strength (algorithmic security and key size) and robustness (implementation and operational security) requirements of the encryption system differ from one processing to another: some processing activities will require from simply securing confidentiality for a few days against unsophisticated adversaries while others will require, up to the need to protect confidentiality against sophisticated unauthorised entities for years, as in the case of commercial and industrial secrets or information with high individual or societal impact. The lifetime of the data, understood as the length of time it is relevant to keep the message confidential (or intact), is the relevant criterion for determining the strength and robustness requirements of the cryptosystem.

Where encryption techniques are used to add additional security measures to the processing of personal data, it is necessary to consider both the impact that disclosure of the data may have and what is the lifetime of the data from the point of view of the GDPR, i.e., the lifetime of the data[10]. As defined by the GDPR in Article 4.1, a personal data is personal data as long as it is information relating to an identified or identifiable natural person[11].

If encryption is to be the decisive protection measure for processing, storing or transmitting information whose disclosure could pose a high risk to fundamental rights and freedoms (geolocation of minors, information on victims of gender violence, medical records, habits of vulnerable persons or intimate habits, profile or financial information of a large part of the subjects of a country, etc.) we would be talking about strength and robustness requirements that offer reasonable protection for many years [12].

2.7 ENCRYPTED INFORMATION AS PERSONAL DATA

The use of encryption is one of the protection measures that can be incorporated in the processing of personal data and could be an appropriate pseudonymisation tool. However, it should be borne in mind that the fact of encrypting data does not remove its nature as personal data, so encrypted information is not anonymised information[13]. The alleged "loss" or deletion of a decryption key will not change this nature[14].

[10] Paragraph 84.3 and footnote 70 of the Recommendations 01/2020 on measures supplementing transfer instruments to ensure compliance with the EU level of protection of personal data Version 2.0 state “3.the strength of encryption and key length takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved”. Note: Public authorities may undertake to access encrypted data in the circumstances described in paragraph 80, and store them until their resources are sufficient for decryption. The accompanying measure can only be considered effective if such decryption and further processing at that time no longer constitute a violation of the data subjects' rights, for example because the data can no longer be used to identify them directly or indirectly.

[11] The Article 29 Working Party's Opinion 4/2007 on the concept of personal data states that " Information relating to dead individuals is therefore in principle not to be considered as personal data subject to the rules of the Directive, as the dead are no longer natural persons in civil law.”

[12] At this stage, it should be considered whether to require them to be quantum-resistant, i.e. capable of withstanding decryption attacks using high-powered quantum computers.

[13] In a formal analysis based on Information Theory, anonymisation implies loss of information, whereas an encrypted dataset implies no loss of information.

[14] For the elimination of the key to imply anonymity, we would have to have a perfect secret cryptosystem, in which the distance of uniqueness is preserved, the birthday limit, the entropy of messages and keys tends to infinity, the implementations (programmes, libraries, operating systems and devices) are flawless, the management and policies perfect, the people perfect, the algorithms perfect and resistant to attacks of any kind for over 50 years (personal data is personal for the life of the person), etc. In other words, we would be demanding an obligation of result, not of means as established by the SC and therefore not legally enforceable. Even if it could be guaranteed, we would be talking about singular cases, not about the common operation of massive data encryption.

2.8 SNLD ATTACKS

In relation to the two previous sections, the increase in digital storage and processing capacities has brought to the table the need to consider future SNLD attacks, an acronym for "Store Now, Decrypt Later", also known as HNLD[15].

Today, it is possible to have huge data storage capacities available for a long time. This makes it possible to collect encrypted data and keep it waiting for the chance to unveil the information (or the right time to apply resources to do so). In addition, technological advances, especially in relation to quantum computing[16], point to the weakness of commonly used encryption systems in the near future[17] [18].

The impact that the materialisation of such attacks could have in the future, both for the privacy of individuals and society as a whole, needs to be assessed[19]. This assessment needs to be particularly careful in cases where huge amounts of personal data under the responsibility of public administrations are hosted on external services that are protected, in transit or in storage, by encryption means.

2.9 THE KEY AS PERSONAL DATA

A natural person's key is a unique identifier and its use makes it possible to identify the person using it and, under these conditions, it is therefore, personal data in the context of specific processing operations.

2.10 ENCRYPTED INFORMATION: AT REST, IN TRANSIT AND IN COMPUTATION

To put it simply, there are two approaches that could be considered as the typical cases of cryptosystems:

- Encryption on data at rest: data is encrypted for secure storage against loss of confidentiality.
- In transit: data is encrypted before it is sent to a recipient, either over networks or using other media. The recipient may or may not have the means for decryption, as may be the case for encrypted cloud storage. Data can be encrypted either for protection during transmission or for remote encrypted storage.
- In computation: data is generated in encrypted form or encrypted and then processed without decryption, only decrypting the result when necessary.

The latter case is in varying degrees of practical application, and is the frontier of the state of the art of encryption, so this paper will deal with the first two cases. The process of encryption of information at rest, broadly speaking, could be considered as consisting of these major blocks:

[15] H stands for “harvest”, although SNLD is also interpreted as Steal now, decrypt later.

[16] Although quantum computing is not necessary for such attacks to materialise: https://dl.acm.org/doi/pdf/10.1145/3560107.3560182

[17] https://newsroom.ibm.com/2023-02-23-IBM,-Vodafone,-Other-GSMA-Taskforce-Members-Outline-Critical-Pathways-to-Protect-Telcos-Against-Quantum-Era-Cyberthreats

[18] https://cacm.acm.org/news/269080-nist-post-quantum-cryptography-candidate-cracked/fulltext

[19] https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf

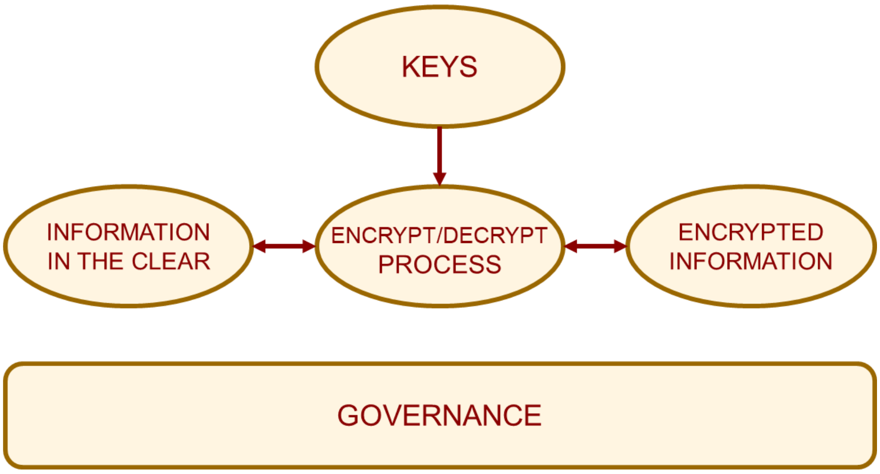


Figure 1 Data encryption at rest

In case of being oriented to the confidential transmission of information, there are new elements to be taken into consideration, such as the agreements of keys with a receiver and the communication of messages, as well as a replication of all elements of the sender at the receiver (which are only hinted at in the attached figure):

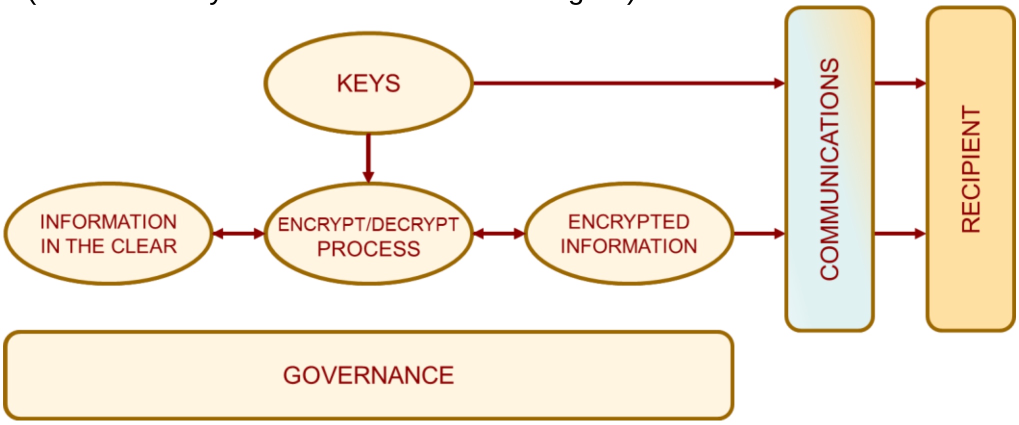


Figure 2 Encryption of data in transmission

In the case of encryption for transmission, ensuring the authenticity and integrity of the message is usually a prerequisite.

The use cases presented here are basic cases for didactic purposes. In practical processing we may find a combination of several processes or the application of different encryption systems in some phases of the same processing activity. For example, in a cloud storage service, where data is transmitted to the cloud through a channel secured by encryption and, in addition, the data is itself encrypted at source or is encrypted at rest by the cloud service.

Some specific processing may show great complexity in the application of encryption systems, such as messaging systems in asynchronous environments[20], polymorphic encryption, proxy re-encryption, encryption of multimedia, etc.

This guidance will serve as a starting point and will have to be adapted to the peculiarities of each system, bearing in mind that this is a field in full development, with some applications available using PET and PEC technologies.

[20] For example, the implementation of the signal-protocol

2.11 PRIVACY ENHANCING CRYPTOGRAPHY

PETs or Privacy Enhancing Technologies are those products and services developed specifically to facilitate the implementation of privacy measures in a processing. A subset of PETs are PECs or Privacy Enhancing Cryptography.

Regarding with PECs, the US National Institute of Standards and Technology (NIST) points to a number of advanced cryptographic tools that are particularly suitable for implementing privacy-by-design strategies:

- Zero-Knowledge Proofs of Knowledge (ZKPoK)
- Secure Multiparty Computing
- Homomorphic Encryption
- Group and Ring Signatures
- Private Intersection Protocols (PSI)
- Private Information Retrieval (PIR)
- Structured encryption (StE)
- Searchable Symmetric Encryption (SSE)

Through these tools, it is possible to implement advanced solutions suitable for different scenarios and use cases, such as, for example:

- Management of credentials for access to services with guarantees of anonymity.
- Management of encrypted and shared databases, with different access levels.
- Designing data analytics and machine learning methods on encrypted data.
- Privacy-assured verification and auditing in different environments.

2.12 DOCUMENTATION OF ENCRYPTION SYSTEM REQUIREMENTS

The controller should determine the requirements for encryption systems by design, and these requirements should be guided by a risk assessment, at least regarding with the risk to the rights and freedoms of data subjects. In design and implementation of the cryptosystem, it may be useful to use the classification introduced in the following section. Then, in addition to providing guidance for the requirements definition, the process of verification, evaluation and assessment will be more efficient.

In turn, the planning, execution and results of verification, evaluation and assessment processes should be documented. In addition, the results and recommendations resulting from these processes should be followed up.

3 VALIDATION OF THE CRYPTOGRAPHIC SYSTEM FOR DATA PROTECTION

The controller and the processor must carry out "*a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing*" (Art. 32). For the sake of brevity, in this document this process of testing, assessing and evaluating has been referred to as validation[21]. If the controller has decided to use encryption to protect personal data, the implemented encryption system must be validated in light of the nature, context, scope, purposes and risks of the processing.

The relevance of encryption as a personal data protection measure in an actual processing activity may be different from other different processing. In the same sense, the validation requirements of the cryptosystem(s) will have to be adapted accordingly. The level of analysis and management of the encryption operations will need to be proportionate to the risk to the rights and freedoms of data subjects and the role of encryption as a measure for the GDPR compliance of the whole processing. Risk management shall determine how risk can be mitigated or avoided by employing technical and organisational measures from the initial stages of the design of the processing of personal data. This management and implementation in the processing must comply with the principle of accountability, which will imply, inter alia, being documented and verifiable.

As with any security system, the overall strength and robustness of the encryption system will be equal to that of the weakest element of the system.

3.1 EVALUATION OF THE ELEMENTS OF ENCRYPTION

Validation of the encryption system may need to include, among others, the selected algorithm; implementation of the algorithm; key management; verification of procedures; cipher suite; pre-processing of data; communication protocols; interaction of encrypted data with applications and storage; and finally, review of organisational aspects of system management and encryption hardware.

The components of an encryption system can be decomposed for further analysis. The decomposition approach proposed here is intended to identify elements that are known to have been a source of vulnerabilities in the past.

.

[21] The documented act of proving that any procedure, process, equipment, material, activity, or system actually leads to the expected results. The process of confirming that an item (a system, a work product or a part thereof) matches the needs of its stakeholders.

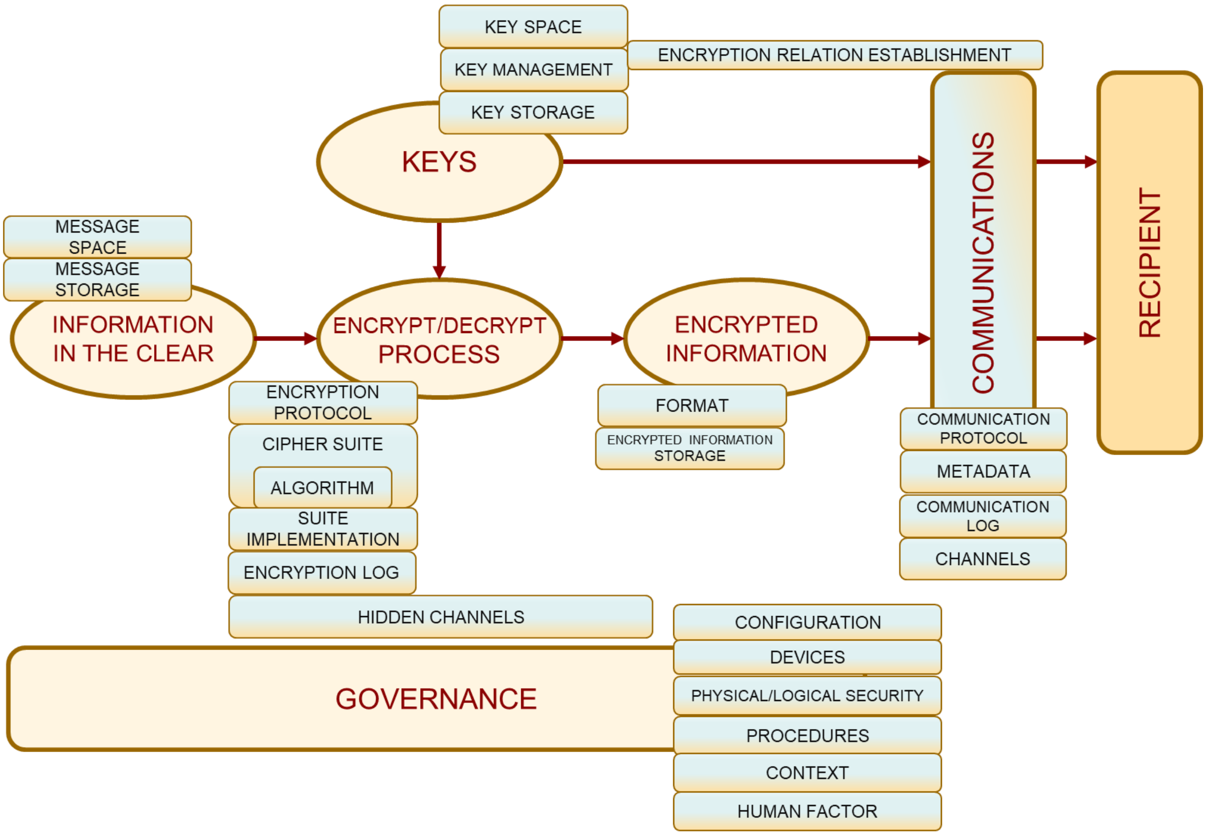


Figure 3 Elements forming part of an encryption system.

3.2 RECOMMENDATION FOR THE LEVEL OF EVALUATION

As noted above, the level of analysis to which the encryption system is subjected in validation will depend on the following factors:

- The risk to the rights and freedoms of data subjects that could be posed by a data breach of processing due to the compromise of the encryption process,
- The importance of encryption as a guarantee that is fundamental for the assessment of the conditions for GDPR compliance,
- The purpose of the encryption system (storage, communication and/or other) as well as the level of compliance it deems appropriate and proportionate.

The level of analysis has to be established by the controller and/or processor, advised by the DPO[22] and with the support of the security officer, by means of a risk assessment for the rights and freedoms of the processing activity.

As a recommendation, this guide suggests four different levels of criticality of the encryption system regarding with a processing of personal data:

- As a less critical level, where the processing is very low risk and encryption is included as a default data protection measure [23].
- As low and medium criticality, where the encryption system is a measure that manages medium and low risks in the processing.

[22] Where appropriate, the data protection specialist

[23] Measures and safeguards put in place in the processing regardless of the level of risk of the processing and which also encompass the default security measures.

- As high criticality, where the encryption system is a measure that, in addition, manages the high risk.
- As highly critical, where encryption is the main safeguard to manage a high risk or even the main measure on which the GDPR compliance assessment relies on.

Depending on this, levels of verification of the different elements of the encryption system are suggested:

- Optional: marked in yellow.
- Medium: marked in orange.
- High: marked in red.

	CRITICALITY OF ENCRYPTION AS A MEASURE TO ENSURE THE PROTECTION OF DATA SUBJECTS' RIGHTS			
ELEMENT TO BE EVALUATED	Data protection by default.	In medium and low risk processing.	In processing in which the high risk is managed by encryption among other safeguards.	In processing where it is the main measure to manage a high risk or to legitimise the processing.
Keys				
1.Key space	🟧	🟥	🟥	🟥
2.Key management	🟧	🟥	🟥	🟥
3.Key storage	🟨	🟧	🟥	🟥
4. Management of the encryption relation	🟨	🟧	🟥	🟥
Message space				
1.Message space	🟧	🟥	🟥	🟥
2.Message storage	🟨	🟨	🟧	🟥
Encrypted information				
1.Format	🟨	🟧	🟥	🟥
2. Encryption storage	🟨	🟨	🟥	🟥
Encryption suite				
1.Suite and algorithm	🟧	🟥	🟥	🟥
2. Encryption protocol	🟨	🟧	🟥	🟥
3.Implementation	🟨	🟨	🟥	🟥

4 Encryption log	🟨	🟨	🟥	🟥
5. Hidden channels	🟨	🟨	🟨	🟥
Communications				
1.Communication protocol	🟧	🟥	🟥	🟥
2.Metadata	🟨	🟨	🟥	🟥
3.Communication log	🟨	🟨	🟥	🟥
4.Channels	🟨	🟨	🟨	🟥
Recipient	🟨	🟨	🟥	🟥
Governance				
1. Configuration control	🟧	🟧	🟥	🟥
2.Devices	🟧	🟧	🟥	🟥
3. Physical/logical security	🟧	🟧	🟥	🟥
4.Policies	🟧	🟧	🟥	🟥
5.Context and data breaches	🟧	🟥	🟥	🟥
6.Human factor	🟨	🟧	🟥	🟥

For each of the elements, a list of possible controls has been drawn up in this document. This list is neither exhaustive nor all controls are required. The list has been compiled to be a guidance to select which checks might be most appropriate for the assessment of each particular element in the framework of a specific processing. This list can used as a starting point to determine which of them are suitable in the actual processing, which are unfit in the actual processing, and, most importantly, which ones should be added that are not on the suggested list of checks.

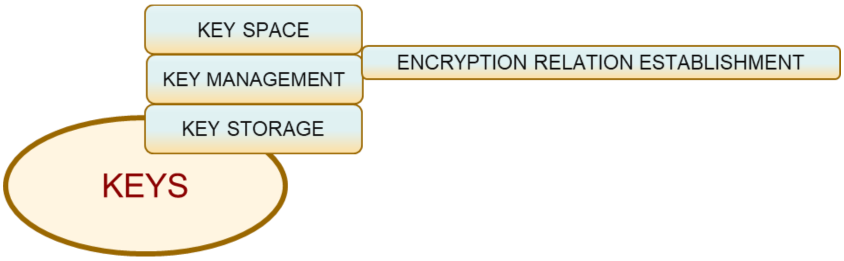
All elements are interrelated, so that there are checks that may well cover different elements. This is evident in the example cases displayed for each set of controls, which show that a holistic view of the whole system is necessary.

3.3 KEYS

The strength of a cryptosystem rests to a large extent on the strength of its keys, and this depends on the key space, their proper selection, their confidentiality[24] and a proper lifecycle management process[25], in particular, the storage of the keys.

[24] In case of asymmetric cryptosystems only in relation to the private key.

[25] Although in some cases they have elements in common, passwords should not be confused with keys.



3.3.1 Key space

The key space is the set of possible keys that could actually (not theoretically) be selected in the actual execution of an encryption system.

Control
1. Key security requirements have to be defined, e.g., length over a number of bits (see Annex), format etc
2. There is a procedure to avoid reuse of keys.
3. It is not possible to use manually generated keys.
4. Passwords are not used as keys.
5. Keys are not generated from user passwords using key derivation functions.
6. There is a procedure for the detection and elimination of weak and predictable keys.
7. High entropy in the key selection process and potential coverage of the entire key space, with uniform distribution, is ensured.
8. The absence of correlation between the keys of different users is guaranteed.
9. Key generation takes place in a protected environment (e.g., in hardware security modules or HSM[26]).
10. Key generation shall be isolated from the operating environment.
11. Key generation protects forward secrecy [27].
12. Key generation protects future secrecy [28].
13. The key generation mechanisms shall be certified and subject to the applicable sectorial regulations.
14. Whether or not the generated keys should be implemented on physical devices or tokens.

Office environment:

Keys generated by hand or derived from the passwords used are vulnerable to social engineering attacks and have been the subject of psychological analysis. A term “password psychology” has even been developed to study the internal mechanisms of password construction. Information posted on social networks, or the analysis of passwords used by the same user in any other service, can provide a lot of information to target brute force attacks.

[26] https://es.wikipedia.org/wiki/HSM

[27] If any key, or set of keys, is compromised, it is not possible to compromise past keys. That is, knowledge of a key does not allow the discovery of old keys with which text has been previously encrypted

[28] If any key, or set of keys, is compromised, it is not possible for a third party to deduce the future keys to be generated in the key relation.

Key generators:

These are local storage devices manufactured by various technology firms, which provide what their creators call "military-grade data protection"; they use the PBKDF2 algorithm as a key derivation function by performing 1,000 iterations of MD5 to derive the encryption key. The "salt" used to derive the keys is constant and encrypted across all solutions and all vendors, which makes it easier for an actor to determine the user's password.[29].

Generation of keys from biometrics:

Key generation using biometric patterns (Genkey Biohash Key Creation) could present risks related to correctness of algorithms, false positive rate, in addition to privacy risk as biometric characteristics of subjects may be revealed. They are susceptible to reversal attacks and other[30].

Cryptocurrencies:

In cryptocurrency digital wallets, keys have been deduced by using procedures that are too simple in their generation, such as brain wallets, or other simplification methods that generate weak keys (truncations, etc[31]).

WiFi communications:

Some routers used to provide Wi-Fi access within institutions use key generation mechanisms with very low entropy that allow simple attacks on the WP protocol[32].

3.3.2 Key management

The encryption system must have a key management process, and this section deals with that key management process. Due to its specificity, it is developed below:

Control
1. The management and lifecycle of the key and certificate relationship is documented: generation, distribution, storage, change or update, revocation, management of compromised, forgotten, or lost keys, activation periods, expiry, recovery of lost or corrupted keys, storage[33], backup and destruction of keys.
2. There are extracts from the management documentation oriented to the different roles involved in the encryption process.
3. If a cryptographic medium or token is not used, the entry of the key and its representation on the screen must not be in a format readable by other persons or users who may be around.
4. Internal key distribution is done through confidential channels and by authenticating the recipients.

[29] https://noticiasseguridad.com/vulnerabilidades/el-cifrado-en-dispositivos-de-almacenamiento-western-digital-y-sandisk-tiene-vulnerabilidades-criticas/

[30] https://www.usenix.org/legacy/event/sec08/tech/full_papers/ballard/ballard_html/index.html

[31] https://www.securityweek.com/most-bitcoin-brain-wallets-drained-attackers
https://www.wired.com/story/blockchain-bandit-ethereum-weak-private-keys/
https://www.ise.io/casestudies/ethercombing/
https://cointelegraph.com/news/blockchain-bandit-how-a-hacker-has-been-stealing-millions-worth-of-eth-by-guessing-weak-private-keys

[32] https://www.dragonjar.org/rompiendo-redes-inalambricas-wpa-y-wpa2-con-wps-en-segundos.xhtml

[33] https://www.dit.upm.es/~pepe/401/index.html#!3677

5.	There are procedures in place to train users never to disclose keys or passwords to third parties on request, even if they identify themselves as administrators of the service.
6.	A user management procedure is in place, both for authorisation and termination procedures or for those whose privileges have been temporarily (absent) or permanently withdrawn.
7.	There is a procedure defining the use of keys that limits reuse in multiple messages, use in different procedures and systems or in different roles [34].
8.	There is a procedure that guarantees a large distance [35] between two keys of consecutive use [36].
9.	A pyramid/hierarchical key structure exists.
10.	There is a key or certificate revocation protocol that takes into account not only the time of use, but also the amount of information exchanged, the context of breaches or attacks, the sensitivity of the information, etc.
11.	Revoked keys or certificates to be stored shall be stored on media isolated from the operational media.

Reuse of keys:

A key is exposed when it is used and becomes more compromised each time it is reused. Therefore, one approach for systems that require greater strength is the use of OTP (One Time Password) systems, which limit the key lifetime to encrypt a single message.

Office environment:

Passwords should not be exchanged in clear text using electronic messaging services. In any case, keys should never be sent in the same communications as encrypted items, but should be sent independently through other secure channels.

Wi-Fi networks:

In WEP encryption (Wi-Fi networks) the reuse of keys and initialisation vectors enables simple brute force attacks to obtain the key [37].

3.3.3 Key storage

Symmetric keys, or public/private key pairs, must be recorded with guarantees of both confidentiality and recovery. Key storage is not only a problem for the individual who encrypts his own data, but also for the organisation insofar as it has to be able to retrieve data encrypted by its employees by having a key storage.

The management of key storage would be a particular case of the previous section, but is developed separately for the sake of clarity.

Control	
1.	The keys are not recorded in clear on any type of media.

[34] Authentication, transmission, storage, key distribution, etc.

[35] Hamming distance

[36] In the case of text keys, two consecutive keys must have at least 50% different characters from the previous key.

[37] https://wiki.elhacker.net/seguridad-wireless/introduccion/vulnerabilidades-del-cifrado-wep

2.	Keys are not stored in a non-volatile or external form when the key is not encrypted (key wrapped[38]).
3.	There is specific key management used to protect keys.
4.	There is a protection or cryptographic devices (HSM, hardware security module) to preserve the confidentiality of the keys.
5.	The protection mechanisms themselves are subject to periodic review.
6.	Storage, backup and key recovery procedures are in place.
7.	Access to passwords is subject to access control and logging
8.	Automatic procedures are in place to detect and alert to improper access to key stores.
9.	Secure key deletion and erasure procedures are in place.

Office environment:

It is typical to use clear text notes in both paper and electronic format in a place without access controls, for example, on a post-it note, on a note stored in a shared Dropbox folder, in email, etc. In many cases it is not user error, but a lack of protocols, policies and tools for key storage and management in the organisation.

Cryptocurrencies:

A citizen lost the keys that allowed him to access his bitcoins when he discarded the disk on which they were stored in the trash. The value of the bitcoins, thus inaccessible, reached 280 million euros[39].

Validation of HSMs:

Using an HSM device is not an absolute guarantee. Such devices are also subject to flaws, vulnerabilities, and attacks, and therefore measures must also be implemented to validate and prove their strength against various attack vectors, including those resulting from implementation errors, such as those that have allowed their software to be reinstalled[40].

3.3.4 Management of the encryption and certificate relationship

When encryption involves the relationship of more than one party, the establishment of an encryption relationship between two (or more) parties is necessary. Establishing the encryption relationship involves more than exchanging keys, it also involves agreeing on the encryption algorithms, as well as other aspects of the cipher suite and the protocol for using the system:

Control	
1.	If two parties agree to exchange information to establish a key relationship, both parties must be certain of the identity and origin of the other party's messages.
2.	In the case of authentication in a Public Key Infrastructure (PKI), the PKI must be trusted.
3.	In the case of symmetric keys, if two parties agree to exchange information to establish a key relationship, the keys they establish between them must be different from the keys that one of the parties establishes with another third party.
4.	If there are common keys for groups of people there must be different keys for different groups

[38] Key Encryption Key (KEK) or Key Wrapping Key are keys that are used to protect the confidentiality of keys. They are also used in key exchange processes as transport keys.

[39] https://www.cnbc.com/2021/01/15/uk-man-makes-last-ditch-effort-to-recover-lost-bitcoin-hard-drive.html

[40] https://www.blackhat.com/us-19/briefings/schedule/?hootPostID=db681a52c6a321681e1f9281b5124457#everybody-be-cool-this-is-a-robbery-16233

not allowed to communicate with each other.

5. The received certificates and the chain of trust are properly validated

6. While two parties are exchanging information to establish a key relation, no other third-party entity should be able to infer the identity of both parties.

7. The establishment of the key relationship (algorithms, suite elements, etc.) is to be done in a confidential manner.

Office environment:

NTLM Relay attacks on Windows domain controllers are possible if certificate-related signature protections are not enabled [41].

Certificate expiry:

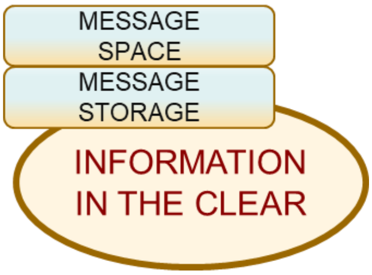
A communications systems provider interrupted service to 32 million users of different communications companies due to mismanagement of digital certificate expiration[42].

Certificate compromise:

The possibility of certificate compromise (by theft, social engineering[43], corruption[44], information leaks[45]…) is a fact that goes beyond just gaining access to systems, and has been used to sign malicious applications[46], to sign malware[47] that can lead to loss of confidentiality or availability of personal data (ransomware)

3.4 MESSAGES IN THE CLEAR

A message in clear is a message that I want to encrypt in order to keep it confidential in storage or transmission.



3.4.1 Message space

The message space is the set of possible messages being encrypted. The more predictable the messages are, the lower the strength of the message. This predictability has more impact the more it affects the initial part of the message to be transmitted. For example,

[41] https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429

[42] https://www.venafi.com/blog/cellular-outage-32-million-brits-caused-expired-certificate

[43] https://www.incibe.es/protege-tu-empresa/avisos-seguridad/multiples-campanas-phishing-intentan-obtener-las-credenciales-tu

[44] https://www.xataka.com/seguridad/buscamos-empleados-microsoft-apple-asi-como-lapsus-esta-hackeando-a-big-tech-dentro

[45] https://9to5google.com/2022/12/01/android-security-leak-samsung-lg/

[46] https://www.linkedin.com/pulse/stolen-security-certificate-compromises-privacy-palanisamy

[47] https://www.malwarebytes.com/blog/news/2022/03/stolen-nvidia-certificates-used-to-sign-malware-heres-what-to-do

standard formats for storing text, video, images or emails usually have headers that are always the same (or with small variations depending on the user) that make cryptanalysis easier.

In addition, certain tools pre-process messages before they are encrypted, which can increase, but also in some cases decrease, the strength of the encyption.

Control
1. Static headers do not exist or are avoided in the messages or set of messages to be encrypted.
2. Messages should avoid predictable and identifiable message structure, such as patterns, abbreviations, public or obvious information.
3. If the message in clear consists of a set of files, the files are preprocessed in order to hide the structure.
4. Compression of the message in the clear is performed before encryption.
5. The adjustment of the message to the block size of the encryption algorithm is done using appropriate padding and without known vulnerabilities.
6. The message space guarantees by design a high entropy (e.g., with the inclusion of random segments especially at the beginning and at the end of the message to be encrypted).

Office environment:

When encrypting two different documents, but generated by the same word processor, the same author and the same key, the first blocks of the encrypted documents are exactly the same. This is because document generation tools, such as word processors, spreadsheets, etc., usually have a set of static headers Such documents are vulnerable to attacks based on known clear text because, even if the key is changed, it is already known what the first blocks contain. Add to this the fact that certain documents have a standard structure where the data that differs between two documents is minimal, and the vulnerability increases. There are examples of decryption tools employing this principle[48].

Protection of fields in a dataset:

In data sets organised in fields, such as telephone number, ID number or other identifiers, it is possible that the fields are encrypted individually. In such cases, it should be noted that these fields may have very little variability. For example, the number of possible combinations of a valid phone number is very low from an automatic analysis point of view (low entropy).

Limits to encryption security:

The uniqueness distance, also called uniqueness point, is the minimum number of ciphertext characters needed to reduce the number of possible keys to one. From that amount the cipher is theoretically breakable given sufficient resources. It does not depend on the algorithm, but on the entropy of the message space and the actual key length. For example, a Spanish text encrypted with AES 256 exceeds the uniqueness distance with more than 95 characters[49].

[48] https://www.acceis.fr/cracking-encrypted-archives-pkzip-zip-zipcrypto-winzip-zip-aes-7-zip-rar/

[49] https://es.wikipedia.org/wiki/Distancia_de_unicidad#C%C3%A1lculo_en_otros_cifradores

3.4.2 Storing messages in the clear

In messaging services, documentation sent in encrypted form, protected backups or data sets sent to third parties in encrypted form, in many cases the original information could be stored in the form of a message in the clear.

The easiest way to compromise an encrypted message is to directly access the message in the clear that originated it (or when the decrypt is stored by the recipient). Also, knowing clear messages about other information that is not the attacker's object of interest can be a source of information about key management processes and encryption in general.

Control
1. The confidentiality of the storage of permanent messages and temporary copies is protected.
2. There is a procedure for controlling access to the storage of messages in the clear.
3. There is a log of access to message in the clear message's storage.
4. Automatic procedures are in place to detect and alert to improper access to the message store.
5. For certain types of messages, there are expiry procedures for messages in the clear that were transmitted or received encrypted.
6. Temporary copies are not accessible by third parties or third-party applications and are subject to secure deletion.
7. Access to message in the clear storage, when enabled, is limited in the set of applications that can exploit it.
8. Secure deletion procedures are in place for messages in the clear and temporary copies.
9. There is no link between messages in the clear and the keys used to encrypt them.
10. There is no link between messages in clear and their encryption.

Instant messaging:

Some instant messaging applications store messages and/or multimedia content in clear on the devices themselves, so that the attack on the confidentiality of messages is carried out on such storage rather than on the messages transmitted[50].

Encrypted disks:

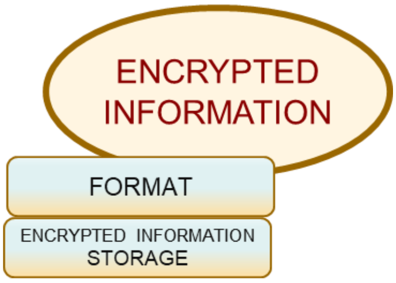
Encrypting the storage of a system or removable data carrier is a basic security measure against theft or loss. However, be aware that it only provides a certain degree of security. Once access to the device is opened, e.g., by logging into the system, the data is available to a multitude of applications, so the data cannot be considered as encrypted during normal system operation[51].

3.5 ENCRYPTED INFORMATION

Encrypted messages may be stored for a long time, in particular when encryption of information at rest is the goal, or they may be stored for very short intervals, while in the transmission queue.

[50] https://www.makeuseof.com/tag/how-whatsapp-messages-can-hacked/

[51] https://www.makeuseof.com/tag/how-whatsapp-messages-can-hacked/ in its section 4.



3.5.1 Format

Encrypted messages usually have a format that depends on the encryption software. The format may include unencrypted information, which facilitates the day-to-day operation of such files, but also incorporates weaknesses in the encryption system.

Control
1. The format of the cryptogram does not include unencrypted information, nor information related to the process or nature of the encrypted information
2. The key is not included in the header of the text before it is encrypted.
3. When the encrypted message consists of several independent files, a description of their contents is not stored in clear.
4. In case steganographic or deniable encryption techniques are used, their effectiveness has been analysed.

Web services:

Some encryption tools reveal information in their format, such as JWE, JSON Web Encryption, generally used as access tokens (version ofJWT, JSON web Tokens with encrypted content).

Office environment:

In some tools that generate encrypted zip files, the default configuration reveals information in the clear about the type of algorithm used, tool version or even the files stored and allows the use of strategies based on a weakness in the Message Space seen above.

Instant messaging:

In mobile messaging services, the first characters of messages are also stored in Notifications, when the application is not open on the mobile phone, so that messages can be retrieved without any protection, even if they were thought to be deleted[52].

3.5.2 Encryption storage

Control
1. Physical and logical access controls to encrypted information repositories are in place.
2. Authentication mechanisms are in place to prevent impersonation of the user who has entered

[52] https://www.xataka.com/basics/recuperar-mensajes-borrados-whatsapp

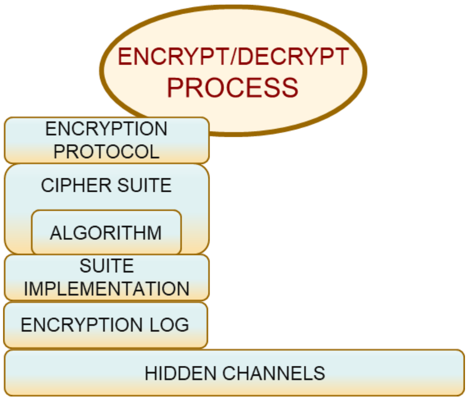
	the access keys to the encryption store.
3.	There is no other side storage in which it is possible to find encrypted messages but in clear, whole or just a fragment.
4.	There is a backup of the encryption storage.

Unauthorised access:

The Truecrypt disk encryption suite was discontinued after it was discovered that it was possible, once a user entered the key to access the encrypted content, for unauthorised third-party access to be made to the contents[53].

3.6 Cypher suite

The cipher suite consists of all the software/hardware/procedural components around the theoretical encryption algorithm that will determine its operation. The algorithm, e.g., AES, will be implemented using a number of libraries and plug-ins necessary for the actual execution of the algorithm. A proposed classification of these plug-ins is as follows:



3.6.1 Suite and algorithm

Algorithms are executed on actual implementations. In addition, it is necessary to use multiple elements that allow the implementation of the cipher system on a specific system: random number generators, prime numbers, block stuffing, key extension, etc. All of them can be a source of vulnerabilities.

Control	
1.	The elements of the suite are identified in name and version and inventoried. In particular, encryption algorithms, MACs, key exchange, padding, random number generators, key generators, certificates, automatic protocols, key management tools, etc.
2.	The security of the suite is provable.
3.	Criteria are identified to determine the elements of the suite appropriate to the context of the application and the life of the personal data.
4.	The elements of the suite are properly certified and comply with sectoral regulations.
5.	Certifications are up to date.

[53] https://thehackernews.com/2015/09/truecrypt-encryption-software.html

6. No compromised, non-certified or “ad-hoc” developed algorithms are used in the suite.
7. The generation of random numbers must be adequate, with a strong algorithm (software or hardware), certified or in accordance with regulations, and verified the next bit test and state commitment.
8. Random number generation seeds must be user-configurable or, there is a seed creation functionality with sufficient entropy and unpredictability.
9. Prime number generation must be unpredictable.
10. The configuration of the suite used to encrypt each message in clear is controlled
11. There is a backup of the elements of the suite.
12. Information about the suite is confidential.

Access to the cloud:

Access to remote or cloud services is provided by tools that allow configuration of the cipher suite that is employed. The default settings should be adjusted so that only those elements of the suite that meet the security requirements are used.[54].

3.6.2 Encryption protocol

The encryption protocol consists of automated processes (which will be part of the wider suite) and non-automated processes used to perform the operations of encrypting and decrypting information.

Control
1. The protocol must be well documented, third party audited or certified.
2. The protocol does not use insecure block processing (e.g., ECB)
3. The protocol includes authenticated encryption mechanisms. (e.g., GCM)
4. The protocol ensures that not only a fragment of the message is encrypted.
5. The protocol ensures that the same message is not sent encrypted and unencrypted.
6. The protocol ensures that the same message is not encrypted using different keys or algorithms.
7. The protocol ensures that the same key is not used for different recipients.
8. The protocol guarantees a maximum of information encrypted with the same key.
9. The protocol ensures that different blocks of the encrypted text cannot be replaced, deleted or jumbled without being detected.

Massive data sets:

One of the limits for a secure cipher is not to exceed the amount of information encrypted with the same key to a power of 2 of half the encrypted block size. This limit, which is known as the "birthday limit", can be easily reached with small block size ciphers, such as those based on DES. In such cases, the key should change[55] before reach such limit.

[54] https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/restrict-cryptographic-algorithms-protocols-schannel

[55] https://sweet32.info/

Loss of integrity in communications:

The use of ECB or unauthenticated encryption modes such as GCM allows attacks on the integrity of transmitted message sets, allowing the interleaving of false information that can alter the meaning of the information and have cascading effects on the processing of personal data[56].

3.6.3 Implementation

Implementation is the translation of theoretically designed systems, algorithms and tools into the real world. This involves actual coding, the definition of algorithm parameters and the use on an actual hardware. There can be a large gap between theoretical protection and actual protection due to limitations introduced in the implementation of the algorithms and problems in integration with the rest of the system.

Control
1. Vulnerability testing of the Hw/Sw elements of the encryption system has been carried out.
2. It has been verified that there is no persistence in memory of keys or clear texts used in the encryption process.
3. It is analysed that there are no keys included in the code (hardcoded).
4. There is a checking procedure to avoid leaking of system behavioural information.
5. There are measures to prevent detection and manipulation of the implementation: non-deterministic duration operations, shielding of circuits, homogenisation of consumption, modifying implementation of registered algorithms, adding noise and useless operations.
6. Implementations use appropriate, certified (FIPS 140-2, 197), or authorised libraries (CCN-STIC-807).
7. The generation of initialisation vectors, "salt" and "nonces" ensures that they are safe (minimum sizes and non-repetitive) and are not reused.
8. Block padding methods are up to date and appropriate for the type of processing. For example, do not use PKCS v1 or v1.5.
9. The hash functions used are suitable for cryptographic use, are modern and not obsolete. For example, do not use MD5 or SHA1.
10. The implementation of the certificate validation is secure.

Corporate applications:

A widely used corporate application maintained an encryption key written in the code itself to protect stored (at rest) data. An inspection of the code allowed access to confidential information stored[57].

Office environment:

The driver of an operating system used by Truecrypt 7 derivative projects was vulnerable to a local elevation of privilege attack by abusing the drive letter symbolic link creation functions to remap the system's primary drive[58].

[56] https://sysfatal.github.io/maleable.html

[57] https://www.cvedetails.com/cve/CVE-2016-3684/

[58] https://www.exploit-db.com/exploits/38403

Lack of implementation review:

In the case of an online video game platform that, while employing asymmetric keys generated with elliptic curves, vulnerability was determined because the key generation seed was constant in all implementations of the platform, introducing determinism in the key space[59].

Communications:

One systems company provided an SSH-encrypted RTU (Remote Terminal Unit) in which the private access key was written in the code itself and was not updated if the default configuration was used[60].

Instant messaging:

In 2019 it was discovered that sending malicious MP4s could cause an instant messaging service to overflow its buffer and thus allow access to messages [61].

3.6.4 Encryption log

The operation of the encryption system generates log files that will be essential in validating and auditing the system but can also become a source of vulnerabilities.

Control
1. There is a log of encryption activities.
2. Do not store keys, text in clear, encrypted text or any other information that can be used for cryptanalysis.
3. Recorded data should be kept to a minimum, with strict criteria for destruction, storage and copying.
4. Encryption logs must be protected in terms of confidentiality and integrity.
5. Very restrictive and traceable access control with real-time alerts is guaranteed.

Communications:

One SSH implementation stored the private key in the log file, accessible to all users who could gain access to it [62].

3.6.5 Hidden channels

A hidden or covert channel is any communication channel that can be exploited by a process to transfer information in a way that violates the security policy of the system. This may be due to bad designs of the system on which the encryption is executed or due to the existence of backdoors.

Control
1. There is a hidden channel checking of the suite.

[59] https://www.edn.com/the-sony-playstation-3-hack-deciphered-what-consumer-electronics-designers-can-learn-from-the-failure-to-protect-a-billion-dollar-product-ecosystem/

[60] https://www.cisa.gov/uscert/ics/advisories/icsa-22-179-06

[61] https://thenextweb.com/news/whatsapp-fixes-bug-that-would-have-let-hackers-exploit-devices-using-mp4-files

[62] https://www.cve.org/CVERecord?id=CVE-2018-1999036

2. There is a checking of hidden channels in automated and non-automated protocols.
3. There is a checking of hidden channels in the communication channels, such as error messages.
4. There is a checking of hidden channels in the implementation in software (libraries) and hardware.
5. There is a checking of hidden channels in the operating system running the encryption system.
6. In processing implemented on complex information systems, including for storage at rest, the security of information flows between load balancers, web servers, back-end systems, and other internal and external systems must be determined[63].
7. If the organisation uses hidden channels in the encryption system for monitoring and inspection of content, the monitoring must be real-time, logged data must be minimised, with strict criteria for early destruction, logs must be protected in terms of confidentiality, and very restrictive and traceable access control with real-time alerts must be ensured.

Instant messaging:

One social network provided an end-to-end encrypted messaging system. However, the emoticons were not embedded in the message, but only a link to the image of the message. When a message was downloaded, the first thing to be done was to request the emoticon pictures contained in the message from the server, which revealed a lot of information about the conversation.

Hidden channels:

An oracle attack is a type of side-channel attack that takes advantage of the fact that the protocol or system makes it possible to deduce whether the adversary is close to achieving a goal. For example, the Vaudenay attack[64] consists of knowing whether an encrypted message sent by the attacker is well padded or not. This can be known if the server returns an error that allows differentiating if there is a padding error or if the error is of another type (e.g., MAC). It could also be known by measuring the time it takes for the server to respond to a request, etc.

Communications:

Although the TLS specifications require servers to check for padding, some implementations do not validate it correctly. POODLE[65] “Padding Oracle On Downgraded Legacy Encryption”) is a security vulnerability that exploits the downgrade to SSL 3.0, making some servers vulnerable to POODLE even if they disable SSL 3.0.

3.7 COMMUNICATIONS

The encryption system may be oriented towards the protection of data at rest, but one of the frequent purposes of an encryption system is the protection of data exchanged over communication networks. The very fact of communication may involve specific vulnerabilities that do not appear in the protection of information at rest.

[63] It is also related to the existence of logs of encrypted material and messages in the clear.

[64] https://sysfatal.github.io/oracle.html

[65] https://es.wikipedia.org/wiki/Ataque_POODLE

COMMUNICATIONS
COMMUNICATION PROTOCOL
METADATA
COMMUNICATION LOG
CHANNELS

3.7.1 Communication protocol

The communication protocol is the system of rules that allow two or more entities of a communication system to exchange messages with each other. In this case it will also include the establishment of the encryption relationship, as well as the encrypted messages themselves.

Control
1. Authentication is ensured at the establishment of each session and at each exchange within a session.
2. Procedures are in place to prevent and detect impersonation of interlocutors. (MITM)
3. Procedures are in place to prevent and detect delays, reordering or deletion of encrypted fragments, selective modification of encrypted information, fabrication of dummy messages from fragments of authentic messages, message invention, message repetition, reflection (return of message to sender), alteration of message recipient, etc.

SSL/TLS:

Numerous security problems with SSL/TLS protocols have been documented. The footnote describes the most significant (recent) attacks focused on bypassing cryptography [66].

3.7.2 Metadata

Metadata in electronic communications is the data processed in a communications network for the purpose of transmitting, distributing or exchanging a message, in this case encrypted. This includes data used to determine and identify the source and destination of a communication, data about the location of the device, and the date, time, duration and type of communication[67].

Control
1. Metadata in communications is minimised and known.
2. The impact of metadata on cryptanalysis has been assessed.

[66] Seguridad del protocolo SSL/TLS. Ataques criptoanalíticos modernos. Author: Dr. Alfonso Muñoz https://raw.githubusercontent.com/mindcrypt/libros/master/Book. Seguridad en el protocolo SSL-TLS. Dr. Alfonso Muñoz - 05082021.pdf

[67] Definition from the ePrivacy Proposal for a Regulation

Wi-Fi networks:

In some implementations of Wi-Fi router manufacturers, which use WPA/WPA2 encryption/WPA2, it is possible to exploit the data in the optional fields of the issued control frames for PMKID attacks[68].

3.7.3 Communication log

Communications also generate log files that will be essential in monitoring and auditing the system, which may in turn become a source of vulnerabilities.

Control	
1.	Log files must not store keys or ciphertext.
2.	Where communication is not direct, the log information generated in the proxy systems must be known and controlled.
3.	Recorded data should be kept to a minimum, with strict criteria for destruction, storage and copying.
4.	Logs must be protected in terms of confidentiality.
5.	Very restrictive and traceable access control is guaranteed (alarms for suspicious access)
6.	The log management tool is audited and/or certified.
7.	Procedures are in place to prevent log poisoning attacks.

Communications logs:

Inadequate log management can be exploited to exploit vulnerabilities such as log poisoning, which is present in some applications [69].

3.7.4 Channels

The channel is the physical medium (and its virtual extensions) that allows the effective exchange of information between two speaker. The channel can take very complex forms on the Internet, with a multitude of intermediate providers and proxies which, in many cases, could be transparent to the user.

Control	
1.	Procedures are in place to prevent and detect the use of open channels.
2.	Procedures are in place to prevent and detect the use of private channels.
3.	Procedures are in place to prevent and detect eavesdropping and collection of encrypted information.
4.	Procedures are in place to prevent and detect traffic analysis and information linkage.
5.	Procedures are in place to prevent and detect attacks on DNS services.
6.	Procedures are in place to prevent and detect denial-of-service attacks.
7.	Procedures are in place to prevent and detect channel outages (physical and logical).
8.	Physical and/or virtual network segmentation mechanisms are implemented (VLAN).

[68] https://kalitut.com/pmkid-attack/

[69] https://www.cvedetails.com/cve/CVE-2019-11642/ https://www.cvedetails.com/cve/CVE-2021-40323/ https://nvd.nist.gov/vuln/detail/CVE-2021-40323

Eavesdropping on network infrastructure:

Tapping/sniffing devices on ethernet or fibre cables. Wi-Fi-jamming devices (causing denial of service) or sniffing.

WiFi de-authentication attacks in conjunction with fake access points (Wi-Fi de-auth and evil-twin).[70])

3.8 RECIPIENT

The receiver is the one who will receive the encrypted messages, in some cases will have the decryption keys and encrypted messages storages and in clear, therefore, will have to comply with the same guarantees as the sender.

Control	
1.	The recipient is authenticated.
2.	Open sessions with the recipient expire. Session keys used are not predictable.
3.	Re-authentication during an open session is performed randomly.
4.	The receiver's level of compliance of the encryption system is equivalent to that of the sender.
5.	The recipient has been assessed with audits and/or certifications.
6.	The recipient's personnel have been trained and have policies and practical manuals for the proper handling of encrypted material.
7.	The history of personal data breaches has been checked.

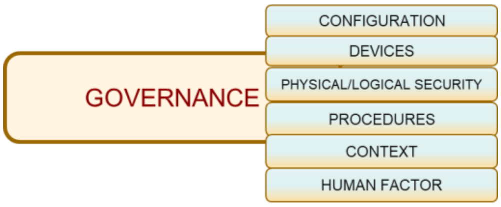
Vulnerability in the receiver that affects the sender:

Cookie and session token theft at the receiver [71]

3.9 GOVERNANCE AND DATA PROTECTION POLICIES

Beyond the theoretical strength of a cryptosystem, the real security of an encryption system has foundations in the correct application of governance and policy measures, which in this case are focused on data protection.

Information governance in the organisation must be a single one and must integrate data protection policies. A processing operation will only be compliant with the principle of accountability, if each of the steps and means it implements are also accountable. Thus, the information governance of the organisation must reflect the requirements for the encryption system to be accountable at least from a data protection point of view.



[70] https://www.nextgov.com/cybersecurity/2020/09/interior-ig-team-used-evil-twins-and-200-tech-hack-department-wi-fi-networks/168521/

[71] https://www.theverge.com/2023/3/24/23654996/linus-tech-tips-channel-hack-session-token-elon-musk-crypto-scam

3.9.1 Configuration control of the encryption system components

Component configuration is the set of parameters that can be adjusted to determine the functionality of the component.

Control	
1.	The elements of the cryptographic system have to be properly configured prior to the production start-up of the processing where the encryption system is used.
2.	The configuration of each element is documented.
3.	The encryption system cannot be run with default settings, or the default settings do not exist.
4.	Automatic updates of any item do not alter the configuration or reset it.
5.	There is an access control policy in place and access to the configuration of each element is logged.

Mobile devices:

There are attack patterns that consist of reinstalling encryption libraries with an all-zero key [72].

Corporate databases:

A complex database encryption architecture can be compromised by access to keys if key storage is not properly configured [73].

3.9.2 Devices

Since all the elements that make up the cipher suite will run on servers, routers, computers, whether on personal systems or in business or corporate environments, improper configuration can compromise the security of the entire cryptographic system.

Control	
1.	There is a security policy and control over BYOD devices that are used in the encryption system, or they are not allowed at all.
2.	There is a control or prohibition on installing applications on devices running encryption systems without the security officer's authorisation.
3.	Operating system versions specially configured for high security are used.
4.	Devices on which the encryption system is running are scanned for device-specific vulnerabilities.
5.	The use of devices that prevent the full encryption system from being kept up to date is not permitted.
6.	Encryption system devices shall only be used in protected environments.

[72] https://www.krackattacks.com/

[73] https://matthewmcgiffen.com/2018/01/03/how-secure-is-transparent-data-encryption-tde-and-how-to-prevent-hacking/

IoT devices, VoIP phones and others:

Many devices do not support 802.1X-type configurations as they have very limited functionality, plus they often have poor implementations of cryptography and password management. The use of alternative mechanisms such as MAC Authentication Bypass[74], which may not be sufficiently secure, can allow external devices to access networks where the cryptographic system is being used.

VoIP systems with vulnerabilities or misconfigured systems can compromise the corporate network[75].

Mobile Device Management (MDM) systems:

MDM must be properly configured to prevent unauthorised external devices from being attached[76]. They are susceptible to vulnerabilities and need to be kept up to date[77].

3.9.3 Physical/logical security

Systems, devices (especially portable devices), backup systems, screens, etc. can be accessed by third parties or stolen outright. The list of controls shown below refers to encryption equipment.

Control
1. There is a policy and definition of restricted areas.
2. Policies define the allowed storage devices.
3. There is authorised physical and logical access control to encryption devices and equipment, message and key files, temporary files, encryption procedures, etc.
4. There is a log of access to encryption devices and equipment, message and key files, temporary files, encryption procedures, etc..
5. There is a list of personnel involved in the execution of the cryptosystem and their roles.
6. There is a protocol for the confidential destruction of all material related to the encryption system.
7. Black-bag attack prevention measures are in place [78].
8. There is no direct display of the elements of the cipher system
9. All backups are controlled.
10. Doesn't exist third-party storage.
11. Hot (Heartbleed SSL) or cold start memory scans are performed.
12. The use of keyloggers and measures to prevent keylogging have been sought.
13. Measures are in place to prevent manipulations of intermediate operations.
14. Tempest attack prevention measures are in place.

[74] https://www.portnox.com/cybersecurity-101/mac-authentication-bypass/

[75] https://thehackernews.com/2023/03/critical-flaw-in-cisco-ip-phone-series.html

[76] https://book.hacktricks.xyz/macos-hardening/macos-security-and-privilege-escalation/macos-mdm/enrolling-devices-in-other-organisations

[77] https://www.securityweek.com/1000-organizations-exposed-remote-attacks-filewave-mdm-vulnerabilities/

[78] https://en.wikipedia.org/wiki/Black-bag_cryptanalysis

Theft or destruction of devices:

Physical access to devices containing encrypted information allows attacks on the availability of information to materialise, directly through the theft or destruction of the data carrier, as well as facilitating the possible breaking of the encryption system and affecting confidentiality.

Disk encryption mechanisms:

Disk encryption systems protect data when computers are switched off. In the event that the user has logged in and left the computer on, the operating system has already decrypted the sensitive data and it will be available to anyone who accesses it.

Physical access to the device:

Repeated physical access can exploit vulnerabilities in cryptographic systems. LUKS has a re-encryption functionality (reencprypt) with a CVE-2021-4122 flow, which reuses a mechanism for the re-encryption operation. An attacker with repeated physical access can simulate an unfinished re-encryption process and achieve decryption of the LUKS device[79]

3.9.4 Management and Policies

The GDPR requires in Art.5.2 a governance model in relation to personal data that is "accountable", i.e., capable of being explained and subject to transparency, justification and explanation of the actions taken. Furthermore, Art.24.2 establishes the opportunity to “Where proportionate in relation to processing activities, […] shall include the implementation of appropriate data protection policies by the controller”.

Control
1. The encryption system fulfil in its design, implementation and validation, the policies and procedures established by the controller.
2. The life cycle of the data in the processing is documented (data categories, data flow from inception to destruction).
3. An assessment of the necessary strength and quality of the encryption system is documented for each processing operation in terms of the risk to fundamental rights and freedoms.
4. There is a unit/person (u/p) in charge of the encryption system.
5. The u/p maintains an adequate and documented policy on the use of encryption in processing in relation to all items and control.
6. Processing is categorised by their necessary strength and different implementations and policies appropriate to how criticality is the encryption system are implemented.
7. The policy reflects the recommendations of the DPO or the data protection advisor.
8. This policy is subject to be recorded and approval cycle of the entity's management.
9. Such a policy states the flow/life cycle of all components of the suite's inventory (as indicated above).
10. Third parties/providers involved (e.g., certificate validators, SaaS, …) are identified.
11. Contracts with intervening third parties are included.
12. In contracts with third parties, to the extent that they perform encryption of personal data, instructions on data encryption are set out, all information necessary to demonstrate compliance with the controls of the cryptosystem selected by the data controller are made available to the

[79] https://linuxiac.com/cryptsetup-vulnerability/

data controller, as well as mechanisms for monitoring and auditing them.

13. Regular monitoring of encryption system providers is in place (e.g., with a vendor assessment).

14. This policy reflects the data protection requirements set by the DPO or the data protection advisor.

15. It includes role definition (administrator, user), access control, authentication, user procedures, destruction of cryptographic material, integrity management, incidents and alerts and contingency plans.

16. The policy sets out the timeframes and events that trigger a validation, maintenance, remove from inventory and/or audit process

17. The policy provides for re-encryption strategies for information at rest appropriate to the technical context and data breaches.

18. The policy includes a procedure for auditing and testing of updated encryption system elements.

19. Updates of procedures, hardware or software are not automatically incorporated into production systems.

20. There is an implemented backup management policy for the suite, configuration and keys.

21. A key escrow policy is in place.

22. This policy is integrated in the security policy.

23. Policy does not rely exclusively on automation.

24. Access to the policy or parts of the policy is restricted on a need-to-know basis.

25. The policy establishes a process for identifying and continually assessing changes in the sensitivity of encrypted information, whether due to changes in data categories, subject categories, volume of affected individuals or other changes.

26. There are communication channels for incidents about the overall encryption process that reach that unit/person.

27. There are channels for internal communication and for communications with external sources.

28. The data protection officer is included in all cryptosystem definition and validation procedures.

29. The administrator cannot bypass encryption procedures.

30. Procedures are in place to prevent the transmission of unencrypted confidential information.

31. The process of receiving and attending to applications by authorities for material of figure is in place.

32. If the organisation implements hidden channels in the encryption system for monitoring and inspection of content, the management is subject to strict criteria for continuous auditing with DPO involvement.

33. Exists a contingency plan in place in case it is detected that the cryptosystem may be compromised.

34. There is a procedure for complying with GDPR obligations in the event that a compromise of the encryption system affecting personal data is detected.

Missing employee:

An employee of the organisation who is the only one who knows a key disappears. The employee has not followed the key escrow policy, or the key does not exist or is not really working in the organisation. In this case, the organisation cannot access all the information that has been previously encrypted by this employee.

Codification:

When updating an encryption library by rewriting C++ to Java, an oversight was made in the ECDS verification by not taking into account null R and S values, which is a vulnerability that allows intercepting communications, forging SSL certificates, etc.[80]

Encryption of documents at rest:

The compromise of the master key in one organisation allowed access by third parties to an undetermined number of customer passports stored by a multinational hotel company, due to a poor policy of configuration, control, evaluation and key management[81].

3.9.5 Context and personal data breaches

The context is the set of circumstances surrounding the organisation, the processing and the state of the art. The context is always dynamically changing. Regarding context changes, a critical indicator is personal data breaches that occur in relation to the encryption system in similar organisations, processing, or types of systems. Such incidents need to be detected, analysed in the context of the processing and appropriate actions must be taken to ensure that they do not affect the organisation itself.

Control
1. There is an ongoing collection and analysis of encryption-related gaps and incidents in organisations, processing or similar systems.
2. There is a continuous collection and analysis of new known vulnerabilities that may affect the entire encryption system.
3. Changes in the legal framework affecting the entity or the processing are identified and assessed on an ongoing basis, and legal risks of future regulation are identified.
4. Technological developments relating to cryptanalysis, both current and estimated changes in the medium term, are identified and assessed on an ongoing basis.

Change of the legal framework:

In relation to the legal framework, consideration should be given to possible regulatory initiatives at European level that are being considered to allow public authorities access to encrypted communications[82].

[80] https://neilmadden.blog/2022/04/19/psychic-signatures-in-java/

[81] https://www.techtarget.com/searchsecurity/news/252455488/Marriott-data-breach-exposed-5-million-unencrypted-passport-numbers

[82] https://appleinsider.com/articles/22/05/11/eu-plans-to-require-backdoor-to-encrypted-messages-for-child-protection

Back doors in certified components:

In some cases, standardisation bodies themselves promote components that include backdoors known to a small circle[83]. One of the best-known cases involved a suite component (random number generator[84]) certified by NIST.

3.9.6 Human factor

The human element is the most important factor in any security system and is sometimes given less attention. In particular, breaches caused by an action or omission of human actors can have the greatest impact on a processing.

Control	
1.	There are written procedures available for personnel handling encryption material.
2.	Staff are required to sign confidentiality undertakings informing them of their duties and responsibilities.
3.	Staff are trained to carry out the procedures for which they are responsible.
4.	There are plans for continuous training on the procedures.
5.	There is training and specific procedures in place to detect the existence and cataloguing of social engineering attacks, as well as possible extortion or coercion.
6.	There is supervision of the manual execution of procedures.
7.	There is an internal sanction procedure for non-compliance with encryption procedures.
8.	In internal/external staff selection processes for positions in charge of the most critical operations, a vetting process and background checks must be completed.
9.	Personnel in charge of the most critical operations regularly undergo a technical and reliability reassessment process.

Access to credentials:

Recently an advertisement was posted on a Telegram channel offering payment via the Darkweb, not for data, but for credentials to access computer systems. This type of attack is becoming more and more frequent as it allows access to the heart of the entity.

[83] https://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220
[84] https://en.wikipedia.org/wiki/Dual_EC_DRBG#Software_and_hardware_which_contained_the_possible_backdoor

4 CONCLUSION

As stated in Article 32(1)(b), the encryption system, like all security safeguards, must be regularly verified, evaluated and assessed with regard to its effectiveness in protecting the rights and freedoms of individuals, among others. This is an obligation of controllers and processors/subprocessors, and the DPO or, in case, data protection advisors should be involved in advising and supervising the regular process of verification, evaluation and assessment of the encryption system.

An encryption system is a complex operation that is included in many processing activities. It shouldn't be implemented in a naïve or superficial way. When encryption is compromised in a processing of personal data, risks to rights and freedoms materialise. The identification of such risks requires, in addition to determining what data have been compromised, an assessment of the impact that the compromise of such data may have on the individuals concerned and on society. The strength and robustness of the encryption system must be proportionate to this impact.

Given that no security system is a guarantee of infallibility, the controller should not limit the measures to manage risks to rights and freedoms to security measures, in particular, resting all risk management solely on the encryption of information. The controller must incorporate, from the very concept of processing, privacy measures to minimise the impacts derived from a possible materialisation of a personal data breach, such as policies for data protection, privacy by default and design (minimisation, early anonymisation, pseudonymisation, data erasure, aggregation, low granularity, transparency, etc.), governance and personal data breach management mechanisms through the development and implementation of contingency plans, among others.

5 REFERENCES

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
- Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights
- Recommendations 01/2020 on measures that suplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0
- AEPD: Encryption and Privacy: Encryption in the GDPR
- AEPD: Encryption and Privacy II: Lifespan of personal data [Jan 2020]
- AEPD: Encryption and Privacy V: The key as personal data [Dec 2021]
- ISO 27002/2022
- CCN Criptología de empleo en el Esquema Nacional de Seguridad
- CCN Taxonomía de productos STICAnexoE.1: Dispositivos de almacenamiento cifrado
- CCN Taxonomía de referencia para productos de seguridad TIC - Anexo E.2: Dispositivos/Herramientas de cifrado offline
- ENISA: Study on cryptographic protocols
- ENISA: Algorithms, key size and parameters report 2014
- ENISA: Data protection Engineering 2022
- NIST: Cryptographic Standards and Guidelines

6 ANNEXES

6.1 ANNEX: SYMMETRIC, ASYMMETRIC AND MIXED KEY SYSTEMS

6.1.1 Symmetrical encryption

Symmetric encryption schemes assume that the users involved in the communication share a secret key (theoretically completely unpredictable to an adversary). Essentially two types of schemes are used:

6.1.1.1 Block Encryption. Modes of operation

A block cipher processes blocks of information of fixed size (typically 128 or 256 bits) that are encrypted or decrypted with keys of similar size. Currently, the most recommended block cipher is AES, standardised by NIST in 2001. The recommended minimum block (and key) size is 128 bits.

As relevant as choosing a suitable block cipher is to implement a mode of operation that dictates how to handle data sets of more than one block. The most recommended are the CCM and GCM modes (see https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38c.pdf and https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38d.pdf).

6.1.1.2 Streaming encryption

A streaming cipher is usually suitable for dynamic encryption of data (e.g., transmitted via streaming). When the AES block cipher is used in CTR mode the result is such a cipher.

6.1.2 Asymmetric encryption

Asymmetric encryption schemes are characterised by the fact that there is a division of the key material, so that only the receiver has a secret key, making his/her so-called public key publicly available so that it is accessible to any sender. The most commonly used symmetric schemes to date are RSA (in particular the so-called RSA-OAEP variant) encryption and those based on the discrete logarithm problem, often in groups associated with elliptic curves (ElGamal). For long-term security it is necessary to look for alternatives, as these schemes are vulnerable to quantum attacks (see 2.1.6.).

6.1.3 Hash functions

Hash functions or digest functions are fundamental parts of many cryptographic schemes, as well as being used in isolation to provide integrity proofs. Thus, it is common for the transmission of a document X (encrypted or not) to be completed by sending a hash H(X), where H is a cryptographic function that allows, to a certain extent, to detect modifications (intentional or not) on the text X that may have occurred in transit. The currently most recommended hash functions belong to the so-called SHA family,; e.g., SHA-256, SHA-512/256, SHA3-256, SHA3-515. The numeric suffix indicates the number of output bits, i.e., the size of the document digest (which is fixed, it does not depend on the size of the input document).

6.1.4 Key establishment mechanisms

The establishment of cryptographic keys (for subsequent use in symmetric scenarios) can be done through both symmetric and asymmetric mechanisms. Usually, in fact, mixed cryptographic mechanisms are considered where after exchanging a cryptographic key using an asymmetric mechanism (such as Diffie-Hellman or EC Diffie-Hellman) this key is used to encrypt with a block cipher (such as AES).

If the key establishment is to be done by symmetric means this is also possible (see ISO/IEC 11770-2:2018).

6.1.5 Authentication

Authentication means verifying the identity of those who communicate with us, or the origin of a message or block of data is crucial to complement the guarantees provided by encryption. There are different mechanisms for this purpose.

6.1.5.1 Passwords

They are a relatively weak authentication mechanism, which has to be implemented exclusively under cover of mechanisms that limit the number of access requests (to avoid dictionary attacks). It is important not to store passwords in clear or hashed form, to avoid access data leakage.

6.1.5.2 Signatures

The use of digital signature schemes is always the best way to authenticate communication, but it is important to have a robust key and certificate management. The most recommended signature mechanisms are RSA-based signatures, discrete logarithm-based signatures (DSA and its variants on elliptic curves ECDSA, ECKDSA), as well as Merkle signatures (XMSS+ or LMS) – the latter being preferable in the long run. RSA and DSA signatures are vulnerable to quantum attacks, so post-quantum tools are recommended for long-term applications.

6.1.5.3 MACs

Message Authentication Codes (MACs) are used to generate labels for data authentication in the symmetric scenario (both the generation and verification of the label will require the same symmetric key). MACs are usually constructed from block ciphers or hash functions. Prominent examples areCMAC, HMAC or GMAC, always with the recommendation that the generated tags should be at least 96 bits and the associated keys should be at least 128 bits.

6.1.6 Post-Quantum Scenario

Since 2017, the US National Institute of Standards and Technology (NIST) has established an international process for selecting cryptographic algorithms that can withstand quantum attacks. This process focuses on key encapsulation mechanisms (called KEM), and digital signature schemes. KEMs have the particularity to be adapted to accommodate asymmetric encryption schemes and key exchange schemes, so having secure KEMs provides a complete set of tools for basic cryptographic uses. In July 2022, the first schemes to be standardised have been identified; the KEM CRYSTALS-Kyber (lattice-based) and the CRYSTALS-Dilithium and FALCON signatures (also lattice-based), as well as the SPHINCS+ signature, which is constructed from hash functions.

Many international bodies are developing guidelines to facilitate the transition to the post-quantum world, i.e., the replacement of discrete logarithm and factorisation-based cryptography by tools based on other mathematical problems, such as decryption or lattice-related problems. See, for example, the recently published European ETSI guide https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf.

6.2 ANNEX: KEY LENGTH

When defining the strength of a key by its length in bits, it must be taken into account that in asymmetric encryption they are one size and in symmetric encryption they are very different sizes (they move in different ranges). AES is the NIST standard for symmetric encryption and uses 128-bit keys, and 128, 192 or 256-bit key lengths (this would, in fact, be the minimum recommended size to resist quantum attacks, in the medium to long term). Asymmetric algorithms use longer keys of 1024 bits, 2048 or 3072 bits.

In 2003 RSA stated that its 1024-bit key is equivalent to an 80-bit symmetric key. Its 2048-bit key is equivalent to a 112-bit symmetric key, and the 3072-bit key is equivalent to a 128-bit key. RSA recommends using at least 1024-bit keys if you want to keep your documents secure until 2010, and using a 2048-bit key if you want to keep documents secure until 2030. The 3072 key is indicated for documents that must remain secure after 2030. A NIST document defines that a 15360-bit asymmetric key is equivalent to a 256-bit symmetric key in post-quantum environments, although in the medium/long term it is advised to use other encryption methods that are more resistant to known quantum attacks.

Recommended key sizes for post-quantum tools can, for example, be found in the recent NIST report https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf . For example, the recommended key sizes for CRYSTALS-Kyber encryption range from 800 to 1568 bits for the public key, doubling the size of the public key.

6.3 ANNEX: ADVICE ON AN ENCRYPTION SYSTEM

Encryption is a very powerful tool to protect data. Encryption as a security measure to reduce or mitigate risk in the processing of personal data will only be effective if it is used properly and correctly. Otherwise, it becomes useless if the device, procedures, protocols or people involved in its operation are compromised.

Cryptography tends to fail in practical application rather than errors in the theoretical algorithm. Real-world encryption systems are implemented on multiple hardware and software products, combining primitives and tools, which can present risks. But even if good algorithms and protocols exist for most cases, errors in configuring and validating the use of the encryption system are the source of most vulnerabilities.

Some common mistakes to avoid include[85]:

- Failure to use cryptography and data protection specialists to define a cryptosystem to protect personal data.
- Relying on third party tools, services, support or your own staff without appropriate regular validations.
- Failure to train employees.
- Failure to validate the cryptosystem that relies on handlers, suppliers and third parties.
- Failure to match the strength of the cryptosystem to the real impact that a breach of the cryptosystem can have.
- Encrypting information that does not need to be encrypted.
- Creating your own algorithm or other elements of the cipher suite.
- Using default settings.
- Making an unvalidated deployment of updates.
- Incorrect protection and/or management of cryptographic keys.
- Reusing elements to implement part of the encryption system.
- Using channels that avoid using cryptography for "convenience”.
- Failure to use overlapping protection methods: encryption-encryption, steganography-encryption, encryption-dedicated lines, etc.

[85] https://crashtest-security.com/owasp-cryptographic-failures/

- Failure to use authenticated encryption systems in communications.
- Employing randomness that does not meet the requirements for a cryptographic system.
- Failure to comply with the "need to know" principle in relation to the cryptosystem.
- Failure to implement a key management life cycle.
- Distribute information or keys at some point in clear text.
- Putting functionality before security.

The final tip is to conduct regular audits of procedures and use of cryptographic material, including periodically preparing "traps" to determine whether you are being monitored, whether your own users are not following procedures and whether the system is sufficiently strong (ethical hacking).

7 TABLE OF ACRONYMS

AEPD. Agencia Española de Protección de Datos

AES. Advanced Encryption Standard

APEP. Asociación Profesional Española de Privacidad

BYOD. Bring Your Own Device

CCM. CBC Counter Mode

CMAC. Cipher-based Message Authentication Code

CTR. Counter

DES. Data Encryption Standard

DPO. Data Protection Officer

DSA. Digital Signature Algorithm

EC Diffie-Hellman. Elliptic-curve Diffie-Hellman

ECB. Electronic Code Book

ECDSA. Elliptic Curve Digital Signature Algorithm

ECKDSA. Korean version of ECDSA

ENS. Esquema Nacional de Seguridad

GCM. Galois/Counter Mode

GDPR. General Data Protection Regulation

GMAC. Galois Message Authentication Code

HMAC. Hash-based Message Authentication Code

HNLD. Harvest Now, Decrypt Later

HSM. Hardware Security Module

HW/SW. Hardware/Software

ICT. Information and Communication Technologies

IoT. Internet of Things

ISMS Forum. Asociación Española para el Fomento de la Seguridad de la Información

JWE. JSON Web Encryption

JWT. JSON Web Token

KEM. Key-encapsulation Mechanism

LMS. Leighton-Micali Signature

LUKS. Linux Unified Key Setup

MAC. Message Authentication Code

MD5. Message Digest Algorithm 5

MDM. Mobile Device Management

MITM. Man In The Middle

NIST. National Institute of Standards and Technology

OAEP. Optimal Assymetric Encryption Padding

OWASP. Open Worldwide Application Security Project

PBKDF2. Password-Based Key Derivation Function 2

PEC. Privacy Enhancing Crytography

PET. Privacy Enhancing Technologies

PIR. Private Information Retrieval

PKCS. Public-Key Cryptography Standards

PMKID. Pairwise Master Key Identifier

POODLE. Padding Oracle On Downgraded Legacy Encryption

PSI. Private Set Intersection

RSA. Rivest-Shamir-Adleman

RTU. Remote Terminal Unit

SaaS. Software as a Service

SHA. Secure Hash Algorithm

SNLD. Store Now, Decrypt Later

SSE. Searchable Symmetric Encryption

SSH. Secure Shell

SSL. Secure Sockets Layer

StE. Structured Encryption

TLS. Transport Layer Security

VoIP. Voice over Internet Protocol

WEP. Wired Equivalent Privacy

WPA. Wi-Fi Protected Access

XMSS. eXtended Merkle Signature Scheme

ZKPoK. Zero-Knowledge Proofs of Knowledge