centro criptológico nacional

ICT Security Guide
CCN-STIC 857

Security requirements for E-health Applications in the context of the ENS

September 2020

MINISTERIO DE DEFENSA

Edit:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.09.21 15:32:28 +02'00'

NIPO: 083-20-194-X

Date of Edition: September 2020

This document is based on material provided by the Bundesamt für Sicherheit der Informationstechnik (BSI). Don Carlos Galán has participated in the drafting of this document that has also had the collaboration in its revision of Sidertia Solutions S.L.

LIMITATION OF RESPONSIBILITY

This document is provided in accordance with the terms compiled in it, expressly rejecting any type of implicit guarantee that might be related to it. In no case can the National Cryptologic Centre be considered liable for direct, indirect, accidental or extraordinary damage derived from using information and software that are indicated even when warning is provided concerning this damage.

LEGAL NOTICE

Without written authorisation from the **National Cryptologic Centre**, it is strictly forbidden, incurring penalties set by law, to partially or totally reproduce this document by any means or procedure, including photocopying and computer processing, or distribute copies of it by means of rental or public lending.

FOREWORD

In an increasingly complex and globalised world, in which information and communication technologies (ICTs) play an extremely important role, we must be aware that the proper management of cybersecurity is a common challenge that we must necessarily address. It is necessary to ensure that our country's economic, technological, and political capacity is protected, especially since the proliferation of targeted attacks and the theft of sensible information is an overwhelming reality.

For this reason, it is essential to be up to date with the threats and vulnerabilities associated with the use of new technologies. Knowledge of the risks that surround cyberspace must be used to implement procedural, technical and organisational measures that allow a safe and reliable environment.

Law 11/2002, of 6 May, regulating the Spanish National Intelligence Centre (CNI), entrusts the Spanish National Intelligence Centre with functions related to information technology security and to the protection of classified information, also gives its Secretary of State-Director the responsibility of managing the National Cryptologic Centre (CCN).

Based on the CNI's knowledge and experience of threats and vulnerabilities in emerging risks, the Centre, through its National Cryptologic Centre, which is regulated by Royal Decree 421/2004, of 12 March, carries out various activities directly related to ICT security aimed at training expert staff on the uses of appropriate security technology and the implementation of security policies and procedures.

This series of CCN-STIC documents is a clear example of the work that is being done by the agency carries out in terms of security implementation, allowing the application of policies and procedures, since the guides have been prepared with a clear objective: to improve the degree of cybersecurity in organisations, aware of the importance of establishing a reference framework in this area that will support government personnel in performing the difficult task of ensuring the security of the ICT systems under their responsibility.

With this series of documents, the National Cryptologic Centre, in compliance with its tasks and with what is reflected in the Royal Decree 3/2010 which regulates the National Framework in the field of Electronic administration, contributes to improve the Spanish cybersecurity and to preserve the infrastructures and the information systems of all the public administrations with optimal security levels. All of this, in the aim of generating confidence and guarantees in the use of these technologies, protecting the confidentiality of the data and guaranteeing their authenticity, integrity and availability.

September 2020

Paz Esteban López
Secretary of State
Director of the National Cryptologic Centre

INDEX

1. INTRODUCTION.. 5
1.1 SUBJECT MATTER AND RECIPIENTS OF THE GUIDE 5
1.2 OBJECTIVE OF THE GUIDE 5
1.3 GENERAL DESCRIPTION OF THE GUIDE...7
1.3.1 METHODOLOGY 7
1.3.2 TERMINOLOGY...7
1.4 PROOF OF CONCEPT...8
2. OVERVIEW OF SECURITY REQUIREMENTS FOR MOBILE APPLICATIONS................. 8
2.1 APPLICATION CONCEPTS ON MOBILE DEVICES 8
2.1.1 NATIVE APPLICATIONS..9
2.1.2 WEB APPLICATIONS 9
2.1.3 HYBRID APPROACHES 10
2.2 *BACKEND* SERVICES 10
2.3 DEFINITION OF THE SECURITY PROBLEM 11
2.3.1 ASSUMPTIONS [A] 11
2.3.2 THREATS [T]..11
2.3.3 SECURITY POLICIES [P] 12
2.3.4 RESIDUAL RISKS..14
3. SECURITY MEASURES FOR E-HEALTH APPLICATIONS.. 15
3.1 SECURITY OBJECTIVES 15
3.1.1 OBJECTIVE (1): PURPOSE OF THE APPLICATION...15
3.1.2 OBJECTIVE (2): ARCHITECTURE 18
3.1.3 OBJECTIVE (3): SOURCE CODE...24
3.1.4 OBJECTIVE (4): THIRD PARTY SOFTWARE...25
3.1.5 OBJECTIVE (5): CRYPTOGRAPHIC IMPLEMENTATION 27
3.1.5.1 RANDOM NUMBERS 29
3.1.6 OBJECTIVE (6): AUTHENTICATION...30
3.1.6.1 AUTHENTICATION BY BIOMETRICS 33
3.1.6.2 *STATEFUL* AUTHENTICATION MEASURES (CONDITIONED) 35
3.1.6.3 *STATELESS* AUTHENTICATION MEASURES (UNCONDITIONAL) 37
3.1.7 OBJECTIVE (7): STORAGE AND DATA PROTECTION..39
3.1.8 OBJECTIVE (8): PAYMENT RESOURCES...44
3.1.9 OBJECTIVE (9): NETWORK COMMUNICATION 45
3.1.10OBJECTIVE (10): SPECIFIC PLATFORM INTERACTIONS 47
3.1.11OBJECTIVE (11): RESILIENCE 50

1. INTRODUCTION

1.1 SUBJECT MATTER AND RECIPIENTS OF THE GUIDE

Since the global irruption of mobile devices in the daily activity of citizens, the use of **mobile applications related to health**, from their different approaches (for professionals, users, providers, health centres, etc.), has spread in such a way that, regardless of their functionalities and benefits, it is necessary to consider, in a formal and rigorous way, their security.

As we have said, these applications are designed to collaborate in the **detection, diagnosis, monitoring and treatment** of a wide variety of pathologies which, by their very nature, have important security requirements in relation to the **availability** of the services involved or the **confidentiality, integrity, traceability** or **authenticity** of the information processed.

Aware of this problem and its relationship with the public sector and citizens, the ultimate beneficiaries of public health efforts, the National Cryptologic Centre (CCN) has published this *CCN-STIC Security Requirements for E-Health Applications Security Guide,* within the framework of the provisions of Royal Decree 3/2010, of 8 January, which regulates the **National Security Framework** (**ENS,** hereinafter), based on previous work by the *Bundesamt für Sicherheit in der Informationstechnik (*BSI)[1].

Important note:

This Guide is primarily aimed at manufacturers of health applications for mobile devices, including the processing and storage of sensitive data, and includes Good Practices on the subject.

1.2 OBJECTIVE OF THE GUIDE

The digitisation of all areas of life, whether at work, in the home environment, in leisure, etc. -continues to advance. By mid-2020, the number of internet users exceeded 4.8 billion people.[2] Two thirds of the world's current population (7.8 billion), use a smartphone, more than three billion people use social networks and 90% of them do so from their mobile device (*smartphone* or *tablet*). This development is also present in the health care sector, with a clear trend towards "self-tracking" and

[1] Oficina Federal de Seguridad de la Información alemana: *Security requirements for digital health applications Technical Directive* BSI TR-03161 (Trial Use, 2020)

[2] https://www.internetworldstats.com/stats.htm

demanding at the same time an efficient and respectful use of the health data processed, being essential to enable access to medical records, regardless of time and place.

As is well known, mobile applications related to health (which we will call **e-health applications**) process a significant amount of personal data, many of them so-called *special categories of data* or data considered sensitive,[3]from heart rate and sleep rhythm records to treatments or medication plans, as well as prescriptions and certificates, in addition to facilitating, in many cases, the user's connection with the corresponding health services, acting as communication nodes. In this way, a compromised smartphone can reveal a multitude of data from the user's "digital life", some of which may be particularly confidential.

Maintaining compliance with the existing security regulations - such as the ENS, where its subjective and material scope of application also includes the use of mobile devices - can make this risk of exposure considerably more difficult and, in many cases, prevent it. Already in the design and further development phases, manufacturers should plan carefully how a mobile application will process, store and protect the personal and other sensitive data of its users[4].

As is known, information security, from the point of view of the ENS, contemplates five dimensions of protection: *Confidentiality, Integrity, Availability, Traceability and Authenticity.* It goes without saying that compliance with these requirements is particularly important in mobile health applications. In contrast to the financial sector, where fraudulently transferred money can be refunded to customers by the banks, the confidentiality of health data that is unwillingly disclosed will be lost once and for all. Although the user could receive compensation or indemnification for this, the disclosure cannot be undone. Furthermore, the non-consensual disclosure of health data, both in the social and professional environment, can have extremely important consequences and repercussions. For example, the manipulation (attack on integrity) by an attacker of the health data of a third party could have a significant impact on treatment decisions and ultimately on the health and life of the individual.

This Guide aims to help developers of e-health applications to develop secure mobile applications.

[3] *Special categories of data,* in the terminology of Regulation (EU) 2016/679 (GPRS): "Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of genetic data, biometric data intended to uniquely identify a natural person, data concerning health or data concerning the sexual life or sexual orientation of a natural person. "(Art. 9).

[4] *Security and Privacy by design,* in terms of Regulation (EU) 2016/679 (RGPD). See the Privacy by *Design Guide,* AEPD (Oct. 2019)

1.3 GENERAL DESCRIPTION OF THE GUIDE

1.3.1 METHODOLOGY

The term *application*[5], as used in this document, refers to a mobile e-health application that can operate autonomously in a mobile application on the mobile device or in combination with a secure *backend.* The term *backend*, as used in this document, also includes cloud computing platforms.

Due to the constant progress, growth and diversity of mobile devices and their platforms, this Guide does not claim to be exhaustive. Instead, it seeks to highlight the **minimum requirements for the secure operation of a health application.**

This Guide includes what has been called a ***Definition of the Security Problem*** *(DPS),* which identifies possible threat scenarios. Therefore, the **security objectives** of mobile applications, their platforms and/or deployment environments will be a consequence of the DPS, and will aim to prevent threats and mitigate risks. The different threat scenarios and security objectives indicated in this Guide are based on the experience that the CCN has acquired over the years, on its collaboration with other national and international counterpart institutions, on the CCN-STIC Guides and on other European[6] and international documents[7].

A basic requirement in e-health applications, in addition to compliance with applicable legislation, is the observance of what are considered *good practices, as well as* other general requirements for secure applications. This includes the performance of rigorous and intensive functional and integration testing and, in particular, positive/negative testing of the application's security features. This Guide also identifies additional and specific requirements.

1.3.2 TERMINOLOGY

The terms used in this Guide have the following meanings:

- **MUST**: The manufacturer <u>must</u> implement a certain property as a mandatory requirement.

[5] NISTIR 7695 under Application ISO/IEC 19770-2: "A system for collecting, saving, processing, and presenting data by means of a computer. The term application is generally used when referring to a component of software that can be executed. The terms application and software application are often used synonymously."

[6] European Union Agency for Network and Information Security, "Smartphone Secure Development Guidelines".

[7] The OWASP Foundation, "Mobile Security Testing Guide (MSTG)" y "Mobile AppSec Verification Standard".

- **MUST NOT**: The application/*backend* must not, under any circumstances, possess a certain property or evidence of a given behaviour.
- **SHOULD**: The application/*backend* should have a certain property or evidence of a given behaviour, unless it is demonstrated that its absence does not pose a risk to the security of the operation or that its implementation is not currently possible due to technical limitations.
- **CAN**: The application/*backend* can have a certain property, which must be pointed out by the solution provider.

1.4 PROOF OF CONCEPT

This Guide is published as a *living document* to which *the* status of "Proof of Concept" is conferred. This means that, although security objectives have been defined, not enough experience has yet been gained in the application of such objectives. During this Proof of Concept, the CCN will seek feedback from the industry, which may involve additions, deletions or modifications to the stated security objectives, which will be incorporated in successive versions of this Guide.

In addition, future versions will be complemented with chapters that allow testing and Certification of Conformity with the ENS of the information systems involved in the development and operation of e-health applications.

2. OVERVIEW OF SECURITY REQUIREMENTS FOR MOBILE APPLICATIONS

2.1 APPLICATION CONCEPTS ON MOBILE DEVICES

The term "mobile application" refers to a programme running on a mobile platform. Such applications can generally be divided into three categories:

- **Native applications** (section 2.1.1), in which all source code is executed on the client (mobile device in this case).
- **Web applications** (section 2.1.2), in which all the source code (except the presentation code) is executed on the web server, and it is the browser that retrieves the result of the operations and represents them to the user.
- **Hybrid approaches** (section 2.1.3), in which the source code is distributed between the client and the server.

Since the use of web applications extends beyond mobile devices, this Guide focuses on native applications and the native part of hybrid approaches[8].

2.1.1 NATIVE APPLICATIONS

A native application is adapted to a platform and its operating system, and is based on the software development tools (*Software Development Kits - SDK*) integrated into the platform itself (such as Android or iOS), providing direct access to the components of the device, such as the GPS function, the camera or the microphone.

Due to its proximity to the operating system, this type of software usually exhibits good performance, high reliability and intuitive operation. It is usually installed from the platform's own application market and can often be run offline.

However, there are also disadvantages associated with proximity to the operating system. Operating system upgrades, for example, may require adaptation of the application if its functionality is to be maintained. In addition, this type of applications cannot be installed on other operating systems: if the same application is to run on different operating systems, separate code must be written for each of them[9], which is a complex and costly requirement.

2.1.2 WEB APPLICATIONS

As it is known, web applications are *websites that are* designed to perceive and behave like a native application, although, unlike these, web applications are not based on the SDK of the underlying platform, but on classic programming tools used for web development (HTML5 and JavaScript, for example), which means that they only allow very limited access to the components of the device.

However, their biggest advantage is that they are independent of the operating system. Since the applications are accessed from a web browser, they can be used in the same way on any platform without the need to make any adjustments at the code level.

[8] Additional information on the development and secure operation of web applications can be found in the CCN-STIC Guide 412 Security requirements in web environments and applications, CCN-STIC Guide 422 Secure development of web applications, CCN-STIC Guide 812 ENS: Security in web environments and applications. The *OWASP Application Security Verification Standard* document can also be consulted.

[9] Another approach is the concept of "*cross-platform*", which is based on the simultaneous development of an application for different platforms, which only transfers the dependence to a very complex middleware, which must cover all the target platforms.

2.1.3 HYBRID APPROACHES

Hybrid applications combine the advantages and disadvantages of native and web applications. With an SDK, a *framework* application is created, with all the features of native applications: it can access the device components and is usually available in the application markets, although it cannot be installed on other platforms without modifying the source code.

The *framework* application makes HTTP requests to a web server containing the business logic and security, in order to perform actions and retrieve data and present it to the user.

2.2 *BACKEND* SERVICES

Most applications do not rely solely on the resources provided by the execution environment to process and store data, but usually move these tasks to a central system in the *background* system (*backend*). These systems not only process and store data, but often also perform user authentication and authorisation tasks, as well as other centralised activities.

This means that not all the application's functionalities necessarily have to be implemented on mobile devices, but very often they are limited to developing a graphic user interface (*frontend*). Each application has its own characteristics in relation to the functionality implemented in the application itself or in an external server.

Obviously, an active Internet connection is required for the use of applications connected to a *backend*. The communication between the *frontend* and the *backend is* normally performed via a secure HTTPS connection. The use of *backend* systems is not limited to mobile applications, but is often used in many other types of applications.

Since this Guide focuses on mobile applications, the following sections refer to the security of the application and, additionally, only to those features of the *backend* that directly affect that security[10].

[10] For more detailed information on the secure operation and development of *backend* systems, please refer to the OWASP Foundation's '*Top 10 Web Application Security Risks'* introduction. Users of Cloud systems can consult the CCN-STIC 823 ENS Guide: Security in Cloud Environments or the BSI document 'Cloud Computing Compliance Criteria Catalogue (C5)'.

2.3 DEFINITION OF THE SECURITY PROBLEM

We have called the ***Definition of the Security Problem*** to the set of **Assumptions [A]**, **Threats [T]** and **Security Policies [P]** that are relevant to the security of e-health applications.

2.3.1 ASSUMPTIONS [A]

Concept	Description
[A.Device]	It refers to the platform on which the application is used, operated by the user himself, and protected against vulnerabilities. For example, through the regular installation of security patches of the operating system. Furthermore, its security has not been compromised by the deliberate execution of *'roots'* or *'jailbreaks'*[11].

2.3.2 THREATS [T]

Concept	Description
[T.LocalAccess]	Unauthorised access to sensitive data in the application, such as unencrypted data stored in the file system or in memory; or also access to sensitive encrypted data in plain text, after the analysis of the encryption mechanism.
[T.RemoteAccess]	Unauthorised access to sensitive *backend* data and assets and applications of the user (e.g. through a broken TLS connection). This can occur, for example, due to misuse of the mobile application or a vulnerability in the implementation of the backend interface in the direction of the *frontend*.
[T.Authentication]	Access to sensitive data of other users with a false user ID or using group credentials.
[T.Interception]	Interception or interference with the application's communication using a weakly encrypted or unauthenticated connection, or establishing a transport connection with an unauthorised component, due, for example, to insufficient verification of the certificate's properties.
[T.Costs]	The application causes unforeseen additional costs to the user.
[T.Integrity]	Unauthorised and undetected manipulation of data, in the

[11] Both behaviours (see CCN-STIC Guide 827 *Management and use of mobile devices*) involve a relaxation of the security functionalities inherent in the operating system, by granting higher level access rights and enabling the installation of applications from unknown sources.

	device's memory or in transit
[T.Discovery]	Discovery of passwords (e.g. via *brute force*[12]*)*, and gaining unauthorised access to sensitive data of another user.
[T.Memory]	Performing reverse engineering in the application, discovering unprotected data structures in the memory, so that credentials, keys or sensitive data can be accessed.
Attack on the database	Due to poor implementation of the servers and their queries, user's data can be accessed by attackers or other users.
Data sharing	The application, due to a lack of review in the assignment of roles and in checking whether a user only accesses his data, may reveal improper information.
Weakness in resetting passwords	The password reset systems if you do not implement a robust validation system can cause the resetting of a user's password or the theft of a legitimate user's account.

2.3.3 SECURITY POLICIES [P]

P. Authorisation	The manufacturer develops and implements an authorisation concept that controls both read and write access to sensitive data. The access permissions must be set in such a way that only the necessary rights are granted to satisfy the main purpose of the application. The authorisation concept must be applied independently of authentication.
[P. *BackendLog*]	Information regarding all outgoing connections is collected in the *backend* to allow a post-mortem analysis of security incidents, including meta-information on *proxies* used and certificates of verified servers.
[P. CriticalUpdates]	The manufacturer permanently monitors the application, *frameworks* and libraries for[13]exploitable vulnerabilities, providing an update in the short term if such vulnerabilities are identified. The *backend* must inform the application about the update and, after a defined period of time, stop using the

[12] Trial and error.

[13] In software development, a *framework* environment is a conceptual and technological structure, usually composed of specific software artifacts or modules, which can serve as a basis for the organisation and development of software. Typically, it can include program support, libraries, and an interpreted language, among other tools to help the development and integration of the different components of a project. A third party *framework* can be understood as a container of functionalities that has not been created under the control of the application developer and that is not part of the functionality of the platform of the operating system used.

	application.
[P.LibIn]	Data obtained from third party libraries or by the user must be validated before being used by the application (e.g. validation of XML schemas, checking for invalid coding, etc.). The objective is to protect the application from attacks resulting from harmful data entries. The input data must be analysed by libraries specialised in the analysis of data against known attacks such as XSS or code injections.
P.LibOut	The application must not send sensitive data in plain text to third party *frameworks* or libraries. The use of appropriate *frameworks* and libraries to protect a communication channel or a local storage container is allowed.
[P.Random]	Random numbers should be obtained using a high entropy[14]generator. The application will initially enter the user's entropy into the platform's random number generator. The application will then obtain the random numbers from the *backend* and enter them into the local random number generator. This applies only to operations of a sensitive nature such as cryptography. For use in operations of little relevance or presentation, the default generator is sufficient.
[P. Purpose]	Any collection, processing, storage and transfer of data may only be carried out for a defined and limited purpose. To this end, the manufacturer must publish the main purpose of the application, what data are processed, and how, where and for how long they are stored. Based on the main purpose, the permissible communication behaviour and the internal and external sensor technology used must be selected. Note/Example: Tracking or location data, such as WiFi-SSID, GPS, and similar, can only be used for the intended purpose, under the principle of data minimisation and properly guarded. Such data may not be kept in the device (e.g. image recordings) unless the intended purpose requires it directly.

[14] In Information Theory, the *entropy of* a random variable is the mean level of "information", "surprise" or "uncertainty" inherent in the possible outcomes of that variable. (Wikipedia). A system with low entropy is more predictable than a system with high entropy.

2.3.4 RESIDUAL RISKS

The operation of e-health applications is subject to particularly demanding requirements, which cannot be fully met using existing cloud devices and solutions. For this reason, some residual risks are identified below:

- Mobile devices are susceptible to theft.
- The open architecture of many platforms facilitates the use of malware.
- Installed applications can exploit existing vulnerabilities.
- A particular challenge is the protection of information during processing in the main memory.
- The installation of the *backend* in public *cloud* service providers entails special risks for users' sensitive data. While the use of secure communications and encryption methods mitigate the risks, the data is virtually unprotected during cloud processing. This places extremely high demands on cloud service providers, as well as on other users who may simultaneously use resources on the same physical machine.

  Indeed, an attacker leaving your virtual machine could access other virtual machines (outside your own client area) and therefore could access and manipulate sensitive data of another client (e.g. application health data).
- Communications between the platform, the application and the *backend* are protected by a cryptographically secure TLS protocol. This Guide contemplates a unilateral authentication in which the application checks the authenticity of the *backend*. The application adds its own randomness to the process of establishing a TLS connection in order to make it difficult for an attacker to penetrate that connection. However, random numbers on smartphone platforms often lack the quality necessary to protect the sensitive data of an e-health application. The residual risk during the connection establishment process is that the attacker can forge the authenticity of his own messages, which would allow the attacker to access and manipulate the sensitive data transmitted from the application to the *backend*. (The measure [O.Random_4] provides a means that can reduce this residual risk for the second TLS connection, which is enriched with new entropy).

3. SECURITY MEASURES FOR E-HEALTH APPLICATIONS

3.1 SECURITY OBJECTIVES

The following objectives should be considered as **minimum security requirements** for e-health applications, to be met by the manufacturers of such applications.

The **Security Objectives** can be divided into the following types:

1. Testing the application purpose
2. Testing the architecture
3. Testing the source code
4. Testing the third party software
5. Testing the application of cryptography
6. Testing the authentication
7. Testing the data storage and data protection
8. Testing of payment resources
9. Testing of platform-specific interactions
10. Testing of network communication
11. Testing resilience

If the e-health application uses a functionality that must be protected, the manufacturer must document, for each aspect of the test, how the requirement has been implemented.

Below, for each of the objectives indicated, we show their codification, description and location within the framework of the National Security Framework (ENS-RD 3/2010)[15]. Regardless of the specific measures applied in each case, the manufacturer must always have an Information Security Policy in relation to the information system used for the development of the e-health application and for its exploitation (measure [org.1] of the ENS), as well as having carried out and maintained the corresponding Risk Analysis (Article 13 and measure [op.pl.1] of the ENS).

3.1.1 OBJECTIVE (1): PURPOSE OF THE APPLICATION

Concept	Description	RD 3/2010 (ENS)
O. Purpose_1	Before installation, the manufacturer **MUST** inform the user of the main purpose of the application and its *backend,* as well	Measures [mp.info.1] and [mp.info.2], in relation to Article 11 and the First Additional

[15] An 'Undetermined' or 'N/A' means that the security requirement is not specifically covered by the ENS.

	as the use of personal data (e.g. in the description given in the application market) and inform the user at least at the time of the first commissioning.	Provision of the LOPDGDD, on the[16]basis of Articles 5, 6, 9 and 13 of the RGPD[17].
O. Purpose_2	The application and its *backend* **MUST NOT** collect and process data that does not correspond to the purpose for which the application is intended.	Measures [mp.info.1] and [mp.info.2], in relation to the First Additional Provision of the LOPDGDD, on the basis of Articles 5 and 6 of the RGPD.
O. Purpose_3	The application and its *backend* **MUST** obtain the explicit consent of the user before collecting or processing any personal data.	Measures [mp.info.1] and [mp.info.2], in relation to Articles 6 and 9 and the First Additional Provision of the LOPDGDD, on the basis of Articles 5, 6, 7 and 9 of the RGPD.
O. Purpose_4	If the user has not expressly accepted the use of certain data, these **MUST NOT** be used by the application or the *backend*.	Measures [mp.info.1] and [mp.info.2], in relation to Article 5 and the first additional provision of the LOPDGDD, on the basis of Article 9 of the RGPD.
O. Purpose_5	The application and its *backend* **MUST** allow the user to withdraw their consent at any time, and **MUST** report on how this could alter the behaviour of the application.	Measures [mp.info.1] and [mp.info.2], in relation to the First Additional Provision of the LOPDGDD, on the basis of Article 7 of the RGPD.

[16] Organic Law 3/2018, of 5 December, on Data Protection and guarantee of digital rights.

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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 - GDPR).

O. Purpose_6	The manufacturer **MUST** keep a record showing which user consents have been obtained. The specific part of the user directory **MUST** be visible to the user as well.	Measures [mp.info.1] and [mp.info.2], in relation to the First Additional Provision of the LOPDGDD, on the basis of Article 7 of the RGPD.
O. Purpose_7	If the application or its *backend* uses third party frameworks or libraries, all functions used from such sources **SHOULD** be necessary for the main purpose of the application. The application **SHOULD** safely disable any other functions.	Art. 16 and Measures [mp.info.1] and [mp.info.2], in relation to Art. 5 and the First Additional Provision of the LOPDGDD, on the basis of Arts. 5 and 6 of the RGPD.
O. Purpose_8	Sensitive data **MUST NOT** be shared with third parties unless it is necessary for the main purpose of the application. The application **MUST** fully inform the user of the consequences of any disclosure of the data and obtain the user's consent (OPT-IN) Note: If, for example, the application uses the display of a map from a third manufacturer, the user must be informed that certain data could be transmitted to third parties.	Measures [mp.info.1] and [mp.info.2], in relation to Article 11 and the First Additional Provision of the LOPDGDD, on the basis of Articles 5, 6, 9 and 13 of the RGPD.
O. Purpose_9	The application **MUST NOT** display sensitive data on the screen unless it is necessary for the purpose of the application.	Measures [mp.info.1] and [mp.info.2], in relation to Article 11 and the First Additional Provision of the LOPDGDD, on the basis of Articles 5 and 13 of the RGPD.
	The insulation of the users must be checked. A user has access to his or her data only.	- Measure [op.acc.3] - Measure [op.acc.4] - Measure [mp.info.3]

	All data sent outside the application, by e-mail or any other channel, must be encrypted, preferably using public-private key systems, if this is not possible using a symmetric key.	
	Security testing should be included in the implementation testing plan.	- Measure [mp.sw.1]
	The source code of the application must be audited and tested for intrusion attacks.	- Measure [mp.sw.2]
	The application must record the administrator's accesses and actions on the application and data.	- Measure [op.acc.1] - Measure [op.acc.2] - Measure [op.acc.4] - Measure [op.exp.8]
O.Purpose_10	It must be reflected who is accessing the data at any given time and what actions they are carrying out on it: • The creation must record date and time and user making the change • In modification you must record who makes the change and record the old data and the new data • The deletion should reflect which data is deleted • When accessing, indicate the index of the data accessed, user and date and time • The validity of the audit table can be the same as the data.	- Measure [op.acc.1] - Measure [op.acc.2] - Measure [op.acc.4] - Measure [op.exp.8]

3.1.2 OBJECTIVE (2): ARCHITECTURE

Concept	Description	RD 3/2010 (ENS)
O.Arq_1	Security **MUST** be an integral part of the software development and life cycle of the application and its	- Art. 39 - Measure [op.exp.11] - Measure [mp.sw.1]

	backend[18].	
O.Arq_2	During the design phase of the application, it **MUST** be taken into account that the application and its *backend* will process sensitive data (special categories of data). To achieve this, the application architecture **MUST** control the collection, processing, storage and secure disposal of sensitive data, throughout its life cycle.	(See Objective (1) measures: Purpose of implementation)
O.Arq_3	The life cycle of cryptographic material **MUST** conform to a policy that includes elements such as the source of random numbers, details of key function segregation, validity period of certificate keys, integrity assurance by hash algorithms, etc. The policy **SHOULD** be based on recognised standards[19].	- Measure [org.4] - Measure [op.acc.5] - Measure [op.exp.11] - Measure [mp.com.2] - Measure [mp.si.2] - Security Technical Instruction of employment cryptology in the National Security Framework.
O.Arq_4	If the application uses a cloud *backend,* the cloud information system **MUST**[20] be ENS compliant or have a security certification for cloud services[21].	- Measures [op.ext], in relation to the other measures of the ENS that are applicable to the cloud system. Observance of the Guidelines: - CCN-STIC 823 Use of cloud services. - CCN-STIC 811 Interconnection in the ENS - CCN-STIC 812 Security in web environments and applications.

[18] Ver *iOS Security Framework* (Apple) y *Security for Android Developers* (Google).

[19] Tales como NIST: "Recommendation for Key Management", Revision 4 y BSI TR-02102 Cryptographic Mechanisms.

[20] In the Basic, Medium or High safety category, depending on the result of the Risk Analysis

[21] Por ejemplo, tal como el *Cloud Computing Compliance Controls Catalogue (C5)-Criteria to assess the information security of cloud services*, de la BSI.

		- CCN-STIC 836 security in VPN.
O.Arq_5	*Backups* and system *backups in the* cloud (*backend*) controlled by the operating system **MUST NOT** contain sensitive data that is not encrypted.	- Measure [mp.info.1] - Measure [mp.info.9]
O.Arq_6	Security functions **MUST** always be implemented, both in the application and in the *backend,* as well as in all external interfaces and API end points.	- Art. 18. - Art. 19. - Art. 20. - Art. 22. - Art. 39. - Measure [mp.com] - Measure [mp.sw.1]
O.Arq_7	The application **MUST** protect the authenticity and integrity of the application and its configuration. The application **SHOULD** regularly perform a self-check of the authenticity and integrity of the application binary using a certificate-based electronic signature form.	- Art. 1.2. - Art. 19. - Art. 20. - Measure [org.3] - Measure [op.exp.2] - Measure [mp.com.3] - Measure [mp.info.4] Observance of the Guidelines: - CCN-STIC 823 Use of cloud services. - CCN-STIC 811 Interconnection in the ENS - CCN-STIC 812 Security in web environments and applications. - CCN-STIC 836 security in VPN.
O.Arq_8	If the application uses third party *frameworks* or libraries (e.g. for object serialisation), the manufacturer **MUST** clearly inform the user about the scope of use and the extent of the security mechanisms used. The application	- Art. 16. - Art. 18. - Art. 39. - Measure[op.pl.3] - Measure [op.pl.5] - Measure [op.exp.2] - Measure [op.exp.3]

	MUST ensure the safe use of these functions. The application **MUST** ensure that unused functions cannot be activated by third parties.	- Measure [mp.sw.1] - Measure [mp.sw.2] - Measure [mp.s.2] - Measure [mp.s.8] Observance of the Guidelines: - CCN-STIC 823 Use of cloud services. - CCN-STIC 811 Interconnection in the ENS - CCN-STIC 812 Security in web environments and applications. - CCN-STIC 834 Protection against harmful code. - CCN-STIC 836 security in VPN.
O.Arq_9	The interpreted code[22] that can interact with the user's inputs (Webviews with JavaScript), **MUST NOT** have access to the encrypted memory or user data, except when it is strictly necessary to fulfill the purpose of the application.	- Measure [mp.sw.1] - Measure [mp.sw.2] - Measure [mp.s.2]
O.Arq_10	The manufacturer **MUST** provide the user with a simple and effective means of notifying security incidents or problems.	- Art. 7. - Art. 15. - Art. 24. - Art. 36. - Art. 37. - Measure [op.exp.3] - Measure [op.exp.7] - Measure [op.exp.9] - Measure [op.ext.2] - Measure [op.mon.2] - Measure [mp.com.3] Observance of the

[22] This does not include the code of the platform-specific programming languages (such as Java or Kotlin for Android).

		Guidelines: - CCN-STIC 817 Management of cyber-incidents
O.Arq_11	The *backend* **SHOULD** be able to force updates relevant to the security of the application.	- Art. 20. - Art. 26. - Measure [op.pl.2] - Measure [op.exp.4] Observance of the Guidelines: - CCN-STIC 823 Use of cloud services. - CCN-STIC 811 Interconnection in the ENS - CCN-STIC 812 Security in web environments and applications. - CCN-STIC 836 security in VPN.
O.Arq_12	The manufacturer **CAN** provide the application and updates through a trusted channel in their own application market.	- Art. 18. - Art. 21. - Art. 22. - Art. 33. - Measure [op.pl.2] - Measure [op.acc.7] - Measure [mp.com.3] Observance of the Guidelines: - CCN-STIC 823 Use of cloud services. - CCN-STIC 811 Interconnection in the ENS - CCN-STIC 812 Security in web environments and applications. - CCN-STIC 836 security in VPN.

O.Arq_13	If the application and updates are not imported from the hardware platform's usual application market mechanisms, they **MUST** be encrypted and signed using cryptographic means.	- Art. 21. - Measure [org.4] - Measure [op.acc.7] - Measure [op.exp.11] - Measure [mp.com.2] - Measure [mp.si.2] - Measure [mp.info.4] Observance of the Guidelines: - CCN-STIC 807 Cryptologic of employment in the ENS. - CCN-STIC 834 Protection against harmful code. - CCN-STIC 836 security in VPN.
	Access to the database (storage system) is always done by a mechanism to prevent attacks on the database and its own data. The use of direct queries from the application to the database is not allowed.	-
	The application should be structured with roles and check that each role only accesses its data space. And each user accesses his or her data.	- Measure [op.acc.1] - Measure [op.acc.2]
	All input data received by the user must be filtered through libraries to avoid code injection attacks.	
	The data to increase their level of access security must have indicated which users can access them. Depending on the functional case, the user can be changed to a role.	- Measure [op.acc.1] - Measure [op.acc.2]
	It must be checked functionally that each user only has access to his or her data. In all functional tests it must be	- Measure [op.acc.1] - Measure [op.acc.4] - Measure [op.acc.5]

	checked whether a user can access data of other users.	
	All communication with an external system must be encrypted, to avoid Man In The Middle (MITM) attacks.	- Measure [op.acc.7] - Measure [mp.info.3]
	As far as possible, a two-factor mechanism should be used to access the application.	- Measure [op.acc.5]
	The password reset system should be reviewed to prevent improper access or resetting without sufficient guarantees of user authenticity.	- Measure [op.exp.2] - Measure [op.acc.1] - Measure [op.acc.6]

3.1.3 OBJECTIVE (3): SOURCE CODE

Concept	Description	RD 3/2010 (ENS)
O.Code_1	User entries **MUST** be checked before use to completely rule out user entry containing harmful values.	- Measure [op.pl.2] - Measure [op.exp.2] - Measure [op.exp.3] - Measure [op.exp.6] - Measure [mp.sw.1] - Measure [mp.sw.2] - Measure [mp.info.1]
O.Code_2	The manufacturer **MUST** provide structured data with an escape syntax.	- Measure [mp.sw.1] - Measure [mp.sw.2] -
O.Code_3	Error messages and notifications **MUST NOT** contain sensitive data (such as a user ID, for example).	- Measure [mp.sw.1] - Measure [mp.sw.2] - Measure [mp.info.1]
O.Code_4	Possible exceptions in the programme flow **MUST** be intercepted, managed in a controlled way and documented.	- Measure [mp.sw.1] - Measure [mp.sw.2]
O.Code_5	In case of exceptions in the program flow with critical effects for the security, the application **MUST** abort the access to sensitive data.	- Measure [mp.sw.1] - Measure [mp.sw.2] - Measure [mp.info.1]
O.Code_6	In those environments with manual memory management (i.e. the	- Measurement [mp.sw.1]

	application itself can define exactly when and where it reads or writes from memory), the application and the *backend* implementation **MUST** use alternative secure functions (e.g. *sprintf_s* instead of *printf)* to read and write to the memory segments or even the possibility to use variables with direct in-memory encryption.	- Measure [mp.sw.2]
O.Code_7	All development support options (such as log calls, developer URLs, testing methods, etc.) **MUST** be removed completely from the production version code.	- Measure [mp.sw.2]
O.Code_8	The manufacturer **MUST** ensure that no debugging mechanisms are left in the production version.	- Measure [mp.sw.2]
O.Code_9	The implementation of the application **SHOULD** allow for state-of-the-art security mechanisms in the development environment, such as code-byte minimisation and battery protection.	- Measure [mp.sw.1] - Measure [mp.sw.2]
Source_10	All data entry by users must be filtered by libraries designed for this purpose, to avoid SQL attacks or inappropriate javascript or html data entry.	
Source_11	No direct database queries should be made, the necessary mechanisms should be used to process the data first (e.g. use of PreparedStatement).	
Source_12	The use of dynamic variables should be taken into account, when they are finished using all of them should be pointed or redirected to *null to* avoid *use after free* attacks.	

3.1.4 OBJECTIVE (4): THIRD PARTY SOFTWARE

Concept	Description	RD 3/2010 (ENS)
O.SwExt_1	Third party libraries and *frameworks* **MUST** use the latest version available	- Art. 20. - Art. 26.

	for the operating system of the platform in use. Taking into account possible interactions with other libraries when choosing the version.	- Measure [op.pl.2] - Measure [op.exp.4] - Measure [op.ext.1] - Measure [mp.sw.1] - Measure [mp.sw.2]
O.SwExt_2	The manufacturer **MUST** perform periodic checks for vulnerabilities in third party libraries and *frameworks.* The functions of the libraries and *frameworks* **MUST NOT** be used if a vulnerability is known.	- Art. 20. - Art. 37. - Measure [op.pl.1] - Measure [op.pl.2] - Measure [op.exp.3] - Measure [op.ext.1] - Measure [op.sw.2]
O.SwExt_3	Security updates for libraries and *frameworks* **MUST** be incorporated without delay. The manufacturer **MUST** possess and communicate a security policy that determines the tolerated usage time of the application and/or *backend* based on the criticality of exploitable vulnerabilities. Once this time period is exceeded, the application **MUST** stop working.	- Art. 20. - Art. 26. - Measure [org.1] - Measure [op.pl.2] - Measure [op.exp.4] - Measure [op.ext.1] - Measure [mp.sw.1] - Measure [mp.sw.2]
O.SwExt_4	The user **MUST** be informed about the mitigation measures that can be applied.	- Art. 7. - Art. 9. - Art. 13. - Measure [org.1] - Measure [op.exp.7] - Measure [op.ext.1] - Measure [mp.per.3] - Measure [mp.per.4]
O.SwExt_5	The manufacturer **MUST** verify the reliability of third party libraries and *frameworks* before use.	- Art. 20. - Art. 26. - Art. 37. - Measure [op.pl.1] - Measure [op.pl.2] - Measure [op.exp.3] - Measure [op.ext.1] - Measure [mp.sw.1] - Measure [op.sw.2]

O.SwExt_6	The application **SHOULD NOT** share sensitive data with third party software.	- Art. 21. - Measure [op.ext.1] - Measure [mp.info.1]
O.SwExt_7	Data received through third party software **SHOULD** be validated. Note / example: Exceptions to O.SwExt_6 and O.SwExt_7 are, for example, *frameworks* and libraries for encryption (TLS).	- Art. 21. - Measure [op.ext.1] - Measure [mp.com.2] - Measure [mp.com.3] - Measure [mp.info.1]
O.SwExt_8	Third party software that is no longer maintained by the manufacturer or developer **MUST NOT** be used.	- Art. 20. - Measure [op.pl.2] - Measure [op.exp.3] - Measure [op.ext.1] - Measure [op.sw.2]

3.1.5 OBJECTIVE (5): CRYPTOGRAPHIC IMPLEMENTATION

Concept	Description	RD 3/2010 (ENS)
O.Cryp_1	When the application uses encryption, *hard-coded*[23] keys **MUST NOT** be used. This will not apply to cutting-edge techniques that robustly hide the key used for reverse engineering (*White Box Cryptography*). If static keys are used, at least one non-static key **MUST** be used in multilayer encryption.	- Measure [org.4] - Measure [op.exp.11] - Measure [mp.si.2] - Measure [mp.sw.1] - Measure [mp.com.2] Observance of the Guide: - CCN-STIC 807 Cryptologic of employment in the ENS.
O.Cryp_2	The application **MUST** use proven implementations to implement cryptographic primitives.	- Measure [org.4] - Measure [op.exp.11] - Measure [mp.si.2] - Measure [mp.sw.1] - Measure [mp.com.2]

[23] The use of *hard-coded keys* (also called embedded keys) refers to the practice of embedding plain text encryption keys (unencrypted) and other secret data (SSH keys, DevOps secrets, etc.) into the source code, which helps simplify development, but at the same time poses a considerable security risk.

		Observance of the Guide: - CCN-STIC 807 Cryptologic of employment in the ENS.
O.Cryp_3	The choice of cryptographic primitives **MUST** be appropriate to the application and meet the specifications of the state of the art.	- Art. 20. - Measure [org.4] - Measure [op.exp.11] - Measure [mp.si.2] - Measure [mp.sw.1] - Measure [mp.com.2] Observance of the Guide: - CCN-STIC 807 Cryptologic of employment in the ENS.
O.Cryp_4	Cryptographic keys **MUST NOT** be used for more than one purpose. Note / example: A distinction must be made between the purpose of protection by encryption and authentication. Different keys must be provided for each purpose.	- Measure [org.4] - Measure [op.exp.11] - Measure [mp.si.2] - Measure [mp.sw.1] - Measure [mp.com.2] Observance of the Guide: - CCN-STIC 807 Cryptologic of employment in the ENS.
O.Cryp_5	The robustness of cryptographic keys **MUST** be in line with the current state of the art.	- Art. 20. - Measure [org.4] - Measure [op.exp.11] - Measure [mp.si.2] - Measure [mp.sw.1] - Measure [mp.com.2] Observance of the Guide: - CCN-STIC 807 Cryptologic of

		employment in the ENS.
O.Cryp_6	All cryptographic keys **SHOULD** be located in a tamper-resistant environment (such as an integrated secure/trusted execution environment). Variants for different hardware platforms will be considered.	- Measure [org.4] - Measure [op.exp.11] - Measure [mp.si.2] - Measure [mp.sw.1] - Measure [mp.com.2] Observance of the Guide: - CCN-STIC 807 Cryptologic of employment in the ENS.

3.1.5.1 RANDOM NUMBERS

Concept	Description	RD 3/2010 (ENS)
O.Random_1	All random values used in sensitive operations **MUST** be generated using a secure cryptographic random number generator.	Not explicitly determined in the ENS.
O.Random_2	The application, in operations of a sensitive nature, **MUST** obtain random numbers from a high entropy random number generator.	Not explicitly determined in the ENS.
O.Random_3	The application **SHOULD** assign the random number generator a seed composed of, at least, three independent system parameters. It **SHOULD NOT** be possible to determine the parameters from outside the application. If the platform provides a random number generator hardware that does not allow seed allocation, such random number generator hardware **CAN** be used instead. Note / example: The above concerns random number generators both in the application device and in the	Not explicitly determined in the ENS.

	backend.	
O.Random_4	The application **SHOULD** obtain a suitable random number from the *backend to* create a seed for the random number generator. <u>Note / example</u>: Before the first TLS connection, the application enters entropy into the local random number generator, according to O.Random_3 (e.g. from the interaction with the user and the device sensors), through a seed. It establishes an initial connection to obtain additional entropy from the *backend* random number source. Then, the connection is immediately closed. The application takes into account the randomness obtained, according to O.Random_4, in the local random number generator. For the TLS connection, the randomness of the local random number source, which has been increased by the entropy of the *backend* random number source, will henceforth be used.	Not explicitly determined in the ENS.

3.1.6 OBJECTIVE (6): AUTHENTICATION

Concept	Description	RD 3/2010 (ENS)
O.Auten_1	The manufacturer **MUST** document a policy for authentication (two-factor), authorisation (role concept) and termination of an application session.	- Measure [org.3] - Measure [op.pl.2] - Measure [mp.acc.5] - Measure [op.acc.6] - Measure [mp.sw.1] - Measure [mp.s.2]
O.Auten_2	For connection to a *backend* system, proper authentication and authorisation **MUST** take place at the *backend* interface.	- Measure [org.3] - Measure [op.pl.2] - Measure [mp.acc.5] - Measure [op.acc.7]

		- Measure [mp.com.3] - Measure [mp.sw.1] - Measure [mp.s.2]
O.Auten_3	The application **SHOULD** implement the authentication mechanisms and authorisation functions separately. If the application requires different functions, authorisation **MUST** be implemented separately for each data access.	- Measure [op.pl.2] - Measure [mp.acc.5] - Measure [op.acc.6] - Measure [op.acc.7] - Measure [mp.com.3] - Measure [mp.sw.1] - Measure [mp.s.2]
O.Auten_4	The user **MUST** be authenticated by a second factor before sensitive data is processed in the application (staged authentication).	- Measure [op.pl.2] - Measure [op.acc.5]
O.Auten_5	For user authentication in the application session, the second factor **CAN** be generated by the *backend* system.	- Measure [op.pl.2] - Measure [mp.acc.5]
O.Auten_6	The evaluation of an authentication process **SHOULD** include additional information (such as the device used, the Wi-Fi access node used, or the time of access). In the event of a deviation from the expected parameters, an additional authentication measure **MUST** be taken (staged authentication).	- Measure [op.pl.1] - Measure [op.pl.2] - Measure [mp.acc.5]
O.Auten_7	Robust password policies **MUST** exist for username and password based authentication.	- Measure [org.2] - Measure [op.pl.2] - Measure [op.acc.5] Compliance with the Guide CCN-STIC 821 Security Standards - Appendix V: Rules for the creation and use of passwords.
O.Auten_8	For authentication based on a user name and password, the strength of the password used **CAN** be shown to	Not explicitly determined in the ENS.

	the user. Information regarding the strength of the chosen password **MUST NOT** be retained in the application memory or *backend*.	Default or complementary application: - Measure [op.pl.2] - Measure [op.acc.5] Compliance with the Guide CCN-STIC 821 Security Standards - Appendix V: Rules for the creation and use of passwords.
O.Auten_9	The user **MUST** be able to change his or her password. This operation **MUST** require authentication data again in order to not be able to do so through a stolen session.	- Measure [op.pl.2] - Measure [op.acc.5] Compliance with the Guide CCN-STIC 821 Security Standards - Appendix V: Rules for the creation and use of passwords.
O.Auten_10	The *backend* and the application **MUST** provide measures that prevent repeated testing of login parameters (e.g. passwords). This can be achieved, for example, by delaying subsequent access attempts or by using so-called *captchas*.	- Measure [op.pl.2] - Measure [op.acc.5] Compliance with the Guide CCN-STIC 821 Security Standards - Appendix V: Rules for the creation and use of passwords.
O.Auten_11	If the application was interrupted (put in the background), a new authentication **MUST** be requested.	- Measure [mp.eq.2]
	The password recovery procedure must be validated to be robust in checking the authenticity of the user and not allow the theft of the user by this mechanism.	- Measure [op.pl.2] - Measure [op.exp.2] - Measure [op.acc.5]

3.1.6.1 AUTHENTICATION BY BIOMETRICS

Concept	Description	RD 3/2010 (ENS)
O.Biom_1	The use of biometric sensors **SHOULD NOT** be used as the only authentication mechanism. It should only be allowed as part of two-factor authentication.	Not explicitly determined in the ENS. Default or complementary application: - Measure [op.pl.2] - Measure [op.acc.5] Compliance with the Guide CCN-STIC 140 Reference Taxonomy for ICT Security Products - Annex A.2: Biometric devices
O.Biom_2	The manufacturer **MUST** define the minimum quality and characteristics of a biometric sensor to be used by the application.	Not explicitly determined in the ENS. Default or complementary application: - Measure [org.3] - Measure [op.pl.2] - Measure [op.acc.5] Compliance with the CCN-STIC Guide 140 Reference Taxonomy for ICT Security Products - Annex A.2: Biometric devices
O.Biom_3	The application **MUST** verify the biometric sensor hardware against a *blacklist* or *whitelist* before use. The manufacturer **SHOULD** maintain a black/white list of safe/unsafe biometric sensors. A black/white list **MUST** be kept available in the *backend*.	Not explicitly determined in the ENS. Default or complementary application: - Art. 20. - Measure [op.pl.2]

		- Measure [op.exp.3] - Measure [op.acc.5] - Measure [mp.sw.2] Compliance with the Guide CCN-STIC 140 Reference Taxonomy for ICT Security Products - Annex A.2: Biometric devices
O.Biom_4	Prior to authentication using a biometric sensor, the application **MUST** always ensure that the available hardware meets the specified requirements.	Not explicitly determined in the ENS. Default or complementary application: - Measure [org.3] - Measure [op.pl.2] - Measure [op.acc.5] Compliance with the Guide CCN-STIC 140 Reference Taxonomy for ICT Security Products - Annex A.2: Biometric devices
O.Biom_5	Before the application uses a biometric sensor, you **MUST** ensure that the sensor has the user's reference biometric characteristics of the device for comparison.	Not explicitly determined in the ENS. Default or complementary application: - Measure [op.pl.2] - Measure [op.acc.5] Compliance with the Guide CCN-STIC 140 Reference Taxonomy for ICT Security Products - Annex A.2: Biometric devices

O.Biom_6	The application **MUST** determine when the biometric reference features have been changed and deny enrollment if the features were subsequently changed (i.e. since the activation of the authentication control mechanism in the application).	Not explicitly determined in the ENS. Default or complementary application: - Measure [op.pl.2] - Measure [op.acc.5] Compliance with the Guide CCN-STIC 140 Reference Taxonomy for ICT Security Products - Annex A.2: Biometric devices
O.Biom_7	The application **MUST** make use of the operating system's own functions (e.g. unlocking the *KeyChain/KeyStore*) to evaluate the biometric authentication.	Not explicitly determined in the ENS. Default or complementary application: - Measure [op.pl.2] - Measure [op.acc.5] Compliance with the Guide CCN-STIC 140 Reference Taxonomy for ICT Security Products - Annex A.2: Biometric devices

3.1.6.2 *STATEFUL* AUTHENTICATION MEASURES (CONDITIONED)[24]

Concept	Description	RD 3/2010 (ENS)
O.AutSF_1	The management of the sessions	Not explicitly

[24] *Stateful Authentication*: After a successful authentication, the application generates a random token to send to the user and creates in memory or in an internal database an authenticated session of the user. When a user tries to access the application with a certain token, the application tries to retrieve the session data from memory, checks if the session is valid and decides if the user has access to the desired resource or not.

	SHOULD be performed through secure frameworks (see O.Red_3).	determined in the ENS.
O.AutSF_2	Session identifiers **MUST** be created by the *backend* random number generator.	Not explicitly determined in the ENS. Default or complementary application: - Measures [acc.op.*]
O.AutSF_3	Session identifiers **MUST** be protected as sensitive data.	Not explicitly determined in the ENS. Default or complementary application: - Measures [acc.op.*]
O.AutSF_4	Session identifiers **MUST NOT** be stored unencrypted on permanent storage media.	Not explicitly determined in the ENS. Default or complementary application: - Art. 21. - Measure [mp.eq.3]
O.AutSF_5	Implementation **MUST** end the implementation session after an appropriate session time limit, according to the best practice recommendations.	- Measure [mp.eq.2]
O.AutSF_6	When a session ends, the application **MUST** securely delete the session ID, both on the device and on the *backend*.	Not explicitly determined in the ENS. Default or complementary application: - Measure [op.acc.6]

3.1.6.3 *STATELESS* AUTHENTICATION MEASURES (UNCONDITIONAL)[25]

Concept	Description	RD 3/2010 (ENS)
O.Tokn_1	The authentication *token* **SHOULD** be located in a secure area of the terminal device's memory (e.g. *KeyChain/KeyStore*). The authentication token **MUST** be protected on the device from easy access by third parties (e.g. rooted/jailbroken devices).	Not explicitly determined in the ENS. Default or complementary application: - Measures [acc.op.*]
O.Tokn_2	Sensitive data **MUST NOT** be embedded in an authentication token.	Not explicitly determined in the ENS. Default or complementary application: - Measure [acc.op.*] - Measure [mp.info.1]
O.Tokn_3	An authentication token **MUST** include the full name of the *backend* and the application **MUST** verify the full name.	Not explicitly determined in the ENS. Default or complementary application: - Measures [acc.op.*]
O.Tokn_4	The *backend* **MUST** use an appropriate procedure to sign the authentication token.	Not explicitly determined in the ENS. Default or complementary application: - Measures [acc.op.*] - Measure [mp.info.4]

[25] *Stateless Authentication*: After a successful authentication, the application generates a token with all the necessary data, signs it with a public key and sends it back to the user. There is a standard for token generation, it is the JWT (JSON Web Token). The process is described in the *OpenID Connect* (OIDC) specification. When a user tries to access the application with a token, the application verifies the signature of the token with a private key, checks if the token has expired, retrieves all data from the token session and makes a decision on whether the user has access to the desired resource or not.

O.Tokn_5	The private key used to sign the authentication token **MUST NOT** be present or stored on the device.	Not explicitly determined in the ENS. Default or complementary application: - Measures [acc.op.*] - Measure [mp.info.4]
O.Tokn_6	The *backend* **MUST** check the token. The signature algorithm **MUST NOT** be "none". It is also not recommended that the signature type be "HS256", "HS384" or "HS512", since it can lead to the *backend* using the public key as a private key if it is not properly configured, as it is a symmetric signature algorithm.	Not explicitly determined in the ENS. Default or complementary application: - Measures [acc.op.*] - Measure [mp.info.4]
O.Tokn_7	The *backend* **MUST** reject the request made with an invalid or unsigned authentication token.	Not explicitly determined in the ENS. Default or complementary application: - Measures [acc.op.*] - Measure [mp.info.4]
O.Tokn_8	The *backend* **MUST** take into account the period of validity when assessing the validity of a token.	Not explicitly determined in the ENS. Default or complementary application: - Measures [op.acc] - Measure [mp.info.4]
O.Tokn_9	The *backend* **MUST** provide the user with existing authentication *tokens* when requested.	Not explicitly determined in the ENS. Default or complementary application: - Measures [op.acc] - Measure [mp.info.4]

O.Tokn_10	The *backend* **MUST** allow the user to override any or all previously issued authentication tokens (e.g. in the event of loss or theft of the device).	Not explicitly determined in the ENS. Default or complementary application: - Measures [op.acc]

3.1.7 OBJECTIVE (7): STORAGE AND DATA PROTECTION

Concept	Description	RD 3/2010 (ENS)
O.PD_1	The factory configuration of the application **MUST** provide maximum data protection and security.	- Art. 16. - Art. 19. - Art. 21. - Measure [op.exp.2] - Measure [op.exp.3]
O.PD_2	All sensitive data **MUST** be stored in encrypted form. This applies to both volatile storage (e.g. in working memory) and permanent storage (e.g. in a cloud environment), including cryptographic keys, with the exception of memory encryption. Preference **SHOULD** be given to hardware-based platform key management. If the platform ensures sufficient protection of the keys (e.g. in the secure/trusted embedded environment, the application **CAN** store the keys in plain text.	- Art. 21. - Measure [op.exp.11] - Measure [mp.eq.3] - Measure [mp.si.2] - Measure [mp.info.1] - Measure [mp.info.3]
O.PD_3	All sensitive data **SHOULD** be stored in an environment protected against viewing, access and manipulation (such as the integrated secure/trusted execution environment). In this way, the highest possible level of protection for the individual platform or end device **SHOULD** be achieved.	- Art. 21. - Measure [mp.eq.3] - Measure [mp.info.1]

O.PD_4	The application **MUST NOT** make available to third parties any resources that allow access to sensitive data.	- Art. 21. - Measure [op.acc.7] - Measure [mp.info.1]
O.Tokn_5	All sensitive data collected **MUST NOT** be saved in the application or its *backend* after use. The application **MUST** respect the principles of data minimisation and purpose[26]limitation.	- Art. 21. - Art. 27. - Measure [mp.info.1]
O.PD_6	Sensitive data **MUST** be stored and processed in the *backend* system.	Not explicitly determined in the ENS. Default or complementary application: - Art. 16. - Art. 19. - Art. 21. - Art. 22. - Measure [op.acc.7] - Measure [op.exp.2] - Measure [mp.sw.1]
O.PD_7	If recording devices (such as cameras, for example) are used, all metadata with relevance to data protection **MUST** be removed, such as the GPS coordinates of the recording location, the hardware used, etc.	- Art. 27. - Measure [mp.info.1]
O.PD_8	When collecting sensitive data, the use of recording devices (such as a camera) **MUST** be avoided, as other applications could access this data (through an image gallery, for example).	Not explicitly determined in the ENS. Default or complementary application: - Measure [op.exp.2] - Measure [op.exp.3] - Measure [mp.sw.1] - Measure [mp.info.1]
O.PD_9	When sensitive data is entered via the keyboard, the application **SHOULD**	Not explicitly determined in the ENS.

[26] Both principles are contained in the RGPD.

	prevent the data from being visible to third parties, specifically contemplating caches, auto-correction and auto-completion procedures, third party input devices and any form of storage that can be analysed by third parties.	Default or complementary application: - Measure [op.exp.2] - Measure [op.exp.3] - Measure [mp.sw.1] - Measure [mp.info.1]
O.PD_10	When sensitive data is entered, its temporary storage in the clipboard **SHOULD** be deactivated. The application, however, **CAN** implement its own clipboard, which will be protected against access by other applications.	Not explicitly determined in the ENS. Default or complementary application: - Measure [op.exp.2] - Measure [op.exp.3] - Measure [mp.sw.1] - Measure [mp.info.1]
O.PD_11	Sensitive data, such as biometrics or private keys, **MUST NOT** be exported from the component in which they were generated.	Not explicitly determined in the ENS. Default or complementary application: - Measure [op.exp.2] - Measure [op.exp.3] - Measure [mp.sw.1] - Measure [mp.info.1]
O.PD_12	When sensitive data is displayed, the application **SHOULD** prevent third party access and the storage of screen contents (e.g. screenshots and screens for application change).	Not explicitly determined in the ENS. Default or complementary application: - Measure [op.exp.2] - Measure [op.exp.3] - Measure [mp.sw.1] - Measure [mp.info.1]
O.PD_13	The application **MUST NOT** write sensitive data in log files or other	Not explicitly determined in the ENS.

	messages or notifications that have not been expressly enabled by the user (see O.Plat_4).	Default or complementary application: - Measure [op.exp.2] - Measure [op.exp.3] - Measure [mp.sw.1] - Measure [mp.info.1]
O.PD_14	The application **MUST** ensure that all sensitive data is encrypted when the device is locked. <u>Note/example</u>: Older platform versions partially allow storage of the application on external storage media that are not subject to storage encryption. This **MUST** be prohibited.	Not explicitly determined in the ENS. Default or complementary application: - Measure [op.exp.2] - Measure [op.exp.3] - Measure [mp.sw.1] - Measure [mp.info.1] - Measure [mp.info.3]
O.PD_15	The application **MUST** provide locally stored data through a secure connection to the device.	- Art. 22. - Measure [op.pl.2] - Measure [mp.eq.3]
O.PD_16	If the platform does not protect against theft of the selected storage medium (e.g. by using unencrypted SD cards), the application **MUST** inform the user of the risk when the storage medium in question is selected. <u>Note / example</u>: Data encryption at application level must be maintained in any case.	Not explicitly determined in the ENS. Default or complementary application: - Measure [op.exp.2] - Measure [op.exp.3] - Measure [mp.sw.1] - Measure [mp.info.1] - Measure [mp.info.3]
O.PD_17	The application **MUST** ensure that all sensitive data and specific login information stored on the device is completely deleted when the application is uninstalled.	Not explicitly determined in the ENS. Default or complementary application: - Art. 19.

		- Art. 21. - Measure [op.exp.2] - Measure [op.exp.3] - Measure [mp.sw.1] - Measure [mp.info.1]
O.PD_18	The application **MUST** provide the user with the option that all sensitive data and application-specific access information is also completely removed from the *backend* when the application is uninstalled. If the user decides not to delete the data in the *backend*, a maximum retention period **MUST** be defined. The user **MUST** be informed of the length of the retention period. After this period has expired, all sensitive data and application-specific login information **MUST** be completely deleted. The user **MUST** be given the opportunity to completely delete all data, even before the end of the retention period. <u>Note/Example</u>: Allow for device change, without loss of history.	Not explicitly determined in the ENS. Default or complementary application: - Art. 19. - Art. 21. - Measure [op.exp.2] - Measure [op.exp.3] - Measure [mp.sw.1] - Measure [mp.info.1]
O.PD_19	To counteract possible data misuse after the loss of a device, the application **CAN** implement a "kill switch", i.e. an intentional and secure overwriting of user data on the device at the application level, activated by the *backend*. The manufacturer **MUST** implement strong authentication mechanisms through the *backend* to prevent unintended activation of the kill switch by the user.	Not explicitly determined in the ENS. Default or complementary application: - Art. 19. - Art. 21. - Measure [op.exp.2] - Measure [op.exp.3] - Measure [mp.sw.1]

3.1.8 OBJECTIVE (8): PAYMENT RESOURCES

Concept	Description	RD 3/2010 (ENS)
O.Payment_1	The application request **MUST** indicate to the user which services are subject to additional costs.	Not explicitly determined in the ENS.
O.Payment_2	The application **MUST** obtain the user's consent before taking any action that is subject to a charge.	Not explicitly determined in the ENS. Default or complementary application: - Art. 16. - Measure [op.exp.2] - Measure [mp.info.1]
O.Payment_3	The application **MUST** obtain the user's consent before requesting access (e.g. Android permissions) to payment resources. Note / example: Sending SMS may involve costs and therefore must require consent.	Not explicitly determined in the ENS. Default or complementary application: - Art. 16. - Measure [op.exp.2] - Measure [mp.info.1]
O.Payment_4	The application **CAN** obtain the user's permanent consent to access frequently used payment resources, to the extent that this is appropriate for the purpose of the application.	Not explicitly determined in the ENS. Default or complementary application: - Art. 16. - Measure [op.exp.2] - Measure [mp.info.1]
O.Payment_5	The application **MUST** allow the user to withdraw the consent previously given.	Not explicitly determined in the ENS. Default or complementary application: - Art. 16.

		- Measure [op.exp.2] - Measure [mp.info.1]
O.Payment_6	The application **SHOULD** store in the *backend* the history of all payments made. The transaction history, including the metadata, **MUST** be treated as sensitive data according to [O. Purpose_8].	Not explicitly determined in the ENS. Default or complementary application: - Art. 16. - Measure [op.exp.2] - Measure [mp.info.1]
O.Payment_7	If the application offers payment features, the manufacturer **MUST** implement a policy that prevents third parties from tracking payment flows for the use of the application's features. Note/example: Processing of recurring payments is one possible method of hiding the actual intensity and frequency of use from third parties.	Not explicitly determined in the ENS. Default or complementary application: - Art. 16. - Measure [org.1] - Measure [op.exp.2] - Measure [mp.info.1]
O.Payment_8	The application **MUST** provide the user with an overview of the costs incurred. If the costs are due to individual accesses, the application **MUST** show an overview of the accesses.	Not explicitly determined in the ENS.
O.Payment_9	Validation of payment transactions **MUST** be carried out in the *backend*.	Not explicitly determined in the ENS.
O.Payment_10	Third party payment procedures **MUST** comply with the requirements of the third party software (see Section 3.1.4).	Not explicitly determined in the ENS.

3.1.9 OBJECTIVE (9): NETWORK COMMUNICATION

Concept	Description	RD 3/2010 (ENS)
O.Red_1	All communication of the application over the network **MUST** be encrypted with TLS all the time.	- Art. 21. - Art. 22. - Measure [mp.com.3]

		- Measure [mp.info.3] - Measure [mp.s.2]
O.Red_2	The configuration of TLS connections **MUST** be state-of-the-art and follow current best practice recommendations[27].	- Art. 21. - Art. 22. - Measure [mp.com.3] - Measure [mp.info.3] - Measure [mp.s.2]
O.Red_3	To establish secure channels, the application **MUST** use the security functionality of the operating system platform or security tested *frameworks* or libraries.	- Art. 20. - Art. 21. - Art. 22. - Measure [op.pl.2] - Measure [op.exp.4] - Measure [mp.eq.3] - Measure [mp.com.3] - Measure [mp.info.3] - Measure [mp.s.2]
O.Red_4	The application **MUST** be based on an appropriate hierarchy of certificates, i.e. it **MUST NOT** accept certificates whose chain of trust is not considered secure by the manufacturer[28].	- Art. 33. - Measure [op.pl.2] - Measure [op.acc.5] - Measure [op.exp.4] - Measure [mp.info.4] - Measure [mp.s.2]
O.Red_5	The application **MUST** check the *backend* server certificate.	- Art. 33. - Measure [op.pl.2] - Measure [op.acc.5] - Measure [op.exp.4] - Measure [mp.info.4] - Measure [mp.s.2]
O.Red_6	The *backend* **MUST** reject connections where the protocol version or encryption suite does not comply with the applicable regulations[29].	- Art. 21. - Art. 22 - Measure [mp.com.3] - Measure [mp.info.3] - Measure [mp.s.2]

[27] Véase, por ejemplo: BSI: Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths - Part 2 - Use of Transport Layer Security (TLS)

[28] See: C. Evans, C. Palmer, R. Sleevi, Google Inc, "Public Key Pinning Extension for HTTP", April 2015 version, available at: https://tools.ietf.org/html/rfc7469

[29] Por ejemplo: BSI: Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths - Part 2 - Use of Transport Layer Security (TLS)

O.Red_7	The application **MUST** validate the integrity of the *backend* responses.	- Measure [mp.com.3] - Measure [mp.s.2]
O.Red_8	The application **MUST** disable platform-specific rollback mechanism (e.g., opting out of clear text traffic).	Not explicitly determined in the ENS.
O.Red_9	The application **SHOULD** keep log files in the *backend* for all established connections. When using intermediate proxy servers, you **MUST** ensure that HTTP headers are captured completely (e.g. X-forwarded-for).	- Art. 14. - Art. 23. - Measure [op.exp.8] - Measure [op.exp.10]
O.Red_10	An aborted start **MUST** be registered as a security event in the *backend*.	- Measure [op.exp.7] - Measure [op.exp.8] - Measure [op.exp.9] - Measure [op.exp.10]

3.1.10 OBJECTIVE (10): SPECIFIC PLATFORM INTERACTIONS

Concept	Description	RD 3/2010 (ENS)
O.Plat_1	To use the application, the terminal device **MUST** have device protection (password, pattern lock, etc.). The manufacturer **MUST** inform the user of the consequences of not having the protection activated.	- Art. 16. - Art. 19. - Art. 21. - Measure [op.pl.2] - Measure [op.acc.5] - Measure [op.acc.6] - Measure [op.exp.2] - Measure [mp.eq.2]
O.Plat_2	The application **MUST NOT** request any permission other than that required to fulfill its main purpose.	- Art. 16. - Measure [op.pl.2] - Measure [op.exp.2] - Measure [op.exp.3] - Measure [mp.sw.1] - Measure [mp.sw.2] - Measure [mp.info.1]
O.Plat_3	The application **MUST** inform the user of the purpose of the permissions being requested and the consequences if the user does not grant them.	Not explicitly determined in the ENS. Default or complementary

		application: - Art. 16. - Measure [op.pl.2] - Measure [op.exp.2] - Measure [op.exp.3] - Measure [mp.sw.1] - Measure [mp.sw.2] - Measure [mp.info.1]
O.Plat_4	The application **CAN** provide the user with options to display messages and notifications, including those with sensitive content, if appropriate. By default, it **MUST** be disabled.	Not explicitly determined in the ENS. Default or complementary application: - Art. 16. - Measure [op.pl.2] - Measure [op.exp.2] - Measure [op.exp.3] - Measure [mp.sw.1] - Measure [mp.sw.2] - Measure [mp.info.1]
O.Plat_5	The application **SHOULD** restrict access to the designated file paths. Note / example: For example, making a white list of file paths.	Not explicitly determined in the ENS. Default or complementary application: - Art. 16. - Measure [op.pl.2] - Measure [op.exp.2] - Measure [op.exp.3] - Measure [mp.sw.1] - Measure [mp.sw.2]
O.Plat_6	The application **MUST** implement access restrictions to all data.	- Art. 16. - Art. 19. - Measure [op.pl.2] - Measure [acc.op.*]
O.Plat_7	The application **MUST** restrict broadcast messages to authorised applications only.	- Art. 16. - Art. 19. - Measure [op.pl.2]

		- Measure [acc.op.*]
O.Plat_8	The application **MUST NOT** send any sensitive data in the broadcast messages.	- Art. 16. - Art. 19. - Measure [op.pl.2] - Measure [mp.info.1]
O.Plat_9	The provision of sensitive functionality through communications between processes **SHOULD** be avoided. If the offering is necessary to fulfill the purpose, the offered functionalities **MUST** be adequately protected.	- Art. 16. - Measure [op.exp.2] - Measure [op.exp.3] - Measure [op.sw.1]
O.Plat_10	The application **SHOULD** prevent JavaScript from being active while using WebView. If JavaScript is indispensable to the application, the application **MUST** reject JavaScript from sources outside the control of the manufacturer.	- Art. 20. - Measure [op.exp.1] - Measure [op.exp.4] - Measure [op.sw.1]
O.Plat_11	If the application changes to the background, it **MUST** remove all sensitive data from the current view (iOS Views and Android Activities).	Not explicitly determined in the ENS. Default or complementary application: - Measure [mp.info.1]
O.Plat_12	The application **MUST** disable any protocol handler that is not needed in WebViews.	- Art. 16. - Art. 19. - Measure [op.exp.2] - Measure [op.exp.3] - Measure [op.sw.1]
O.Plat_13	The application **MUST** delete application-specific cookies after exiting the application.	- Measure [op.exp.2] - Measure [op.exp.3] - Measure [op.sw.1] - Measure [mp.info.1]
O.Plat_14	Upon completion, the application **MUST** securely overwrite all user-specific data in the working memory.	- Measure [op.exp.2] - Measure [op.exp.3] - Measure [op.sw.1] - Measure [mp.info.1]

3.1.11 OBJECTIVE (11): RESILIENCE

Concept	Description	RD 3/2010 (ENS)
O.Resi_1	The application **MUST** provide the user with accessible best practice recommendations for the secure use of the application and its configuration.	- Measure [org.2] - Measure [org.3] - Measure [mp.sw.1]
O.Resi_2	The application **MUST** detect *rooted* or *jailbroken* devices according to the current state of the art and respond accordingly. The manufacturer **MUST** point out the risks to the user's data if the application is continued (e.g. that data may be disclosed). Another appropriate response would be to terminate the application.	- Measure [org.2] - Measure [mp.sw.1] - Measure [mp.info.1]
O.Resi_3	The application **MUST** reliably detect and prevent start-up in a development/debugging environment.	- Measure [op.acc.3] - Measure [mp.sw. 1] - Measure [mp.sw.2]
O.Resi_4	The application **MUST** be aborted if it is started with unusual user rights (e.g. *root* or "*nobody*").	Not explicitly determined in the ENS. Default or complementary application: - Measure [mp.sw.1]
O.Resi_5	The application **MUST** verify the integrity of the device before processing sensitive data (such as Google Safety.Net).	- Measure [mp.com.3] - Measure [op.info.1] - Measure [mp.sw.1]
O.Resi_6	The application **MUST** verify the integrity of the *backend* before accessing it (see also O.Red_4).	- Art. 33. - Measure [op.pl.2] - Measure [mp.s.2]
O.Resi_7	The application **MUST** implement *hardening* measures, such as integrity checks, before each processing of sensitive data within the program flow.	- Art. 20. - Measure [mp.com.3]

O.Resi_8	The application **MUST** implement stringent measures against reverse engineering and **CAN** use obfuscation measures, such as code obfuscation and string encryption.	Not explicitly determined in the ENS. Default or complementary application: - Measure [mp.sw.1]
O.Resi_9	The application **MUST** implement access control mechanisms, taking into account the different platforms and their versions, in order to avoid the misuse of resources when changing the platform version and to achieve sufficient protection of all the assets in each execution environment.	- Art. 16. - Measure [op.pl.2] - Measures [acc.op.*] - Measure [mp.eq.3] - Measure [mp.s.2]