Towards a Healthcare Cybersecurity Certification Scheme

Kristine Hovhannisyan
Centre for Digital Forensics and Cyber Security
Tallinn University of Technology
Tallinn, Estonia
kristine.hovhannisyan@taltech.ee

Piotr Bogacki
Department of Telecommunications
AGH University of Science and Technology
Kraków, Poland
pbogacki@agh.edu.pl

Consuelo Assunta Colabuono
Security Services and Operations
RHEA Group
Rome, Italy
c.colabuono@rheagroup.com

Domenico Lofù
Department of Electrical and Information Engineering
Politecnico di Bari
Bari, Italy
domenico.lofu@poliba.it

Maria Vittoria Marabello
Innovation, Marketing and Technology
Exprivia S.p.A
Rome, Italy
vittoria.marabello@exprivia.com

Brady Eugene Maxwell
School of Information Technologies
Tallinn University of Technology
Tallinn, Estonia
brmaxw@taltech.ee

***Abstract*—The EU Cybersecurity Act introduces cybersecurity certification framework for ICT products, services and processes. Following ENISA's EUCC (the Common Criteria based European candidate cybersecurity certification scheme), we provide the Security Problem and identify Security Requirements of a healthcare specific product through a Protection Profile. We consult ENISA's reports to identify the most impactful assets in healthcare that should be prioritized for certification. We select a sub-category system of Clinical Information Systems, such as Picture Archiving and Communication System (PACS) for Protection Profile. Based on five use-cases of PACS, we define the Security Problem (assumptions, organizational security policies, threats) and we elaborate the Security Objectives. We, further, conduct a sector specific analysis of challenges and threats in healthcare sector to supplement the PACS specific threats. We detail Security Objectives from the Cybersecurity Act, and we offer a combination of these two elements, the broader scope of threats and objectives, as a baseline for future Protection Profiles of healthcare specific products. We further provide PACS specific Security Functional Requirements, and we conclude with a guideline for selecting suitable Security Assurance Requirements.**

Keywords—cybersecurity, certification, common criteria, protection profile, security problem definition, healthcare, PACS, security requirements, security objectives, assurance level

I. Introduction

The devastating effects of WannaCry in 2017 crippled nearly two million unique devices worldwide [1]. The hardest hit was the UK's national healthcare infrastructure, completely locking out users and disrupting systems of nearly 80 healthcare facilities. Among the effected systems were acute medical units [2]. In 2020 one patient seeking emergency treatment for a life-threatening condition died in Düsseldorf as the systems were paralyzed by a ransomware [3][4]. Although, the German Federal Office for Information Security warned earlier in January about the critical vulnerability (CVE-2019-19781) for the US software manufacturer Citrix [5][6], that very vulnerability was exploited in the Düsseldorf University Hospital.

Whilst the healthcare sector has been listed in the EU Commission's tentative list of Critical Infrastructure since 2005 [7], a strong motivation for establishing a level of security within the EU materializes with the Directive on security of network and information systems (NIS Directive) [8] and the EU Cybersecurity Act [9]. These two regulatory acts substantially contribute to molding of the cyber security resilience in the EU, particularly their relevance is timely for essential services provided in healthcare.

The EU Cybersecurity Act with the help of ENISA will operationalize sector specific certification scheme(s). This EU certification framework concentrates on ICT products, services, and processes. Following the EUCC scheme by ENISA [10], our work concentrates on offering an approach for a sector specific candidate certification scheme for the healthcare sector products. We combine a top-down and bottom-up approach to define a Security Problem and to unveil a predefined bucket of Threats and Security Objectives for a healthcare system that can serve as a basis for a healthcare product certification scheme. We, further, explain how to select suitable Security Assurance Requirements.

II. Challenges and Opportunities of Certification

A. Challenges of Certification Ecosystem

Certification of a product, service and a process is a formal evaluation by an independent and accredited body against a defined set of evaluation criteria standards with a final output of issuing a certificate indicating conformance [11]. To build confidence and increase trust in security of product in the EU's internal market, cybersecurity certification is one step forward towards achieving that goal. A major contributing legal act to enforce the roll out of cybersecurity certification EU-wide is the Cybersecurity Act [9], which is not *the silver bullet* but a steppingstone that introduces a framework upon which certification scheme(s) for different sectors should be built. On this path, however, one of the challenges is to elaborate the building blocks of a sector specific cybersecurity certification scheme that has the right level of abstraction and universal applicability so that it can be utilized for multiple products in a singular sector. In order to devise a flexible-enough methodology for a sector specific scheme for products, it would be helpful to look into the core challenges of both the certification ecosystem and the sector specific challenges. To date, among the missing binding ingredients for a successful EU-wide certification ecosystem, the industry partners pointed out the following issues [12][9][13][14]:

- Harmonization issue of certificates.
- Costly, tedious and formal characterization of the certification process.
- Lack of security baseline definition.
- Issue of composite certification of several independent systems in interaction.
- Certificates are static, lack agility and don't address patching and software updates and changes in the initial system configurations.
- Lack of common language/vocabulary for certification and labelling.
- Varying ICT landscapes of systems and lifespan, vendors, protocols, and technologies.

B. Challenges of Certification for Healthcare Sector

Besides the broad spectrum of sector agnostic challenges, every specific sector (e.g., healthcare, transportation, energy etc.) has its own functional and security challenges that make the elaboration of a sector specific certification scheme even more laborious. Healthcare sector stands out for several reasons [13]:

- This sector falls under the category of essential services according to Article 4 of NIS Directive, therefore it merits special attention in terms of security [8].
- Healthcare nowadays greatly depends on ICT systems and interfaces.
- The ICT connected databases hold and/or exchange patients' sensitive health data for administrative purposes. Health data, under the GDPR (General Data Protection Regulation), is categorized as special category of data that solicits strict processing requirements and secure technical environment [15].
- The lifespan of medical devices affects their security (e.g., some of the Magnetic Resonance Imaging machines are nearly a decade old, and new sophisticated vulnerability may arise).

C. State-of-the-art Analysis of Standards

The healthcare service providers, as other service providers, should undergo information security evaluations due to the fact that these medical institutions process vast amount of personal and sensitive health data. Information security certifications are mainly based on ISO standards from series ISO 27000 [16] and ISO 20000 [17].

One of the most important standards covering several general aspects of information security is ISO 27001[18]. It specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context organisation, along with the generic requirements for the assessment and treatment of information security risks tailored to the needs of any type of organisation. This standard can be complemented with the ISO/IEC 27002 [19] that guides organisations on selection, implementation and management of information security controls.

Within the ISO family, the ISO 27799 [20] is designed for information security management for health informatics, but it heavily relies on ISO/IEC 27002. The ISO 27799 determines guidelines to support the interpretation and implementation of the information security controls under the 27002 in health informatics. The ISO 27779 standard can be applied by healthcare institutions and other possessors of health information to satisfy the requirements of confidentiality, integrity and availability of personal health information in their care. It applies to processing of any data format (e.g., words, sound and video recordings, digits, medical images), to any medium for storing (e.g., printing or writing on a paper or storing electronically) and transmitting (e.g., fax, computer networks).

Another generally applicable standard is the ISO 9001 [21]. This standard helps to govern the implementation of a Quality Management System (QMS) in companies, aiming at verifying customer satisfaction with the products and services provided, as well as the continuous improvement of company performance, enabling the certified company to assure its customers that the quality of its goods and services is maintained and improved over time. A similar Canadian regulation, the Canadian Medical Devices Conformity Assessment System (CMDCAS), requires the medical devices to be designed and manufactured according to a registered Quality Management System (QMS).

The ISO 62304 standard [22] provides a framework for safe design and maintenance of software for medical devices, and its requirements apply throughout the life cycle process, sub-activities and tasks.

The ISO 13485 [23] targets medical instrument(s) and machine(s) that are intended for use in the diagnosis, prevention and treatment of diseases or other medical conditions. This standard is designed to be used by organisations involved in the design, production, installation and servicing of such medical devices, as well as by the certification bodies, to help them with auditing processes in these organisations.

The ISO 14971 [24] standard helps medical device manufacturers identify the hazards associated with medical devices. It specifies terminology, processes for managing device risks, including the software itself and the medical diagnostic devices used.

The Medical Device Directive (MDD) 93/42/EEC [25] specifies the requirements for device manufacturers and importers for meeting the CE mark to legally market or sell their devices in the EU. There are specific requirements for devices depending on the classification and intended use of the device. In addition, to market access requirements, in the healthcare domain, the in vitro diagnostic medical devices (IVDD) are subject to regulation. The IVDD 98/79/EC [26] regulates a subset of medical products, their market access, and their use.

In a different format an initiative is formed under the International Medical Device Regulators Forum (IMDRF) at an international level [27]. Representatives of medical devices regulatory authorities around the world come together to set standard requirements for auditing organisations that perform certification on the Quality Management Systems of medical device manufacturers. Similarly, the Medical Device Single Audit Program (MDSAP) represents requirements that apply to regulatory authorities as well as to third-party organisations performing this type of audit.

In addition, to all these standards, the IT Health Check (ITHC) [28] provides assurance that the organization's external and internal systems are protected from unauthorized access and/or change, and they do not provide an unauthorized entry point into systems that consume PSN (Public Services Network) services. A follow-up to unauthorized access to health data, the Health Insurance Portability and Accountability Act (HIPAA) [29] compliance standard can serve as an example. These regulations allow physicians or other health care professionals to share information directly with parties related to the patient (e.g., spouse and other family members, and/or friends).

D. Opportunities of Certification for Healthcare Sector

The state-of-the-art analysis showcases the vastness of the landscape of standards and regulations. It becomes evident that it is a tremendous effort to try certifying the healthcare sector as one due to the immense diversification of healthcare systems, components, infrastructures and medical devices. However, in order to build trust in these systems and components used in the healthcare sector, some acceptable level of security and privacy should be achieved. The goal of certification is to help reduce the potential societal risk that would have been otherwise overlooked without establishing baseline security for products, with the main approach of targeting first and foremost the critical services provided in the healthcare sector [14].

The healthcare systems' dependency on ICTs creates a vector for potential attacks or failures that can result in a much greater impact to the sectors' constituencies in contrast to other non-essential services. According to ENISA's study, picture archiving and control systems (e.g., Picture Archiving and Communication System), that fall under the category of Clinical Information Systems, are listed among the most impactful equipment within the healthcare that should be prioritised for certification [13]. Safety and availability of services are important factors for hospitals, because of the importance of the integrity of health data and for the need of that data to remain private. Personal health data is valuable for various reasons: threat actors may be interested in having access to patient health data for a myriad of malicious purposes. [13].

Fundamentally, the healthcare sector specific challenges can be credible for shaping the sector specific certification scheme bottom-up. In the meantime, to be able to apply a sector specific scheme to various products within the sector, the approach for the methodology of product evaluation should be based on a principle of re-usability and cost-effectiveness. Any scheme developed should not jeopardize the safety of patients and their health data[14][30].

By analysing this wide-ranging spectrum of standards and regulations, we arrive to an understanding that *Security Problem* definition is a feasible approach. This approach would allow us to describe the asset for evaluation and help scope the product boundaries, as well as help map the potential threats based on those boundaries defined. This approach will provide flexibility for security evaluation for any product in this specific sector. Additionally, Security Problem definition would allow elaboration of relevant Security Objectives which would lead to Security Requirements.

An opportunity that forms here, for this universally applicable scheme, is to identify a healthcare specific asset as a target of evaluation, detail the Security Problem and elicit specific Security Requirements [14] to showcase this approach.

In this regard ENISA's guidance on the methodology for establishing the cybersecurity certification framework at EU level is pertinent. The ENISA's candidate cybersecurity certification schemes of ICT product(s), services and processes is based on Common Criteria (CC) [10] with a rationale that the CC have proven its efficiency previously with regards to certifying chips and smartcards.

Based on ENISA's EUCC scheme [10], we use the Protection Profiles to elaborate the Security Problem and derive Security Requirements for the Picture Archiving and Communication System (PACS). We offer an initial Threat landscape and, concurrently, the Security Objectives specific for PACS. We then supplement the Threats, from the sector-based analysis of threats and challenges, and Security Objectives, by detailing the Security Objectives from the Cybersecurity Act. The Threats and the Security Objectives with the broader scope can be potentially applied to other products in the healthcare sector. This system falls under the definition of the Article 2 of the Cybersecurity Act, that defines the product as '"product" means an element or a group of elements of a network or information system'[9].

III. Methodology for Identifying Security Requirements Through Protection Profile

Protection Profile (PP) is an "implementation independent" set of Security Requirements for a category of ICT product that meets specific consumer needs [31]. Identification of Security Requirements is reached through the steps described in this section (through A to E) and defined by Common Criteria methodology of building Protection Profile. In particular, the purpose of the PP is to state a Security Problem (SP) for a given system or a product category and specify Security Requirements to solve a problem. The SP is a formal statement defining the nature and the scope of the security that TOE is intended to address.

Although flexible structuring of PPs content is allowed, they however have an imperative content outline, that should record the description of the *Target of Evaluation (ToE); Conformance Claim; Security Problem Definition (Threats, Organisational Security Policies, Assumptions); Security Objectives; Definition of the Extended Components; Security Requirements (Security Functional and Security Assurance Requirements).*

The PPs are not designed to have detailed security specifications but they describe the security needs at a high level of abstraction. Its purpose is to specify generic security evaluation criteria. The PPs should be used where it is necessary to define a common set of security requirements that will help the consumer, the IT developer and/or the regulatory entity to obtain, use and/or produce the evaluated information technology in accordance with the baseline

Security Requirements. The identification of Security Requirements will contribute to achieving the Security Objectives for the TOE. All these characteristics of the Protection Profiles will help devise the Security Problem that, potentially, can meet both the generic and specific challenges related to certification and help develop security requirements for the healthcare sector.

A. Target of Evaluation (TOE)

Under the Common Criteria, the scope of the target(s) for security evaluation is rather flexible: it may be an IT product or a part of an IT product, it may also be a set of IT products, or a combination of these [31]. For the purpose of our work, the ToE is Picture Archiving and Communication System with specific use-cases in scope. PACSs are nowadays a backbone in the effective management of imaging departments in the hospitals, where a large number of medical images and reports are being transmitted digitally on a daily basis.

The PACS is a complex and a hybrid system, comprised of both the software and the hardware. The system serves the purpose of transferring, storing and displaying medical images and reports. The PACS are integrated with the Radiology Information System (RIS) and Hospital Information System (HIS) [32], using the Digital Imaging and Communications in Medicine (DICOM) standard [33]. PACS are interoperable [34] systems capable of handling numerous medical imaging instruments: Computed Tomography (CT), Magnetic Resonance (MR), Digital Radiography (DR), Mammography (MG), Ultrasound (US), X-ray angiography, Endoscopy (ES), Computed Radiography (CR) and other types of imaging systems.

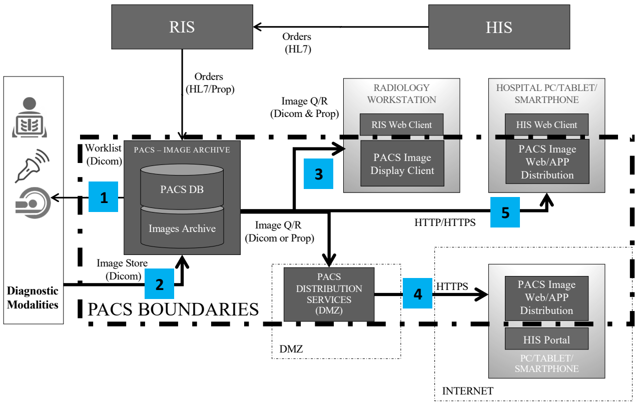


Fig. 1. Scope of the Target of Evaluation and Five Use-cases

The five Use-cases are as follows:

1) Worklist to Modalities

After having received the information from the Hospital Information System (HIS), the RIS publishes a list of patients' demographics data and examination details to the Modalities (DICOM Worklist). All information passes through the hospital network in clear text.

2) Image Store

When the examination is executed, the Modalities acquire the images and send them (DICOM Study) with patient demographics to PACS (DICOM Store). The PACS stores the DICOM Study. The DICOM Study allows a patient to have *n* number (from 1 to *n*) of studies (examinations or other procedures). Each Study consists of N number of series. A series generally refers to a specific data type (modality), or the position of a patient on the acquisition device. Each series contains *n* number of DICOM object instances (mainly images, but also reports, signal objects, etc.). All of this information is contained in each DICOM object of a study. Therefore, if a study is performed on a patient, containing, for instance, of 2 series, all of the instances will contain both the patient and the study information. The instances will also point to the series they are located in, they will also provide information about itself.

3) Image Display on Radiology Workstation

The Radiologist, through a reporting worklist on the RIS, selects a patient examination that it wished to report. Then the RIS calls the PACS Workstation component with Patient/Study information. The PACS opens the related images and information (the DICOM Study). The Radiologist can then read the images on the PACS Workstation, work and writes, signs the Report on the RIS. After the radiologist has finalized the report, the RIS sends the signed Report to HIS, together with a reference, a unique global identifier to the DICOM Study (StudyUID).

4) Image Display on Web Browser or App (Hospital)

The clinical reports are now available for the HIS. The Ward/Intensive Care Unit (ICU)/Emergency Room (ER) clinicians can view them; the StudyUID reference is the identifier through which the HIS can open the PACS Web Viewer.

5) Image Display on Web Browser or App (Remote)

This use case deals with access through a Web Portal or a Mobile Service, of the DICOM studies. The HIS can publish Reports and show DICOM Studies, by invoking PACS Web Viewer on a specific DICOM Study. It is then possible to access them from the outside, thus improving to Tele-radiology/Second Opinion networks for tele-consultation.

B. Conformance Claim

The Conformance Claim indicates three main elements: 1) to which version of the Common Criteria the TOE or the PP claim conformance; 2) to which Security Functional Requirements it conforms and 3) describes to which Security Assurance Requirements it conforms.

C. Security Problem Definition

The Security Problem is comprised of three elements. We commence defining the Security Problem by describing the Threats that the TOE is expected to address, Assumptions about the operational environment, and any relevant Organisational Security Policies (OSP) that the TOE is expected to enforce. We formulate three OSPs, eight Assumptions and six Threats. We mark the Threats with "T.", the Organisational Security Policies are marked with "P." and the Assumptions are marked with "A.". The Objectives for the Operational Environment are marked with "OE.". We use the five use-cases marked on Figure 1 to list potential Threats that the TOE might counter. These Threats are PACS specific. We follow the methodology of the Protection Profile development and define the Security Objectives based on the identified Threats.

For *Organisational Security Policies*, we list the following: P. USER; P. ROLES; P. ACCOUNTABILITY. For *Assumptions*, we list the following: A.RIS; A.HIS; A.DIAGNOSTIC_MODALITIES; A.UPS; A.PHYSICAL;

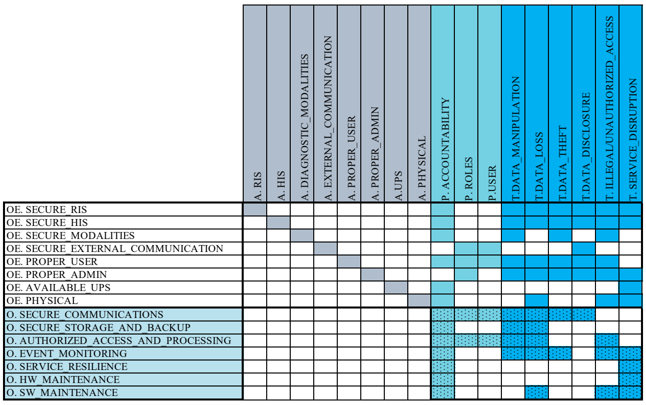
A.EXTERNAL_COMMUNICATION; A.PROPER_USER; A.PROPER_ADMIN.

For PACS specific *Threats*, we identified the following: T.DATA_MANIPULATION; T.DATA_LOSS; T.SERVICE_DISRUPTION; T.DATA_DISCLOSURE; T. ILLEGAL/UNAUTHORIZED_ACCESS; T.DATA_THEFT.

For PACS specific *Security Objectives*, we define the following: O.SECURE_COMMUNICATIONS; O. SECURE_STORAGE_AND_BACKUP; O.AUTHORIZED_ACCESS_AND_PROCESSING; O. EVENT_MONITORING; O.SERVICE_RESILIENCE; O. HW_MAINTENANCE; O.SW_MAINTENANCE.

D. *Security Objectives*

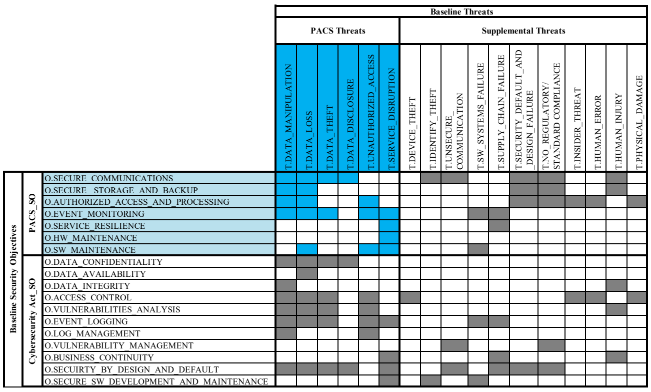
The Security Objectives intend to solve security problem, they can be traced to TOE and to the operational environment. The Security Objectives have relationship with Threats in terms of countering and/or mitigating them; they enforce the Organizational Security Policies (OSP) and uphold the Assumptions. There are two paths for tracing the security objectives; a) the Security Objectives of the TOE trace back to *Threats* and OSPs; b) the Security Objectives for the Operational Environment trace back to Threats, OSPs and Assumptions. The Figure 2 showcases these relationships.



	A. RIS	A. HIS	A. DIAGNOSTIC_MODALITIES	A. EXTERNAL_COMMUNICATION	A. PROPER_USER	A. PROPER_ADMIN	A.UPS	A. PHYSICAL	P. ACCOUNTABILITY	P. ROLES	P.USER	T.DATA_MANIPULATION	T.DATA_LOSS	T.DATA_THEFT	T.DATA_DISCLOSURE	T. ILLEGAL/UNAUTHORIZED_ACCESS	T. SERVICE_DISRUPTION
OE. SECURE_RIS	■								■			■	■	■	■	■	■
OE. SECURE_HIS		■							■			■	■	■	■	■	■
OE. SECURE_MODALITIES			■						■			■		■		■	
OE. SECURE_EXTERNAL_COMMUNICATION				■						■	■				■		
OE. PROPER_USER					■				■	■	■	■	■	■	■	■	
OE. PROPER_ADMIN						■				■		■	■	■	■	■	■
OE. AVAILABLE_UPS							■		■								■
OE. PHYSICAL								■	■				■			■	■
O. SECURE_COMMUNICATIONS									▨	▨	▨	▨	▨	▨	▨		
O. SECURE_STORAGE_AND_BACKUP									▨			▨	▨				
O. AUTHORIZED_ACCESS_AND_PROCESSING									▨	▨	▨	▨	▨			▨	
O. EVENT_MONITORING									▨			▨	▨	▨		▨	▨
O. SERVICE_RESILIENCE									▨								▨
O. HW_MAINTENANCE									▨								▨
O. SW_MAINTENANCE									▨				▨			▨	▨

Fig. 2. Tracing between Security Problem Definition and Security Objectives

To enhance this mapping and to be able to provide a broader scope of threats for the healthcare sector, we use sector-based analysis of threats and challenges conducted within the ECHO Project [35][36][37] and the ENISA's report [38] to complement this initial bucket of threats, and offer a baseline of Threats for the healthcare specific scheme security problem definition. To ensure that these newly supplemental Threats gain Security Objectives, we detail these objectives from the Cybersecurity Act. Figure 3 summarizes both PACS specific Threats and Security Objectives, as well as the baseline Threats and Security Objectives that we offer for further consideration when building a healthcare specific certification scheme with the use of Protection Profile.



			Baseline Threats																
			PACS Threats						Supplemental Threats										
			T.DATA_MANIPULATION	T.DATA_LOSS	T.DATA_THEFT	T.DATA_DISCLOSURE	T.UNAUTHORIZED_ACCESS	T.SERVICE_DISRUPTION	T.DEVICE_THEFT	T.IDENTIFY_THEFT	T.UNSECURE_ COMMUNICATION	T.SW_SYSTEMS_FAILURE	T.SUPPLY_CHAIN_FAILURE	T.SECURITY_DEFAULT_AND _DESIGN_FAILURE	T.NO_REGULATORY/ STANDARD COMPLIANCE	T.INSIDER_THREAT	T.HUMAN_ERROR	T.HUMAN_INJURY	T.PHYSICAL_DAMAGE
Baseline Security Objectives	PACS_SO	O.SECURE_COMMUNICATIONS	■	■	■	■				■	■			■	■			■	
		O.SECURE_ STORAGE_AND_BACKUP	■	■										■	■			■	
		O.AUTHORIZED_ACCESS_AND_PROCESSING	■	■			■							■	■	■	■		■
		O.EVENT_MONITORING	■	■	■		■	■				■	■						
		O.SERVICE_RESILIENCE						■					■						
		O.HW_MAINTENANCE						■											
		O.SW_MAINTENANCE		■			■	■				■							
	Cybersecurity Act_SO	O.DATA_CONFIDENTIALITY	■	■	■	■													
		O.DATA_AVAILABILITY		■															
		O.DATA_INTEGRITY	■															■	
		O.ACCESS_CONTROL	■	■	■		■		■							■	■		■
		O.VULNERABILITIES_ANALYSIS	■	■	■		■											■	
		O.EVENT_LOGGING	■	■	■		■	■				■	■						
		O.LOG_MANAGEMENT	■				■												
		O.VULNERABILITY_MANAGEMENT									■				■				
		O.BUSINESS_CONTINUITY						■					■					■	
		O.SECUIRTY_BY_DESIGN_AND_DEFAULT	■	■	■	■		■			■		■	■	■				
		O.SECURE_SW_DEVELOPMENT_AND_MAINTENANCE						■		■		■							

Fig. 3. The Baseline Threats and the Security Objectives for a Healthcare Specific Certification Scheme

The supplemental Threats are: T.DEVICE_THEFT; T.IDENTITY_THEFT; T.UNSECURE_CIMMUNICATIO; T.SOFTWARE_SYSTEM_FAILURE;T.SUPPLY_CHAIN_FAILURE;T.INSIDER_THREAT;T.PHYSICAL_THREAT; T.SECURITY_DEFAULT_AND_DESIGN_FAILURE; T.NO_REGULATORY_STANDARD_COMPLIANCE; T.HUMAN_ERROR;T.HUMAN_INJURY.

The Security Objectives detailed from the Cybersecurity Act are:O.DATA_CONFIDENTIALITY;O.DATA_AVAILABILITY;O.DATA_INTEGRITY;O.ACCESS_CONTROL; O.VULNARABILITIES_ANALYSIS;O.EVENT_LOGGING;O.LOG_MANAGEMENT;O.VULNARABILITY_MANAGEMENT;O.BUSINESS_CONTINUITY;O.SECURITY_BY_DESIGN_AND_DEFAULT;O.SECURE_SOFTWARE_DEVELOPMENT_AND_MAINTENANCE.

E. *Security Requirements*

The goal for conducting security evaluation of the TOE is to ensure that the determined Security Functional Requirements (SFRs) are enforced on the TOE and its resources [39]. The SFRs may impose various security policies, each of them must specify scope of control (defining the subjects, objects, resources or information, and operations to which it applies). Each SFR is manifested via classes, families, and components.

For PACS and for the given scope of Threats and Security Objectives, we have applied the following SFRs as shown on Figure 4: FDP: User Data Protection; FAU: Security Audit; FPT: Protection of the TOE; FIA: Identification and Authentication; FMT: Security Management; FTA: TOE Access; FTP: Trusted Path/Channel; FRU: Resources Utilisation.

As the healthcare sector processes primarily personal sensitive data, maintaining privacy is paramount. We use this opportunity to develop one of the elements of the PP, the *Definition of the Extended Components*. We develop a one distinct SFR Class named - FPP: Personal Data Protection, along with the families and customized components. The Figure 5 presents the application of the extended SFRs to PACS Security Objectives. The detailed description of these SFRs can be found in one of the ECHO Project's deliverables [40].

		Common Criteria Security Functional Requirements																																	
		FDP: User Data Protection			FAU: Security Audit						FPT: Protection of the TOE							FIA: Identification and Authentication					FMT: Security Management			FTA: TOE Access						FTP: Trusted Path/Channels		FRU: Resource Utilisation	
		SDI: Stored Data Integrity	ROL: Rollback	DAU: Data Authentication	ARP: Security Audit Automatic Response	SAA: Security Audit Analysis	GEN: Security Audit Data Generation	SAR: Security Audit Review	SEL: Security Audit Event Selection	STG: Security Audit Event Storage	STM: Time Stamps	PHP: TSF Physical Protection	TST: Self-test	TEE: Testing of External Entities	FLS: Fail Secure	RCV: Trusted Recovery	FLS: Fail Secure	AFL: Authentication Failure	ATD: User Attribute Definition	SOS: Specification of Secrets	UAU: User Authentication	UID: User Identification	MOF: Management of Functions TSF	SMF: Specification of Management Functions	SMR: Security Management Roles	LSA: Limitation on Scope of Selectable Attributes	MCS: Limitation on Multiple Concurrent Sessions	SSL: Session Locking	TAH: TOE Access History	TSE: TOE Session Establishment	TAB: TOE Access Banners	ITC: Inter-TSF Trusted Channel	TRP: Trusted Path	FLT: Fault Tolerance	RSA: Resource Allocation
PACS_SO	O.SECURE_COMMUNICATIONS																															1.1-3	1.1-3		
	O.SECURE_ STORAGE_AND_BACKUP	2.1-2	2.1-2	1.1-2																															
	O.AUTHORIZED_ACCESS_ AND_PROCESSING											1.1-2 3.1						1.1-2	1.1	1.1	2.1 5.1-2	2.1	1.1	1.1	1.1-2 2.1-3	1.1	1.1-2	1.1-2 2.1-2 3.1 4.1	1.1-3	1.1	1.1				
	O.EVENT_MONITORING				1.1	1.1-2 2.1 3.1-3	1.1-2 2.1	1.1 2.1	1.1	3.1 4.1	1.1																								
	O.SERVICE_RESILIENCE															3.1-4	1.1																	1.1	2.1-2
	O.HW_MAINTENANCE														1.1																				
	O.SW_MAINTENANCE												1.1-3	1.1-2																					

Fig. 4. PACS Specific Security Functional Requirements, Components are marked with numbers

		Customized Security Functional Requirements											
		FPP: Personal Data Protection											
		PIIP: Personal Identifiable Information Processing	STG: Secure Data at Rest	ACC: Access Control Policy	ACF: Personal Data Access Functions	PFC: Personal Data Flow Control Policy	IFF: Personal Data Flow Control Functions	ITA: Availability of Exported Personal Data	ITC: Confidentiality of Exported Personal Data	ITI: Integrity of Exported Personal Data	ITT: Internal TOE Transfer	ETC: Export of Personal Data Control	CST: Consent Management
PACS_SO	O.SECURE_COMMUNICATIONS							1.1	1.1	1.1-3	1.1-2	1.1-4	
	O.SECURE_ STORAGE_AND_BACKUP	1.1-4	1.1-5 2.1-6										
	O.AUTHORIZED_ACCESS_ AND_PROCESSING			1.1-2	1.1-4	1.1-2	1.1-5 2.1						1.1-6
	O.EVENT_MONITORING												
	O.SERVICE_RESILIENCE												
	O.HW_MAINTENANCE												
	O.SW_MAINTENANCE												

Fig. 5. Definition of the Extended Components

The Security Requirements for the Protection Profiles have two categories: 1) the Security Functional Requirements (SFRs), which we addressed above and 2) the Security Assurance Requirements (SARs). The SARs are the descriptions of how TOE is being evaluated, and they are structured similarly in a hierarchical way by class, family and component. Before any of the SARs can be selected, the Evaluation Assurance Level (EAL) should be defined.

The Article 52 of the Cybersecurity Act mentions that each certification scheme should provide the assurance requirements matching to its respective assurance level.

The Cybersecurity Act defined three levels of assurance: *Basic*, *Substantial* and *High*. The following definition applies to these levels:

- If cybersecurity certificate or statement of conformity refers to assurance level *Basic*, the evaluation activities should include at least the review of technical documentation.
- If cybersecurity certificate refers to assurance level *Substantial,* the evaluation activities should include at least the review to showcase that the publicly known vulnerabilities are absent and conduct a testing to demonstrate that the SFRs are correctly implemented.
- If cybersecurity certificate refers to assurance level *High,* the evaluation activities should include at least a review to showcase that the publicly known vulnerabilities are absent, a test to demonstrate that the SFRs are implemented at the state of the art, and a penetration testing.

The selection of an assurance level may seem to be a straightforward process, however, in practice it is a challenging activity as several documents should be consulted simultaneously:

- **ENISA:** The EUCC scheme or products covers two assurance levels out of the three: the *Substantial* and the *High*. In the meantime, Common Criteria itself defines seven evaluation assurance levels and each of these levels have their minimum corresponding activities [10].
- **ENISA:** Our next step is to follow the mapping of the assurance levels between the Cybersecurity Act and the Common Criteria (Part 3). ENISA notes that the selection of the assurance levels of the Cybersecurity Act should be based on the assurance components of a specific assurance class, the AVA: Vulnerability Assessment class (AVA_VAN),

defined by Common Criteria Part 3. According to this formulation, the mapping of the assurance levels between these two documents are represented in Table 1 [10]:

TABLE 1. MAPPING OF EVALUATION ASSURANCE LEVELS BETWEEN CYBERSECURITY ACT AND COMMON CRITERIA

Item Number	**Mapping of Evaluation Assurance Levels**		
	Cybersecurity Act	***Common Criteria (AVA_VAN)***	***Common Criteria Corresponding EAL***
1	Basic	-	-
2	Substantial	AVA_VAN.1 AVA_VAN.2	EAL 1 EAL 2, EAL 3
3	High	AVA_VAN.3 AVA_VAN.4 AVA_VAN.5	EAL 4 EAL 5 EAL 6, EAL 7

- **ENISA:** ENISA defines, that the products that do not fall under the "Technical Domains", such as the Smart Cards (and similar devices) and the Hardware Devices with Security Boxes, cannot apply SAR components AVA_VAN.4 and AVA_VAN.5 [10].

- **ENISA:** Further, we exclude the entire assurance level *High* (including AVA_VAN.3), as ENISA suggest that assurance claim for level *High* originates from the authorization of a Governmental agency, leaving us with level *Substantial* with corresponding AVA_VAN components.

- **Common Criteria Part 3:** We are left with AVA_VAN.1 and AVA_VAN.2. We refer to Common Criteria Part 3, to determine which of these two components is more appropriate for our TOE. In the description of AVA_VAN.1 it is stated that the evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE. In case of AVA_VAN.2 the evaluator shall perform an independent vulnerability analysis of the TOE using guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE. Since PACS is rather more complex product, the use of its specific design and architecture information is definitely required. For that reason, we select AVA_VAN.2.

- **ENISA:** It is stated in the ENISA's guidance, that based on the selection of the AVA_VAN, the first EAL should apply along with its all dependencies of components that are associated with the selected AVA_VAN [10]. In our case, the first EAL corresponding to AVA_VAN.2 would be the EAL 2 (refer to Table 1. Evaluation assurance level summary of Common Criteria Part 3, p. 32)[41].

- **Common Criteria Part 3:** The dependencies marked by the Common Criteria with respect to AVA_VAN.2 are selected from the assurance classes of ADV (Development) and AGD (Guidance) and the components are the following: ADV_ARC.1 Security Architecture Description; ADV_FSP.2 Security-enforcing functional specification; ADV_TDS.1 Basic Design; AGD_PRE.1 Preparative procedures; AGD_OPE.1 Operational user guidance.

- **Common Criteria Part 3:** Based on the selected EAL, ENISA indicates what are the other further applicable SARs, apart from the direct dependencies indicated by Common Criteria Part 3. The additional classes are ALC (Life-cycle), ATE (Tests), ASE (ST Evaluation), APE (PP Evaluation) and the selected components are the following: ALC_CMC.2 Use of a CM system; ALC_CMS.2 Parts of the TOE CM coverage; ALC_DEL.1 Delivery procedures; ATE_COV.1 Evidence of Coverage; ATE_FUN.1 Functional Testing; ATE_IND.2 Independent Testing – Sample: ASE_TSS.1 TOE Summary Specification and these following SARs that refer to Security Target (ST), and not to Protection Profile: ASE_CCL.1 Conformance Claims; ASE_ECD.1 Extended Components Definition; ASE_INT.1 ST introduction; ASE_OBJ.2 Security Objectives; ASE_REQ.2 Derived Security Requirements; ASE_SPD.1 Security Problem Definition. Therefore, we find equivalent components that apply to PP, which are the following: APE_CCL.1; APE_ECD.1; APE_INT.1; APE_OBJ.2; APE_REQ.2; APE_SPD.1; APE_TSS.1.

DISCUSSION AND CONCLUSION

In our work towards a healthcare cybersecurity certification scheme, we commence by identifying categories of assets in healthcare and selecting one asset from the sub-category of Clinical Information Systems, such as Picture Archiving and Communication System. Our motivation to use this asset for Protection Profile relates to the fact that this system is categorized as one the most critical systems in healthcare, they are complex and there are privacy concerns for the transmission of personal data through these types of systems.

With this work, we create a baseline of healthcare-wide Threats and Security Objectives. We use a top-down approach by analysing ENISA's report(s), the EUCC, and the Cybersecurity Act and we use a bottom-up approach by examining the use-cases elaborated within the ECHO Project and incorporating the project partners' expertise contribution. These Threats and Security Objectives can equally be used for other healthcare ICT products with respective additions if identified and/or applicable, for instance, to Networked Medical Devices, Remote Care Systems and to other systems[38].

This methodology will be extended within the ECHO Project to other sectors, maritime and energy. Use of Cyber Ranges for the Conformity Assessment of a TOE will also be investigated.

This work is the very first step in the complete cycle of certification under Common Criteria. The main stakeholders involved in the certification and evaluation process are the consumers, developers and the evaluators. The consumers or communities of interest can draft the PPs to identify the Security Requirements, which are implementation-independent. Developers use the PP to draft the Security Target for a specific asset belonging to the asset category for which the PP is developed. Although, the Security Target is a construct similar in its structure to Protection Profile, it provides general technical mechanisms that the TOE uses to satisfy the PP. The level of detail in the description of the technical mechanisms should be enough to enable potential consumers to understand the general form and implementation of the TOE. In contrast to PP, the Security Requirements in the ST are more restrictive, and the ST serves as an agreement between the developer and the evaluator on the specific security properties of the TOE to be evaluated [31].

ACKNOWLEDGMENT

This work was partially supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no 830943.

REFERENCES

[1] S. on Oversight, S. on R. and Technology, A. Committee on Science, Space, & Technology, and H. of Representatives, "Serial No. 115-17: Bolstering the Government's Cybersecurity: Lessons Learned from Wannacry, Joint Hearing Before the Subcommittee on Oversight & Subcommittee on Research and Technology Committee on Science, Space, and Technology, House of Representatives," in *Homeland Security Digital Library*, 15-Jun-2017.

[2] C. and A. General, "Investigation: WannaCry cyber attack and the NHS," *UK Department of Health*, 25-Apr-2018. [Online]. Available: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

[3] C. Cimpanu, "First death reported following a ransomware attack on a German hospital," *ZDNet*, 17-Sep-2020.

[4] D. Goodin, "A Patient Dies After a Ransomware Attack Hits a Hospital," *Wired*, 19-Sep-2020. [Online]. Available: https://www.wired.com/story/a-patient-dies-after-a-ransomware-attack-hits-a-hospital/.

[5] "Aktive Ausnutzung der Citrix Schwachstelle," *BSI*, 2020. [Online]. Available: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Citrix_Schwachstelle_160120.html.

[6] "CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance," *Citrix*, 17-Dec-2019. [Online]. Available: https://support.citrix.com/article/CTX267027.

[7] "Green Paper on a European programme for critical infrastructure protection | EUR-Lex - 52005DC0576," *EU Commission*, 17-Nov-2005. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576.

[8] "The Directive on security of network and information systems (NIS Directive)," *the European Parliament and the Council*, 06-Jul-2016. [Online]. Available: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

[9] "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 52," *the European Parliament and the Council*, 17-Apr-2019. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2019/881/oj.

[10] "Cybersecurity Certification: EUCC Candidate Scheme," *European Union Agency for Cybersecurity (ENISA)*, 02-Jul-2020. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme.

[11] "Proposal for a Regulation of the European Parliament and of the Council on ENISA (the EU Cybersecurity Agency) and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act'), Expla," *the European Parliament and the Council*, 13-Sep-2017. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477&from=EN.

[12] "European Cyber Security Certification: A Meta-Scheme Approach v1.0," ECSO, Dec. 2017.

[13] "Challenges of security certification in emerging ICT environments," *ENISA*, 06-Feb-2017. [Online]. Available: https://www.enisa.europa.eu/publications/challenges-of-security-certification-in-emerging-ict-environments/.

[14] "European Cyber Security Certification: Challenges ahead for the roll-out of the Cybersecurity Act," ECSO, Dec. 2020.

[15] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da." [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[16] "ISO/IEC 27000 - Information technology — Security techniques — Information security management systems." [Online]. Available: https://www.iso.org/standard/73906.html.

[17] "ISO/IEC 20000 - Information technology — Service management." [Online]. Available: https://www.iso.org/standard/51986.html.

[18] "ISO/IEC 27001- Information technology — Security techniques — Information security management systems — Requirements." [Online]. Available: https://www.iso.org/standard/54534.html.

[19] "ISO/IEC 27002 - Information technology — Security techniques — Code of practice for information security controls." [Online]. Available: https://www.iso.org/standard/54533.html.

[20] "ISO 27799 - Health informatics — Information security management in health using ISO/IEC 27002." [Online]. Available: https://www.iso.org/standard/62777.html.

[21] "ISO 9001 - Quality management systems — Requirements." [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:en.

[22] "IEC 62304 - Medical device software — Software life cycle processes." [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iec:62304:ed-1:v1:en.

[23] "ISO 13485 - Medical devices — Quality management systems — Requirements for regulatory purposes." [Online]. Available: https://www.iso.org/standard/59752.html.

[24] "ISO 14971 - Medical devices — Application of risk management to medical devices." [Online]. Available: https://www.iso.org/standard/72704.html. [Accessed: 19-Jan-2021].

[25] "Council Directive 93/42/EEC of 14 June 1993 Concerning Medical Devices," *EU Council*, 14-Jun-1993. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31993L0042.

[26] "Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices," 1998. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31998L0079&from=IT.

[27] "International Medical Device Regulators Forum (IMDRF)." [Online]. Available: https://www.fda.gov/medical-devices/cdrh-international-programs/international-medical-device-regulators-forum-imdrf.

[28] "IT Health Check (ITHC): supporting guidance." [Online]. Available: https://www.gov.uk/government/publications/it-health-check-ithc-supporting-guidance.

[29] "Health Insurance Portability and Accountability Act of 1996 (HIPAA)," *The US Department of Health and Human Services (HHS)*, 1996. [Online]. Available: https://www.cdc.gov/phlp/publications/topic/hipaa.html.

[30] "ICT security certification opportunities in the healthcare sector," *ENISA*, 31-Jan-2019. [Online]. Available: https://www.enisa.europa.eu/publications/healthcare-certification.

[31] "Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model," Common Criteria, Apr. 2017.

[32] H. Khaleel, R. Wirza, and D. Zamrin, "Components and implementation of a picture archiving and communication system in a prototype application," *Reports Med. Imaging*, vol. Volume 12, pp. 1–8, Dec. 2018.

[33] "Standard: PS3.21 DICOM PS3.21 2020e-Transformations between DICOM and other Representations," *National Electrical Manufacturers Association*, 2020. [Online]. Available: http://dicom.nema.org/medical/dicom/current/output/pdf/part21.pdf.

[34] Y. alSafadi, W. P. Lord, and N. J. Mankovich, "PACS/information systems interoperability using Enterprise Communication Framework," *IEEE Trans. Inf. Technol. Biomed.*, vol. 2, no. 2, pp. 42–47, 1998.

[35] "D4.2 Inter-sector Technical Cybersecurity Challenges Report,"

European Network of Cybersecurity centres and competence Hub for innovation and Operations, Jun. 2020.

[36] "D2.5 Multi-sector Requirements Definition and Demonstration Cases," European Network of Cybersecurity centres and competence Hub for innovation and Operations, Mar. 2020.

[37] "D2.4 Inter-sector Technology Challenges and Opportunities," European network of Cybersecurity centres and competence Hub for innovation and Operations, Jan. 2020.

[38] "Procurement Guidelines for Cybersecurity in Hospitals," *ENISA*, 24-Feb-2020. [Online]. Available: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

[39] "Common Criteria for Information Technology Security Evaluation: Part 2. Security Functional Components," Common Criteria, Apr. 2017.

[40] "D2.9 ECHO Cybersecurity Certification Scheme," European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations, 2021.

[41] "Common Criteria for Information Technology Security Evaluation: Part 3 Security assurance components," Common Criteria, Apr. 2017.