CV

Stefan Santesson
Consultant, 3xA Security AB (http://aaa-sec.com)
Born November 2, 1962 in Malmö, Sweden

Björnstorp 744
240 13 Genarp
Sweden

sts@aaa-sec.com
Tel +46-767 861337
Skype: Razumain

COMPETENCE PROFILE

Internationally renowned expertise in the area of Public Key Infrastructure (PKI), electronic signatures, Authentication Authorization and Accounting (AAA), Identity Management (IdM) solutions, cryptographic protocols, Internet security protocols and related international standardization.

BACKGROUND

Stefan Santesson has 30 years of experience within the field of computer science and over 25 years of experience with Information Security, ranging from advanced crypto algorithm development to being CEO of an international information security organization. Stefan is very active and well positioned internationally in particular as chairman for the Internet Engineering Task Force (IETF) PKIX group, as selected member of the IETF Security Area Directorate and as contributor to European electronic identification and electronic signature standards.

Most notably, Stefan is co-author of the most commonly deployed PKI standard RFC 5280. He is also the editor of the IETF Qualified Certificate standard RFC 3739 as well as the European Qualified Certificate standard ETSI TS 101 862 and co-author of the European Certificate Policy for issuers of Qualified Certificates TS 101 456.

NOTABLE POSITIONS IN THE STANDARDS COMMUNITY

- *Chairman for the IETF PKIX group, since July 2006 (http://ietf.org/html.charters/pkix-charter.html)*
- *Member of the IETF Security Area Directorate, since March 2006*

SUMMARY OF AUTHORED IETF STANDARDS

- *RFC 3709, standard for logotypes in X.509 Certificates. Published in January 2004 (http://www.ietf.org/rfc/rfc3709.txt)*
- *RFC 3739, standard profile for Qualified Certificates. Published in March 2004, replacing RFC 3039 (http://www.ietf.org/rfc/rfc3739.txt) and (http://www.ietf.org/rfc/rfc3039.txt)*
- *RFC 4262, standard for S/MIME Capabilities in X.509 Certificates. Approved by IETF June 2005 (http://www.ietf.org/rfc/rfc4262.txt)*
- *RFC 4325, standard for CRL signer certificate discovery using the Authority Information Access extension. (http://www.ietf.org/rfc/rfc4325.txt)*
- *RFC 4680, TLS Handshake Message for Supplemental Data (http://www.ietf.org/rfc/rfc4680.txt)*
- *RFC 4681, standards for the TLS User Mapping Extension. (http://www.ietf.org/rfc/rfc4681.txt)*
- *RFC 4985, standard for a Subject Alt Name for Service Resource Records in X.509 certificates. (http://www.ietf.org/rfc/rfc4985.txt)*
- *RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. (http://tools.ietf.org/html/rfc5280)*

- *RFC XXX, Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA (Approved October 2009) (http://tools.ietf.org/html/draft-ietf-pkix-sha2-dsa-ecdsa-10)*

CONTRIBUTION TO PUBLIC STANDARDS

- *Co-Author of Swedish standards for electronic ID-Cards SS-614330 – Electronic ID Application, SS-614331- Electronic ID Certificate and SS-614332 – Electronic ID Card – Swedish profile. Published 1998*
- *Author of the SEIS S-10 standard policy for issuing of electronic ID-cards. Published June 1998*
- *Author of Internet RFC 3039, standard for Qualified Certificates. Published in January 2001*
- *Author of ETSI TS 101 862 Version 1.1.1, European Standard for Qualified Certificates. Published in January 2001*
- *Co-Author of ETSI TS 101456, Policy requirements for certification authorities issuing qualified certificates. Published January 2001*
- *Author of Internet RFC 3709, standard for logotypes in X.509 Certificates. Published in January 2004*
- *Author of Internet RFC 3739, revised standard profile for Qualified Certificates. Published in March 2004*
- *Author of ETSI TS 102 280 Version 1.1.1, X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons, European interoperability standard, Published March 2004*
- *Author of ETSI TS 101 862, revised version 1.3.1, European Standard for Qualified Certificates. Published in March 2004*
- *Author of IETF standard for S/MIME Capabilities in X.509 Certificates. Approved by IETF June 2005*
- *Co-author of Internet RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, successor of RFC 3280. Published in May 2008.*
- *Author of IETF standard for CRL signer certificate discovery using the Authority Information Access extension. Approved by IETF August 2005. RFC 4325*
- *Author of IETF standard for a Subject Alt Name for Service Resource Records in X.509 certificates. Ongoing task within the IETF PKIX group. RFC 4985*
- *Author of IETF standard for a TLS User Mapping Extension. RFC 4680 and 4681.*
- *Author of ESSCertIDv2 update for RFC 3161 (draft-ietf-pkix-rfc3161-update)*
- *Author of Internet X.509 Public Key Infrastructure: Certificate Image (draft-ietf-pkix-certimage)*
- *Author of OCSP Algorithm Agility (draft-ietf-pkix-ocspagility)*
- *Author of Transport Layer Security (TLS) Cached Information Extension draft-ietf-tls-cached-info)*
- *Author of Channel binding for HTTP Digest Authentication (draft-santesson-digestbind)*

SIGNIFICANT ASSIGNEMTS

3XA SECURITY (2009-)

- *E-delegationen, A strategy for Swedish government agencies provision of e-services - SOU 2009:86. Providing the technical content of the strategy for electronic identification and support of electronic signatures (eLegitimationer) - http://www.edelegationen.se/node/254*
- *Invited expert by the European Commission to the High level experts consultation meeting on an electronic identity management infrastructure for a trustworthy information society, October 2009.*
- *Invited Speaker at the RSA Europe 2009 conference - Fostering Electronic Signature Interoperability in Europe - Panelists: Reinhard Posch, CIO, Government of Austria; Gerard Galler, Policy Officer, European Commission; Riccardo Genghini, Chair, ETSI, TC/ESI; Stefan Santesson, chair, IETF PKIX.*

MICROSOFT CORPORATE, REDMOND USA (2004-2009)

- *Principal Consultant, Microsoft Security Center of Excellence (July 2004 - April 2005)*
- *Senior Program Manager, Windows Security - Standards (April 2005 – February 2009)*

MICROSOFT DENMARK, PRINCIPAL CONSULTANT (2003-2004)

- *Editor of QuEST – The Qualified Electronic Signatures Tutorial, produced under the EMEA Trustworthy Computing team as guidance for implementation of Qualified Electronic signatures, according to the European Union Directive on electronic signature.*
- *Delivery to the PKI product group: A full inventory of the wide range of X.509 certificate extensions, attributes and options supported by MS CAPI. April 2004.*
- *Delivery to the PKI product group: Delta specification between public PKI standards and MS CAPI processing of X.509 certificate chains (path processing).*
- *Delivery to the PKI product group: Implementation specification for X.509 certificate processing in the Longhorn version of MS CAPI. June 2004.*

ADDTRUST, MALMÖ SWEDEN (2000-2003)

- *CEO for at most 64 employees (January 2000 - July 2000)*
- *Executive VP and member of the board (July 2000 - January 2003)*

ACCURATA SYSTEMSÄKERHET, CONSULTANT 1992-1999

- *Co-author of the requirement specification for the Swedish Allterminal procurement (the first official European procurement of an integrated SmartCard and PKI based security solution) ,*

executed by Swedish Police, Swedish Tax board, RFV (Government body for Social Insurance) and the Swedish Agency for Administrative development. 1992

- *Consultant within the Allterminal procurement evaluation and selection process (as above), 1993*
- *Editor of the Swedish Allterminal specifications (post procurement specifications for interoperability purposes), 1993-1994*
- *Consultant at the introduction of the Allterminal concept at the Swedish Police., 1993 – 1994*
- *Consultant at the introduction of the Allterminal concept at the Swedish tax board. 1994-1995*
- *Consultant at the introduction of the Allterminal concept at RFV Sweden, 1994-1995*
- *Co-author of the joint banking proposal for a common electronic purse system, Issued by Kontocentralen, 1995*
- *Editor of the technical requirements of the security protocol for the procurement of the Stockholm road toll system, 1995*
- *Technical evaluator of tenders within the Stockholm road toll procurement, 1995*
- *Editor of the first electronic ID-card specification written by the joint banking/industry project "Strategic cooperation for an electronic ID-card", 1995*
- *Member of the steering board that founded the Swedish SEIS-organization (Secured Electronic Information In Society, founded by members of the Banking, Industrial, Government, Military and Educational sectors) as a continuation of the Allterminal project, 1995*
- *Responsible for security issues at the EU-commission SONAH project (preparatory work for the ACTS and INFOWIN program), 1995*
- *Contributor to the SEIS Certificate specification SEIS S3, 1996-1998*
- *Contributor to the SEIS Card specification SEIS S1, 1996-1998*
- *Project leader for SEIS regulations group, 1997-1998*
- *Author of SEIS Certificate policy SEIS S10 for certificates related to Swedish national electronic ID-cards, 1998*
- *Assistant project leader of Sweden Post CA-project, including development of the Sweden Post electronic ID-card concept 1997-1998*
- *Project leader and author of the Swedish Single Face to Industry (SFTI) recommendation on a security standard for secure EDI over Internet, 1999*
- *Author of a proposal for a general PKI structure within the Swedish health care, issued by the healthcare project SITHS-CA, 1999-2000*
- *Initiator and lead editor of the IETF/PKIX standard RFC 3039, Certificate profile for Qualified Certificates, 1998-2000*
- *Editor of the European standard for Qualified Certificates (ETSI standard TS 101862) and Task leader for ETSI STF 155 Task 3. Standard was developed by ETSI (European Telecom Standards Institute) in response to the European electronic signature directive by the Commission of the European Union, 1999 – 2000*
- *Co-Editor of the European ETSI standard for Certificate Policies for Certification Service Providers issuing Qualified Certificates. 1999 – 2000*

EMPLOYMENTS (REVERSE CHRONOLIGAL ORDER)

Independent Consultant and founder/owner of 3xA Security AB	***February 2009 - Current***
Senior Program Manager for Security Standards at Microsoft Windows Security	*April 2005 – February 2009*
Consultant at Microsoft Security Center of Excellence	*July 2004 - April 2005*
Program Manager in Microsoft Windows Security division	*January 2004 – June 2004*
Principal Consultant at Microsoft Denmark	*June 2003 – June 2004*
Independent Information Security Consultant and Manager/Owner of consultancy company Retrospekt AB	*January 2003 – June 2003*
Executive VP & CTO of AddTrust AB	*July 2000 – January 2003*
Founder and CEO of AddTrust AB, A European PKI service company with a global branding strategy.	*January 2000 – June 2000*
Independent Information Security Consultant and Manager/Owner of the consulting company Accurata Systemsäkerhet AB	*August 1992 – December 1999*
Cryptologist and R&D manager and co-founder of, SecuriCrypto AB, Crypto solutions company, provider of crypto solutions to the Banking industry and Defense industry in Sweden.	*March 1984 – August 1992*
Manager of Swedish Infotech in Malmö, Retail store for computers and peripherals	*July 1983 – March 1984*
Military Service within the field of communication and cryptography, Swedish Armed Forces	*June 1982 – July1983*
Computer software and hardware engineer at Datahuset i Malmö AB, A local computer store in Malmö Sweden	*August 1979 – June 1982*