



Stephen Wilson PKI profile

Stephen Wilson is a leading international authority on Public Key Infrastructure, and one of the most influential figures in the evolution of PKI in Australia. He has helped organisations across the Asia Pacific establish effective PKI systems, providing advice on strategy, architecture, policy, privacy, application enablement, technology selection and governance. He has been intimately involved with such pivotal PKI programs as Gatekeeper, Identrus, HeSA, Webtrust for CAs, the American Bar Association PKI Guidelines, and numerous commercial CAs in Australia, the US, Malaysia and Hong Kong. Stephen chaired the international OASIS PKI Adoption Technical Committee 2007-08, and has been an independent member of the Gatekeeper Policy Committee since its inception. He has been awarded three PKI patents. See www.lockstep.com.au/library/pki.

PKI strategy experience

- **National e-Health Transition Authority (NEHTA) 2007-08:** Principal Consultant providing strategic advice on the business case and detailed requirements for a proposed PKI-based national authentication service for healthcare providers.
- **South Australia Department of Health 2008:** Developed PKI strategic needs analysis and a decision making framework in support of enterprise-wide authentication and identity management reform (see also “operations” below)
- **Project Gatekeeper, Australian Govt Info Management Office (AGIMO) 2006:** Subject matter expert in a consortium implementing the revised Gatekeeper Framework; responsible for Relationship Certificate Guidelines, template certificate policies, and new digital credential specifications.
- **Project Gatekeeper, AGIMO 2005:** Principal Consultant undertaking a strategic review of the Gatekeeper program; responsible for introduction of community of interest, “Relationship Certificates” and “Security Printer” models that have dramatically reduced the cost and overhead of Gatekeeper conformance.
- **Medicare Australia Health eSignature Authority (HeSA) 2005-06:** Developed new certificate ‘push’ distribution models for healthcare professionals, including new community-of-interest and “Known Customer” methods; developed new short form CPs for multiple Medicare Australia programs; analysed and workshopped detailed business requirements across internal and external organisations.
- **eASEAN secretariat, 2004-06:** PKI subject matter expert on a two year project developing harmonised e-commerce legal infrastructure for 10 S.E. Asian nations.
- **Indonesian Ministry of Telecommunications, 2002:** Developed strategy, business case, operations model and pilot plan for the proposed Indonesian National CA.
- **New Zealand Cabinet, 2000:** Drafted the Cabinet’s PKI policy position paper.
- **South Australia Department of Administration and Information Services, 2000:** Developed the Whole of Government PKI Strategy.
- **New Zealand State Services Commission, 2001:** Developed offshore CA accreditation guidelines.

- **New Zealand Bankers Association, 2000:** Wrote the finance sector PKI strategy.
- **“Accreditation based PKI” model, 1999:** Conceived this breakthrough proposal for international PKI governance, with better interoperability and cross recognition, contestable audit and international upgrade paths; see [12], [14], [19].

PKI operations achievements

- **South Australia Department of Health, 2009:** Drafted the Certificate Policy and Certification Practice Statements for enterprise wide PKI services.
- **Major financial institution, 2007:** Conducted a detailed Gatekeeper gap analysis to underpin project planning for accreditation of a new PKI operation.
- **Health eSignature Authority, 2003-04:** Technical Account Manager overseeing business process reengineering and Gatekeeper re-accreditation after the acquisition of Baltimore Technologies by SecureNet.
- **Australian Tax Office, 2003:** Led the Gatekeeper Environmental Impact Statement for the PKI re-accreditation when the ATO gateway environment was upgraded.
- **Identrus, 2001:** Led the development of the innovative *Starterpak* documentation template system to support fast-tracked managed PKI services.
- **Cybersign Malaysia, 2001:** Principal consultant working on site (in Cyberjaya) in support of this new CA business and operation.
- **PricewaterhouseCoopers beTRUSTed, 1999-2001:** Founding Asia Pacific Director and core management team member during the build phase of what was the world’s most sophisticated managed PKI service; lead author and editor for the beTRUSTed global CP/CPS.
- **Dun & Bradstreet-KPMG Enshrine, 1999:** Conceived, developed and launched the world’s first SSL site certificate service offering two year evergreen certificates and automatic vetting against securities commission databases, now industry standards.
- **Certificates Australia Pty Ltd (CAPL), 1997:** Project manager for the first Gatekeeper accredited CA in Australia.

PKI policy, governance & regulatory experience

- **Macau Bureau of Telecommunications Regulation, 2008:** Principal Consultant on the development of a strategic cross-recognition framework for digital certificates, including worldwide survey of e-government applications and state-of-the-art PKI.
- **Singapore National Authentication Framework, 2006:** PKI subject matter expert helping an international team develop a new national identity management service.
- **Kazakhstan Ministry of Internal Affairs, 2006:** Principal Consultant undertaking a feasibility study for the establishment of a national multi-purpose PKI.
- **Hong Kong Post CA, 2001:** Business case review.
- **Privacy Commissioner’s PKI Reference Group, 2001:** Invited member of a task force to review privacy provisions in the Gatekeeper framework.
- **Hong Kong CA Recognition Office (CARO), 1999:** Led the international team that won the consultancy to establish this new regulatory function under the HK electronic transaction ordinance.

- **Certification Forum of Australasia, 1998-2001:** Elected unopposed three years running to chair the peak PKI industry body.
- **National Electronic Authentication Council, 1998-2001:** Founding member of this policy advisory body convened by the Federal Department of Communications.
- **WebTrust for CAs scheme, 2000:** Major reviewer of the draft assurance scheme on behalf of the Institute of Chartered Accountants Australia; see www.pkilaw.com/AICPA_WebTrustForCAs_v1.0_sgwcomm000328.zip.

PKI research achievements

- **Australian patents 743570 (2001), 2004201058 (2004) and 2004100268 (2004):** for PKI and smartcard based privacy and web authentication methods.
- **Standard Chartered Bank Singapore, 2001:** Led an international survey of digital signature regulations and interoperability with Identrus.
- **OASIS, 2005:** Researched and developed a new PKI ROI model, featuring a novel digital certificate supply chain model (see [5]).
- **OASIS, 2004 & 2007:** Researched, designed and collated the new OASIS PKI website (see <http://idtrust.xml.org/wiki>).
- **OASIS, 2005-06:** Designed the 3rd International PKI Survey.
- **PricewaterhouseCoopers Cryptographic Centre of Excellence, 2000:** Led the Asia Pacific Chapter of the biggest private sector team of cryptographers in the world.

Committees & Associations

- Gatekeeper Policy Committee (since 2004)
- AiG Digital Technologies Forum (formerly the Australian IT Security Forum; Co-chair 2006-07; member since 1998)
- NATA IT Testing Accreditation Advisory Committee (since 2003)
- Standards Australia Information Security Committee IT-12-4 (since 2004)
- OASIS PKI Adoption Technical Committee (Chair 2007-08; member 2004-08)
- Australian Law Reform Commission Emerging Technology Committee (2007-08)
- Asia PKI Forum (elected OASIS Liaison Representative, 2005-08)
- Certification Forum of Australasia (Chair, 1998-2001)
- National Electronic Authentication Council NEAC (1998-2001)
- American Bar Association Information Security Committee (1999-2002)
- APEC e-Authentication Task Group (1998-2001)
- Federal Privacy Commissioner's PKI Reference Group (2001)
- Standards Australia PKAF Committee IT 12-4-1 (1997-2001).

Selected PKI publications

- [1]. *Public Key Superstructure: It's PKI Jim but Not As We Know It*, 7th Symposium on Identity and Trust on the Internet, NIST, Gaithersburg, USA, 2008
<http://middleware.internet2.edu/idtrust/2008/papers/07-wilson-public-key-superstructure.pdf>

- [2]. *An easily validated security model for e-voting based on anonymous public key certificates* AusCERT2005 Refereed Academic Stream May 2008
<http://conference.auscert.org.au/conf2008/Proceedings-SETMAPE.pdf>
- [3]. *The importance of PKI today* China Communications, Dec 2005 www.china-cic.org.cn/english/digital%20library/200512/3.pdf
- [4]. *A new manifesto for smartcards as national information infrastructure*, 5th Homeland Security Conference Canberra, September 2006
- [5]. *Guidelines on how to determine Return on Investment in PKI* OASIS White Paper June 2005
www.pkiforum.org/whitepaper/roi.pdf
- [6]. *A novel application of PKI smartcards to anonymise Health Identifiers* AusCERT2005 Refereed Academic Stream May 2005
<http://conf.isi.qut.edu.au/auscert/proceedings/2005/wilson05novel.pdf>
- [7]. *Patient Privacy and Security – Not a zero sum game!* Wilson, Connolly and Denney-Wilson, Journal of the Australian Epidemiology Association V12.1 April 2005
- [8]. *A summary of PKI data for Australia* Asia PKI Forum, Tokyo, Feb 2005
- [9]. *Position Statement on PKI of the Australian Security Industry* Australian IT Security Forum Nov 2003
- [10]. *Rethinking PKI – the electronic business card* SC Magazine June 2003
<http://www.scmagazine.com/asia/news/article/419737/rethinking-pki>
- [11]. *PKI without Tears* American Bar Association eBlast Jan 2003
www.abanet.org/scitech/nosearch/eblast/eblastarticle1.html
- [12]. *Demystifying international cross-recognition of PKI: we've been barking up the wrong tree* International Security Solutions Europe Conf., London Sept 2001
- [13]. *Comparison of Authentication Technologies* Asia Business Law Review 2001
- [14]. *Leveraging external accreditation to achieve PKI cross-recognition* Attorney Generals Privacy & Security conference Melbourne 2001
- [15]. *PKI and the Acceleration of B2B* European-American Business Journal Spring 2001
- [16]. *Will Biometrics Obsolete PKI?* American Bar Assoc. Bulletin of Law, Science & Tech, June 2001 www.abanet.org/scitech/eblast/may01/2may01.html#Bio
- [17]. *Audit based public key infrastructure* Certification Forum of Australia Nov 2000
http://www.lockstep.com.au/library/pki/audit_based_public_key_infras
- [18]. *Attribute Certificates and their Limitations* Journal of the PricewaterhouseCoopers Cryptographic Centre of Excellence Issue 3, 2000
- [19]. *New models for the management of public key infrastructure and root certification authorities.* Proceedings of 7th IFIP Conference Info Security, Amsterdam 1999
- [20]. *Privacy positive aspects of public key infrastructures* Privacy Law & Policy Reporter, Vol 5.10, 1999 <http://bar.austlii.edu.au/au/journals/PLPR/1999/26.html>
- [21]. *Current issues in the rollout of a National Authentication Framework* Information Industry Outlook Conference, Canberra 1998
- [22]. *Some limitations of web of trust models* Information Management & Computer Security, Vol. 6, No. 5, 1998 (Highly Commended Award winner, MCB University Press).