Ned M. Smith

(mobile) 503.830.9733
(email) entropyworks@outlook.com

Objective: Trusted computing technology innovation

Employment History

Independent Consultant

(August 2025 – present)

- **Projects**

  Integration of Verifiable Legal Entity Identifiers (vLEI) with the Secure Asset Transfer Protocol (SATP) – see IETF draft-smith-satp-vlei-binding

- **Chair Positions**

  IETF Remote Attestation Procedures (RATS) Working Group

  TCG Attestation Working Group

Intel Corporation

(1995 – August 2025) – details follow

- **Intel Product Assurance and Security** (Asmae Mhassni)
  2024(Sep) – 2025(July): Principal Engineer – OS Kernel Development and standards.
  Attestation and root of trust standards for the Internet Engineering Task Force (IETF), Trusted Computing Group (TCG), and Confidential Compute Consortium (CCC).

  Trusted / confidential computing standards enable HW-based interoperable CC ecosystem. Ned developed a suite of attestation and RoT standards (DICE, CoRIM, Concise Evidence, Message Wrap, and EAT) are in server, client, edge, and FPGA platforms. Ned made sure Intel products have HW-based RoT and implement industry standard attestation evidence and manifest formats.

  Intel Product Impact:
  - Intel TDX – DICE RoT, Concise Evidence, CoRIM
  - Security and Management Controller (S3M) – DICE, CoRIM
  - Memory Controller – DICE RoT
  - Embedded Security Engine (ESE) – DICE RoT, Concise Evidence, CoRIM
  - Agilex FPGA: Falcon Mesa, Diamond Mesa (structured ASIC), Sundance Mesa, Kinneloa Mesa
  - Intel Foundry Services (IFS) / Intel Key Generation certificates
  - Intel Profiles for IETF RATS covering evidence, reference values, and attestation results

  Industry Impact:
  Ned's influence is felt across the industry as chair of IETF RATS working group and author of several specifications that are adopted by Microsoft, Google, Dell, HP, nVidia, ARM, AMD and others.

- **SATG / Security, Privacy and Mitigation** (Dave Stewart mgr.)
  2021 (Jun) – 2024(Sep): Principal Engineer – Hardware security engine, attestation design and standards.

  Standards:
  - Primary author: TCG Endorsement Manifest for Devices Specification
  - Primary author: TCG Attestation Framework Requirements Specification
  - Co-author: IETF Internet draft: Concise Reference Integrity Manifest

  - See additional detail below

- **IAGS / Security Practices and Engineering** (Judi Goldstien / Deneen Dock mgrs.)
  2019 –2021 (Jun): Principal Engineer – Hardware security engine and attestation design and standards. Worked across several Intel teams on HW security engine designs that included cryptographic device identity, secure device layering and interoperable attestation features.
  Projects influenced include:
  - Programable Solutions Group (PSG): Falcon Mesa – DICE root of trust, layering and embedded certificate authority architecture. Secure Protocol and Data Model (SPDM) attestation interactions semantics.
  - Client Computing Group (CCG): Enhanced Security Engine (ESE) – Composite device architecture with DICE and TPM roots of trust.
  - Client Computing Group (CCG): On Die Certificate Authority (ODCA) – Integration of ODCA certificate hierarchy with TCG Embedded Certificate Authority (ECA) standards.
  - DICE and Attestation cross-group consulting:
    - Data Center Group (DCG): Server Platform Firmware Resilience (PFR), Secure System Startup Manager (S3M), Software Guard Extensions (SGX) / Trust Domain Extensions (TDX), Millcreek falls platform root of trust.
    - Internet of Things Group (IoTG): Movidius for servers.

  Standards:
  - Primary author: TCG DICE Attestation Architecture Specification – See Publications.
  - Primary author: TCG DICE Layering Architecture Specification – See Publications.
  - Primary author: TCG DICE Certificate Profiles Specification – See Publications.
  - Co-author: IETF Internet draft: Remote Attestation Procedures Architecture – See Publications.

- **SSP / OTC / Orchestration and Automation Pathfinding** (Jenny Koerv mgr.)
  2017 – 2019: Principal Engineer – Edge innovation and standards.
  Researched edge computing and architecture for securing and trusting edge computing using containers. Filed more than 100 patents.

  Technical Strategic Long-Range Plan (TSLRP):
    - Contributed to the Edge Transformation topic by co-authoring presentation content targeting Intel executive staff members. Member of security and storage sub-teams. Filed related patents. See additional detail below.

- **SSG / Open Technology Center (OTC) / Internet of Things Engineering**
(Kathleen Kovatch / Mark Skarpness mgrs.)
  2014 – 2017: Principal Engineer – Consumer IoT standards and frameworks.
  Defined the security architecture for Open Connectivity Foundation (OCF) IoT framework.
  - Author/editor: OCF Security Specification, See Publications. OCF standards are implemented broadly by consumer electronics vendors including Samsung, LG, Electrolux, Cisco, Microsoft etc.
  - Security software architecture for IoTivity (*IoTivity is the reference implementation of OCF*).

- **SSG / Software Pathfinding** (Dave Cobbley mgr.)
  2012 – 2014: Principal Engineer – Contextual computing pathfinding and innovation.
  Projects:
  - Contextual Authentication Technology (CAT) – Machine learning classifiers use sensors to automatically adjust user's login policy to improve user convenience by avoiding re-authentication prompts in low-risk situations. – *Incorporated into Android for smartphones and automobiles* as Google Smart Lock™ technology.
  - Personalization with Privacy (PwP) – Online advertising ecosystems exploit privacy sensitive information to improve advertiser need to personalize. PwP enables personalization while allowing users to retain control over privacy sensitive information. – *Incorporated into OHSU/Intel Health Services joint project.*

    - Digital Relationship Management (DReM) and Self-Encrypted Email (SEE) – Person-to-person key exchange is integrated into social interactions that establish ‘digital relationship’ context that links social trust to encryption keys.

- **PC Client Group / Business Client Platform Group** (Steve Grobman / Yasser Rasheed mgrs.)
  2008 – 2012: Principal Engineer – Business Client Platforms / Intel vPro Technology:
    - Intel Authenticate - Multi-factor authentication architecture. Designed multi-factor user authentication for CSME. Shipped in Skylake and subsequent mobile and desktop platforms.
    - Identity Protection Technology (IPT) - Public Key Infrastructure. Designed pre-boot user authentication and key management module for Self Encrypting Drives (SED). Shipped with Skylake desktop platforms.
    - Danbury/Anti-theft technology - Chipset Full-disk encryption (FDE) architecture. Designed pre-boot user authentication and key manager for Danbury Technology (chipset level FDE). (Was not incorporated into product for business reasons).
    - Intel vPro Technology brand accounted for >$2B increased revenue.

- **Digital Office Group** (Steve Grobman)
  2005 – 2008: Staff Security Architect – Digital Office.
    - Intel Platform Trust Technology (PPT) architecture for desktop platforms. Co-designed software TPM task for Converged Security and Manageability Engine (CSME) in desktop platforms. Shipped with mobile and desktop platforms.
    - Platform architecture specification for vPro platforms. Shipped with multiple Intel vPro™ branded PCs.
        - Intel vPro Manageability Engine (ME) security architecture.
        - Intel vPro virtualization technology (VT-x) security – secure boot architecture for desktop platforms.
        - Intel Trusted Execution Technology (TXT) design – secure boot architecture for desktop platforms.

- **Desktop Architecture Labs** (David Grawrock mgr.)
  2002 – 2005: Staff Security Architect - Trusted Computing Architecture and Standards:
    - Digital Office security architecture / TPM infrastructure enabling.
    - Co-chair: TCG Infrastructure Workgroup (IWG). Developed and co-authored public key infrastructure (PKI) for TPM-based trusted computing and attestation.
    - Co-chair: TCG Trusted Network Connect (TNC) work group. Developed and co-authored the first industry standard Network Access Control (NAC) specification with more than 30 participating companies in the network equipment manufacturing and system software ecosystem. MIcrosoft Network Access Protection (NAP) was a leading adopter.

- **Intel Architecture Labs** (George Cox / David Riss / David Aucsmith mgrs.)
  2001 – 2002: Security Architect - Control Networks Architecture:
    - Directed control network market analysis and control network gateway. Successfully identified a $200M - $1B market opportunity (in 2005) for Intel in embedded control network industry.
    - W3C Web Ontology Working Group representative.

  2000 - 2001: Security Architect - Trusted Business and Mobile Data Services Architecture:
    - Designed person-person key exchange methods for establishing varying degrees of trust between ad-hoc groups or individuals.
    - Defined protocols for exchanging authenticated information over wireless channels.
    - Defined electronic contracts and electronic contract lifecycle procedures for negotiating business transactions between trading partners.
    - Designed distributed authorization in workflow system. Intel representative at Workflow Management Coalition (WFMC).
    - Technical reviewer of RosettaNet - a standard for automated B2B transactions.

  1998 - 2000: Senior Software Design Engineer – Crypto APIs and Standards:

- Co-author and technical reviewer of Common Data Security Architecture (CDSA) in The Open Group industry forum. http://www.opengroup.org/security/cdsa.htm
- Designed and patented distributed signing and key management system for CDSA.
- Designed secret sharing technique – project later moved to Intel Key Generation Facility (iKGF).

1995 (Aug) –1997: Secure Communications Senior Software Design Engineer:

- Represented Intel at the IETF Transport Layer Security (TLS) working group.
- Designed & implemented a Winsock2 layered service provider that applied Microsoft PCT / Secure Sockets Layer (SSL) encryption of TCP/IP.

Sequent Computer Systems Inc.
(1989 – 1995) details follow

- **Trusted Systems, Decision Support, Firewalls & Video on Demand** (David Aucsmith mgr.): Software Engineer
  - Performance measurement of decision support databases on Dynix/PTX.
  - Designed & implemented a Windows 3.1 based human interface to CISCO packet filtering router (IOS v11) for improved firewall configuration by field sales personnel.
  - Designed & implemented buffer manager for streaming video on a modified Dynix/PTX.
  - Trusted Dynix/PTX design & implementation based on TCSEC "Orange Book" requirements for B1 compliant operating system.
  - Configuration Management & Defect Tracking System, A1 TCSEC compliant (highest possible rating)
  - Ported X-Windows to Trusted Dynix/PTX.
  - Ported Dynix/PTX OS loader environment to load Trusted Dynix/PTX.

Brigham Young University Computer Science Department
(1987 –1989)

Systems Administrator – Unix System V, BSD, Mt. Zinu, Netware, DEC-Vax

Education

August 1989: BS/CS – Brigham Young University
GPA: 3.4/4.0 cumulative 3.7/4.0 major
December 1997: MS/CS – Portland State University
GPA: 3.5/4.0

Masters Project: Java implementation of the PolicyMaker trust management system with credential mapping using the Common Data Security Architecture (CDSA).

Leadership

Chair/Editor Positions:

- TCG Board of Director (2024 – 2025)
- TCG Assistant Borad of Director (2022 – 2024)
- IEEE Associate Editor, Consumer Electronics Magazine (2022 - present)
- TCG Attestation Working Group – co-chair – (2020 – present)
- Intel Attestation Core Team – chair - (2020 – 2025)
- IETF Remote Attestation Procedures (RATS) WG co-chair – (2019 – present)
- TCG Device Identity Composition Engine Architecture – editor (2018 – present)
- Open Connectivity Foundation Security WG – editor (2015 - 2016)
- TCG Infrastructure Working Group – co-chair (2002 – 2005)
- TCG Trusted Network Connect Working Group – co-chair (2004 – 2005)

Leadership Awards:

1. 2024 Intel Security Leadership Award - Advancing Edge cybersecurity in standards to enable wider adoption of Intel products
2. 2022 Trusted Computing Group – Leadership Award
3. 2019 Trusted Computing Group – Key Contributor Award
4. 2018 DRA SSG/OTC – Driving approval of the Open Connectivity Foundation (OCF) standard
5. 2017 DRA SSG/OTC – Fostering IoT device interoperability with IoTivity 1.3
6. 2015 DRA SSG/OTC – Open Connectivity Foundation (OCF) Security Specification Published
7. 2007 DRA Business Client Group BCG/DO – Danbury Architecture
8. 2005 TCG Recognition for PC Client Specification for Conventional BIOS, v1.2
9. 2005 TCG Recognition for PC Client TPM Interface Specification, v1.2
10. 2005 TCG Recognition for Specification Publications by the IWG & TNC Workgroups (numerous)
11. 2001 DRA Intel Labs – Common Data Security Architecture published by Open Group

Technical Strategic Long-Range Planning (TSLRP)

- 2022: Workstream Lead – Root of Trust Openness (honorable mention)
- 2022: Workstream Lead – Cloud to Edge Security / Security Fabric (adopted)
- 2019: Workstream Contributor – Edge as a Service / Storage and Security (finalist)
- 2017: Workstream Contributor – Frictionless Data Analytics / Attribute Attestation (finalist)
- 2016: Workstream Lead – Mediated Social Reality (aka DRM) with Brain-Computer-Interface (honorable mention)
- 2010: Topic Lead – Trusted Cloud using Secure Enclaves/SGX (adopted)
- 2008: Topic Lead - A Converged I/O Controller Hub (honorable mention)

Inventor Awards:

- 2024 Intel Top Inventor Award
- 2023 Intel Top Inventor Award
- 2022 Intel Top Inventor Award
- 2021 Intel Top Inventor Award
- 2019 Intel Top Inventor Award
- 2018 Nominated for Intel Distinguished Inventor
- 2016 Intel Top Inventor Award
- 2015 Intel Top Patent Filer Award
- 2014 Intel Top Patent Filer Award
- 2012 Intel Top Patent Filer in SSG

Other Awards:

- 2015 IH&MMSec '15: ACM Information Hiding & Multimedia Security Workshop Co-chair Service Award

Other Innovation:

- Patent Harvesting Efforts (each result in ~ 20 – 150 inventions)
    - Internet of Things (IoT) – 2016
    - Mobile Edge / Multi-access Edge Computing (MEC) – 2018
    - Visual Fog – 2018
    - Information Centric Networking (ICN) – 2019
    - Edge Computing – 2019
    - Edge Security – 2020
    - Satellite Premium – 2020
    - Nova Compute Graphics Premium – 2020

- Edge as a Service Premium – 2020
- Mobility as a Service Premium – 2020
- Intelligent Transportation System Verticals – 2021
- Resilient & Intelligent Next Generation Systems – 2021
- Intelligent Transportation System Verticals - 2022
- Autonomous Systems and Intelligent Transportation Edge – 2022
- Cloud to Edge Security - 2022

Publications:

Books:

1) "Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment", Sunil Cheruvu, Anil Kumar, Ned Smith, David M. Wheeler, APress, 1st Ed., 23 August 2019. ISBN-13: 978-1484228951 https://www.apress.com/us/demystifying-internet-of-things-security/17097958
2) "Building the Infrastructure for Cloud Security A Solutions View", Raghu Yeluri, Enrique Castro-Leon, Springer, Apr 2, 2014. ISBN-13: 978-1-4302-6145-2 (Print) 978-1-4302-6146-9 https://link.springer.com/book/10.1007/978-1-4302-6146-9 – *Chapter 7 co-author.*

Papers:

1) D. Sabella, K. Maloor, N. Smith, M. Vanderveen and A. Kourtis, "Edge Computing Cybersecurity Standards: Protecting Infrastructure and Applications," in *IEEE Access*, vol. 12, pp. 185328-185335, 2024, doi: 10.1109/ACCESS.2024.3506212.
2) "MEC security; Status of standards support and future evolutions", ETSI White Paper No. #46, 2nd edition – September 2022. ISBN No. 979109262041 https://www.etsi.org/images/files/etsiwhitepapers/etsi-wp-46-2nd-ed-mec-security.pdf
3) "An Attestation Architecture for Blockchain Networks", Hardjono, Smith, DeepAI, 08 May 2020. https://deepai.org/publication/an-attestation-architecture-for-blockchain-networks
4) "Decentralized Trusted Computing Base for Blockchain Infrastructure Security", Thomas Hardjono, Ned Smith, Frontiers in Blockchain, 06 December 2019. https://doi.org/10.3389/fbloc.2019.00024
5) "Toward A Common Modeling Standard for Software Update and IoT Objects", Ned Smith, IAB, IoTSU Workshop, June 2016. https://down.dsg.cs.tcd.ie/iotsu/subs/IoTSU_2016_paper_5.pdf and https://tools.ietf.org/html/draft-farrell-iotsu-workshop-01
6) "Key Semantic Interoperability Gaps in the Internet-of-Things Meta-Models", Ned Smith et.al. IAB IoTSI Workshop, March 2016. https://www.iab.org/wp-content/IAB-uploads/2016/03/IAB-Semantic-Interop-Intel-Perspective-Final.pdf
7) "Cloud-Based Commissioning of Constrained Devices using Permissioned Blockchains", Thomas Hardjono, Ned Smith, IoTPTS '16 Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security, Pages 29-36, ACM New York, NY, USA ©2016.
8) "Adding Non-Traditional Authentication to Android", Ned Smith et.al., Intel Technology Journal, Volume 18, Issue 4, Apr 1, 2014.
9) "Storage Protection with Intel® Anti-Theft Technology - Data Protection (Intel® AT-d)", Ned Smith, Intel Technology Journal, Volume 12, Issue04, 23 Dec 2008.
10) "New Client Virtualization Usage Models Using Intel Virtualization Technology", Mahendra Ramachandran et.al., Intel Technical Journal, Volume 10, Issue3, pp204-216, Aug. 2006.

Standards:

1) "Remote Attestation Procedures Architecture", IETF, RFC9334, 28Dec, 2025. Available Online: https://datatracker.ietf.org/doc/rfc9334/
2) "RATS Conceptual Messages Wrapper", IETF, draft-ietf-rats-msg-wrap, 11Dec, 2025. Available Online: https://datatracker.ietf.org/doc/draft-ietf-rats-msg-wrap/

3) "Intel Profile for CoRIM", IETF, draft-cds-rats-intel-corim-profile, 26Nov, 2025. Available Online: https://datatracker.ietf.org/doc/draft-cds-rats-intel-corim-profile/
4) “TCG Attestation Framework Part 1: Terminology, Concepts, and Requirements”, Version 1.0, 1Nov, 2025. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/TCG-Attestation-Framework-Part-1_pub.pdf
5) “Concise Reference Integrity Manifest”, IETF, draft-ietf-rats-corim, 27Oct, 2025. Available Online: https://datatracker.ietf.org/doc/draft-ietf-rats-corim/
6) “A SATP Core Binding for vLEI Identities”, IETF, draft-smith-satp-vlei-binding, 16Oct, 2025. Available Online: https://datatracker.ietf.org/doc/draft-smith-satp-vlei-binding/
7) "TCG DICE Concise Evidence Binding for SPDM", Version 1.1, 4Sep, 2025. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/TCG-DICE-Concise-Evidence-Binding-for-SPDM-V1.1_pub.pdf
8) "Secure Asset Transfer (SAT) Interoperability Architecture", IETF, draft-ietf-satp-architecture, 31Jul, 2025. Available Online: https://datatracker.ietf.org/doc/draft-ietf-satp-architecture/
9) “DICE Certificate Profiles Specification”, Version 1.1, 24Apr, 2025. Available online: https://trustedcomputinggroup.org/wp-content/uploads/DICE-Certificate-Profiles-v1.1_pub.pdf
10) “DICE Endorsement Architecture for Devices”, Version 1.0, Revision 0.38, 15Nov, 2022. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/TCG-Endorsement-Architecture-for-Devices-V1-R38_pub.pdf
11) “DICE Attestation Architecture Specification”, Version 1.2, 24Apr, 2022. Available online: https://trustedcomputinggroup.org/wp-content/uploads/DICE-Attestation-Architecture-v1.2_pub.pdf
12) “DICE Layering Architecture Specification”, Version 1.0, Revision 0.19, 23Jul, 2020. Available online: https://trustedcomputinggroup.org/wp-content/uploads/DICE-Layering-Architecture-r19_pub.pdf
13) “Symmetric Identity Based Device Attestation”, Version 1.0, Revision 0.95, 7Jan, 2020. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/TCG_DICE_SymIDAttest_v1_r0p95_pub-1.pdf
14) “TCG Trusted Attestation Protocol (TAP) Information Model for TPM Families 1.2 and 2.0 and DICE Family 1.0”, Version 1.0, Revision 0.36, 3Sep, 2019. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/TNC_TAP_Information_Model_v1.00_r0.36-FINAL.pdf
15) “TCG Platform Attribute Credential Profile”, Version 1.0, Revision 16, 16Jan, 2018. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/TCG-Platform-Attribute-Credential-Profile-Version-1.0.pdf
16) “OCF Security Specification”, Open Connectivity Foundation (OCF), Version 1.0.0, June 2017. Available online: https://openconnectivity.org/specs/OCF_Security_Specification_v1.0.0.pdf.
17) “TCG Trusted Network Connect Communications TNC IF-T: Protocol Bindings for Tunneled EAP Methods”, Version 2.0, Revision 5, 8May, 2014. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/TNC_IFT_EAP_v2_0_r5-a2.pdf
18) “TCG Credential Profiles for TPM Family 1.2; Level 2”, Version 1.2, Revision 8, 3Jul, 2013. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/Credential_Profiles_V1.2_Level2_Revision8.pdf
19) “TCG Attestation PTS Protocol: Binding to TNC IF-M”, Version 1.0, Revision 28, 24Aug, 2011. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/IFM_PTS_v1_0_r28.pdf
20) “TCG Infrastructure Working Group Integrity Report Schema”, Version 2.0, Revision 5, 24Aug, 2011. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/IWG_Integrity_Report_Schema_v2.0.r5.pdf
21) “TCG Infrastructure Working Group Core Integrity Schema”, Version 2.0, Revision 5, 24Aug, 2011. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/CoreIntegrity_Schema_Specification_v2.0.r5.pdf
22) “TCG Trusted Network Connect TNC IF-M: TLV Binding”, Version 1.0, Revision 37, 10Mar, 2010. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/TNC_IFM_TLVBinding_v1_0_r37a.pdf
23) “TCG Trusted Network Connect TNC Architecture for Interoperability”, Version 1.4, Revision 4, 18May, 2009. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/TNC_Architecture_v1_4_r4.pdf

24) “TCG Trusted Network Connect TNC IF-MAP binding for SOAP”, Version 1.0, Revision 25. 28Apr, 2008. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/TNC_IFMAP_v1_0_r25.pdf
25) “TCG Infrastructure Working Group Verification Result Schema”, Version 1.0, Revision 1.00, 21May, 2007. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/IWG-Verification_Result_v1_0.pdf
26) “TCG Infrastructure Working Group Security Qualities Schema”, Version 1.1, Revision 7, 21May, 2007. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/IWG_Security_Qualities_Schema_v1_1_r07.pdf
27) “TCG Trusted Networkk Connect TNC IF-TNCCS”, Version 1.1, Revision 1.00, 5Feb, 2007. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/TNC_IF-TNCCS_v1_1_r15.pdf
28) “TCG Trusted Network Communications TNC IF-PEP: Protocol Bindings for RADIUS”, Version 1.1, Revision 0.8, 5Feb, 2007. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/TNC_IF-PEP-v1.1-rev-0.8.pdf
29) “TCG Trusted Network Connect TNC IF-IMV”, Version 1.2, Revision 8, 5Feb, 2007. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/TNC_IFIMV_v1_2_r8.pdf
30) “TCG Trusted Network Connect TNC IF-IMC”, Version 1.2, Revision 8, 5Feb, 2007. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/TNC_IFIMC_v1_2_r8.pdf
31) “TCG Infrastructure Working Group Architecture Part II – Integrity management”, Version 1.0, Revision 1.0, 17Nov, 2006. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/IWG_ArchitecturePartII_v1.0.pdf
32) “TCG Infrastructure Working Group Reference Manifest (RM) Schema Specification”, Version 1.0, Revision 1.0. 17Nov, 2006. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/IWG-Reference_Manifest_Schema_Specification_v1.pdf
33) “TCG Infrastructure Working Group Platform Trust Services Interface Specification (IF-PTS)”, Version 1.0, Revision 1.0, 17Nov, 2006. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/IWG-IF-PTS_v1.pdf
34) “Interoperability Specification for Backup and Migration Services”, Version 1.0, Revision 1.0, 30Jun, 2005. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/IWG_Backup_and_Migration_Services_1-00_1-00.pdf
35) “TCG Infrastructure Working Group Reference Architecture for Interoperability (Part 1)”, Version 1.0, Revision 1, 16Jun, 2005. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/IWG_Architecture_v1_0_r1.pdf
36) “TCG Infrastructure Working Group Subject Key Attestation Evidence Extension”, Version 1.0, Revision 7, 16Jun, 2005. Available Online: https://trustedcomputinggroup.org/wp-content/uploads/IWG_SKAE_Extension_1-00.pdf
37) “Common Data Security Architecture (CDSA) and CSSM” (with Corrigenda), Version 2.3, May, 2000. Available online: https://publications.opengroup.org/downloadable/download/link/id/MC4yNjg5MjIwMCAxNjI4MDk2NTkyMTAyNDY4NjEwNDg3NDM2NTE%2C/

Patents:
499 granted patents US Patent Office
See: https://ppubs.uspto.gov/pubwebapp/ Query: "smith ned"[IN]
970+ total granted patents world wide

Talks:

Speaker: “Attestation Ecosystem”, Global Platform Open Workshop on Attestation”, 20Nov, 2025.
Speaker: “Device Attestation vs. Artifact Provenance”, MIT BRAINS, 15Sep, 2025.
Keynote: “Trusted Computing Future: Emerging Use Cases and Solutions”, TCG Members Meeting, 17-20 Feb, 2025.
Speaker: “TCG Attestation Framework and IETF Remote Attestation Procedures: An
Overview of TCG and IETF Attestation Working Groups”, Japan Regional Forum Open Workshop, 29Feb, 2024.

Speaker: “Remote Attestation Procedures”, ORANGE Attestation workshop and roundtable, 2Nov, 2023.
Speaker: “Turtles all the way down”, MIT Connection Science, Imagination in Action, 26 April 2019.
Speaker: ”Trusted Containers as a vehicle for secure orchestration”, Intel SSG SecCon, 27-29 June 2018.
Speaker: “A Few Ideas about Trust”, 4th Annual Northwest Technology Summit on Blockchain, 12 September 2018.
Speaker: “Gateways: The center of complexity for update”, Linuxcon EU, Open IoT Summit – Berlin, 4-6 October 2016.
Speaker: “Open Internet Consortium Ecosystem, Specifications and Framework”, IEEE World Forum on Internet of Things, 14-16 December 2015.
Speaker: “Mirror Pass User Authentication System”, PCCG Tech Summit, 4Apr, 2012.
Speaker: “Mirror Pass: How client-based authentication gets the user out of password hell”, SSG SES Conference, 28Nov, 2012.
Panel: “Client to Cloud Security Panel”, Embedded user authentication, VM World, 29Aug – 1Sep, 2011.
Speaker: “Integrating User Authentication with Platform Authentication and Key Management”, CardTech / SecureTech, 16May, 2007.
Speaker: “Integrity Management Infrastructure…”, Ministry of Economic Trade and Industry (METI), 2nd Workshop on Advances in Trusted Computing (WATC) Tokyo, 1Dec, 2006.
Speaker: TCG Infrastructure WG chair 2002-2005 (numerous)
See www.linkedin.com/in/nedmsmith