

# Tulio de Souza

Computer Scientist, M.Sc.

5 Ellison Apartments, Merchant Street  
E3 4PT

☎ 07594640627

✉ [contact@tuliosouza.com](mailto:contact@tuliosouza.com)

---

## Education

2006–2008 **M.Sc. in Computer Science**, *Federal University of Santa Catarina*, Florianópolis, Brazil.

Master Thesis

title *Technical and theoretical aspects of the management of the life cycle of cryptographic keys in the OpenHSM*

grade First Class Honour

supervisor Professor Ricardo Felipe Custódio

2007–2007 **General English (GE) and CAE Classes**, *Waterloo School of English*, London - UK.  
GE - All the way from intermediate to advanced level  
CAE - Approved in the Certificate in Advanced English exam in December/2007

2001–2005 **Bachelor in Information Systems**, *Federal University of Santa Catarina*, Florianópolis, Brazil.

Undergraduate Thesis

title *Embedded applications for management of cryptographic keys*

grade First Class Honour

supervisor Jean Everson Martina

co-supervisor Professor Ricardo Felipe Custódio

---

## Work Experience

2007–now **Software Architect and Software Engineering Team Leader**, *Avanti Communications Ltd*, London/UK, <http://www.avantiplc.com/>.

Avanti Communications is a supplier of satellite communications services for business, institutional and residential customers. Avanti delivers broadband and corporate data connectivity as well as critical applications such as Business Continuity. All these services are delivered across Europe directly or via its comprehensive network of resellers, wholesalers and virtual network operators. On top of that, Avanti's first satellite will be launched late 2009.

Software Architect

description Design and Implementation of the Operation Support System (OSS) for the operations area of the company. It is a WEB application that supports multi-vendors' satellite terminals and wireless equipment, providing Avanti and its partners with an easy and intuitive way of installing and troubleshooting satellite broadband services.

resources PHP, Drupal, CSS, JavaScript, MySQL, Oracle, MsSQL, Eclipse, Linux, Satellite Controller (HUB), Java, C, Traffic Shapper, DNS, SNMP, SAP Business One.

#### Software Engineering Team Leader

description Allocating activities across the team in order to suite deadlines. Definition and enforcement of processes to be followed by the team and other members of the company, for example in the creation and/or changes of requirements. Attendance in operations, networking and new products development meetings as the member representative of the team. The recruitment of new developers is also part of the responsibility.

resources Projects Management Tool (Redmine), control version system (subversion), wiki, regular meetings, agile methodology (XP Programming).

2004–2007 **Project Manager and Security Developer, LabSEC - Computer Security Laboratory, Florianópolis/BR, <http://www.labsec.ufsc.br/>.**

LabSEC is part of the Department of Computer Science of the Federal University of Santa Catarina. The Lab's main goals are: to study, research, evaluate and implement solutions in the computer security field. In particular: cryptography, digital signature, computer security systems, public key infrastructure and cryptographic protocols. The two main projects in the lab were ICP EDU and João de Barro. The ICP EDU project developed a low cost Hardware Security Module (OpenHSM) for Educational Institutions and built a public key infrastructure across the Education Institutions in Brazil, using the developed HSM. The João de Barro Project developed the new root certification authority solution to be used in the Brazilian Public Key Infrastructure. The LabSEC was responsible for developing the certificate management suite (YWAPA).

#### Quality Manager

project João de Barro - YWAPA

description Responsible for the quality management of the project. It was used CMMI level 2 as reference.

resources CMMI, Quality Management Document, Regular Meetings, Code Inspection

#### Security Module Developer

project João de Barro - YWAPA

description Development of a Cryptographic Security Provider in C++ to support the requirements coming from other modules (core, user interface and persistence). Its result was a fully object oriented library (libcryptosec) that has been used for other projects in the Lab. A detailed study of OpenSSL internal functionality had to be performed.

resources C++, OpenSSL, Object Oriented Programming, CMMI, UML, Red Hat, PKI, Smart cards, Secret Sharing, PKCS#11

#### Development Team Leader

project ICPEDU

description Development of an embedded application in C to manage the life-cycle of cryptographic keys. Another 2 applications written in C were required: client application to allow remote management of the HSM and an OpenSSL engine to allow the use of those keys managed by the HSM.

resources C, OpenSSL, OpenSSL Engines, PKI, Sockets, SSL, Embedded Application, Secret sharing, FreeBSD, Smart cards.

2003–2004 **Network Administrator, Web Developer and User Support**, *COPERVE*, Florianópolis/BR, <http://www.coperve.ufsc.br/>.

This organisation writes and applies the Federal University of Santa Catarina (UFSC) admission exams. This exam is required in order to join the university. UFSC is a free public University and every year around 40,000 people take this exam.

#### Network Administrator

description Installation, maintenance and upgrades of the network. These activities were developed with full control over the whole network.

technologies Linux, Routers, Web servers (Apache + SSL), Mail servers (Qmail and Postfix), Firewalls (iptables, DMZ, snort, nat, ipw), Database servers (Sybase and MySQL), Anti-virus server, File sharing server (Samba), DNS Server (Bind).

#### User Support

description assist COPERVE's employees in computer related enquiries

#### Web developer

description implementation of the subscription system for the admission exam and other additional applications

resources PHP, HTML, CSS, JavaScript, SQL, Sybase, MySQL

2002–2002 **Network Administrator, Hardware maintenance and User Support**, *Secretary of the Treasury - SEF-SC*, Florianópolis/BR, <http://www.sef.sc.gov.br/>.

SEF-SC is a Government Institution that manages the finance sector of Santa Catarina state. It includes more than 30 branches distributed around the state and has a main building in Florianópolis, capital of Santa Catarina. In this site works more than 300 people.

#### Network Administrator

description Keep the existent network environment up and running.

resources Linux, Windows 2000 Server, Print Servers, Routers, Routers, Switches, Active Directory.

#### User Support

description assist the SEF's employees in all kinds of problems involving computers: from software to network issues.

#### Hardware Maintenance

description Troubleshoot computer related equipments in order to fix their problems. It includes formatting hard-disk, operational system installations, peripherals replacement, and others.

resources Microsoft Windows, Installation of windows applications, hardware troubleshooting and replacement

---

## Languages

portuguese **Native Speaker**

english **CAE Certified**, in *December 2007*.

CAE is offered by Cambridge ESOL Examinations. Homepage: [www.cambridgeesol.org](http://www.cambridgeesol.org).

CAE is at Level C1 of the Common European Framework of Reference for Languages (CEFR)

---

## Publications

- SBSEG 2009 J. E. Martina, **T. C. S. de Souza** and R. F. Custódio. Ceremonies Design for PKI's Hardware Security Modules. In SBSEG 2009: 9th Brazilian Symposium on Information and Computer System Security, Campinas, São Paulo, Brazil, September 2009.
- PASSAT 2009 J. E. Martina, **T. C. S. de Souza** and R. F. Custódio. Ceremonies Formal Analysis in PKI's Context. In PASSAT 2009: The 2009 IEEE International Conference on Information Privacy, Security, Risk and Trust, Vancouver, Canada, August 2009.
- IDTrust 2008 **T. C. S. de Souza**, J. E. Martina, and R. F. Custódio. Audit and backup procedures for hardware security modules. In IDtrust '08: Proceedings of the 2008 7th Symposium on Identity and Trust on the Internet, Gaithersburg, MD, USA, March 2008. ACM.
- EuroPKI 2007 J. E. Martina, **T. C. S. de Souza**, and R. F. Custódio. Openhsm: An open key life cycle protocol for public key infrastructure's hardware security modules. In Fourth European PKI Workshop: Theory and Practice, volume 4582 of Lecture Notes in Computer Science, pages 220–235, Palma de Mallorca, Spain, June 2007. Springer-Verlag Berlin Heidelberg.

---

## Personal Information

gender Male  
date of birth 06 September 1983  
nationality Italian  
Brazilian

---

## References

**Professor Ricardo Felipe Custódio** (Master thesis supervisor)

e-mail [custodio@inf.ufsc.br](mailto:custodio@inf.ufsc.br)  
homepage <http://www.inf.ufsc.br/~custodio>  
location Federal University of Santa Catarina  
Florianópolis, SC, Brazil

**Jean Everson Martina, Ph.D Student** (Undergraduate thesis supervisor)

e-mail [jean.martina@cl.cam.ac.uk](mailto:jean.martina@cl.cam.ac.uk)

homepage <http://www.cl.cam.ac.uk/~jem74>  
location University of Cambridge – Computer Laboratory  
Cambridge, UK