Moez Ben Mbarka
Cryptolog, 6 rue Basfroi
75011 Paris – France

Date of birth: March 27, 1983

+33(0) 758241940
+216 52270383

moez@ben-mbarka.com
http://moez.ben-mbarka.com/

Eng., Ph.D, Electronic Signature Expert, Project Manager

PROFESSIONAL EXPERIENCE

November 2011 – Today, TrustTIC CEO and Mobile Development Manager, TrustTIC (Tunis), Cryptolog (Paris)
TrustTIC is a Cryptolog R&D division installed in Tunis, Tunisia.

- Since 2012, I manage the mobile development team developing Mobile (iOS and Android) electronic signature solutions based on Universign (www.universign.eu).
- As a CEO of TrustTIC, played the role of devlopment coordinator between Cryptolog and TrustTIC development teams.
- Involved in the devlopment of Cryptolog products for electronic signatures creation and validation.

December 2007 – Today, Electronic Signature Expert, Cryptolog

- Involved in the development of Cryptolog products and the implementation of the main ETSI standards related to electronic signatures such as XAdES, CAdES, PAdES, Signature Validation Policies, Trusted Service Status List, …
- ETSI member and involved in ETSI standards**:**
  - Appointed as an expert in the Specialist Task Force 427 (ETSI/ESI) on “Quick fixes to electronic signatures standards”. Main contributor to the document Electronic Signatures and Infrastructures (ESI);Signature validation procedures and policies (ETSI TS 102 853 V1.1.2)
  - Involved in the Specialist Task Force 426 (TC ESI) "Quick fixes to electronic signatures profiles".
  - Participated in several ESI meetings on behalf of Cryptolog.
  - Participated in several CAdES and XAdES plugtests organized by ETSI and ECOM.
- Managed and was involved in several French and European research projects with focus on security and cryptography. Main projects include:
  - TURBINE (TrUsted Revocable Biometric IdeNtitiEs): based on innovative developments in cryptography and fingerprint biometrics, TURBINE aims to resolve the current privacy concerns regarding the use of fingerprint biometrics for ID management.
  - PAMPA (Password Authentication and Methods for Privacy and Anonymity): One of the goals of this project is to improve existing password-based techniques, not only by using a stronger security model but also by integrating one-time passwords (OTP).

- SAVE (Sécurité et Audit du Vote Electronique): The objective of the project is to define cryptographic protocols for a novel voting system ensuring the confidentiality, the anonymity and the verifiability of votes.

February – July 2007, intern as R&D engineer at Cryptolog – France
Implemented W3C XML Signature and ETSI XML Advanced Electronic Signature standards.

Juin – September 2006, intern as web developer at Esmology Group - Malaysia
Developed Web modules to integrate Cardipay payment system into e-commerce software: XCart and OsCommerce.

August 2005, intern as web developer at Elgazella Communication Centre - Tunisia
Developed a web tool to manage online conference room reservation.

EDUCATION

May 2008 – April 2011, Cryptolog/University of Bordeaux 1, France
Ph.D in Security and Electronic Signatures.
Research interest: focuses on long term validation of electronic signatures and techniques to renew cryptographic archiving proofs. One of the objectives is to develop formal methods to deal with advanced signature validation and extension. The research deals also with signature keys security, access APIs, and compromise mitigation.

Key words: public key infrastructure, long term validation and archiving, advanced electronic signatures, X.509, hardware security module (HSM).

2006 – 2007, University of Bordeaux 1, France
Research Master in Computer Science, specialized in “Parallelism and Distributed Computation”.

2004 – 2007, ENSEIRB (Ecole Nationale Supérieure d’Electronique, d’Informatique et de Radiocom de Bordeaux), France
Engineering degree in Computer Science, specialized in Parallelism and Distributed Computation.

PUBLICATIONS

M. Ben MBarka, F. Krief, and O. Ly.
Entrusting Remote Software Executed in an Untrusted Computation Helper. In the First International Conference on Network and Service Security, 2009

M. Ben MBarka and J. P. Stern.
Observations on Certication Authority Key Compromise. In the Seventh European Workshop on Public Key Services, Applications and Infrastructures, Athens, Greece, June 2010.

M. Ben MBarka, L. Granboulan, and F. Krief.
Using OTP with PAKE: An Optimized Implementation of a Synchronization Window. In the 4th IFIP International Conference on New Technologies, Mobility and Security - Security Track, Paris, France, 2011

M. Ben MBarka, F. Krief, and O. Ly.
Modeling Long-Term Signature Validation for Resolution of Dispute. In Theory of Security and Applications, TOSCA'2011, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2011, Saarbrücken – Germany

M. Ben MBarka and J. P. Stern.
Certificate Validation: Back to the Past. In the Eighth European Workshop on Public Key Services, Applications and Infrastructures, Leuven, Belgium, September 2011

M. Ben MBarka and J. P. Stern.
Certificate Validation: Back to the Past (extended version) in Computers & Mathematics with Applications. DOI: 10.1016/j.camwa.2012.07.012, March 2013.

TECHNICAL PROJECTS

Java Global Platform Shell (JGPShell), http://sourceforge.net/projects/jgpshell
An API and a shell in Java to communicate with Java Cards following Global Platform specifications.

Java Shell RPC, http://jsrpc.fisoft1.com/
An API to do RPC calls in a shell mode.

More info : http://moez.ben-mbarka.com/

TECHNICAL SKILLS

- Experienced Java developers (more than 7 years)
- Advanced knowledge in iOS (Objective-C, C, C++) and Android development.
- Familiar with European standards (ETSI) related to electronic signature (XAdES, CAdES, PAdES, Signature Validation Policies, Trusted Service Status List,…)
- Familiar with IETF and W3C standards related to PKI and XML Securiy (X.509, CRL, OCSP, ERS, XML Signatures,...)

LANGUAGES

Arabic: mother tongue.
French: spoken and written fluently.
English: spoken and written fluently.