Stephen Wilson
PKI profile

Stephen Wilson is a leading international authority on Public Key Infrastructure. He has helped organisations across the Asia Pacific establish effective PKI systems, advising on strategy, architecture, policy, privacy, business process change, technology selection and governance. He has been intimately involved with such pivotal PKI programs as Gatekeeper (the Australian government PKI regulator), Identrus, Medicare Australia's Health eSignature Authority, Webtrust for CAs, the American Bar Association PKI Guidelines (PAG), and numerous commercial CAs in Australia, the US and Asia. He has provided PKI advice to the governments of New Zealand, Singapore, Hong Kong, Macau, Indonesia, Kazakhstan and Australia. Stephen chaired the international OASIS PKI Adoption Technical Committee, and was an independent member of the Gatekeeper Policy Committee for all of its 12 year existence. He has been awarded nine PKI patents, and is currently undertaking a PhD on the evolution and ecology of digital identity, at the Australian Defence Force Academy. See also www.lockstep.com.au/library/pki.

PKI solutions and operations

- **"Mobile Device Attributes Validation" (MDAV), Dept Homeland Security 2016-18**: Awarded an R&D contact with the DHS Science & Technology Directorate to develop an attribute certificate mobile wallet and managed PKI backplane, for an initial use case of First Responder credential management.
- **National eHealth Transition Authority (NEHTA) 2011-12**: PKI Manager, National Authentication Service for Health (NASH); led Gatekeeper compliance work stream; reviewed and maintained CP/CPS; drafted the risk management strategy for a push distribution model interfaced to the national health provider registry.
- **South Australia Department of Health, 2009-11**: Drafted the Certificate Policy and Certification Practice Statements for enterprise-wide PKI services; designed and conducted the Root CA key signing ceremony; liaised with legal counsel on new PKI user terms & conditions.
- **Major financial institution, 2007**: Conducted a detailed Gatekeeper gap analysis to underpin project planning for accreditation of a new PKI operation.
- **Medicare Australia Health eSignature Authority (HeSA) 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, Malaysia) 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 standard.
- **Certificates Australia Pty Ltd (CAPL) 1997**: Project manager for the first Gatekeeper accredited CA in Australia.

PKI strategy experience

- **National eHealth Transition Authority (NEHTA) 2011**: Conducted a Threat & Risk Assessment of electronic signature patterns, in the context of the National E-Authentication Framework, across a comprehensive range of e-health use cases
- **NEHTA 2007-08**: Developed the business case for a national PKI for health service providers, the "National Authentication Service for Health" (NASH), and an initial fast tracked procurement strategy (not subsequently taken up).
- **South Australia Health, 2008**: Developed a strategic PKI needs analysis and decision making framework in support of enterprise-wide authentication and identity management reform (see also *Operations* below)
- **Project Gatekeeper, Aust Govt Info Mgt Office (AGIMO) 2006**: Subject matter expert implementing the revised Gatekeeper Framework; responsible for *Relationship Certificate* Guidelines, template certificate policies, and new digital credential specifications.
- **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 Certificate Policies for multiple Medicare programs; worked with Medicare legal counsel to develop core liability clauses still in use today; developed detailed business requirements across internal and external health organisations.
- **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.
- **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.
- **NZ State Services Commission, 2001**: Wrote the offshore CA accreditation guide.
- **New Zealand Bankers Association, 2000**: Wrote the finance sector PKI strategy.
- **"Accreditation based PKI" model, 1999**: Conceived this breakthrough proposal for international PKI governance; see [27], [29], [34].

PKI policy, governance & regulatory work

- **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.
- **Asia PKI Forum, 2005-8**: OASIS Liaison Member.
- **Hong Kong Post CA, 2001**: Undertook a PKI business case review.
- **Privacy Commissioner's PKI Reference Group, 2001**: Invited member of a task force to review the privacy provisions in the Gatekeeper framework.
- **Hong Kong CA Recognition Office (CARO) 1999**: Led the international team appointed 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).

PKI research achievements

- Multiple patents for ***Authenticating electronic financial transactions*** US 8,608,065, US 8,286,865, AU 2009238204 and NZ 589160
- Multiple patents for ***System and method for anonymously indexing electronic record systems*** US 8,347,101 and AU 2005220988
- Australian patent ***Verified anonymous code signing*** AU 2012101460
- **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 [18]).
- **"Relationship Certificates", 2005**: Created this new formulation for X.509 certificates, to represent a user's attribute(s) in the context of a community of interest, instead of their general identity; Relationship Certificates were adopted in the Australian Government PKI framework, and implemented in several health sector projects, including NASH.
- **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

- Kantara Initiative (since 2016)
- International Association of Privacy Professionals (since 2008)
- Privacy Track Chair, Cloud Identity Summit (since 2016)
- Judge, Mobile World Congress GLOMO Awards – Identity (since 2016)
- Standards Australia Information Security Committee IT-12-4 (since 2004)

- Gatekeeper Policy Committee (2004-16)
- NATA IT Testing Accreditation Advisory Committee (2003-14)
- 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)
- Australian IT Security Forum (1998-2009; Co-chair 2006-07)
- 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).

PKI related publications

[1]. *A Digital Identity Stack to Improve Privacy in the Internet of Things*, S. Wilson, N. Moustafa & E. Sitnikova, IEEE World Forum on IoT, Singapore, Feb 2018

[2]. *FIDO Alliance Update: Certification and Disruption,* Constellation Research, Oct 2017

[3]. *FIDO and the Broader Identity Landscape,* FIDO Alliance Seminar, Sydney, Sep 2017

[4]. *Attribute Certificates Redux – Mobile Device Attributes Validation* Dept of Homeland Security Cyber Showcase, Washington DC, July 13, 2017

[5]. *PKI Post Blockchain* Cloud Identity Summit, Chicago, June 20, 2017

[6]. *FIDO Alliance Update: On Track to a Standard,* Constellation Research, April 2015

[7]. *FIDO Alliance Update: Identity Management Implications for a World of Digital Business*, Constellation Research, Aug 2014

[8]. *Forget identity!* Australian Info Security Assoc Annual Conference, Sydney, 2013

[9]. *Identity Evolves: Why Federated Identity is easier said than done*, AusCERT 2011 Security Conference, Gold Coast, May 2011

[10]. *Anonymity & Pseudonymity in eResearch via smartcards and Public Key Infrastructure* eResearch Australasia conference, Manly (Sydney), 2009 www.eresearch.edu.au/wilson2009

[11]. *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

[12]. *An easily validated security model for e-voting based on anonymous public key certificates* AusCERT2008 Refereed Academic Stream, 2008

[13]. *Embedded PKI: the emerging state-of-the-art*, 6th Asia PKI Forum International Symposium, Chengdu, China, 2006

[14]. *A new manifesto for smartcards as national information infrastructure*, 5th Homeland Security Conference, Canberra, 2006

[15]. *Smartcards and PKI at Medicare Australia*, Brewer, J. & Wilson, S., Australian Electrical & Electronic Manufacturers Association ICT Forums, 2006

[16]. *The importance of PKI today*, China Communications, December 2005

[17]. *Relationship Certificates for Known Customers - a new PKI paradigm*, 5th Asia PKI Forum International Symposium, Beijing, 2005

[18]. *Guidelines on how to determine Return on Investment in PKI* OASIS White Paper June 2005 http://idtrust.xml.org/sites/idtrust.xml.org/files/roi.pdf

[19]. *A novel application of PKI smartcards to anonymise Health Identifiers* AusCERT2005 Refereed Academic Stream, Gold Coast, 2005

[20]. *Patient Privacy and Security – Not a zero sum game!* Wilson, Connolly and Denney-Wilson, Journal of the Australian Epidemiology Association, V12.1, 2005

[21]. *A summary of PKI data for Australia* Asia PKI Forum, Tokyo, Feb 2005

[22]. *PKI State of Play*, Argus Foundation Forum, Canberra, 2004

[23]. *PKI lessons from Australia* Global e-Business Forum, Geneva, 2003

[24]. *PKI Position Statement of the Australian Security Industry* AU IT Security Forum, 2003

[25]. *Rethinking PKI – the electronic business card*, Secure Computing Magazine, June 2003 www.scmagazineus.com/rethinking-pki/article/30733

[26]. *PKI without Tears* American Bar Association eBlast, V1.1, January 2003

[27]. *Demystifying international cross-recognition of PKI: we've been barking up the wrong tree* International Security Solutions Europe (ISSE), London, 2001

[28]. *Comparison of Authentication Technologies* Asia Business Law Review, No. 33, 2001

[29]. *Leveraging external accreditation to achieve PKI cross-recognition* Attorney Generals Privacy & Security conference, Melbourne, 2001 http://bit.ly/o3g0rc

[30]. *PKI and the Acceleration of B2B* European-American Business Journal, Spring 2001

[31]. *Will Biometrics Obsolete PKI?* American Bar Assoc. Bulletin of Law, Science & Tech, May 2001 www.abanet.org/scitech/eblast/may01/2may01.html#Bio

[32]. *Audit based public key infrastructure* Certification Forum of Australia, Nov 2000

[33]. *Attribute Certificates and their Limitations* Journal of the PricewaterhouseCoopers Cryptographic Centre of Excellence, Issue 3, 2000

[34]. *New models for the management of public key infrastructure and root certification authorities* 7th IFIP Conference on Info Security, Amsterdam, 1999

[35]. *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

[36]. *Some limitations of web of trust models* Information Management & Computer Security, Vol. 6, No. 5, 1998 (Highly Commended Award winner, MCB University Press).