

**Persönliche Daten:**

**Name:** Henrich C. Pöhls  
**Geburt:** 14. März 1976 in Hamburg  
**Familienst.:** verheiratet, einen Sohn  
**Private Adresse:** Göttweiger Str. 44  
 94032 Passau  
**Telefon:** ++49-178-78-29428  
**E-Mail:** [hp@poehls.com](mailto:hp@poehls.com)  
**Webseite:** <https://henrich.poehls.com>

**Abschlüsse: Studium, Zivildienst und Schule**

**Sept. 2018** **Promotion – Universität Passau**  
 Doktorarbeit: „Increasing the Legal Probative Value of Cryptographically Private Malleable Signatures“  
 am Lehrstuhl: „IT-Sicherheit“ (Prof. J. Posegga) Note: magna cum laude

**Nov. 2003 –** **Diplom Informatiker – Universität Hamburg**  
**Okt. 1995** Diplomarbeit: „Risk Analysis of Mobile Devices with Special Concern of Malware Contamination“  
 am Lehrstuhl: „Anwendungen der Informatik in Geistes- und Naturwissenschaften“ (Prof. K. Brunnstein) Note: sehr gut

**Nov. 2001 –** **M.Sc. Information Security – Royal Holloway University of London**  
**Nov. 2000** Masterarbeit: „Security Requirements for Wireless Networks and their Satisfaction in IEEE 802.11b and Bluetooth“  
 (Prof. C. Mitchell) Note: with Distinction

**Feb. 1997 –** **Zivildienst**  
**Feb. 1996** bei der Martha-Stiftung in Hamburg; *Unterbrechung des Studiums im 1. Semester*

**Jun. 1995 –** **Allgemeine Hochschulreife – Gymnasium Hummelsbüttel, Hamburg**  
**Aug. 1982** Note: 1,3

**Akademischer Werdegang:**

**heute –** **Universität Passau:** (Post-)Doktorand und Wissenschaftlicher Mitarbeiter  
**Aug. 2008** Fakultät für Informatik und Mathematik – Lehrstuhl: „IT-Sicherheit“ (Prof. J. Posegga)

- **Leitung, Beantragung und Konzeption von Drittmittel-Forschungsprojekten** mit industriellen und akademischen Partnern; Förderer: EU, BMBF, Freistaat Bayern
- **Vorlesungen**, z.Z. „M.Sc. Advanced IT-Security“
- Konzeption und **Durchführung von Seminaren, Praktika, und Übungen**

**Jul. 2008 –** **Universität Hamburg:** Doktorand und Wissenschaftlicher Mitarbeiter  
**Apr. 2004** Fakultät für Mathematik, Informatik und Naturwissenschaften – Arbeitsbereich: „Sicherheit in verteilten Systemen“ (Prof. J. Posegga)

- **Durchführung, Beantragung und Konzeption von Drittmittel-Forschungsprojekten** mit industriellen und akademischen Partnern; Förderer: BMBF, BSI
- Konzeption und **Durchführung von Seminaren, Praktika, und Übungen**

**Feb. 2004 –** **Universität Hamburg:** Stud. Hilfskraft im Praktikum „Reverse Engineering (RE)“  
**Mär. 2004** Fakultät für Mathematik, Informatik und Naturwissenschaften – Arbeitsbereich: „Anwendungen der Informatik in Geistes- und Naturwissenschaften“ (Prof. K. Brunnstein)

## Forschungsprojekte (1/2) in leitender Funktion:

Die folgenden Drittmittel-geförderte Forschungsprojekte wurden jeweils

- von der **Antragsstellung** (incl. Budget-Planung und Verhandlung mit Partnern und EU / BMBF),
- über die **wissenschaftliche Durchführung** (Koordination aller Arbeiten an der Universität die durch andere (Post-)Doktoranden oder Studentische Hilfskräfte durchgeführt wurden),
- bis zum **Abschluss** (incl. Budget-Controlling, Kommunikation innerhalb der univ. Verwaltung)

von mir geleitet und betreut:

*Jul. 2018 –* **Leitung eines Arbeitspaketes** im Projekt **PRISMACLOUD**

*Feb. 2015* „PRivacy & Security MAintaining Services in the CLOUD“

(3,5 Jahre – 16 Partner – EU H2020 gefördert mit ~8 Mio. EUR – Umfang: ~919 PM)

- Leitung und Controlling aller Arbeiten der Univ. Passau (~0,7 Mio. EUR)
- Leitung des Arbeitspaketes „Composition of next-generation secure cloud services“ mit 103 Personenmonaten (PM) Umfang unter Beteiligung industrieller und akademischer Partner
- Partner: AIT, ATOS, CEA, TU Darmstadt, ETRA, FCSR, TU Graz, IBM Israel, Interroute, Karlstad University, LISPA, MikroPlan, Newcastle University, Université de Lausanne, XiTrust, Univ. Passau

Projekt-Ziel: *Cloud Dienste mittels kryptographischer Verfahren sicherer und datensparsamer zu machen (Redactable Signatures, Secret Sharing, Format-Preserving-Encryption, Verifiable Computing)* <https://prismacloud.eu>

*Sept. 2016 –* **Wissenschaftlich/Technische Gesamt-Projektleitung** des Projektes **RERUM**

*Aug. 2013* „REliable, Resilient and secUre IoT for sMART city applications“

(3 Jahre – 12 Partner – EU FP7 gefördert mit ~5,2 Mio. EUR – Umfang: ~554 PM)

- Stellvertretender wissenschaftlicher/technischer Koordinator (bis Dez. 2015)
- Partner: Eurescom, ATOS, Siemens AG, Zolertia, CYTA, Municipality of Heraklion, City of Tarragona, SIEMENS SSL, FORTH, Univ. Bristol, Univ. Linköping, Univ. Passau
- Leitung und Controlling aller Arbeiten der Univ. Passau (~0,5 Mio. EUR)
- Leitung des Arbeitspaketes „Security“ mit 118 Personenmonaten (PM) Umfang unter Beteiligung industrieller und akademischer Partner

Projekt-Ziel: *Erhöhung der Sicherheit und des Schutzes der Privatsphäre im Internet-der-Dinge (IoT)* <https://ict-rerum.eu>

*Aug. 2013 –* **Leitung eines Arbeitspaketes** im Projekt **RESCUEIT**

*Mär. 2010* „Robustes und verfügbares Supply-Chain-Management - Unterstützende IT-Plattform“

(3,5 Jahre – 14 Partner – BMBF / ANR gefördert – Umfang: ~471 PM)

- Leitung und Controlling aller Arbeiten der Univ. Passau (~472 Mio. EUR)
- Leitung des Arbeitspaketes „Rechtssicheres Lifecycle-Management von Authentizitäts- und Integritätszusagen für Daten (TruLy)“ mit 72 PM Umfang
- Partner: SAP AG, REWE Group, Eisbär Eis GmbH, BAAM Logistik, Dr. Oetker, Univ. Köln, Uni. Siegen, LOGPRO-CONSEIL, Telecom Sud Paris, SOGET, Institut Supérieur d'Etudes Logistiques (ISEL), Kuehne+Nagel, Univ. Passau

Projekt-Ziel: *Aufbau einer IT-Plattform für robustes und verfügbares Supply-Chain Management; Kryptographisches Design und Implementation von rechtssicheren und gleichzeitig datensparsamen Digitalen Signaturen*

## Forschungsprojekte (2/2):

An den folgenden Drittmittel-geförderten Forschungsprojekten habe ich entweder als Wissenschaftler an Teilaspekten mitgearbeitet oder an der Antragsanbahnung mitgewirkt:

Aug. 2018 – **Durchführung der Arbeiten** innerhalb des Projektes **SEMIOTICS** (EU H2020)  
 Sep. 2018 „Smart End-to-end Massive IoT Interoperability, Connectivity and Security“  
 • Partner: Siemens AG, FORTH, Centre Tecnologic de Telecomunicacions de Catalunya, Sphynx Technology Solutions AG, Engineering Ingegneria Informatica, ST Microelectronics, BlueSoft, Iquadrat Informatica, Univ. Passau

2017 – **Mitarbeit bei der Konzeption** des Projektes **FORSEC** (Bay. Staatsministerium  
 2013 für Wissenschaft, Forschung und Kunst)  
 „Sicherheit hochgradig vernetzter IT-Systeme“  
 • Partner: Univ. Regensburg, FAU Erlangen-Nürnberg, Fraunhofer AISEC, TU München, Univ. Passau

2005 – **Durchführung der Arbeiten** innerhalb des Projektes **PERCENTA**  
 2004 „Pervasive Computing Entwicklungen und Auswirkungen“  
 • Partner: EUROSEC, Univ. Kassel, ETH Zürich, M-LAB & ITEM-HSG, SAP, Univ. Hamburg

## Vorlesungen und andere Lehrveranstaltungen:

Folgende Vorlesungen und Übungen lese ich zur Zeit:

WS 2018/19 **Vorlesung: Advanced IT-Security** (3 SWS – english – M.Sc.)

WS 2018/19 **Übung: Advanced IT-Security** (1 SWS – english – M.Sc.)

Folgende Lehrveranstaltungen habe ich mit Lehrberechtigung inkl. Prüfungsberechtigung durchgeführt:

SS 2008 **Projekt Netzwerksicherheit** (Hands-On Praktikum – 6 SWS – eng./deu. – M.Sc.)

SS 2008 **Klausur: Grundlagen Sicherer Systeme (GSS)** (deu. – Diplom, B.Sc.)

Auswahl an Lehrveranstaltungen (insb. Praktika, Seminare und Übungen) die ich mit-konzipiert und zum größten Teil über mehrere Semester weiterentwickelt und gehalten habe (Semesterangabe ist die der ersten Veranstaltung):

WS 2008/09 **Seminar: Real Life Security / IT Security Unleashed** (2 SWS – eng./deu. – M.Sc.)

WS 2009/10 **Seminar: Interdisziplinäres Seminar zur Informationssicherheit unter Berücksichtigung juristischer Aspekte** (zus. mit Fakultät Jura – deu. – M.Sc.)

WS 2009/10 **Praktikum: Sicherheits-Infrastrukturen** (Hands-On – 6 SWS – eng./deu. – M.Sc.)

SS 2007 **Übung: Grundlagen Sicherer Systeme (GSS)** (1 SWS – deu. – Diplom, B.Sc.)

WS 2006/07 **Projekt: Software-Sicherheit I** (Hands-On – 6 SWS – deu. – Diplom, M.Sc.)

SS 2006 **Projekt: Software-Sicherheit II** (Hands-On – 6 SWS – deu. – Diplom, M.Sc.)

SS 2006 **Projekt Netzwerksicherheit** (Hands-On – 6 SWS – deutsch – Diplom, M.Sc.)

WS 2003/04 **Praktikum: Reverse Engineering** (Kompakt Veranstaltung – deutsch – Diplom)

Auswahl an weiteren Lehrveranstaltungen die ich gehalten habe:

WS 2005/06 **Übung: Technische Informatik 3** (1 SWS – deutsch – Diplom, M.Sc.)

SS 2005 **Übung: Grundlagen Beherrschbarer System (GBI)** (1 SWS – deu. – Diplom)

WS 2004/05 **Übung: Praktische Informatik P1** (1 SWS – deutsch – Diplom, M.Sc.)

SS 2004 **Übung: Praktische Informatik P2** (1 SWS – deutsch – Diplom, M.Sc.)

## Publikationen (Auswahl)

Im folgenden eine Auswahl der über 50 wissenschaftlichen Publikationen in Zeitschriften und auf internationalen Konferenzen; sowie eine Übersicht über mehrere Buchkapitel. Eine vollständigere Liste findet sich bei [dblp](#) und [Google scholar](#) (h-index 13), sowie auf meiner [persönlichen Homepage](#):

### Artikel in Zeitschriften (alle)

- H. C. Pöhls and T. Länger. **Einsetzbare Kryptografie für die Cloud.**  
In Zeitschrift für Datenrecht und Informationssicherheit (digma), 17 (1): 78-81, Mar., 2017.
- H. de Meer, H. C. Pöhls, J. Posegga and K. Samelin.  
**Redactable Signature Schemes for Tree with Signer-Controlled Non-Leaf-Redactions.**  
In Journal of E-Business and Telecommunications, 455: 155-171, 2014.
- F. Höhne, H. C. Pöhls and K. Samelin. **Rechtsfolgen editierbarer Signaturen.**  
In Datenschutz und Datenrecht (DuD), Volume 36 (6): 485-491, Juni, 2012.

### Publikationen in Konferenzbänden (alle, aber nur 2018 – 2015)

- L. Sell, H. C. Pöhls and T. Lorünser. **C3S: Cryptographically Combine Cloud Storage for Cost-Efficient Availability and Confidentiality.**  
In 10<sup>th</sup> Intl. Conf. on Cloud Computing Technology and Science (**CLOUDCOM 2018**), IEEE, 2018.
- S. Krenn, H. C. Pöhls, K. Samelin and D. Slamanig. **Protean Signature Schemes.**  
In 17<sup>th</sup> Conf. on Cryptology and Network Security (**CANS 2018**), Springer, 2018.
- S. Krenn, H. C. Pöhls, K. Samelin and D. Slamanig.  
**Chameleon-Hashes with Dual Long-Term Trapdoors and Their Applications.**  
In Progress in Cryptology (**AFRICACRYPT 2018**), Springer, 2018.
- T. Lorünser, H. C. Pöhls, L. Sell and T. Länger. **CryptSDLC: Embedding Cryptographic Engineering into Secure Software Development Lifecycle.**  
In 13<sup>th</sup> Intl. Conf. on Availability, Reliability and Security (**ARES 2018**), ACM, 2018.
- R. C. Staudemeyer, H. C. Pöhls and M. Wójcik. **The road to privacy in IoT: beyond encryption and signatures, towards unobservable communication.**  
In 7<sup>th</sup> Workshop on IoT Smart Objects and Services (**WOWMOM SOS-IOT 2018**), IEEE, 2018.
- A. Bilzhaue, H. C. Pöhls and K. Samelin.  
**Position Paper: The Past, Present, and Future of Sanitizable and Redactable Signatures.**  
In 12<sup>th</sup> Intl. Conf. on Availability, Reliability and Security (**ARES SECPID 2017**), CPS, 2017.
- H. C. Pöhls and B. Petschkuhn. **Towards compactly encoded signed IoT messages.**  
In 22<sup>nd</sup> Intl. Workshop on Computer-Aided Modeling Analysis and Design of Communication Links and Networks (**IEEE CAMAD 2017**), IEEE, 2017.
- M. T. Beck, J. Camenisch, D. Derler, S. Krenn, H. C. Pöhls, K. Samelin and D. Slamanig.  
**Practical Strongly Invisible and Strongly Accountable Sanitizable Signatures.**  
In 22<sup>nd</sup> Australasian Conf. on Information Security and Privacy (**ACISP 2017**), Springer, 2017.
- J. Camenisch, D. Derler, S. Krenn, H. C. Pöhls, K. Samelin and D. Slamanig. **Chameleon-Hashes with Ephemeral Trapdoors And Applications to Invisible Sanitizable Signatures.**  
In 20<sup>th</sup> IACR Intl. Conf. on Practice and Theory in Public-Key Cryptography (**PKC 2017**), 2017.
- G. Moldovan, E. Z. Tragos, A. Fragkiadakis, H. C. Pöhls and D. Calvo.  
**An IoT middleware for enhanced security and privacy: the RERUM approach.**  
In 8<sup>th</sup> IFIP Intl. Conference on New Technologies, Mobility and Security (**NTMS 2016**), IEEE, 2016.
- C. Frädrieh, H. C. Pöhls, W. Popp, N. Rakotondravony and K. Samelin. **Integrity and Authenticity Protection with Selective Disclosure Control in the Cloud and IoT.**  
In 18<sup>th</sup> Intl. Conf. on Information and Communications Security (**ICICS 2016**), Springer, 2016.
- J. Bauer, R. C. Staudemeyer, H. C. Pöhls and A. Fragkiadakis.  
**ECDSA on things: IoT integrity protection in practise.**  
In 18<sup>th</sup> Intl. Conf. on Information and Communications Security (**ICICS 2016**), Springer, 2016.

- T. Länger, H. C. Pöhls and S. Ghernaoui. **Selected Cloud Security Patterns to Improve End User Security and Privacy in Public Clouds.**  
In Privacy Technologies and Policy - 4<sup>th</sup> Annual Privacy Forum (**APF 2016**), Springer, 2016.
- T. Lorünser, D. Slamanig, T. Länger and H. C. Pöhls.  
**PRISMACLOUD Tools: A Cryptographic Toolbox for Increasing Security in Cloud Services.**  
In 11<sup>th</sup> Intl. Conference on Availability, Reliability and Security (**ARES SECPID 2016**), CPS, 2016.
- A. Bilzhaue, M. Huber, H. C. Pöhls and K. Samelin.  
**Cryptographically Enforced Four-Eyes Principle.**  
In 11<sup>th</sup> Intl. Conference on Availability, Reliability and Security (**ARES SECPID 2016**), CPS, 2016.
- M. Mössinger, B. Petschkuhn, J. Bauer, R. C. Staudemeyer, M. Wójcik and H. C. Pöhls.  
**Towards quantifying the cost of a secure IoT: Overhead and energy consumption of ECC signatures on an ARM-based device.**  
In 5<sup>th</sup> Workshop on IoT Smart Objects and Services (**WOWMOM SOS-IOT 2016**), IEEE, 2016.
- A. Kung, F. Kargl, S. Suppan, J. Cuellar, H. C. Pöhls, A. Kapovits, N. Notario and Y. S. Martin.  
**A Privacy Engineering Framework for the Internet of Things.**  
In 9<sup>th</sup> Intl. Conf. on Computers, Privacy and Data Protection 2016 (**CDPD 2016**), 2016.
- D. Derler, C. Hanser, H. C. Pöhls and D. Slamanig.  
**Towards Authenticity and Privacy Preserving Accountable Workflows.**  
In 10<sup>th</sup> IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 Intl. Summer School, Springer, 2016.

Ausgewählte Publikationen in Konferenzbänden (ausgewählte, Jahrgänge 2015 – 2004)

- D. Derler, H. C. Pöhls, K. Samelin and D. Slamanig.  
**A General Framework for Redactable Signatures and New Constructions.**  
In 18<sup>th</sup> Intl. Conference on Information Security and Cryptology (**ICISC 2015**), Springer, 2015.
- H. C. Pöhls.  
**JSON Sensor Signatures (JSS): End-to-End Integrity Protection from Constrained Device to IoT Application.**  
In 9<sup>th</sup> Intl. Conf. on Innovative Mobile and Internet Services in Ubiquitous Computing (**IMIS-2015**), IEEE, 2015.
- H. C. Pöhls, B. Petschkuhn, J. Rückert and M. Mössinger.  
**Aggregation and Perturbation in Practice: Case-Study of Privacy, Accuracy and Performance.**  
In 19<sup>th</sup> Intl. Workshop on Computer-Aided Modeling Analysis and Design of Communication Links and Networks (**CAMAD 2014**), IEEE, 2014.
- H. C. Pöhls and K. Samelin.  
**On Updatable Redactable Signatures.**  
In 12<sup>th</sup> Intl. Conf. on Applied Cryptography and Network Security (**ACNS 2014**), Springer, 2014.
- E. Z. Tragos, V. Angelakis, A. Fragkiadakis, D. Gundlegard, S. Nechifor, G. Oikonomou, H. C. Pöhls and A. Gavras. **Enabling Reliable and Secure IoT-based Smart City Applications.**  
In Wireless Communications and Networking Conference Workshops (**WCNC 2014**), IEEE, 2014.
- H. C. Pöhls, V. Angelakis, S. Suppan, K. Fischer, G. Oikonomou, E. Z. Tragos, R. D. Rodriguez and T. Mouroutis.  
**RERUM: Building a Reliable IoT upon Privacy- and Security- enabled Smart Objects.**  
In Wireless Communications and Networking Conference Workshops (**WCNC 2014**), IEEE, 2014.
- C. Brzuska, H. C. Pöhls and K. Samelin.  
**Efficient and Perfectly Unlinkable Sanitizable Signatures without Group Signatures.**  
In 10<sup>th</sup> European PKI Workshop: Services and Applications (EuroPKI 2013), Springer, 2013.
- H. C. Pöhls.  
**Contingency Revisited: Secure Construction and Legal Implications of Verifiably Weak Integrity.**  
In Trust Management VII (**IFIP TM 2013**), Springer, 2013.
- C. Brzuska, H. C. Pöhls and K. Samelin.  
**Non-Interactive Public Accountability for Sanitizable Signatures.**  
In 9<sup>th</sup> European PKI Workshop: Research and Applications (**EuroPKI 2012**), Springer, 2012.

- H. C. Pöhls and F. Höhne.  
**Sticky Signatures: Legal Advantages of Redactable Signatures and Credentials in the Food Supply Chain.**  
In 5<sup>th</sup> **Interdisciplinary Conference on Current Issues in IT Security**, Dunker & Humblot, 2012.
- K. Samelin, H. C. Pöhls, A. Bilzhause, J. Posegga and H. de Meer.  
**On Structural Signatures for Tree Structured Data.**  
In 10<sup>th</sup> Intl. Conf. on Applied Cryptography and Network Security (**ACNS 2012**), Springer, 2012.
- H. C. Pöhls and F. Höhne.  
**The Role of Data Integrity in EU Digital Signature Legislation - Achieving Statutory Trust for Sanitizable Signature Schemes.**  
In 7<sup>th</sup> Intl. Workshop on Security and Trust Management (**STM 2011**), Springer, 2012.
- H. C. Pöhls, K. Samelin and J. Posegga.  
**Sanitizable Signatures in XML Signature - Performance, Mixing Properties, and Revisiting the Property of Transparency.**  
In 9<sup>th</sup> Intl. Conf. on Applied Cryptography and Network Security (**ACNS 2011**), Springer, 2011.
- F. Höhne and H. C. Pöhls. **Staatliche Schutzpflichten für die IT-Infrastruktur.**  
In **D-A-CH Security 2010**, September, 2010.
- F. Höhne and H. C. Pöhls.  
**Grund und Grenzen staatlicher Schutzpflichten für die IT-Infrastruktur.**  
In 11. Herbstakademie der Deutschen Stiftung für Recht und Informatik (**DSRI**), OIWIR, 2010.
- R. Herkenhöner, M. Jensen, H. C. Pöhls and H. de Meer.  
**Towards Automated Processing of the Right of Access in Inter-Organizational Web Service Compositions.**  
In Intl. Workshop on WebService and Business Process Security (**WSBPS 2010**), IEEE, 2010.
- B. Braun and H. C. Pöhls. **Authenticity: The missing link in the social semantic web.**  
In **INFORMATIK 2008**, Springer, 2008.
- H. C. Pöhls. **Verifiable and Revocable Expression of Consent to Processing of Aggregated Personal Data.**  
In 10<sup>th</sup> Information and Communications Security (**ICICS 2008**), Springer, 2008
- H. C. Pöhls and J. Posegga. **Smartcard Firewalls Revisited.**  
In 7<sup>th</sup> Intl. Conf. on Smart Card Research and Applications (**CARDIS 2006**), Springer, 2006.

#### Ausgewählte Bücher und Buchkapitel

- V. Angelakis, E. Tragos, H. C. Pöhls, A. Kapovits and A. Bassi, Ed.  
**Designing, Developing, and Facilitating Smart Cities: Urban Design to IoT Solutions.**  
Springer Intl. Publishing, 2017.
- A. Fragkiadakis, G. Oikonomou, H. C. Pöhls, E. Z. Tragos and M. Wójcik.  
**Securing Communications Among Severely Constrained, Wireless Embedded Devices.**  
In Engineering Secure Internet of Things Systems, The Institute of Engineering and Technology, Oct., 2016.
- R. C. Staudemeyer, H. C. Pöhls and B. W. Watson.  
**Security & Privacy for the Internet-of-Things communication in the SmartCity.**  
In Designing, Developing, and Facilitating Smart Cities, Springer, 2016.
- E. Z. Tragos, A. Fragkiadakis, V. Angelakis and H. C. Pöhls.  
**Designing Secure IoT Architectures for Smart City Applications.**  
In Designing, Developing, and Facilitating Smart Cities, Springer, 2016.
- G. Baldini, et al.. **Internet of Things -- Governance, Privacy and Security Issues.** IERC, 2015.
- E. Z. Tragos, et al.. **Securing the Internet of Things - Security and Privacy in a Hyperconnected World.**  
In Building the Hyperconnected Society - IoT Research and Innovation Value Chains, Ecosystems and Markets, River Publishers, 2015.

## **Akademische Aktivitäten:**

---

Folgende Konferenzen und Workshops habe ich als Mitglied des Programmkomitees und Reviewer unterstützt:

- IEEE Intl. Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'19),
- Open Identity Summit 2019 (OID'19),
- Human Computer Interaction Intl. (HCI'18) - HCI for Cybersecurity, Privacy and Trust (HCI-CPT'19),
- 3rd Workshop on Security, Privacy, and Identity Management in the Cloud (SECPID'18),
- Intl. Conference on Emerging Electronic Solutions for IoT (ICEESI'17),
- 3rd Annual IoT Global Innovation Forum (IoTGIF'17),
- 2nd Workshop on Security, Privacy, and Identity Management in the Cloud (SECPID'17),
- IEEE World Forum on IoT - Workshop on User centric security, privacy and interoperability in the context of Internet of Things and Smart Cities (WF-IoT'16),
- Workshop on Security, Privacy, and Identity Management in the Cloud (SECPID'16),
- Open Identity Summit 2016 (OID'16),
- Open Identity Summit 2015 (OID'15),
- Workshop in Information Security Theory and Practice (WISTP'15),
- Intl. Conference on Mobile, Secure and Programmable Networking (MSPN'15),
- Smart Energy Grid Security Workshop 2014 (SEGS'14),
- Workshop in Information Security Theory and Practice (WISTP'14),
- Open Identity Summit 2013 (OID'13),
- Workshop in Information Security Theory and Practice (WISTP'12),
- Workshop GI INFORMATIK 2011 "Datenschutz und Identitätsmanagement für Communities - Communities für Datenschutz und Identitätsmanagement" (DICCDI'11).

Folgende Zeitschriften, Konferenzen, Workshops habe ich als Reviewer unterstützt:

SECRYPT 2016, SECRYPT 2015, WISTP 2014, ESORICS 2014, Crisis 2014, SECRYPT 2013, WISTP 2013, Information Security Technical Report (ISTR), Crisis 2012, ABPSM 2011, WSNSCM 2011, IEEE Pervasive Computing, SECRYPT 2011, IPTComm 2010, SECRYPT 2010, TrustBus 2010, SPCC 2010, TrustBus 2009, WOSIS 2009, SecureComm 2007, WOSIS 2007, WISTP 2007, Computer Networks - Special Issue on Smartcards, KiVS 2007, Aml.d 2006, CARDIS 2006, International Journal of Information Security (IJIS), TSPUC 2006, SEC 2006, ISAS 2005, TSPUC 2005, IEEE Security & Privacy, MCTA 2005, SPC 2005, EURESCOM Summit 2005, CCS 2004

## **Internationale Standardisierung:**

---

Ich bin akkreditierter Experte und unterstütze aktiv die internationale Standardisierung in der ISO/IEC JTC 1/SC 27 „IT Security techniques“. Des Weiteren bin ich Editor (resp. Co-Editor) folgender Standard-Projekte:

- ISO 23264-1 IT Security techniques – Redaction of Authentic Data – Part:1 General**
- ISO 23264-2 IT Security techniques – Redaction of Authentic Data – Part:2 Redactable signature schemes based on asymmetric mechanisms**

Zur Deckung der dabei entstehenden (Reise-)Kosten habe ich 2018 eigene EU Fördermittel im OpenCall des standICT.eu Projektes einwerben können.

Passau, den 09.12.2018

