Stephen Wilson
PKI profile

Stephen Wilson is a leading international authority on Public Key Infrastructure. He has helped organisations around the world establish effective PKI systems, advising on strategy, architecture, policy, privacy, business process change, technology selection and governance. He has been intimately involved with pivotal PKI programs including Australian government PKI *Gatekeeper*, Identrus, Medicare Australia's Health eSignature Authority, Webtrust for CAs, and the American Bar Association PKI Guidelines (PAG). He held senior management positions at the commercial CAs of Certificates Australia Pty Ltd, KPMG Australia, PwC beTRUSTed (US/UK) and SecureNet (AU). He has provided PKI advice to the governments of New Zealand, Singapore, Hong Kong, Macau, Indonesia, Kazakhstan and Australia. Stephen chaired the OASIS PKI Adoption Technical Committee and was an independent member of the Gatekeeper Policy Committee through its 12 year existence. He conceived and led an attribute certificate project under contract to the U.S. Dept of Homeland Security. He has been awarded nine PKI patents. See also www.lockstep.com.au/library/pki.

PKI solutions and operations

- **Queralt Inc. (U.S.) 2022-2023:** Product Strategy for this early-stage FIDO / PIV PKI middleware solution developer.
- **U.S. Dept of Homeland Security 2016-19**: Awarded a three-stage competitive R&D commercialisation contract with the DHS Science & Technology Directorate to develop an attribute certificate mobile wallet and managed PKI, for an initial use case of First Responder mobile credentials. Lockstep is the only Australian company to be awarded a DHS commercialisation contract.
- **National eHealth Transition Authority (NEHTA) 2011-12**: PKI Manager, National Authentication Service for Health (NASH); led the Gatekeeper compliance work stream; wrote the 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**: Wrote the Certificate Policy and Certification Practice Statements for enterprise-wide PKI services; designed and MC'ed the Root CA key signing ceremony; liaised with legal counsel on new PKI user terms & conditions.
- **Westpac Bank, 2007**: Conducted a detailed Gatekeeper gap analysis to underpin project planning for accreditation of a new PKI operation.
- **Project Gatekeeper, AU Govt Information Management Office (AGIMO) 2005-06**: Principal Consultant on a strategic review of the Gatekeeper program; responsible for community of interest, "Relationship Certificates" and "Security Printer" models to dramatically reduce the cost and overhead of Gatekeeper.
- **"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 general identity. Relationship Certificates were adopted as a new category in the Australian Government PKI framework, and implemented in several

health sector projects, including NASH. I coined core liability language for the Medicare CP/CPS which is still in use today.

- **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 (Cyberjaya, Malaysia) in support of this new CA business and operation.
- **PricewaterhouseCoopers beTRUSTed, 1999-2001**: Founding Asia Pacific Director and core team member during the build phase of 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.

Original PKI research

- ***Decoupling identity from devices in the Internet of Things*** (2018) US patent 10,164,966
- ***Authenticating electronic financial transactions*** (2014) US patents 8,286,865 & 8,608,065; AU patent 2009238204
- ***System and method for anonymously indexing electronic record systems*** (2013) US patent 8,347,101; AU patent 2005220988
- ***Verified anonymous code signing*** (2012) AU patent 2012101460
- **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
- **OASIS, 2005**: Researched and developed a new PKI ROI model, featuring a novel digital certificate supply chain model (see [25]).
- **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.
- **Standard Chartered Bank Singapore, 2001**: Led an international survey of digital signature regulations and interoperability with Identrus.
- **PricewaterhouseCoopers Cryptographic Centre of Excellence, 2000**: Led the Asia Pacific Chapter of the biggest private sector team of cryptographers in the world.

PKI strategy experience

- **Healthlink New Zealand 2018**: Provided a regulatory gap analysis and managed PKI acquisition road map for this multi-national health messaging service provider.

- **NEHTA 2007-08**: Developed the business case for a 600,000 user national PKI for health service providers, the *National Authentication Service for Health* (NASH). Retained to draft a fast-tracked procurement strategy (but 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 *Solutions and operations* above).
- **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 detailed business requirements across internal and external health organisations; drafted innovative new short form Certificate Policies for multiple programs; worked with Medicare legal counsel to develop core liability clauses still in use today.
- **Law Society of NSW, 2005**: PKI subject matter expert consulting on the potential for digital credentials for lawyers.
- **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 [34], [36], [41].

PKI policy, governance & regulatory work

- **COVID Vaccination Certificates, 2020-21**: Designed a "digital yellow book" proposal based on PKI certificates, and published a peer-reviewed paper with the IEEE [5]. Subsequently invited onto the World Health Organisation working group on Digital Documentation of COVID Certificates. My PKI analysis was reflected in the guidelines, which deprecate distributed ledger technology for globally scalable authentication of credentials. https://www.who.int/publications/i/item/WHO-2019-nCoV-Digital_certificates-vaccination-2021.1
- **American Association of Motor Vehicle Administrators AAMVA 2020-21**: Advisory Board member for this peak body's development of a Mobile Driver Licence based *Digital Trust Service* and PKI.
- **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 Representative.
- **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 Australia's 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 international assurance scheme on behalf of the Institute of Chartered Accountants Australia.

Committees & Associations

- Standards Australia *Cards and security devices for personal ID* IT-17 (since 2022)
- Turing Institute Trusted Digital Identity Interest Group (since 2021)
- Privacy & Ethics Track Chair, *Identiverse* / Cloud Identity Summit (since 2016)
- International Association of Privacy Professionals (since 2008)

- Digital Identity Ministerial Advisory Council, NSW Minister for Digital (2021-23)
- World Health Organisation Smart Vaccination Certificate Working Group (2021)
- National Blockchain Roadmap Cybersecurity Working Group (2020-21)
- Kantara Initiative (2016-19)
- Judge, Mobile World Congress GLOMO Awards, Identity category (2016-18)
- Standards Australia Information Security Committee IT-12-4 (2004-16)
- Gatekeeper PKI 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 & presentations

[1]. *The identity of things? We're gonna need a bigger idea!* FIDO Authenticate, Oct 20, 2021

[2]. *A Goldilocks point for Digitised Vaccination Certificates*, Turing trustworthy digital identity conference, Sept 13, 2021

[3]. *Why Isn't Identity Easy?* Identiverse (virtual) June 2021

[4]. *Reframing Digital Identity in the Era of Trust Data*, GS1 Innovation Summit, Mar 30, 2021
[5]. *A digital "Yellow Card" for securely recording vaccinations using Community PKI certificates*, IEEE International Symposium on Technology and Society, Nov 12-15
[6]. *Authenticate the World!* FIDO Authenticate Conference (virtual), Nov 19, 2020
[7]. *Identity: It's the Data, Stupid* Identiverse Virtual, July 23, 2020
[8]. *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
[9]. *FIDO Alliance Update: Certification and Disruption,* Constellation Research, Oct 2017
[10]. *FIDO and the Broader Identity Landscape,* FIDO Alliance Seminar, Sydney, Sep 2017
[11]. *Attribute Certificates Redux – Mobile Device Attributes Validation* Dept of Homeland Security Cyber Showcase, Washington DC, July 13, 2017
[12]. *PKI Post Blockchain* Cloud Identity Summit, Chicago, June 20, 2017
[13]. *FIDO Alliance Update: On Track to a Standard,* Constellation Research, April 2015
[14]. *FIDO Alliance Update: Identity Management Implications for a World of Digital Business*, Constellation Research, Aug 2014
[15]. *Forget identity!* Australian Info Security Assoc Annual Conference, Sydney, 2013
[16]. *Identity Evolves: Why Federated Identity is easier said than done*, AusCERT 2011 Security Conference, Gold Coast, May 2011
[17]. *Anonymity & Pseudonymity in eResearch via smartcards and Public Key Infrastructure* eResearch Australasia conference, Manly (Sydney), 2009
[18]. *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 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2548224
[19]. *An easily validated security model for e-voting based on anonymous public key certificates* AusCERT2008 Refereed Academic Stream, 2008
[20]. *Embedded PKI: the emerging state-of-the-art*, 6th Asia PKI Forum International Symposium, Chengdu, China, 2006
[21]. *A new manifesto for smartcards as national information infrastructure*, 5th Homeland Security Conference, Canberra, 2006
[22]. *Smartcards and PKI at Medicare Australia*, Brewer, J. & Wilson, S., Australian Electrical & Electronic Manufacturers Association ICT Forums, 2006
[23]. *The importance of PKI today*, China Communications, December 2005
[24]. *Relationship Certificates for Known Customers - a new PKI paradigm*, 5th Asia PKI Forum International Symposium, Beijing, 2005
[25]. *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
[26]. *A novel application of PKI smartcards to anonymise Health Identifiers* AusCERT2005 Refereed Academic Stream, Gold Coast, 2005
[27]. *Patient Privacy and Security – Not a zero sum game!* Wilson, Connolly and Denney-Wilson, Journal of the Australian Epidemiology Association, V12.1, 2005
[28]. *A summary of PKI data for Australia* Asia PKI Forum, Tokyo, Feb 2005

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

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

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

[32]. *Rethinking PKI – the electronic business card*, Secure Computing Magazine, June 2003

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

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

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

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

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

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

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

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

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

[42]. *Privacy positive aspects of public key infrastructures* Privacy Law & Policy Reporter, Vol 5.10, 1999
https://classic.austlii.edu.au/au/journals/PrivLawPRpr/1999/26.html

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