

Massimiliano Pala

Research Fellow
computer science, Dartmouth College

6211 Sudikoff Labs, Hanover, NH 03755, US
tel: (603) 369 9332 | fax: (603) 646 1672
pala@cs.dartmouth.edu | project.manager@openca.org
<http://www.cs.dartmouth.edu/~pala/>

interests Usable Security

Public Key Infrastructures, Digital Certificates, Usability, Distributed Systems, Network Applications, Peer-to-Peer systems

education

Mar 2007 **PhD, Computer Engineering**, Politecnico of Turin (Italy)
Improving PKI Usability and Interoperability
Adviser: Antonio Lioy

Jul 2003 **Laurea(BS+MS), Computer Engineering**, University of Modena (Italy)
The OpenCA project
Adviser: Michele Colajanni

experience

2009-now **Research Fellow**, Computer Science, Dartmouth College
2007-2009 **Research Fellow**, Institute for Security, Technology and Society (ISTS)
2004 **Security Software Engineer**, Solving S.r.l
2003-2004 **Software Engineer**, UnoX1 Project, Modena's Municipality
2001-2006 **Company Founder and Project Manager**, Nabra2 S.r.l
2001-2002 **PKI Architect**, University of Modena and Reggio Emilia
2001 **PKI Architect**, Modena's Municipality

fellowships

2004-2006 Italian National PhD Fellowship

teaching Classes

2008 **Teaching Assistant**, *Advanced Operating Systems*, Dartmouth College
2006 **Instructor**, *Security and Architecture of Distributed Systems*, Politecnico di Torino

- 2005 **Teaching Assistant**, *Organizational Models and Strategies for e-Business*, Politecnico di Torino

teaching Other

- 2006 Massimiliano Pala. **OpenCA OCSPD: from the O to the Daemon**, OCSPD tutorial, Free and Open Source Software Developers European Meeting, Brussels, Feb 25-26, 2006

mentoring undergraduate students

- 2009 Yifei Wang, Women in Science Program, Dartmouth College
2009 Sehwan Ahn, Google Summer of Code, Dartmouth College and Google
2005 Riccardo Re (undergraduate), Politecnico di Torino
Giampiero Restaino (undergraduate), Politecnico di Torino
2004 Paolo Serra (undergraduate), Politecnico di Torino

publications journal articles

- 2009 [J3] Massimiliano Pala and Shreyas Cholia and Scott A. Rea and Sean W. Smith. *Interoperable PKI Data Distribution in Computational Grids*. In *International Journal of Grid and High Performance Computing (IJGHPC)*, Volume 1, Issue 2, pages 56-73. January-March 2009.
[J2] Massimiliano Pala and Sean W. Smith. *Finding the PKI Needles in the Internet Haystack*. In *Journal of Computer Security*, To Appear (Accepted for publication).
2006 [J1] M. Pala, M. Marian, N. Moltchanova, A.Lioy. *PKI past, present and future*. In *International Journal on Information Security*, Springer Verlag, Vol. 5, No. 1, January 2006, pp. 18-29, ISSN:1615-5262 (Paper) 1615-5270 (Online)

conference articles

- 2009 [C8] Massimiliano Pala and Yifei Wang. *On the Usability of User Interfaces for Secure Website Authentication in Browsers*, In *EuroPKI 2009: Proceedings of the 6th European PKI Workshop on Public Key Infrastructure*, Pisa, Italy, September 2009
[C7] Massimiliano Pala and Scott A. Rea. *Usable Trust Anchor Management*. In *8th Symposium on Identity and Trust on the Internet (IDtrust 2009)*, NIST, Gaithersburg, MD, April 2009.
2008 [C6] Massimiliano Pala and Sean W. Smith. *Peaches & Peers*. In *EuroPKI-2008: Proceedings of the 5th European PKI workshop on Public Key Infrastructure*, vol. 5057/2008 of *Lecture Notes in Computer Science*, pp. 223-238, Springer-Verlag. ISBN:978-3-540-69484-7
[C5] Massimiliano Pala, Scott A. Rea, Shreyas Cholia, and Sean W. Smith. *Extending PKI interoperability in Computational Grids*. In *Proceedings of the 8th IEEE International Symposium on Cluster Computing and the Grid (CCGrid 2008)*, pp. 645-650, IEEE Computer Society, May 2008
2007 [C4] Massimiliano Pala and Sean W. Smith. *AutoPKI: a PKI Resources Discovery System*. In *EuroPKI-2007: Proceedings of the 4th European PKI Workshop on Public Key Infrastructure*, vol. 4582/2007 of *Lecture Notes in Computer Science*, pp. 154-169, Springer-Verlag. ISBN: 978-3-540-73407-9, DOI: 10.1007/978-3-540-73408-6

- 2006 [C3] Massimiliano Pala and Antonio Lioy. *Fighting e-mail abuses: the EMPE approach*. In *EuroPKI-2006: Proceedings of the 3rd European PKI Workshop on Public Key Infrastructure*, vol. 4043/2006 of *Lecture Notes in Computer Science*, pp.130-144, Springer-Verlag. ISBN: 3-540-35151-5, DOI: 10.1007/11774716_11
- 2005 [C2] Gianluca Ramunno, Massimiliano Pala, Marco Aime, and Antonio Lioy. *Motivations for a Theoretical Approach to WYSIWYS*. In *CMS-2005: Proceedings of IFIP International Conference on Communications and Multimedia Security*, Vol. 3677/2005 of *Lecture Notes in Computer Science*, pp. 289-290, Springer-Verlag. ISBN: 3-540-28791-4, ISSN: 0302-9743
- 2004 [C1] Massimiliano Pala, Marius Marian, Natalia Moltchanova, and Antonio Lioy. *The EuroPKI Experience*. In *EuroPKI 2004: Proceedings of the 1st European Workshop on Public-Key Infrastructures*, Vol. 3093/2004 of *Lecture Notes in Computer Science*, pp. 14-27, Springer-Verlag. ISBN: 3-540-22216-2, ISSN: 0302-9742

other relevant publications

- 2009 [O2] Massimiliano Pala. *The PKI Resource Query Protocol (PRQP)*. Internet Draft, PKIX WG, Experimental, IETF Archive, November 2009, <draft-ietf-pkix-prqp-03.txt>
- 2006 [O1] Massimiliano Pala, Diana Berbecaru, and Antonio Lioy. *System Description Language*. In *POSITIF Project*, March, 2006, Available Online: <http://www.positif.org/isdl.html>

awards

- 2008 “*Extending PKI interoperability in Computational Grids*”—Selected Paper for extended publication (STPG)
- 2007 “*AutoPKI: a PKI Resources Discovery System*”—Selected Paper for extended publication (EuroPKI)
- 2004 “*The EuroPKI Experience*”—Selected Paper for extended publication (EuroPKI)

services professional

- 2009 EuroPKI, Papers Committee Member
- 2009 IDTrust, Papers Committee Member

funds awarded

- 2009-2010 Michael Locasto, Sean W. Smith, Duminda Wijesekera, Angelos Stavrou, Massimiliano Pala, Scott A. Rea, Sergey Bratus. *Securing the Railway IT Infrastructure*. A proposal to I3P, Nov 2009 — Mar 2010.
- 2007-2009 Sean. W. Smith (PI), Massimiliano Pala (Investigator), Scott A. Rea. *Interoperability and Usability for PKI Management*
Institute for Security Technologies Studies and Department of Homeland Security, Jan 2007—Mar 2009

submitted

- 2009 Massimiliano Pala. *Portable PKI System Interface for Internet Enabled Operating Systems*. A proposal to CISCO, Submitted for review - Nov 2009
Massimiliano Pala (PI), Scott A. Rea. *TC: Small: Trusted Computing PKI Globally-available Locally-managed Usable Environment*. A proposal to NSF, Submitted for review - Nov 2009
Denise Anthony (PI), Sergey Bratus, Massimiliano Pala (Investigator), Anna Shubina. *Empirical Approach to Security Evaluation (EASE)*. A proposal to NIST, Submitted for review - Aug 2009
Sean W. Smith (PI), Massimiliano Pala (Co-PI), David Nicol (PI), Jingwei Huang (Co-PI), Scott A. Rea. *Trust Metrics in PKI*. A proposal to NIST, Submitted for review - Aug 2009

invited talks

- 2009 [T6] Massimiliano Pala. *Issuing Grid Credentials with OpenCA*
25th Open Grid Forum, Catania, Italy, Mar. 1-6, 2009
- 2008 [T] Massimiliano Pala. *Under the OpenCA 1.0.2 Hood*
8th TAGPMA F2f Meeting, La Plata, Argentina, November 2008
[T] Massimiliano Pala. *OpenCA 1.0.0: Really ?*
7th TAGPMA Meeting, Oakland, US, April 2008
Massimiliano Pala. *iPKI* Updates: OpenCA, OpenCA-NG and PKI Discovery System*
CAOPS Working Group, 22nd Open Grid Forum, Boston, US, February 25-28, 2008
- 2007 [T5] Massimiliano Pala. *The PKI Resource Query Protocol Explained*
TAGPMA Conference, Santiago, Chile, Nov 6-9, 2007
[T4] Massimiliano Pala. *OpenCA-NG: Usable PKI and PKI enabling library*
TAGPMA Conference, Santiago, Chile, Nov 6-9, 2007
- 2006 [T] Massimiliano Pala. *Toward OpenCA's Next Generation: Technical Aspects and Insights of the New Codebase*
Free and Open Source Software Developers' European Meeting, Brussels, Feb 25-26, 2006
- 2005 [T3] Massimiliano Pala. *The OpenCA Project and The EuroPKI Infrastructure*
African and Arab Regional Conference on Electronic Transaction Security Digital Signature and PKI, Tunis, June 20-22, 2005
- 2002 [T2] Massimiliano Pala. *OpenCA Project status and SmartCards usage in PKIs*
ERLUG2002, Engineering faculty - University of Modena and Reggio Emilia, Modena, Italy, November 23, 2002
- 2000 [T1] Massimiliano Pala. *The OpenCA project*
LIME2000, Engineering faculty - University La Sapienza, Rome, Italy, November 11 - 12, 2000