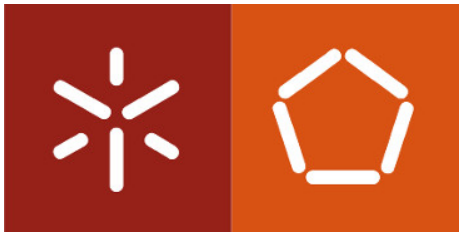
Engenharia de Segurança

23 de Março de 2021

Grupo 7	
a83899	André Morais
a84485	Tiago Magalhães

PA - Sistema de identificação eletrónica



Mestrado Integrado em Engenharia Informática
Universidade do Minho

Conteúdo

Glossário

One Time Pad Cifra de uso único, é uma técnica de criptografia que não pode ser quebrada se utilizada corretamente.

Siglas

CMD Chave Móvel Digital.

eID Sistema de identificação digital.

ENISA Agência Europeia para a Segurança das Redes e da Informação.

OTP *One Time Pad*.

1 Introdução

O objetivo deste trabalho é analisar o modelo de maturidade da ENISA e avaliar em que nível neste modelo é que se encontra o sistema de identificação português Chave Móvel Digital.

No decorrer do relatório faremos uma breve explicação sobre o sistema de identificação eletrónica Chave Móvel Digital, sobre do que se trata o modelo de maturidade e como é avaliado e por fim faremos uma análise a enquadrar o sistema CMD neste mesmo modelo.

2 Chave Móvel Digital

A Chave Móvel Digital é um serviço de identidade digital *online* que tem como objectivo:

- Autenticar cidadãos portugueses e estrangeiros, quando acedem a serviços em portais e *websites* de entidades públicas ou privadas, com dois fatores de segurança: uma palavra-chave e um código recebido;
- Permitir assinar digitalmente documentos.

A Chave Móvel Digital serve, assim, como uma prova administrativa de identidade, associando um número de telemóvel ao número de identificação civil para um cidadão português, e o número de passaporte ou título/cartão de residência para um cidadão estrangeiro.

3 ENISA - Modelo de Maturidade

O modelo de maturidade elaborado pela ENISA tem como objetivos:

- Promoção das melhores práticas nos sistemas de identificação digital, confiando na informação fornecida no contexto dos esquemas de sistemas de identificação digital notificados;
- Aperfeiçoamento para sistemas já existentes.

3.1 Arquitetura - Modelo de Maturidade

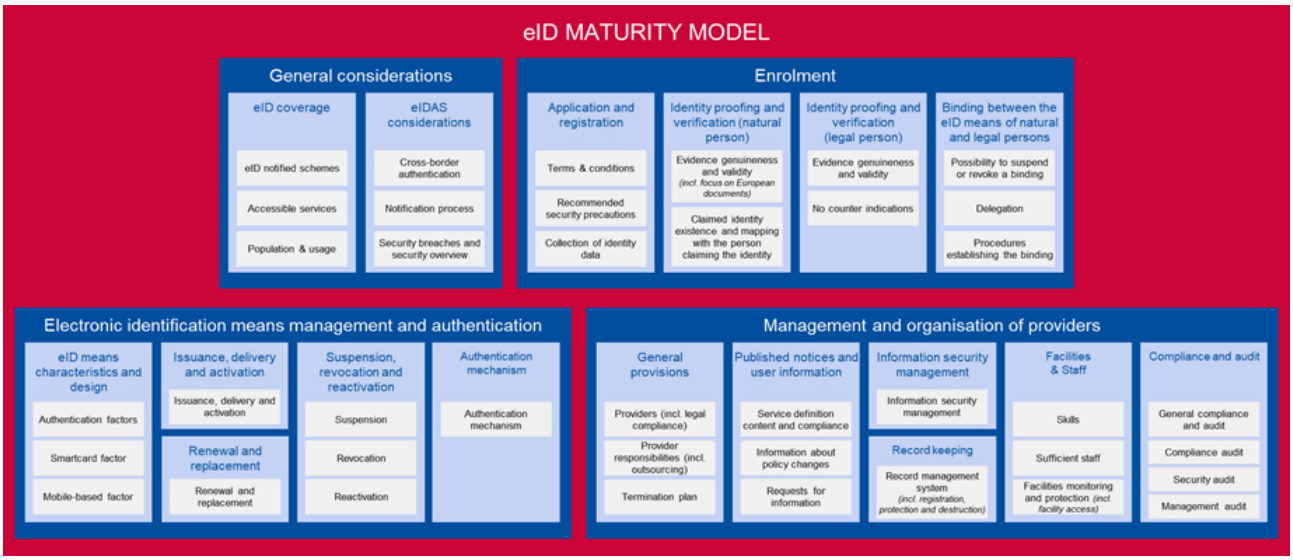


Figura 1: Arquitetura do modelo de maturidade

Como se pode observar pela imagem anterior(Figura 1) o modelo de maturidade encontra-se dividido em quatro dimensões:

- Geral - Avalia o nível de maturidade do sistema de modo geral;
- Registo - Avalia a maturidade ao nível da inscrição/registo para acesso ao sistema de identificação;

- Meios de gestão de identificação eletrónica e autenticação - Avalia o nível de maturidade de como é processado o mecanismo de autenticação e de organização;

- Organização e gestão de fornecedores - Avalia o nível de maturidade de como se desenrola o processo de gestão das entidades que fornecem o servido de identificação.

Também se encontra dividido por fatores e aspeto, sendo estes representados na imagem antreiror pelos quadrados de cor azul claro e branco respetivamente.

Os fatores e os aspetos representam maiores especificidades, isto é, cada dimensão tem um conjunto de fatores que identificam as diferentes nuances dentro da dimensão, por sua vez os fatores compreendem um número de aspetos que fornecem questões, que indicam em quantas partes diferentes um fator pode ser entendido.

3.2 Mecanismo de pontuação

Este modelo de maturidade avalia o sistema com base em dois parâmetros, o **nível de maturidade** e o **índice de cobertura**, cada um destes parâmetros pode ser calculado por aspeto, dimensionalmente e globalmente.

3.2.1 Níveis de Maturidade

Representam níveis crescentes de maturação, começando no nível inicial, **nível 1**, um eID com segurança e maturidade limitada, acabando com o **nível 5**, sendo este o maior nível de segurança e de maturidade existente. Os níveis de maturação são propostos para estruturar as melhores práticas e medir as melhorias alcançadas quando relevantes.

3.2.2 *Coverage Ratio*

O *coverage ratio* (Índice de cobertura/abrangência) mostra o grau de cobertura de todos os indicadores de níveis superiores ao do nível de maturação, para quais a resposta é positiva de forma a indicar os esforços feitos para atingir um nível de maturidade superior.

É um valor complementar calculado como a proporção entre o número de questões e o número de questões em que a resposta é positiva. Todas as questões respondidas com **N/A** ou **?** não entram na contagem.

4 Análise e Avaliação da Maturidade do sistema CMD

Para a avaliação do nível de maturidade do serviço CMD, decidimos avaliar de acordo com os aspetos, de forma a identificarmos e percebermos mais facilmente onde se encontram a principais lacunas deste.

4.1 *General Dimension*

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
eID coverage	eID notified schemes	Does the member state have enacted legislation for eID?	S	Does the member state have eID schemes (incl. not notified ones)?	S	Does the member state have at least 1 notified eID scheme?	S	Does the member state have notified eID schemes with different authentication factors?	S	In line with the importance of having mobile-based eID schemes for citizens, can one of the notified eID schemes be used within a mobile environment?	S
	Accessible services	Have you identified the benefits when providing digital public services to citizens and businesses?	S	Do you have a roadmap or a strategy to build and maintain secure national electronic identification schemes (eIDs) for citizens and businesses?	S	Is the eID roadmap documented and steered, detailing clear actions for the implementation of the strategy and the involvement of various stakeholders?	S	Is the eID roadmap managed by an official national body?	S	Is the eID roadmap steered and monitored with relevant KPIs? (e.g. end-user satisfaction, eID downtime, user preferences)	?
		Do the country's eID schemes enable access to at least one digital public service?	S	Is there an inventory of services offered digitally and through eID means?	S	Do the country's eID schemes enable access to multiple federal public services?	S	Do the country's eID schemes enable access to multiple federal and regional public services?	S	Does the country eID schemes enable access to multiple federal, regional and local public services?	S
				Do the country's eID schemes enable access to at least ten digital public services?	S	Do the country's eID schemes enable access to a few private services such as utility, medical or banking services?	S	Do the country's eID schemes enable access to multiple private services?	S		
				Do the country's eID schemes enable access to at least one private service?	S			Do the country's eID schemes enable access to the country's most popular services?	S		
	Population & usage					If eID means are issued to natural persons, can citizens who live abroad obtain one of the eID means?	S	If eID means are issued to natural persons, can citizens from other member states who live in the member state that issues the eID means in question, obtain one of the eID means?	S	If eID means are issued to natural persons, can non-EU citizens who live in the member state, obtain one of the eID means?	S
						If Eid means are issued to natural persons, can minors have one of the Eid means?	S			Are the country's Eid means issued to both natural and legal persons?	N
								If the Eid mean is issued to natural persons, are the processes adapted to people with disabilities (e.g. visually impaired)?	S	Is there a national awareness program in place regarding the Eid?	N
		Is the adoption rate of the Eid scheme tracked (i.e. the number of Eid means issued)?	S	Compared to the targeted population, is the adoption rate at least 10%?	S	Is the adoption rate at least 20%?	S	Is the adoption rate at least 40%?	N	Is the adoption rate at least 60%?	N

				Is the utilization rate of the Eid scheme tracked (i.e. number of active users per month vs. number of issued Eid means)?	?	Is the utilization rate at least 15% per month?	?	Is the utilization rate at least 30% per month?	?	Is the utilization rate at least 50% per month?	?
eIDAS considerations	**Cross-border authentication**			Are the member state's digital services accessible to other European citizens using their own eID means?	N	Is the number of successful cross-border authentications tracked?	N	Is the percentage of services offered locally vs cross-border tracked?	N	Is there a significant number of successful cross-border authentications to digital services of the member state?	N
	Notification process	Does the member state have an officially designated body to perform the notification process?	S			Is the notification process documented?	S	Is the notification process documented and applied?	S	Is the notification process subject to continuous improvement?	?
						Does the notification process include an internal review?	S				
		Is there a mechanism in place to make the Commission aware of any subsequent change to a notified eID scheme, at least in the 12 months?	N	Is the Commission made aware of any subsequent change to a notified eID scheme in the 6 months following this change?	N	Is the Commission made aware of any subsequent change to a notified eID scheme in the 3 months following this change?	N	Is the Commission made aware of any subsequent change to a notified eID scheme in the month following this change?	N	Is the Commission made aware of any subsequent change to a notified eID scheme before the change takes place?	N
						Are the notification documents detailed enough to allow other member states to efficiently review the eID scheme in a timely manner?	S	Is the member state responsive enough to answer questions from peer reviewers during the notification process?	S	Is there a strategic guidance document regarding the notification process?	S
						Does the member state regularly inform the CN of the state of implementation of the commitments taken during the peer review process, as reflected in the opinions adopted by the CN?	N	Before notifying an eID scheme, are there discussions with other member states who previously notified a scheme to gather initial feedback and speed-up the notification process?	S	Is the peer review report published publicly (without any confidential information) at the end of the peer review process?	N

			Does the member state actively participate in the peer review processes?	S	Does the member state have representatives as observers to peer reviews (at least 50%) or active members to at least 30% of peer reviews?	N	Does the member state have representatives as observers to at least 75% of peer reviews and active members to at least 50% of these reviews?	N	Does the member state have representatives as observers to at least 90% of peer reviews and active members to at least 75% of these reviews (incl. rapporteur)?	N
Security breaches and security overview	Does the member state have at least an informal group assigned to inform the other member states and the Commission of any breach or compromise?	S	Does the member state have a formal group assigned to inform the other member states and the Commission of any breach or compromise?	S	Is the security breach process documented (including at least the suspension or revocation of the eID scheme)?	S	Is the security breach process documented and applied?	S	Is the security breach process subject to continuous improvement?	S
	Is the Commission made aware of any security breach within 3 months following the identification of the breach?	?	Is the Commission made aware of any security breach within 1 month following the identification of the breach?	?	Is the Commission made aware of any security breach within 2 weeks following the identification of the breach?	?	Is the Commission made aware of any security breach within 1 week following the identification of the breach?	?	Is the Commission made aware of any security breach within 3 day following the identification of the breach?	?
	Does the member state have at least an informal body to monitor security breaches of eID schemes?	S	Does the member state have an officially designated body to monitor security breaches of eID schemes?	S			Is there a documented and applied process to monitor security breaches of eID schemes?	?	Is the process to monitor security breaches of eID schemes subject to continuous improvement?	?
	Does the member state have enacted legislation for eID?	S	Is there an incident response plan including the withdrawal of the eID scheme and the subsequent notification of other member states and of the Cooperation Network if a breach or compromise is not remedied within three months of the suspension or revocation?	S			Does the member state monitor security breaches of other member states eID schemes?	N	Does the member state or the eID provider carry out a technological watch on electronic identification means and solutions as well as on the evolution of the threat landscape in this area?	S

4.1.1 Pontuação

4.1.1.1 *eID notified schemes*

- **Nível de Maturidade**: Nível 5
- ***Coverage Ratio***: **100%**

4.1.1.2 *Acessible Services*

- **Nível de Maturidade**: Nível 5
- ***Coverage Ratio***: **100%**

4.1.1.3 *Population & usage*

- **Nível de Maturidade**: Nível 3
- ***Coverage Ratio***: **67%**

4.1.1.4 *Crossborder authentication*

- **Nível de Maturidade**: Nível 1
- ***Coverage Ratio***: **0%**

4.1.1.5 *Notification process*

- **Nível de Maturidade**: Nível 0
- ***Coverage Ratio***: **47%**

4.1.1.6 *Security breaches and security overview*

- **Nível de Maturidade**: Nível 3
- ***Coverage Ratio***: **91%**

4.1.2 Principais lacunas

Nesta dimensão a principais lacunas encontram-se ao nível dos aspetos, do processo de notificação, em que não existe nenhum mecanismo para informar a comissão em caso de existência de alterações na arquitetura do sistema, da interoperabilidade do mecanismo de autenticação com sistemas de identificação digital de outros estados europeus.

Também os níveis de adoção não são os mais elevados de modo a permitir que o aspeto do Uso e da População tenha um nível de maturidade máximo, talvez isso deva-se ao facto de não existir um programa nacional de consciencialização.

4.2 *Enrolment Dimension*

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
Application and registration	Terms & conditions	Is the applicant aware of the terms and conditions (T&C) related to the use of the electronic identification means during the enrolment process?	S	Is there a web portal informing users about the functions and use of the eID?	S	Does the applicant need to agree to the T&C before starting the registration?	S	Does the applicant need to sign the T&C?	S	Is the service definition translated into most common European languages?	S
				Is informational material offered to the applicant to communicate the T&C effectively, through a brochure or a downloadable file through a mobile app for example?	S	Can a printout of the T&C be delivered to the applicant?	S	If the signature can be provided electronically, can the applicant sign the T&C with a qualified electronic signature?	N/A	Is the agreement to the T&C archived?	S
	Recommended security precautions	Is the applicant made aware of recommended security precautions related to the use of the electronic identification mean during the enrolment process?	S	Is there a web portal informing users about the recommended security precautions related to the eID means?	S	Does the applicant need to agree to the recommended security precautions before starting the registration?	S	Does the applicant need to sign the recommended security precautions?	S	Are the recommended security precautions regulated or included in National legislation?	S
				Is informational material offered to the applicant to effectively communicate the recommended security precautions, through a brochure for example?	S	Can the security recommendations be delivered to the applicant?	S	Are the security precautions updated when necessary?	S	Does the National legislation include recommended security precautions as well as updated precautions when relevant?	S
						If the eID is mobile-based and optionally allows users to store the keys in Trusted Execution Environments (TEEs) or Secure Enclaves (SEs), are the two options presented to the user by clearly	N/A				

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
						indicating that not using the TEE/SE is less secure?					
	Collection of identity data (incl. representativeness, e.g. for someone legally incapable)					Is the process to collect identity data, physically and/or remotely, documented in detail, taking into account multiple ID documents that can be used?	S	Is there a process to collect data remotely taking into account the specificities of not having the applicant physically present (e.g. asking him to perform random actions, ask for more documents, retrieval in person of the eID, security of the transmission channel)?	S	Is the process to collect identity data regulated and updated when necessary?	S
						Is there a process for a legally incapable person to apply for an eID (incl. verification of representativeness)?	S	Does the legal representative need to have an identity document for the country to which the eID is related?	S		
						Are the requirements for identity proofing the same for the person who is legally incapable and his/her representative?	S			Is there an exceptional process where a staff member visits the residence of an applicant to collect identity data?	N
						Does the representative need to be same or another family member (if the applicant is a minor) during the enrolment phase?	N/A			If the applicant is already registered in another authoritative source (e.g. other eID or VISA application), is his/her identity data retrieved from this authoritative source to simplify the enrolment process?	S
Identity proofing and verification (natural person)	Evidence genuineness and validity (incl. focus on European documents)	Is the evidence at least assumed to be genuine through an informal process?	N	Is the evidence at least assumed to exist according to an authoritative source?	S	Is the genuineness of the evidence checked through a formal procedure?	S			Is the verification of physical security features performed on the evidence?	S
		Is the validity of the evidence assessed through an informal process?	N			Is the existence of the evidence checked against an authoritative source?	S			Is the existence of the evidence checked against multiple authoritative sources to increase the trust in the fact that this evidence exists?	S

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
						Is the evidence checked to ensure it has not been lost, stolen, suspended or revoked?	S	Is the validity of the evidence checked against an authoritative source?	S	Is the validity of the evidence checked against multiple authoritative sources?	S
						Is foreign evidence compared to sample documents from another member state (e.g. PRADO and EDISON)?	N	Are European databases used to validate the authenticity and validity of the evidence (e.g. Schengen Information System, the INTERPOL database of lost and stolen documents, iFADO: Internet False and Authentic Documents Online)?	N	Should foreign identification documents be registered in an authoritative source by national authorities?	S
						If the identity proofing is automated and not successful, is manual verification performed as a backup process to proceed with the verification?	S			If the identification process is performed remotely does it rely on an evidence using an electronic chip (read with NFC or a contact card reader with a PIN) to check its authenticity and retrieve the data?	S
						If the identification process is performed remotely, is the authenticity of the evidence checked, for example with Machine Readable Zone (MRZ) or optical security features (photographs, font type, quality, holograms, laminate integrity, spelling mistakes, print quality, etc.)?	S			Is the identity verification performed by certified suppliers for identity verification (e.g. ETSI QTSP services or equivalent)?	S
										Is there a formal internal process to assume, check and validate the evidence?	S
										Are there KPIs to check the performance of the enrolment phase?	S

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
	Claimed identity existence and mapping with the person claiming the identity	Is the existence of claimed identities validated by an authoritative source?	S	Are steps taken to minimize the risk that the person's identity is not the claimed identity?	S			When there is a photo or biometric identification evidence recognised by the member state, are the applicants identified as the claimed identity through comparison of one or more physical characteristics of the person with an authoritative source?	S	Is there an alternative process in case of doubt that the applicant is who he claims to be?	S
		Can it be assumed that the person claiming the identity is one and the same?	S	If the identification process is performed remotely, is more than one document asked to prove the identity existence and mapping?	N	If the identification process is performed remotely, is anti-spoofing liveness detection implemented?	S	If the identification process is performed remotely, is there a check of the pictures taken against an authoritative source?	S	If the identification process is performed remotely, is anti-deepfake attacks implemented?	N/A
						If the identification process is performed remotely, does an agent compare the pictures that were taken against the picture on the evidence?	N	Are checks performed to see if the applicant has previous encounters with the member state to ensure there is no counter indication to provide the applicant with an eID?	N/A		
Identity proofing and verification (legal person)	Evidence genuineness and validity	Is the evidence at least assumed to be genuine?	N/A	Is the evidence at least assumed to exist according to an authoritative source?	N/A	Is the genuineness of the evidence checked?	N/A	Is the evidence checked to ensure it has not been lost, stolen, suspended or revoked?	N/A	Is the validity of the evidence checked against an authoritative source?	N/A
		Is the validity of the evidence assessed?	N/A			Is the existence of the evidence checked against an authoritative source?	N/A				
	No counter-indications									Is the legal person checked to not be in a status that would prevent the natural person from acting on the behalf of that legal person (e.g. bankruptcy, financial status)?	N/A
Binding between the electronic identification means of	Possibility to suspend or revoke a binding	Is it possible to suspend and/or revoke a binding?	N/A							Is the life cycle of a binding (e.g. activation, suspension, renewal, revocation) administered according to nationally recognised procedures?	N/A

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
natural and legal persons	Delegation	Can the natural person whose electronic identification means is bound to the electronic identification means of the legal person delegate the exercise of the binding to another natural person?	N/A							Can the natural person whose electronic identification means is bound to the electronic identification means of the legal person delegate the exercise of the binding to another natural person on the basis of nationally recognised procedures?	N/A
	Procedures establishing the binding	Is the binding established on the basis of nationally recognized procedures?	N/A	Is the binding registered in an authoritative source?	N/A	Is there a direct extract from the authoritative source in the application?	N/A	Is the status and position of the natural person in the legal person's organisation verified, including the fact that there are no restrictions for this natural person to represent the legal person?	N/A	Is there a process to manage the fact that the applicant is not listed as a legal representative?	N/A
						Is the involvement of the natural person with the legal person verified?	N/A			Is the evidence of the binding stored and attached to the application?	N/A

4.2.1 Pontuação

4.2.1.1 *Terms & Conditions*

- **Nível de Maturidade**: Nível 5
- ***Coverage Ratio***: **100%**

4.2.1.2 *Recommended security precautions*

- **Nível de Maturidade**: Nível 5
- ***Coverage Ratio***: **100%**

4.2.1.3 *Collection of identity (incl. representativeness, e.g. for someone legally incapable)*

- **Nível de Maturidade**: Nível 4
- ***Coverage Ratio***: **87,5%**

4.2.1.4 *Evidence genuineness and validity (incl. focus on European documents)*

- **Nível de Maturidade**: Nível 0
- ***Coverage Ratio***: **79%**

4.2.1.5 *Claimed identity existence and mapping with the person claiming the identity*

- **Nível de Maturidade**: Nível 1
- ***Coverage Ratio***: **78%**

4.2.1.6 *Identity proofing and verification (legal person)*

Uma vez que não se aplica para este sistema, não há pontuação para este fator.

4.2.2 Principais lacunas

Uma das principais lacunas que não permite que o sistema no aspeto *Evidence genuineness and validity (incl. focus on European documents)* possua nível máximo, deve-se ao facto de não existir integração com bases dados europeias e documentos europeus, tal como processos informais para verificação pessoal.

No aspeto *Claimed identity existence and mapping with the person claiming the identity*, não existe nível máximo, pois o processo de identificação feito remotamente não necessita de mais de que um documento para provar identidade, nem de um agente para comparar fotografias.

No aspeto *Collection of identity (incl. representativeness, e.g. for someone legally incapable)*, o nível máximo não é atingido, em consequência da não existência de um procedimento excepcional para membros do *staff* irem requisitar dados à residencia do candidato.

4.3 *eID means Management and Authetication Mechanism Dimension*

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
Electronic identification means characteristics and design	Authentication factors	Does the eID means utilise at least one authentication factor?	N/A	Does the eID means utilise at least two authentication factors from different categories?	S	Are multiple options offered to users as a second factor for authentication?	S				
		If one authentication factor is a password or a PIN, is it chosen by the user?	S	If one authentication factor is a password, should it be changed on a regular basis?	N	If one authentication factor is a password or a PIN, does it have a minimum length and a complexity policy (e.g. for password: at least 8 characters, contains at least one uppercase, one lowercase, one number and one special character; for PINs: forbid identical digits, sequences of numbers or palindromes) in accordance with the desired attack potential to protect from?	S	Does the possession factor include a hardware cryptographic module (e.g. a smartcard or secure enclaves on smartphones)?	S	Is there a process on how to design and implement cryptographic algorithms, and to monitor if they get outdated?	S
				If one authentication factor is a password or a PIN, is the password reset process secure to at least assume only the user can perform it, in accordance with the desired attack potential to protect from? (e.g. leverage security questions or a previously entered email address)	S	Is the use of deprecated cryptographic algorithms forbidden?	S	For 2-factor eID schemes, is OTP SMS forbidden as an authentication factor?	N	If a cryptographic algorithm used is not state of the art, is there a defined phasing out strategy and a timely reporting to the Cooperation Network, in accordance with the desired attack potential to protect from?	N/A
				Is OTP email forbidden as a second factor because of the risk that an e-mail account can be taken over by an attacker?	N	Are some security measures in place to ensure the security of the OTP SMS (e.g. increase security of the protocol by mobile operators, measures to avoid SIM swapping, monitoring and detection processes, controls using	S	Are the FAR (False Acceptance Rate) and resistance against presentation attacks of biometrics recognition tracked over time to ensure it does not bring a vulnerability to the authentication process	N/A	For 2-factors eID schemes, are biometrics avoided when not secure enough, in accordance with the desired attack potential to protect from?	N/A

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
						national sources that the mobile phone belongs to the user), in accordance with the desired attack potential to protect from?		and that acceptable thresholds to protect against desired attack potential are not exceeded?			
				Is 2D facial recognition forbidden as an authentication factor because of the risk introduced by using a picture instead of capturing the person in real time?	N/A	Is the biometrics recognition algorithm tested and benchmarked using market-known procedures?	N/A	Is smartphone-embedded fingerprint recognition avoided as an authentication factor (the risks being that multiple fingerprints belonging to multiple people can be saved, fingerprint recognition is not immune to circumvention and it raises privacy concerns because fingerprints can be collected without the user's consent)?	N/A		
	Smartcard factor	Is the eID mean designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs?	N/A	For contactless smartcard, are there security measures in place to avoid non-authorised readings by a card reader in close proximity, in accordance with the desired attack potential to protect from?	N/A	Is the smartcard (contact or contactless) certified according to an applicable security framework, in accordance with the desired attack potential to protect from?	N/A	If a security weakness is detected in the microchip of a smartcard, is its use forbidden in a timely matter, in accordance with the desired attack potential to protect from?	N/A	Is the smartcard certified as QSCD or equivalent?	N/A
								If the eID mean is based on a contactless smartcard, is it ICAO compliant?	N/A	In addition to the Common Criteria, is the smartcard security assessed over time (e.g. cryptographic review, periodic recertification, yearly report), through a national certification framework (as an example)?	N/A

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
								Is the microchip security level evaluated against the Common Criteria framework with an Evaluation Assurance Level (EAL) 4 augmented with AVA_VAN.5 (Vulnerability Assessment and Analysis) to ensure protection against attackers with high potential, according to the state of the art?	N/A		
	Mobile-based factor	Is the eID means designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs?	N/A	Is the mobile registration procedure secured via a code sent via SMS?	N/A	Can the user reasonably know if the request came from the service to which the user is trying to authenticate, for example to avoid phishing attacks (e.g. by displaying the same code or picture on both devices)?	N/A	Is the context of the authentication presented to the end-users (e.g. access to a given website, approving a payment for a given amount, etc.) in order to offer additional protection against social engineering attacks?	N/A	Is the security of the mobile application assessed in order to obtain comparable assurance to certification that proves the resistance against attackers with the targeted attack potential?	N/A
				Is a security code needed to unlock the mobile application?	N/A			Are the secret keys envisaged to be stored in Trusted Execution Environments (TEEs) or Secure Enclaves (SE) or SIM card?	N/A	Are smartphones SEs/TEEs' security regularly reviewed and excluded when they have known vulnerabilities, in accordance with the desired attack potential to protect from?	N/A
				Are the keys stored in software keystores of Android and iOS?	N/A			Are smartphones excluded from the eID scheme if they are considered insecure (e.g. rooted or jailbroken device, weak PIN code), in accordance with the desired attack potential to protect from?	N/A	Is the security of mobile device SEs/TEEs assessed in order to obtain comparable assurance to certification that proves the resistance against attackers with the targeted attack potential, and to increase the number of supported smartphones that provide certified SEs/TEEs?	N/A
Issuance, delivery and activation	**Issuance, delivery and activation**	Is the eID means delivered via a mechanism by which it can be at least assumed to	S	Is the activation PIN or equivalent randomly generated?	S	If a PIN or a card is sent by mail, is the envelope not conveyed through the registration office in order to	N/A	If the delivery is not remote, is the eID card handed over to the applicant in person or to a person entitled by the	N/A	Is the delivery of the eID means regulated by national law and is the legislation updated when necessary?	S

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
		reach only the intended person?				reduce the risk of internal fraud?		applicant to receive the card?			
				If the delivery is remote and if the eID means and the PIN code (or equivalent) are sent by mail, are they sent in two different letters?	N/A	If the delivery is remote and if the eID means and the PIN code (or equivalent) are sent by mail, are the two letters sent on different days with a different "look and feel"?	N/A	If the delivery is remote, are the letters sent as registered mails with return receipts?	N/A	If the delivery is postal, is it available only for whitelisted countries, whose list is managed by a national authority? Whitelisting countries could take into account the adequate training and qualifications of the postal services.	N/A
						Is the PIN or equivalent protected in order to avoid and detect unauthorised access by others, for example by a tamper-evident scratch code?	S	If an authentication factor is sent via mail, should the applicant confirm he/she received the letter containing the PIN or equivalent?	N/A	Is the activation data (e.g. the activation PIN) not stored nor retained once it is handed over to the applicant?	N
						If an activation code is sent via email, does the link have a limited lifetime of a few minutes or can only be used once?	N/A	Does the activation require a second factor? (e.g. card and PIN, or PIN + OTP)	S		
Suspension, revocation and reactivation	**Suspension**	If it is possible to suspend an eID mean, can it be achieved in a timely and efficient manner (from the suspension request to the actual suspension of the eID mean)?	S	Can users ask for suspension 24/7?	S	If the suspension request process has a degraded version to ensure its processing time, are there additional verifications to perform in a limited timeframe before automatically revoking the eID to protect against a risk of impersonation? (e.g. a mandatory face to face at a police station before a fixed number of days)	S	Is there more than one way to request the suspension of an eID mean? (e.g. at the issuing authority, online, via a hotline, via certified electronic email or signed document with a qualified signature)	S	Is the suspension process regulated by National law and is the law updated when necessary?	S
		If it is possible to suspend an eID means, are there measures to prevent unauthorised suspensions?	S					Can both the identity provider and the user suspend an eID (e.g. based on legal or administrative order)?	S	Are potential reports for abuse and complaints regarding requests for suspension monitored?	S
		If it is possible to revoke an eID means, can it be achieved in a timely	S	Can users ask for revocation 24/7?	S	If the revocation process includes a face to face meeting, is the eID holder	S	Is there more than one way to request the revocation of an eID means? (e.g. at the	S	Is the revocation process regulated by National law and is the law updated when necessary?	S

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
	Revocation	and efficient manner (from the suspension request to the actual suspension of the eID means)?				identified by checking an authoritative source?		issuing authority, online, via a hotline, via certified electronic email or signed document with a qualified signature)			
				If it is possible to revoke an eID means, are there measures to prevent unauthorised revocations? (e.g. through face-to-face meeting or a "something you know" factor such as a revocation PIN during a remote process)	S			If, according to your organisation, preventing unauthorised revocations is considered more important than revoking as soon as there is a doubt of malicious use of an eID, are two factors from two different categories required to ask for the revocation of an eID means?	S		
	Reactivation	Are there measures to prevent unauthorised reactivation?	S	Is automatic reactivation forbidden?	S	If a suspension can be lifted online, are there sufficient measures to ensure it is performed by the owner of the eID means?	N	Must the reactivation request be checked by the issuing authority before the eID mean is reactivated?	S	Must the reactivation process include a face to face meeting to present the eID mean whose reactivation is requested?	S
		If the reactivation process exists, are the same assurance requirements (established before the suspension/revocation) still checked?	S					Are two factors from two different categories required to ask for the reactivation of an eID mean online?	N	Is the reactivation process regulated by national law and is the law updated when necessary?	S
Renewal and replacement	**Renewal and replacement**	Do the renewal and replacement processes require the same assurance requirements as the initial identity proofing and verification, or based on a valid identification means of the same, or higher, assurance level?	N/A					If the renewal and/or replacement processes are based on a valid electronic identification means, is the identity data verified with an authoritative source to ensure the personal identification data is up to date?	N/A	Does the renewal and replacement process include the same checks with these specified in the enrolment process?	N/A

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
Authentication mechanism	**Authentication mechanism**	Is the messaging channel used to exchange personal identification data between the web-browser (on a computer or a smartphone) and the service provider encrypted and authenticated, for example with the latest version of the TLS protocol, in accordance with the desired attack potential to protect from? Is the TLS protocol hardened based on recognised guides such as the French agency's (ANSSI's) or the NIST's?	S	Is the messaging channel used to exchange personal identification data between the eID means and the device in use (computer or smartphone) encrypted and authenticated, for example with the PACE protocol, in accordance with the desired attack potential to protect from?	S	Is every authentication recorded and available to the applicant through a specific application?	S	Is keeping the PIN code to unlock the cryptographic module in a cache forbidden to ensure that it must be typed for every authentication in order to prevent phishing attacks even on compromised computers or smartphones?	S	When a password/PIN is used in an eID scheme, is it verified after successfully using another factor, to avoid denial-of-service attacks by entering successive wrong passwords?	S
		Is the validity of the eID means checked during the authentication mechanism to ensure it is not suspended, revoked or expired (e.g. with a CRL or OCSP for certificates)?	S	Is the authentication mechanism secured using secure and proven protocols (e.g. SAML, OAuth, WebAuthn)?	S	If one authentication factor is a password or a PIN, is the authentication process blocked after a number of attempts, in accordance with the desired attack potential to protect from?	S			Is the PIN code typed and verified directly on the card reader (PIN Pad) to avoid storing it in the memory of the computer or the smartphone?	N/A

4.3.1 Pontuação

4.3.1.1 *Authentication factors*

- **Nível de Maturidade**: Nível 5
- ***Coverage Ratio***: **100%**

4.3.1.2 *Smartcard factor*

Uma vez que não se aplica para este sistema, não há pontuação para este aspeto.

4.3.1.3 *Mobile-based factor*

Uma vez que não se aplica para este sistema, não há pontuação para este aspeto.

4.3.1.4 *Issuance, delivery and activation*

- **Nível de Maturidade**: Nível 4
- ***Coverage Ratio***: **83%**

4.3.1.5 *Suspension*

- **Nível de Maturidade**: Nível 5
- ***Coverage Ratio***: **100%**

4.3.1.6 *Revocation*

- **Nível de Maturidade**: Nível 5
- ***Coverage Ratio***: **100%**

4.3.1.7 *Reactivation*

- **Nível de Maturidade**: Nível 2
- ***Coverage Ratio***: **75%**

4.3.1.8 *Renewal and replacement*

Uma vez que não se aplica para este sistema, não há pontuação para este aspeto

4.3.1.9 *Authentication mechanism*

- **Nível de Maturidade**: Nível 0
- ***Coverage Ratio***: **87,5%**

4.3.2 Principais lacunas

Ao nível do fator reativação, não possui nível máximo, pois a não existe um mecanismo *online* para a reativação da CMD.

No fator *Authentication factors*, não possui nível máximo, por motivo de uso do OTP como fator de autenticação.

4.4 *Providers Management and Organisation*

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
General provisions	Providers (incl. legal compliance)	Are the providers a public authority or a legal entity recognised as such by National law of a member state?	S			To become a provider, should the legal entity go through a procedure aimed at verifying the requirements of reliability and security?	N/A	To become a provider, is the procedure based on national and European standards?	N/A	Are the statutes of the providers defined in a National legislation and is the legislation updated when necessary?	S
		Do the providers comply with any legal requirements incumbent on them?	S			Is the legal compliance of private entities specifically managed, through National legislation for example?	S			Is the legal compliance of the providers monitored by accredited bodies to ensure adoption and compliance to standards?	S
	Provider responsibilities (incl. outsourcing)	Are providers checked if they are able to demonstrate their ability to assume the risk of liability for damages, as well as for having sufficient financial resources to ensure continuity of operations and the provided services? The checks can take the form of financial and legal requirements which should be fulfilled before allowed to become a provider.	S	If the provider outsources some activities, are the new third-parties untrusted by default and are checks performed, including their security, processes, and financial situation?	?	Is there a minimum turnover required to be a provider?	N/A	If the provider is a private entity, does it provide bank and insurance guarantees?	N/A	Is the provider's responsibility guaranteed by an official national and/or public agency?	S
		Are the providers responsible for the fulfilment of any of the commitments outsourced to another entity, and compliance with the scheme policy, as if the providers themselves had performed the duties?	S	Should proofs be provided by the provider to a Supervisory Body to demonstrate that the outsourced requirements are compliant?	?	Should proofs be provided regularly by the provider to a Supervisory Body to demonstrate that the outsourced requirements remain compliant overtime?	?	If the providers are required to provide bank and insurance guarantees, are there minimum amounts required?	?	Is it forbidden for a private provider to outsource operative phases?	N/A
				If the provider outsources some activities to independent contractors, are associated requirements (such as not having trusted roles within the CA) described in internal procedures?	?	If the provider outsources some activities, is this new third-party subject to the same constraints of the provider (e.g. certifications, audits)?	?				

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
				Is outsourcing refused if there is no GDPR agreement for data processing or if the processing of personal data is occurring outside Europe?	?						
	Termination plan	For eID schemes not constituted by National law, is there an effective termination plan?	N/A			Does the private provider submit its own termination plan to authorities?	N/A			For eID schemes not constituted by National law, is the termination plan constituted by National law and regulations and are the laws and regulations updated when necessary?	N/A
Published notices and user information	**Service definition content and compliance**	Is there a service definition?	S	Does the service definition include all the following points: a privacy policy, terms, conditions, fees and limitations?	S	Is the privacy policy GDPR compliant?	S	Is the service defined in such a way that the end-user can understand it, while following GDPR principles?	S	Are the T&C regulated or included in National legislation and is the legislation updated when necessary?	S
										If the provider is a private entity, does a public authority validate the service definition?	N/A
	Information about policy changes	Are users informed in a timely fashion of any change in the service definition, or to any applicable privacy policy and T&C?	S	Is there a process determining which channels to use for each type of policy change?	S	Is there at least one channel to communicate changes that ensure the user is informed (e.g. with a formal acknowledgement of the change through the mobile app)?	S	Are the users notified when any changes to any service definition, applicable T&C or privacy policy are published, for example via email or a smartphone notification?	S	If the provider is a private entity, does a public authority validate any notification informing the modification of the service definition or any applicable privacy policy and T&C? Alternatively, is a public authority responsible for this task?	N/A
				If there is no acknowledgment of the change, are there at least 2 channels to communicate changes to users (e.g. online, mail, SMS, etc.)?	N	Can users choose how to be notified?	N			For announcements with significant changes, can all types of national media be used?	?
	Requests for information	Are there procedures and policies in place to manage requests for information and provide full and correct responses?	S	Are the users informed of the ways to perform a request for information?	S	Are there at least 2 ways to make a request?	S	Are there at least 3 ways to make a request?	S	Is at least 1 way of answering requests managed by a human with real-time interactions?	S

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
						Is at least 1 way of answering requests managed by a human?	S	Is there a chatbot, FAQ or a forum to simplify the request process and allow users to receive their answers more quickly when possible?	S	Is there an internal process providing guidelines for services related to eID after their issuance (e.g. PIN replacement, certificate renewal) to participate to the quality of the answers?	?
								Are there escalation levels to manage complex requests?	?	Is there a KPI related to the performance of the replies provided?	?
Information security management	**Information security management**	Is there an effective information security management system for the management and control of information security risks?	S			Are there documented procedures for the management and control of information security risks?	S	Is the information security management system compliant to proven standards or principles for the management and control of information security risks? It can for example be based on international standards such as ISO 27001 and ISO 9001.	S	Is the information security management system standard proven to enhance security by being locally adapted or translated from an international standard?	S
								Are the private providers obliged to share their audit results to the competent authorities?	N/A	Is the information security management system regularly audited?	S
Record keeping	**Record management system (incl. registration, protection and destruction)**	Is relevant information recorded and maintained using an effective record-management system?	S	Does this record management system take into account applicable legislation and good practices in relation to data protection and data retention?	S	Are all requests from users and the subsequent responses from the provider stored for audit purposes (e.g. over the last 24 months)?	N	Is the destruction management subject to international standards?	S	Is the record management system precisely defined in National legislation and is the legislation updated when relevant?	S
		Are records retained and protected as long as they are required for the purpose of auditing and investigation of security breaches? Does retention of records take into account national laws?	S	Are the records securely destroyed when they are no longer needed, in a way that data cannot be recovered?	S	Are users informed of the retention duration of any records of the data concerning them?	S	Are the security measures defined with a risk-based approach?	S	Is the data registration and protection based on international standards?	S
		Is the actual retention duration of records defined and documented?	S	Are organisational, physical and technology security measures	S	Are the security measures to protect records documented?	S	Do the security measures follow a market-known	S	Is the implementation of measures checked as well as their effectiveness, for	?

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
				implemented (e.g. encryption of data)?				framework (e.g. NIST, OWASP for web developments)?		example through technical inspections?	
				Is there a destruction certificate issued?	?	Are the backups subject to the same or higher security requirements than the one defined in the original data storage?	S	Are the backups stored offsite?	?	Is the destruction management defined in National legislation and is the legislation updated when necessary?	S
				Are there access management measures to access the records to ensure information is only accessible to authorised people?	S	Are access rights backward traceable (who, where, when, why the access was granted)?	S	Is each access to records tracked and available for later investigation, incl. the reason for access?	S	Is it ensured that sensitive data is restricted to the staff needed to operate by following the "need to know" approach?	?
								Are the reasons and means for collecting, keeping and handling data defined in the status of a database??	N	Is there a continuous analysis of generated audit logs, for example through a SIEM/SOC?	?
Facilities & Staff	**Skills**	Are there procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil?	S	Are the key skills and relevant trainings identified?	S	Are the identified trainings available?	S	Are background checks performed for sensitive job applications?	S	Does a public authority monitor the human resources processes?	S
				Is the staff who perform the identity proofing specifically trained to perform this task?	S	Are specific job procedures redacted (e.g. security precautions, steps or rules to follow, training material)?	S	Is the staff who perform the identity proofing specifically trained to recognise European identity documents?	S	Is there a background check performed for all job applications?	S
						Are there detailed job descriptions tailored for each job offer?	S	Is there a 4 eyes principle in place during the identity proofing to reduce the risk of fraud?	S	If the identity proofing is performed remotely, is the agent specifically trained?	N
				Is it ensured that the staff have all the necessary tools to adequately operate? (e.g. a tool to ensure the authenticity of identity documents)	S			If the identity proofing is performed remotely, is there an agent to compare the photo of the identity document to the selfies?	N	Is the CA staff assigned to trusted roles in relation to the management of cryptographic keys subjected to regular suitability re-assessments?	?
	Sufficient staff	Is there sufficient staff and subcontractors to adequately operate and	S			Are there periodic reviews of staff numbers to ensure there	?	When a key staff member is absent, is there a backup identified	?	Are there identified mandatory job positions that need to be appointed (e.g. a security	?

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
		resource the service according to its policies and procedures?				exists sufficient personnel to adequately operate?		and trained to perform their newly actions?		officer, a verification manager, an officer responsible for verifying the identity of the applicant, a contact for personal data protection)?	
	Facilities monitoring and protection (incl. facility access)	Are the facilities used for providing the service continuously monitored for, and protected against, damage caused by environmental events that may impact the security of the service?	S	Is there a prior study of each facility's environmental risks?	S	Are the requirements for physical protection of the facilities regulated by international standards (PCI/ISO/ICAO)? Measures can include physical barriers, video surveillance, access control, fire protection system, anti-robbery protection.	S	Is the Business Continuity Plan regularly tested (e.g. once a year)?	S	Is the security plan for each facility approved by public authorities?	?
		Are the facilities used for providing the service continuously monitored for, and protect against, damage caused by unauthorised access that may impact the security of the service?	S	Are there continuity plans for key facilities?	S	Is there a security plan for each facility provided by each service provider, including plans that consider environmental events?	S	Are the facilities unmarked buildings with no indications on their role so that they are not easily identified as "eID related facilities"?	S	Are the requirements for physical protection of the facilities defined in National legislation and is the legislation updated when necessary?	N
						Are there specific physical security measures for subcontractors (e.g. being accompanied by staff members when accessing a non-public zone, being subject to appropriate registration)?	S				
Compliance and audit	**General compliance and audit**	Are there periodical internal audits that include all parts relevant to the supply of the provided services to ensure compliance with relevant policies?	N/A			Are the trust services which are regulated by eIDAS and used by the eID scheme regularly audited (e.g. every 2 years) by a national or international accredited auditor?	S	Where a scheme is directly managed by a government body, is it audited in accordance with the national law?	S	Are there compulsory standard certificates (e.g. ISO 27001, ISO 9001) to be able to provide a service related to electronic identification (e.g. enrolment actor, monitoring for security breach, identity provider, etc.)?	S
	Compliance audit	Is there a compliance audit performed (the provider complies with certifications, standards and legislation)?	S					Is the conformity audit performed by an external structure?	S	Does the conformity audit comply with international standards (ISO, QTS, PCI)?	S
		Is there a conformity audit performed every 3 years?	?			Is there a conformity audit performed every 2 years?	?	Is there a conformity audit performed every year?	?		

Factor	Aspect	Level 1		Level 2		Level 3		Level 4		Level 5	
	Security audit	Is there a security audit performed (penetration tests, reviews, assessments)?	?					Is the security audit performed by an external structure?	S	Does the security audit comply with international standards (ISO, QTS, PCI)?	S
		Is the security audit performed every 3 years?	?	Is there a security audit performed every 2 years?	?	Is there a security audit performed every year?	?			Is there a security audit performed every 6 months?	?
	Management audit	Is there a management audit performed (staffing, governance)?	S					Is the management audit performed by an external structure?	N	Does the management audit comply with international standards (ISO, QTS, PCI)?	S
		Is there a management audit performed every 3 years?	S			Is there a management audit performed every 2 years?	S	Is there a management audit performed every year?	S		

4.4.1 Pontuação

4.4.1.1 *Providers (incl. legal compliance)*

- **Nível de Maturidade**: Nível 5
- ***Coverage Ratio***: **100%**

4.4.1.2 *Provider responsibilities (incl. outsourcing)*

- **Nível de Maturidade**: Nível 5
- ***Coverage Ratio***: **100%**

4.4.1.3 *Termination plan*

Uma vez que não se aplica para este sistema, não há pontuação para este aspeto

4.4.1.4 *Service definition content and compliance*

- **Nível de Maturidade**: Nível 5
- ***Coverage Ratio***: **100%**

4.4.1.5 *Information about policy changes*

- **Nível de Maturidade**: Nível 1
- ***Coverage Ratio***: **67%**

4.4.1.6 *Requests for information*

- **Nível de Maturidade**: Nível 5
- ***Coverage Ratio***: **100%**

4.4.1.7 *Information security management*

- **Nível de Maturidade**: Nível 5
- ***Coverage Ratio***: **100%**

4.4.1.8 *Record management system (incl. registration protection and destruction*

- **Nível de Maturidade**: Nível 2
- ***Coverage Ratio***: **90%**

4.4.1.9 *Skills*

- **Nível de Maturidade**: Nível 3
- ***Coverage Ratio***: **86%**

4.4.1.10 *Sufficient staff*

- **Nível de Maturidade**: Nível 1
- ***Coverage Ratio***: **100%**

4.4.1.11 *Facilities monitoring and protection (incl. facility acess)*

- **Nível de Maturidade**: Nível 4
- ***Coverage Ratio***: **90%**

4.4.1.12 *General compliance and audit*

- **Nível de Maturidade**: Nível 5
- ***Coverage Ratio***: **100%**

4.4.1.13 *Compliance audit*

- **Nível de Maturidade**: Nível 5
- ***Coverage Ratio***: **100%**

4.4.1.14 *Security audit*

- **Nível de Maturidade**: Nível 5
- ***Coverage Ratio***: **100%**

4.4.1.15 *Management audit*

- **Nível de Maturidade**: Nível 3
- ***Coverage Ratio***: **83%**

4.4.2 Principais lacunas

No aspeto *Information about policy changes* este serviço não possui nível de maturidade máximo, uma vez que os utilizadores não têm opção de escolher como querem ser notificados acerca de alterações que ocorrem ao nível de politicas, bem como apenas existe um meio(*online*) para os informar. Apesar de no aspeto *Facilities monitoring and protection (incl. facility acess)* não possuir nível máximo, devido à proteção física das instalações não estar definidas por lei, esta è seguida de acordo com *standards* internacionais.

Quanto ao tema de *Record management system (incl. registration protection and destruction)* apresenta um nível de maturidade 2 porque nem todos os pedidos dos utilizadores são guardados para auditoria, caso contrário apresentava nível 5 (ou seja 100% coverage ratio)

5 Conclusão

Conseguimos perceber que o nível de maturidade é um bocado abstrato e pode induzir em erro tendo em conta apenas este fator de pontuação. O *coverage ratio* vem complementar esta forma de pontuar proposta pela **ENISA** .

Cotando o nível de maturidade aspeto a aspeto, no geral, está numa média de nível 3/4, o que já consideravelmente bom, enquanto o *coverage ratio* está quase sempre acima dos 80%.

Em suma, conseguimos entender o porquê dos modelos de maturidade são necessários para o desenvolvimento correto do software, uma vez que permite avaliar o sistema de modo a saber em que estado se encontra e também saber como melhorar o sistema de lacunas existente e fazer uso de práticas recomendados.