

EUROPEAN  
CURRICULUM VITAE  
FORMAT



PERSONAL INFORMATION

Name Stefan Santesson  
Address Scheelev. 17, 223 70, Lund, Sweden  
Telephone **+46-767861337**  
Fax  
E-mail **stefan@aaa-sec.com**  
Nationality Swedish  
Date of birth November 02, 1962

WORK EXPERIENCE

- Dates (from – to)
- Name and address of employer
  - Type of business or sector
  - Occupation or position held
- Main activities and responsibilities

**February 2009 to current**

3xA Security, Schelev 17, 223 70, Lund, Sweden

Consultancy

Owner

- Chairman of the PKIX workgroup in the Internet Engineering Task Force (IETF) responsible for use of X.509 certificates in Internet protocols.
- Member of the IETF Security Area Directorate
- Member of the IETF General Area review team
- Selected expert in ETSI Specialist task force 425 providing input to the Electronic Signature Standardisation in Rationalised Framework in response to the European standardisation mandate M/460.
- Selected expert in ETSI Specialist task force 427 with the task of providing “Quick fixes to electronic signatures standards” in response to the EU Commission standardisation mandate M/460. Sub-task leader of the QF2 (Certificate profiles) area, providing updates to the standard for Qualified Certificates ETSI TS 101 82 and the profile for certificates issued to natural persons, TS 102 280. Contributing expert in the QF 3 (Procedures for Signature Verification) area.
- Preparations to establishment of a Swedish governmental agency for electronic identification, August 2010, Responsible for coordinating technical work specifying a new Swedish infrastructure for Identity Federation and a new Swedish infrastructure for electronic signatures.
- Swedish Agency for Regional and Economic Growth (Sweden Single point of Contact). Development of a solution for validating electronic signatures from EU member states based on TSL issued in support of implementation of the Services directive. Development of software in Java based on the Belgian FedICT TSL library. Presentation of results for the EU expert group for the implementation of the Services directive. May 2010.
- Expert witness representing BBS (Bankernas Betalningscentral) in Norway in patent case trial, Oslo, January 2010. Case resulted in BBS

defending their right to use their technology without patent infringement.

- Expert witness representing the film industry in the Pirate Bay trial concerning the ability for the Internet service provider to block Internet traffic to the Pirate Bay torrent file sharing services. Case won May 2010.
- E-delegationen Sweden, June 2010, Responsible for the technical strategy for e-identification and e-signatures in the Swedish government agencies provision of e-services - SOU 2009:86.  
<http://www.edelegationen.se/node/254>
- 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.

- Dates (from – to)
- Name and address of employer
  - Type of business or sector
  - Occupation or position held
- Main activities and responsibilities

**April 2005 - February 2009**

Microsoft, One Microsoft Way, Redmond, USA

Windows Security division

Senior Program Manager

Responsibility for security standard engagements, including

- Representation of Microsoft in the IETF and ETSI standards organizations
- Co-author of the main global PKI standard RFC 5280
- Author of the Microsoft solution for user name hints in TLS
- Author of the inclusion of AIA extension in Certificate Revocation Lists
- Author of proposals to improve Kerberos authentication in TLS
- Editor of FIPS evaluation documentation of MS CAPI for Windows Vista and Windows Server 2008.

- Dates (from – to)
- Name and address of employer
  - Type of business or sector
  - Occupation or position held
- Main activities and responsibilities

**April 2005 - February 2009**

Microsoft, One Microsoft Way, Redmond, USA

Windows Security division

Senior Program Manager

Responsibility for security standard engagements, including

- Representation of Microsoft in the IETF and ETSI standards organizations
- Co-author of the main global PKI standard RFC 5280
- Author of the Microsoft solution for user name hints in TLS
- Author of the inclusion of AIA extension in Certificate Revocation Lists
- Author of proposals to improve Kerberos authentication in TLS
- Editor of FIPS evaluation documentation of MS CAPI for Windows Vista and Windows Server 2008.

- Dates (from – to)
- Name and address of employer
  - Type of business or sector
  - Occupation or position held
- Main activities and responsibilities

**July 2004 - April 2005**

Microsoft Security Center of Excellence, One Microsoft Way, Redmond, USA

Consultancy

Principal Consultant

- Handling standards engagements for the Windows Security division
- Contributing to the prescriptive guidance to Microsoft customers following the Blaster worm attack

- Dates (from – to)
- Name and address of employer
  - Type of business or sector
  - Occupation or position held
- Main activities and responsibilities

**June 2003 - June 2004**

Microsoft Denmark, Tuborg Boulevard 12, Copenhagen, Denmark

Consultancy

Principal Security Consultant

- Editor of the Microsoft Europe, Middle East and Africa Qualified Electronic Signature Tutorial (QUEST).
- Providing a complete review of the MS CAPI certificate path validation algorithm.

Providing the design for the updated certificate path validation algorithm in MS CAPI for Windows XP SP2 as well as test cases and code for compliance testing

- Dates (from – to)
- Name and address of employer
  - Type of business or sector
  - Occupation or position held
- Main activities and responsibilities

**January 2003 - June 2003**

Retrospect AB

Consultancy

Owner

- Swedish Tax Agency: Providing guidance on user interface for national implementation of electronic signatures and identification in government services

- Dates (from – to)
- Name and address of employer
  - Type of business or sector
  - Occupation or position held
- Main activities and responsibilities

**July 2000 - January 2003**

AddTrust AB

Certification Service Provider

Executive VP & CTO and Board member

Leading the technical strategy of an international Certification Service Provider

- Dates (from – to)
- Name and address of employer
  - Type of business or sector
  - Occupation or position held
- Main activities and responsibilities

**January 2000 - July 2000**

AddTrust AB

Certification Service Provider

CEO and Board member

Building up the company from start to 64 Employees in 6 countries

- Dates (from – to)
- Name and address of employer
  - Type of business or sector
  - Occupation or position held
- Main activities and responsibilities

**August 1992 - December 1999**

Accurata Systemsäkerhet AB

Consultancy

Owner

- 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

- Dates (from – to)
- Name and address of employer
  - Type of business or sector
- Occupation or position held
- Main activities and responsibilities

**March 1984 - August 1992**

SecuriCrypto AB

Crypto product development. Provider of crypto solutions to the Swedish defence industry and the Swedish Banking sector

co-owner, Cryptologist and R&D Manager

- Developing the crypto algorithm SBLH, approved by the Swedish armed forces for use in the Swedish defence industry
- Developing crypto solutions for encrypting communications over V.24, V.35, X.28, X.25, T1, G.703, Fax and Voice
- Crypto hardware design
- Programming CPU logic for crypto solutions

- Dates (from – to)
- Name and address of employer
  - Type of business or sector
  - Occupation or position held
- Main activities and responsibilities

**July 2003 - March 2004**

Sweden Armed Forces

Sergeant

Crypto and field communication services

- Dates (from – to)
- Name and address of employer
  - Type of business or sector
  - Occupation or position held
- Main activities and responsibilities

**August 1979 - June 1982**

Datahuset i Malmö AB

Computer retail

Service engineer and developer

Microcomputer service

Development of hardware and software solutions

**EDUCATION AND TRAINING**

- Dates (from – to)
- Name and type of organisation providing education and training
- Principal subjects/occupational skills covered
- Title of qualification awarded

1989

University of Lund

*Information Theory and Encryption*

- Level in national classification (if appropriate)

- Dates (from – to)

- Name and type of organisation providing education and training

- Principal subjects/occupational skills covered

- Title of qualification awarded

- Level in national classification (if appropriate)

2005  
(ISC)2

*Information Security*

*Certified Information Security Professional (CISSP)*

## PERSONAL SKILLS AND COMPETENCES

*Acquired in the course of life and career but not necessarily covered by formal certificates and diplomas.*

MOTHER TONGUE

**Swedish**

OTHER LANGUAGES

- Reading skills
- Writing skills
- Verbal skills

English  
English  
English

SOCIAL SKILLS AND COMPETENCES

*Living and working with other people, in multicultural environments, in positions where communication is important and situations where teamwork is essential (for example culture and sports), etc.*

Successfully selling consultancy services as independent consultant for 10 years  
Successfully negotiating standards in the international standards community for over 10 years  
Leading technical role in Microsoft Windows Security

ORGANISATIONAL SKILLS AND COMPETENCES

*Coordination and administration of people, projects and budgets; at work, in voluntary work (for example culture and sports) and at home, etc.*

Chariman of the PKIX working group in the IETF since 2006  
CEO of AddTrust AB managing 64 people employed in 6 countries  
Member of the board of directors of AddTrust AB  
Officer in the Swedish armed forces

TECHNICAL SKILLS AND COMPETENCES

*With computers, specific kinds of equipment, machinery, etc.*

### Expert skills

- Public Key Infrastructure
- Identity Management
- Electronic signatures
- Internet Security Protocols
  - PKI
  - IPsec

- Kerberos
- Transport Layer Security (TLS/SSL)
- S/MIME
- EAP
- Other security protocols
  - SAML
  - XML Digital Signatures
- European Security Protocols
  - Qualified Certificates
  - EU Signature Formats
  - TSL (Trust Status List)

#### **Programming Languages**

- Java
- Java Script
- C
- Basic
- Assembler
- Expect Scripting
- TCL Scripting

#### **Development environments and tools**

- Visual Studio
- Net Beans
- Subversion
- Maven
- Ant
- Hibernate

#### **Operating systems**

- Windows
- UNIX
- Mac OS X

#### **Databases**

- Java DB
- MySQL
- SQLite

#### **OTHER SKILLS AND COMPETENCES**

*Competences not mentioned above.*

Extensive experience in working with lawyers in projects that cross technical and legal boundaries.

- Extensive experience with working with patents, including experience from patent litigations
- Extensive experience with working close to lawyers in preparing legal investigations related to e-identification and e-signatures on both national and international level

#### **DRIVING LICENCE(S)**

Motorbike, Car and Trucks (over 3.5 tons)

## ADDITIONAL INFORMATION

### ANNEXES

#### STANDARDS

#### 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 IETF standard for Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA, RFC 5758, Published January 2010.*
- *Author of ESSCertIDv2 update for RFC 3161, RFC 5816*
- *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)*

**ADDITIONAL INFORMATION**

**ANNEXES**

**POSITIONS**

POSITIONS HELD IN THE STANDARDS COMMUNITY

- *Chairman of the PKIX workgroup in the Internet Engineering Task Force (IETF) responsible for use of X,509 certificates in Internet protocols. Since 2006 to present.*
- *Member of the IETF Security Area Directorate. Since 2006 to present*
- *Member of the IETF General Area review team. Since 2010 to present*