Mihai TOGAN
Email: mihai.togan@mta.ro, mihai.togan@gmail.com
Phone: 004-0722859825

Curriculum Vitae

Education:

PhD in Computers Science, 2009
"*Contributions to development of trusted third party services within the computer networks"*
(Main topics: Trusted Third Parties, PKI, Electronic Signatures Services)
Ph.D. Advisor: Professor Dr. Victor-Valeriu Patriciu
Military Technical Academy, Bucharest

Bachelor's Degree in Computers Science, 1994 – 2000
Graduating mark: **9.20 / 10**
Military Technical Academy, Bucharest

High School of Informatics, 1990 – 1994
Tudor Vianu College, Bucharest

Other training courses
CCNA (Cisco Certified Network Associate), ATM, 2001
Microsoft SQL Server, Romania, 2002

Professional Experience:

Military Technical Academy, 2000 – present
Professor
Head of Computer Science Dept. (2016 – present)

Main activities and responsibilities*:*
Teaching area
- Courses for: *Computer Programming, Techniques and Programming Languages, Object Oriented Programming, Computer Networks, Software Engineering, Informatics Security, Cryptography.*
- Laboratories for: *Computer Programming, Cryptography, Informatics Security, Techniques and Programming Languages, Object Oriented Programming, Computer Networks, Database Programming, Operating Systems.*
- Laboratories for Academic master programs *Security of Information Technology (*Military Technical Academy, Bucharest) and *IT&C Security* (Academy of Economic Studies, Bucharest): *Cryptography, Digital Signatures and security infrastructures, Security of Electronic Payment Systems.*
- Diploma and dissertations projects for students (over 120 student projects)

Research area
- Usage of computational cryptography in information security
- Usage of trusted third parties services to ensure trust between entities participating in electronic transactions
- Interoperability analysis of public key infrastructures (PKI) domains
- Usage of smart cards for ensuring of electronic identity
- Usage of hardware mechanisms for optimizing cryptographic operations
- Applications of fully homomorphic encryption

CERTSIGN, 2000 – present
Software developer, Security product team leader, Security Software Architect

Main activities and responsibilities*:*
- Design and development of software solutions for electronic signatures.
- Design and development of smart card based security applications.
- Design and development of solutions for digital certificates issuing and management.
- Design and development of software solutions for digital certificates validation.
- Design and development of software solutions for digital documents time stamping.
- Development and implementation of technical solutions intended to provide public key based digital certificates nationwide.
- Design, development and implementation of technical solutions intended to provide time stamps nationwide.
- Participation (technical consultant) to design the technical rules of timestamp law enforcement in Romania.
- Participation (remote) to working groups and initiatives of the European Telecommunications Standards Institute regarding interoperability of advanced electronic signatures services.
- Design and development of e-Invoicing/e-Archiving solutions
- Design and development of smart cards personalization software solutions for Romanian tachograph nationwide system.
- Development and implementation of PKI technology based on technical solutions designed for the structures of National Defense System.

List of the significant projects:
certSAFE – complete X.509 certificates management solution.
- Analysis and overall design of the solution architecture
- Design and development of the solution basis PKI framework
- Design and development of the key-recovery module
- Design and development of the smartcard logon specific certificates issuing module
- Design and development of the HSM (hardware secure module) integration module
- Design and development of other components (LDAP publishing modules, CGI based UI components, database architecture, etc.)
- Technologies: C/C++, Linux, LDAP, CGI, SQL, PKCS#1, PKCS#11, PKCS#12, PKCS#10, PKCS#5, secret sharing schemes, smartcards, HSMs.

certSAFE-ProxyOCSP – RFC#6960 fully compliant solution for X.509 certificates status validation.
It works as a Linux service and includes proprietary proxy functionalities for certificates validation (extension to OCSP RFC standard).
- Design and development of the solution modules (HTTP request/response management, OCSP data structures, validation module, software/hardware response signing module, proxy extension module)
- Technologies: C/C++, Linux, PKCS#11, LDAP, HTTP.

certSAFE-TS – RFC#3161 solution for documents and digital signatures timestamping.
- Design of overall architecture for solution.
- Design and development of the specific signing modules. Integration with HSM hardware signing/key protection devices. Technical support for the development team.
- Technologies: C/C++, Linux, PKCS#7, PKCS#11.

tachoSAFE – Solution for personalizing and issuing European digital tachograph smartcards.
- Design of the solution modules
- Design of the certification and cryptographic keys management components. These are integrated within European Digital Tachograph Public Key Infrastructure
- Development of the specific cryptographic modules
- Technologies: C++, RSA.

invoSAFE – HTTP service that generates and manages electronic invoices.

- Development of the invoices signing components
- Technical support to the design and development team
- Technologies: C, C++, Linux, PKCS#7, PKCS#11.

SSEAPI. API designed to management of CAdES/CMS/PKCS#7 compliant electronic signatures. It was tested within ETSI remote plug tests sessions.

- Design and development of the specific API components
- Technologies: C++, PKCS#7, PKCS#11, PKCS#12, ETSI TS101-733.

LIBTS. RFC3161 client API for timestamping

- Development of the specific API components, Technologies: C++

CRYU-API – security framework for Android and IOS mobile platforms

- Design and development of the API components to support encryption, electronic signature, key management, secure elements,
- Technologies: C, security standards.

Research projects:

Project Director/ Responsible

1. *Technologies for processing and guaranteeing of the electronic content (TAPE)*. The National Plan for Research, Development and Innovation II (PN-II-IN-DPST-2012-1-0087), 2013-2015, **Project Director**.
2. *Cloud based cryptographic mechanisms under the sole control of the user (MC3Ex)*. The National Plan for Research, Development and Innovation III (PN-III-P2-2.1-PTE-2016-0191), **Project Responsible**.
3. *Advanced models for the design and evolution of modern cryptographic systems (ADECS)*. The National Plan for Research, Development and Innovation II (PN-II-PT-PCCA-2011-3), 2011 – 2016, **Project Responsible**.
4. *Advanced security mechanisms implemented in hardware (MASH).* The National Plan for Research, Development and Innovation II (PN-II PARTENERIATE, CTR.81-038/2007), 2007-2010, **Project Responsible**.

Team member

5. *From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control (ReCRED)*. ProjRef. 653417, H2020-EU.3.7 European Project, European Research Executive Agency (REA), 2015-2018.
6. *Trusted multi-application receiver for trucks (TACOT).* ProjRef. GA-287180, FP7 European Project Galileo.2011.1.2-1, 2012-2014.
7. *Development of technologies for securing data in the Cloud (DTSDC)*. The National Plan for Research, Development and Innovation II (PN-II-IN-DPST-2012-1-0086), 2013-2015.
8. *New Innovative System for Radiation Safety of Patients Investigated by Radiological Imaging Methods based on Smart Cards and PKI Infrastructures (SRSPRIM)*. PN-II-PT-PCCA-2011-3.2-1517, 2011-2015.
9. *Encryption equipment for traffic protection in computer networks (ECRI)*. SMIS-CSNR-39278, POSCCE-A2-O2.3.3, 2013-2015.
10. *Non-repudiable email service with legal value (SPENS)*. The National Plan for Research, Development and Innovation II (PN-II INOVARE, CTR. 139/2008), 2008-2011.
11. *Efficient and secure electronic healthcare services based on PKI infrastructures and smart cards (SMESIS)*. The National Plan for Research, Development and Innovation II (PN-II PARTENERIATE, CTR. 12-125/2008), 2008-2011.

12. *Integrated IT platform for secure management of personal data based on smart cards and PKI infrastructure (PLATSEC).* The National Plan for Research, Development and Innovation II (PN-II PARTENERIATE, CTR. 82-105/2008), 2008-2011.
13. *Technologies and equipments for voice and data secure communications over switched telephone networks (CSVDT)*. The National Plan for Research, Development and Innovation II (PN-II PARTENERIATE, CTR. 81-019/2007), 2007-2010.
14. *Technology demonstrator for the management of electronic identity cards based on multi-application smart cards (SMCID)*. The Romanian National Research Program *SECURITATE*, 2005-2006.
15. C*ryptographic systems based on new technologies (SCTN)*. The Romanian National Research Program *SECURITATE*, 2005-2006.
16. *Secure LAN model based on a public key infrastructure interoperable with public key infrastructure of the National Defense System (LANSEC)*. The Romanian National Research Program *SECURITATE*, 2005-2006.
17. *Cryptographic methods and techniques for authentication of electronic commerce and business processes using digital signatures. Probative value of digitally signed electronic documents*. The National Research Program *ORIZONT-2000*, 2000-2002.
18. *Using computational cryptography in computer security in Internet*, CNCSI grant, 1999-2000.

Membership of professional organizations

- Committee Member, COST Association COST Action CA15127 - Resilient communication services protecting end-user applications from disaster-based failures (RECODIS): 2016 – Present
- Member of NATO IST Information Systems Technology Panel: 2016 – Present
- Technical Committee Member of Romanian Standards Association, Techniques for Informatics Security Panel

In the program/technical committee/chair of:

- International Conference of the Security for Information Technology and Communication (SECITC), Bucharest, 2008 –2018 editions.
- 10th Jubilee IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI2015), Timisoara, 2015.
- 11th International Conference on COMMUNICATIONS (COMM-2016), IEEE, 2016.
- 9th international Conference on ELECTRONICS, COMPUTERS and ARTIFICIAL INTELLIGENCE, ECAI, 2017.

Review activity for:

- Proceedings of the IEEE Journal, ISSN 0018-9219.
- IEEE Access Journal (ieeeaccess.ieee.org)
- 11th International Conference on COMMUNICATIONS (COMM-2016), IEEE, 2016.
- International Conference on ELECTRONICS, COMPUTERS and ARTIFICIAL INTELLIGENCE (ECAI), 2017, 2018, 2019 editions.
- International Conference of the Security for Information Technology and Communication (SECITC), Bucharest, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2017, 2018, 2019 editions.
- The 5th Edition of Romanian Cryptology Days Conference (RCD 2019), September 2019

Publications:

Books

1. **M. Togan** (2017), „*Cryptographic Technologies for Data Protection in Cloud*", Ed. Matrix Rom, ISBN 978-606-25-0357-4, pp. 1-160 (in Romanian).
2. **M. Togan**, I. Florea (2017), „*Security Infrastructures for Electronic Services in Internet*", Ed. Matrix Rom, ISBN 978-606-25-0356-7, pp. 1-215 (in Romanian).
3. I. Bica, **M. Togan** (2015), *„Security Protocols for Computer Networks"*, Ed. Univers Ştiinţific, ISBN 978-973-1944-68-5, pp. 1-162 (in Romanian).
4. V. Podaru, M. Popescu, **M. Togan** (2007), *„Programming in C"*, Ed. of Military Technical Academy, ISBN 978-973-640-117-6, pp. 1-168 (in Romanian).

Research papers

- 50 papers (Annex 1)

Mihai TOGAN