# ABSTRACT

Domeniul e-Sănătate a cunoscut o creştere exponenţială care a fost accentuată şi de interesul susţinut al industriei medicale şi a organizaţiilor de standardizare. Una din cele mai active organizaţii este Continua Health Alliance, a cărei principală contribuţie a fost dezvoltarea unei arhitecturi generice care defineşte comunicarea datelor medicale între sisteme de e-Sănătate. Teza se concentrează pe analiza unui model derivat din arhitectura Continua, model ce defineşte un lanţ complet de comunicare de la achiziţia datelor de la pacienţi la transferul datelor către sisteme informatice specializate prin intermediul a două standarde de comunicaţie: ISO/IEEE 11073-20601 (OEP) şi HL7 V3. Teza analizează aceste standarde şi identifică o serie de îmbunătăţiri ce asigură securitatea şi confidenţialitatea datelor medicale şi interoperabilitatea sistemelor medicale. Teza propune un algoritm de autentificare mutuală între dispozitivele ce implementează OEP. Protocolul de autentificare foloseşte chei de criptare derivate din date biometrice. Teza prezintă o nouă abordare pentru a rezolva problema cheilor biometrice robuste, problemă deschisă la nivelul comunităţii ştiinţifice. Sunt introduse două extensii ale mecanismului de asociere al OEP şi se oferă detalii şi exemple de implementare. În plus, este proiectat şi implementat un analizator de mesaje OEP, pentru interceptarea şi analiza traficului dintre dispozitivele medicale. Analiza standardului HL7 V3 arată că există probleme de interoperabilitate datorate complexităţii standardului şi a metodologiei de dezvoltare a mesajelor şi profilurilor HL7 V3. Astfel, cercetarea s-a concentrat pe definirea unei metodologii de testare de conformitate a aplicaţiilor bazate pe HL7 V3. Soluţia propusă se bazează pe tehnologiile de testare standardizate TTCN-3. Rezultatul metodologiei de testare este un framework de testare automată. Pentru a reduce costurile şi probabilitatea apariţiei erorilor umane au fost proiectate şi implementate o serie de unelte de automatizare a procesului de testare: a) un generator de tipuri de date HL7 V3 pentru Java, b) un generator de tipuri de date TTCN-3 definite de utilizator, c) un editor/generator de template-uri TTCN-3 şi d) un generator de date de test de intrare. Ultimul menţionat este un generator automat cu potenţial imens, ce poate fi personalizat pentru a genera seturi de date de test potrivite pentru diferite metodologii de testare. Acesta este totodata primul generator de mesaje HL7 V3 dezvoltat. Aceste soluţii au apărut ca răspuns la nevoile de îmbunătăţire a securităţii şi confidenţialităţii datelor medicale şi a interoperabilităţii între sistemele medicale şi pot fi aplicate cu succes în aplicaţii reale.

eHealth domain faces a exponential growth, which is accentuated by the interest shown by the industry and standardization organizations. One of the most active organizations is Continua Health Alliance. Continua developed a generic architecture that defines medical data communication between eHealth systems. The thesis focuses on the analysis of a model derived from the Continua Architecture. This model defines a complete communication chain from the data acquisition to the transfer of data to information systems. This model is based on thwo communication standards: ISO/IEEE 11073-20601 (OEP) and HL7 V3. The thesis analyzes these standards and identifies a set of enhancements that ensure security and privacy of medical data and interoperability between eHealth systems. The thesis proposes a mutual authentication protocol between OEP devices. The protocol uses cryptographic keys derived from biometric data. A new approach is taken for solving the problem of robust biometric keys, which is still an open problem addressed by the scientific community. The thesis introduces two extensions of the OEP association mechanism and presents the design and implementation of a new OEP message analyzer. The analysis conducted on HL7 V3 standard shows that there are several interoperability problems caused by the complexity of the standard and the development methodology of HL7 V3 messages and profiles. Thus, the research has focused on defining a conformance testing methodology based on the standardized TTCN-3 testing technologies. As a result of this methodology, a complete testing framework was implemented. Moreover, in order to minimize the probability of human errors, a set of automation tools were designed and implemented: a) generator for HL7 V3 data types definitions in Java, b) TTCN-3 type system generator, c) editor/generator for TTCN-3 templates and d) test data input generator. The latter is a generation tool with huge potential. It can be used to customize the generation process to adapt the testing input to various testing methodologies. In the case study presented in the thesis it was used as the first HL7 V3 message generation tool. These solutions appeared as a response to the needs of improvement of security and privacy of medical data and improvement of interoperability between eHealth systems and can be successfully applied to real eHealth applications.