Moez Ben Mbarka

6 rue Leonard Euler, BP 6/38
Créteil - 94000 France

Date of birth: March 27, 1983 in Bizerte (Tunisia)

+33(0)758241940
+216 52270383
moez@ben-mbarka.com
http://moez.ben-mbarka.com/

Ingénieur Docteur en Informatique

Expert en signatures électroniques

Expérience professionnelle

Depuis Novembre 2011, Directeur de TrustTIC et chef de projets, Cryptolog/TrustTIC

- J'assume la direction de TrustTIC depuis son lancement en Novembre 2011. TrustTIC est le centre R&D de Cryptolog à Tunis en Tunisie.
- Depuis 2012, je gère l'équipe de développement mobile pour la platforme Universign (www.universign.eu).
- Impliqué activement dans le développement des produits de Cryptolog; en particulier les implémentations de standards Européens pour la création et validation des signatures électronique.

Décembre 2007 – Septembre 2011, Expert en signature électroniques, Cryptolog - France

- J'ai activement participé dans le développement de plusieurs produits de Cryptolog de création, de validation et d'archivage de signatures électroniques.
- J'ai participé dans des groupes de travail ETSI (The European Telecommunications Standards Institute) spécialisés dans la signature électronique :
  - Sélectionné comme expert dans le groupe de travail Specialist Task Force 427 (ETSI/ESI) “Quick fixes to electronic signatures standards”. Je travaille particulièrement sur la définition et la mise au point de procédures de validation de signatures électroniques avancées.
  - J'ai participé dans le groupe de travail Specialist Task Force 426 (TC ESI) "Quick fixes to electronic signatures profiles".
  - J'ai également participé dans plusieurs PlugTests internationaux pour les standards de signatures électroniques organisés par ETSI et ECOM.
  - J'ai participé dans plusieurs réunions ESI au nom de Cryptolog.
- J'ai participé et géré plusieurs projets de recherche Français et Européens :
  - TURBINE (TrUsted Revocable Biometric IdeNtitiEs) : le but du projet est de mettre au point des protocoles innovants combinant des protocoles cryptographiques et biométriques dans des systèmes de gestion d'identité.
  - PAMPA (Password Authentication and Methods for Privacy and Anonymity) : le projet consiste à améliorer des protocoles d'authentification basés sur des mots de passe.
  - SAVE (Sécurité et Audit du Vote Electronique) : le projet consiste à développer un nouveau système de vote avec des protocoles cryptographiques innovants et qui assure plusieurs propriétés telle que : la confidentialité, l'anonymat et la vérifiabilité des votes.

Février – Juillet 2007, stage ingénieur R&D, Cryptolog – France
Implémentation du standard W3C «XML Signature Syntax and Processing» et le standard ETSI « XML Advanced Electronic Signature ».

Juin – Septembre 2006, stage développement web, Esmology Group - Malaisie
Développement de modules Internet pour l'intégration du système de payement Cardipay dans des logiciels de vente en ligne (Xcart et OsCommerce).

Aout 2005, stage développement web, Centre de Communication ElGazella - Tunisie
Développement d'outils web pour la gestion et la réservation de salles de conférence.

Education

Mai 2008 – April 2011, Cryptolog/LaBRI (Université de Bordeaux 1), France
Thèse en sécurité et signature électronique. Thèse CIFRE préparée en collaboration entre l'entreprise Cryptolog et le Laboratoire Bordelais de Recherche en Informatique (Labri) spécialisée dans le domaine de la signature électronique et la gestion de preuves.
Soutenance : thèse défendue le 06/04/2011. Mention : très honorable.

Titre : Signatures Electroniques avancées : modélisation de la validation à long terme et sécurité des autorités de certification

Mots clé : infrastructure de clé publique, signature électronique, sécurité conditionnelle, autorité de certification, externalisation de code.

Principaux sujets de recherche :

- Modélisation et formalisation de la validation de signature électronique dans le contexte de dispute à long terme. Le modèle doit supporter les notions de base de la validation de signatures électroniques et l'infrastructure de clé publique. La formalisation doit permettre de modéliser plusieurs protocoles utilisés en pratique (IETF ERS et ETSI AdES).
- Etude de la sécurité de clés de signatures des Autorités de Certification. L'étude porte sur les paramètres optimales pour la gestion de la révocation et sur l'externalisation de code pour permettre à un module cryptographique, disposant d'une puissance de calcul limitée, à utiliser une machine plus puissante mais moins sécurisée.

2006 – 2007, Université de Bordeaux 1, France
Master de recherche 2. Spécialité : « Parallélisme, calcule distribué et haute performance ».

2004 – 2007, ENSEIRB (Ecole Nationale Supérieure d'Electronique, d'Informatique et de Radiocom de Bordeaux), France
Etude d'ingénieur en Informatique. Spécialité : « Parallélisme, calcule distribué et haute performance ».

2002 – 2004 : Institut Préparatoire aux Etudes Scientifiques et techniques (IPEST) - Marsa, Tunisie
Classes préparatoires, filière MP

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, Paris, France, 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, LNCS 6711. Springer-Verlag, Athens, Greece, 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), Saarbrücken, Germany, 2011.

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.

Projets techniques

Java Global Platform Shell (JGPShell), http://sourceforge.net/projects/jgpshell
Une API et un shell Java pour gérer le contenu des cartes à puce (Java Card) et respectant les standards Global Platform.

Java Shell RPC, http://jsrpc.fisoft1.com/
Une façon (en Java) simple pour créer des services RPC sous forme d'un shell.

Plus de détails : http://moez.ben-mbarka.com/

Divers

- Une expérience de plus de 7 ans en développement Java
- Solides connaissances en développement iOS (Objective-C, C et C++) et Android
- Très familier avec les divers standards Européens (ETSI) en relation avec les signatures électroniques tels que : XAdES, CAdES, PAdES, Signature Validation Policies, Trusted Service Status List,…
- Très familier avec les divers standards IETF et W3C portant sur la PKI (Public Key Infrastructure) et les signatures électroniques : X.509, CRL, OCSP, ERS, XML Signature,...

LANGUAGES

Arabe : langue maternelle.
Français : courant.
Anglais : bon niveau, 560 au TOEFL, stage linguistique de 1 mois (Juillet 2005) à Malte (Cours en Anglais général).