CONFERENCE PROGRAM

PLATINUM SPONSOR

GOLD SPONSOR

SILVER SPONSORS

INTERNATIONAL CRYPTOGRAPHIC MODULE CONFERENCE 2018

May 8-11, 2018 ■ Ottawa, Ontario, Canada

the information security provider

Security First!

Use FIPS validated crypto modules whenever available.

Protect your data - wherever it is

USB stick, mobile device, server, network, Internet of Things and/or cloud: a validated cryptographic module provides assurance and compliance with the FIPS 140-2 standard.

Make competence your partner

atsec information security will support you through the challenges of the validation process.

Come and talk to us at our booth!

www.atsec.com

Welcome

On behalf of the conference organizers, atsec would like to welcome you all to ICMC18.

Since 2012 this community has met every year and organized itself in a spirit of cooperation, sharing and promotion of the FIPS 140-2 standard. This standard is critical not just to government agencies, but to industry as well many countries' economies and base infrastructures. In recent years the conference has also expanded to include the ISO/IEC 19790 and Common Criteria standards.

The conference continues to grow significantly. This year we have over 400 participants from over 22 countries. The agenda is compelling, with over 100 expert speakers from leading companies. There are nine different content tracks addressing certification programs, general technology, industry verticals, imbedded cryptography, post-quantum cryptography, the common criteria standard, open-source cryptography, end-user experience, advanced technology, and industry perspectives.

There are more than twenty exhibitors, please take the opportunity to learn more about their service offerings during the intermission for lunches and coffee.

ICMC18 is blessed to be held in Canada's capital. Ottawa is a city rich in culture, including architecture, museums and performing arts as well as many historical sites. Take advantage of any free time you may have by exploring Ottawa's many riches.

Security First is the theme for this year's ICMC. During the year all stakeholders: US NIST, Canada CSE, Vendors, Laboratories, Academia and End Users take on an active role in promoting, improving and applying the FIPS 140-2 standard. During this conference we will demonstrate what also comes first is the interest of this community to continue to work together.

Thanks to the conference program committee, especially the chairs, all the sponsors, and conference production management.

ICMC gives you the opportunity for both business and social contacts to enjoy. Let's make the best use of both. Enjoy the event and let's get to the work: Security First.

Sal
President & CEO atsec information security

Table of Contents

Contact Information

Program Committee

Michael Angelo, Micro Focus
Joshua Brickman,Oracle
Erin Connor, EWA Canada (Chair)
Fabien Deboyser, Thales
Valerie Fenwick, Intel
Shawn Geddis, Apple Inc.
Ryan Hill, atsec information security (Chair)
Tim Hudson, Cryptsoft Pty Ltd
Laurie Mack, Gemalto
Michele Mosca, University of Waterloo
Seth Nielson, Johns Hopkins University
Fiona Pattinson, atsec information security (Chair Emeritus)
Nithya Rachamadugu, CygnaCom Solutions (Chair)
Rich Salz, Akamai
Michael Scanlin, NetApp
Loren Shade, Allegro Software
Marcus Streets, Linux Foundation (Chair)
William Supernor, KoolSpan
Lachlan Turner, Ark Infosec (Chair)
Ashit Vora, Acumen Security
Steve Weingart, Aruba Networks (Chair)
William Whyte, Security Innovation
Brian Wood, Samsung Electronics

Conference Staff

Bill Rutledge, Project Director, 1.212.866.2169, bill.rutledge@ICMConference.org

Amy Nicewick, Program Manager, Amy.Nicewick@ICMConference.org

Fredo Martin, Sales Manager, +1.559.462.5002, Fredo@cnxtd.com

Nikki Principe, Operations Manager, 1.571.249.5680, nikki@cnxtd.com

Presented by CMUF

The Cryptographic Module User Forum (CMUF) provides a voice and communications channel between the community of unclassified cryptographic module (CM) and unclassified cryptographic algorithm developers, vendors, test labs and other interested parties, and the various national, international, and multi-lateral organizational committees, schemes, and policy makers. Join the Forum at cmuf.org.

Sponsors and Exhibitors

Title Sponsors

PLATINUM SPONSOR

GOLD SPONSOR

SILVER SPONSOR

SILVER SPONSOR

SILVER SPONSOR

Leading Sponsors

OPENING RECEPTION, TRACK SPONSOR

BADGE SPONSOR

BAG SPONSOR

Exhibitors

Supporting Sponsors

Association and Media Sponsors

Conference Agenda

Detailed session descriptions are online at www.ICMConference.org

ICMC18 begins with one day of pre-conference workshops, followed by conference plenary keynotes and three days of sessions in nine tracks:

Advanced Technology [A] High-level technology issues, or special-focus subject matte

Certification Programs [C] Issues related to the CMVP, government programs and global certification

Industry Perspectives [Y] Issues related to policy, economics, and ethics affecting encryption-based security

End-User Experience [U] CM products, certifications, and vulnerabilities for organizations that rely on crypto security

Industry Vertical/ Embedded Crypto [E] Embedded encryption in specific industry verticals.

General Technology [G] Tools and techniques relating to cryptographic modules

Open-Source Crypto [S] Efforts to audit, improve and certify the security of the leading OS crypto projects

Post-Quantum Crypto [Q] The quantum computing threat and efforts to transition to quantum-safe algorithms

Common Criteria [R] Issues related to Common Criteria and NIAP-compliant products

Tuesday, May 8

Pre-Conference Workshops

08:00	**Registration** (Rideau Canal Atrium)		
	Ottawa Salon 210	Ottawa Salon 212	Ottawa Salon 211
09:00	**Decrypting Crypto: An Introduction to Cryptography** (W00a) Jon Green, HPE	**Intro to FIPS 140** (W00b) Yi Mao, atsec information security	**Introduction to Blockchain** (W00c) Arthur Nicewick, SalusSec LLC
12:30	**Lunch** (Rideau Canal Atrium)		
13:30	**The Post Quantum Crypto World and the Need for Crypto Agility** (W01a) Tomislav Nad, InfoSec Global; Vladimir Soukharev, InfoSec Global	**FIPS 140-2 Validation Process: Overview and Case Study** (W01b) Tammy Green, Symantec; Ian Hall, Symantec; Brad Proffitt, Lightship Security	**Introduction to Common Criteria** (W01c) Lachlan Turner, Partner, Lightship Security
17:00	**Adjourn**		

Wednesday, May 9

Conference Plenary Session

08:00	**Registration** (Rideau Canal Atrium)	
	Plenary Keynote Session	Ottawa Salon 213-215
09:00	**Welcome Address**, Yi Mao, atsec information security [09:10] **Plenary Keynote Address: Digital Disruption and the Implications for Cybersecurity and Cryptography** (P10a) Jason Hart, CTO Data Protection, Gemalto, United Kingdom [09:50] **Plenary Keynote Address: What's Next for Cryptography? How CSE Balances Privacy and Innovation in the Public and Private Sectors** (P10b) Scott Jones, Assistant Deputy Minister, Information Technology Security, Communications Security Establishment	
10:30	**Networking Break in Exhibits** (Ottawa Salon 214)	

Wednesday, May 9

Certification Programs

Ottawa Salon 210

General Technology

Ottawa Salon 209

	Certification Programs — Ottawa Salon 210	General Technology — Ottawa Salon 209
11:15	**Certification Track Keynote Address: Increasing the Value of Certifications to the End-User** (C11a) Jeff Blank, Technical Director, Endpoint Solutions, NSA Cybersecurity	**General Technology Track Keynote: Hardware Security Modules (HSM), Past, Present and Future** (G11a) Bruno Couillard, Crypto4A
11:45	**CMVP Programmatic Update** (C11b) Carolyn French, GoC; Beverly Trapnell, NIST	**Usability, Validation and Abuse** (G11b) Valerie Fenwick, Director of Software Engineering, Platform Security Division, Intel
12:15	**NIAP Update** (C11c) Dianne Hale, NIAP	**SP800-90B: Testing Process, Result Bounds, and Current Issues** (G11c) Joshua Hill, Information Security Scientist, UL
12:45	**Lunch in Exhibit Area** (Ottawa Salon 213-215)	
13:45	**Update on the Automated Cryptographic Validation Program (ACVP)** (C12a) Apostol Vassilev, NIST; Tim Anderson, Amazon; Harold Booth, NIST; Shawn Geddis, Apple; Barry Fussell, Cisco; Bradley Moore, NIST; Robert Relyea, Red Hat `[90 min]`	**Using FPGAs in the Cloud for Decentralized Trusted Execution** (G12a) Ahmed Ferozpuri, George Mason University
14:15		**GlobalPlatform: Cryptography Algorithm Classification and Crypto Agility** (G12b) Olivier Van Nieuwenhuyze, GlobalPlatform Board Member and Security Task Force Chair
14:45		**Deep Inside: The Benefits and Implications of Sub-Chip FIPS Modules** (G12c) Renaudt Nunez, atsec information security
15:15	**Networking Break in Exhibits** (Ottawa Salon 213-215)	
15:45	**Mandating CMVP for NIAP Evaluations Panel Presentation** (C13a) Moderator: Dianne Hale, NIAP, Panelists: Michael Cooper, IT Specialist, NIST; Terrie Diaz, Product Certification Engineer, Cisco Systems; Matt Keller, Corsec; Edward Morris, Co-founder, Gossamer Security Solutions; Nithya Rachamadugu, Director Cygnacom [60 min]	**Boundaries: Where Do You Draw the Line?** (G13a) Alan Gornall, Rycombe Consulting
16:15		**FIPS 140-2 Validations in a Secure Enclave** (G13b) Chris Conlon, wolfSSL
16:45	**FIPS 140-3 Update** (C13c) Michael Cooper, IT Specialist, NIST	**EncryptedQuery: A Practical Solution for PIR** (G13c) John Petro, Envieta Systems
17:45	**Welcome Reception in Exhibits** (Ottawa Salon 213-215)	DARKMATTER Reception Sponsor
18:45	**Dine-Around Ottawa** (See page 10)	

Conference Presentations

Presentations will be available after the conference at www.ICMConference.org
Password: **XXXX**

Join the Conversation on Twitter

#CryptoModConf

Industry Vertical/Embedded Crypto

Ottawa Salon 211

Post-Quantum Crypto

Ottawa Salon 212

11:15	**Industry Vertical/Embedded Crypto Track Keynote: Embedded Encryption and Blockchain Technologies for IoT Security** (E11a) Dr. Najwa Aaraj	**Post-Quantum Crypto Track Keynote: Progress in Post-Quantum Cryptography** (Q11a) Tanja Lange, Eindhoven University of Technology
11:45	**"FIPS 140-2 Inside"—You're (Probably) Doing It Wrong** (E11b) Mark Minnoch, KeyPair Consulting	**Quantum Update** (Q11b) Michele Mosca, Institute for Quantum Computing, University of Waterloo & evolutionQ
12:15	**IoT Security—GAME OF TRUST** (E11c) Roland Atoui, Red Alert Labs, France; Isaac Dangana, Red Alert Labs	**Chairman's Report from ETSI TC Cyber Working Group for Quantum Safe Cryptography** (Q11c) Mark Pecen, CEO, Approach Infinity & COO, ISARA
12:45	**Lunch in Exhibit Area** (Ottawa Salon 213-215)	
13:45	**FIPS, IoT Medical Devices and the DoD/VA** (E12a) Loren Shade, Allegro Software	**NIST Post-Quantum Cryptography Standardization Update** (Q12a) Lily Lidong Chen, NIST; Dustin Moody, NIST
14:15	**FIPS 140-2 Perspectives on IoT Devices in a Blockchain Setting** (E12b) William Sandberg-Maitland, SPYRUS	**The Libpqcrypto Software Library For Post-Quantum Cryptography** (Q12b) Daniel J. Bernstein, University of Illinois at Chicago
14:45	**Secrets of Crypto Technology Revealed for Enhanced ICS Cybersecurity** (E12c) Chris Guo, Ultra Electronics, 3eTI.com	**Practical Quantum-Resistant Cryptography from Supersingular Isogenies** (Q12c) Patrick Longa, Microsoft Research
15:15	**Networking Break in Exhibits** (Ottawa Salon 213-215)	
15:45	**Trusted and Localized Entropy Source for Advanced IoT Security** (E13a) Jongwon JP Park, EYL; Junghyun Francis Baik, EYL	**Recent Progress in Hardware Implementations of Post-Quantum Isogeny-Based Cryptography** (Q13a) Reza Azarderakhsh, Florida Atlantic University and PQSecure Technologies
16:15	**Blockchain Internals Made Simple** (E13b) Arthur Nicewick CTO SalusSec	**Integrating Quantum-Resistant Algorithms into Applications** (Q13b) Christian Paquin, Microsoft
16:45	**Security Certification Schemes for Smart Cars** (E13c) Jose Emilio Rico, Lab Manager, DEKRA	**Open Quantum Safe** (Q13c) Vlad Gheorghiu, University of Waterloo
17:45	**Welcome Reception in Exhibits** (Ottawa Salon 213-215)	DARKMATTER Reception Sponsor
18:45	**Dine-Around Ottawa** (See page 10)	

Thursday, May 10

08:00	**Coffee in Exhibits** (Ottawa Salon 213-215)	
	 **Certification Programs** Ottawa Salon 210	 **General Technology** Ottawa Salon 209
09:00	**NIST and NIAP Working Together** (C20a) Mary Baish, NIAP; Michael Cooper, NIST	**Tamper Labels Examined** (G20a) Steve Weingart, Aruba, a Hewlett Packard Enterprise company
09:30	**"Revalidation in Response to CVE" Working Group** (C20b) Fabien Deboyser, Thales eSecurity; Carolyn French, CSE; Ryan Thomas, Acumen Security	**GPU-Accelerated High-Performance Hardware Security Module** (G20b) Fangyu Zheng, Institute of Information Engineering, CAS
10:00	**Touch the Cloud: Closing the FIPS Validation Gap** (C20c) Yi Mao, atsec information security	**Meeting FIPS 140 Requirements—An RSA Story** (G20c) Steven Schmalz, RSA
10:30	**Networking Break in Exhibits** (Ottawa Salon 213-215)	
11:00	**Comments on NIST Standards for Random Number Testing** (C21a) Yuan Ma, Institute of Information Engineering, Chinese Academy of Sciences	**10 Years of FIPS 140-2 Certifications at Red Hat** (G21a) Tomas Mraz, Red Hat
11:30	**Structured Entropy Assessment and Practical Evaluation Considerations** (C21b) Greg McLearn, Lightship Security	**Panel Discussion: Technology Challenges in CM Validation** (G21b) Moderator: Nithya Rachamadugu, CygnaCom Panelists: Tomas Mraz, Red Hat; Steven Schmalz, RSA—the Security Division of EMC; Fangyu Zheng, Institute of Information Engineering, CAS `[60 min]`
12:00	**Automation of CAVS Testing: Bringing CAVP and Vendor Together** (C21c) Stephan Mueller, atsec information security	
12:30	**Lunch in Exhibits** (Ottawa Salon 213-215)	
13:30	**State of CAVP** (C22a) Harold Booth, NIST	**Analyzing Block Device Timing Events as a Source of Entropy** (G22a) Kirill Sinitski, CygnaCom; Mike Ounsworth, EntrustDatacard
14:00	**Panel Discussion: ACVP—How It Will Change the Way You Work** (C22b) Moderator: Harold Booth, NIST; Panelists: Shawn Geddis, Apple; Stephan Mueller, atsec; Dayanandini Pathmanathan, Cygnacom Solutions; Alicia Squires, Cisco Systems `[60 min]`	**The Use of /dev/urandom as the Entropy Source in the Real World** (G22b) Rumman Mahmud, Cisco Systems; Zhiqiang Wang, Gossamer Security Solutions
14:30		**Abstractions To Help Developers Write Good Crypto** (G22c) Isaac Potoczny-Jones, CEO, Tozny
15:00	**Networking Break in Exhibits** (Ottawa Salon 213-215)	
15:30	**ACVP Client Integration for FIPS Algorithm Testing and Runtime Crypto Assessment** (C23a) Barry Fussell, Cisco Systems; Ellie Daw, Cisco Systems	**Traditional Hardware Security Modules vs Real World Requirements. Is There a Gap?** (G23a) Martin Oczko, PrimeKey Labs
16:00	**Realigning (Not Re-inventing!) the Wheel: Applying a Composition Model to FIPS 140-2 Validation** (C23b) Steve Weymann, KeyPair Consulting	**The Details of an Ongoing Transition to the Stronger Key Establishment Methods** (G23b) Allen Roginsky, NIST
16:30	**In FIPS 140-2 Validations, Why So Much Redundant Data Redundancy in FIPS 140-2 Validations?** (C23c) Quentin Gouchet, atsec information security	**KMIP 2.0 vs Crypto in a Cybersecurity Context** (G23c) Tony Cox, Cryptsoft; Chuck White, Fornetix
17:00	**Cryptographic Module Game Program** (Ottawa Salon 213, 215)	

08:00	**Coffee in Exhibits** (Ottawa Salon 213-215)	
	 **Common Criteria** Ottawa Salon 211	 **Post-Quantum Crypto** Ottawa Salon 212
09:00	**Common Criteria Track Keynote** (R20a) Michael Grimm, CCUF	**Advances in Quantum Key Distribution: Standardization, Networking, and Space Applications** (Q20a) Bruno Huttner, ID Quantique
09:30	**Is 2018 a Make or Break Year for CC?** (R20b) John Boggie, NXP Semiconductors, United Kingdom	**A Session Key Service for Post-Quantum Security in Standard Protocols** (Q20b) David McGrew, Cisco Systems
10:00	**Making Objectivity Work Harder: Text, Tools and Fuzzing** (R20c) Tony Boswell, DNV GL Technical Assurance Laboratory	**Isogeny-Based Quantum-Resistant Group Key Agreement** (Q20c) Vladimir Soukharev, InfoSec Global
10:30	**Networking Break in Exhibits** (Ottawa Salon 213-215)	
11:00	**Identifying Cryptographic Implementations in Common Criteria** (R21a) Cory Clark, Government of Canada	**A Brief Introduction to Quantum Random Number Generation Technologies** (Q21a) Jeong Woon Choi, Quantum Technology Lab, SK Telecom
11:30	**A Survey of Common Criteria Certification Scheme Cryptographic Algorithm Requirements** (R21b) King Ables, atsec information security corporation	**Panel Discussion: QRNG Outlook** (Q21b) Moderator: Michele Mosca, Institute for Quantum Computing, University of Waterloo, evolutionQ; Panelists: David Sabourin, CSE; Sae Woo Nam, NIST; Bruno Huttner, ID Quantique SA; Bertrand Reulet, Université de Sherbrooke `[60 min]`
12:00	**Smart Application of CC: CC Can Actually Be Efficient, Lean and Useful!** (R21c) Wouter Slegers, Your Creative Solutions	
12:30	**Lunch in Exhibits** (Ottawa Salon 213-215)	
13:30	**CC and Crypto Evaluations in Turkey** (R22a) İbrahim Halil Kirimizi, Turkish Standards Institution	**OS Crypto Track Keynote: Challenges in Implementing Usable Advanced Crypto** (S22a) Shai Halevi, IBM T. J. Watson Research Center
14:00	**Completeness in High Assurance Common Criteria Evaluation for eIDAS in Europe** (R22b) Leo Kool, Brightsight	**Avoiding Burning at Sunset – Future Certification Planning in Bouncy Castle** (S22b) David Hook, Crypto Workshop
14:30	**Spanish Catalogue of Qualified Products: A New Way of Using CC for Procurement** (R22c) Jose Ruiz Gualda, jtsec	**OpenSSL Project Overview** (S22c) Rich Salz, OpenSSL Dev Team
15:00	**Networking Break in Exhibits** (Ottawa Salon 213-215 Exhibits Close at 15:30)	
15:30	**Flaw Remediation Begins Where Product Certification Finishes** (R23a) Malcolm Levy, Check Point Software Technologies	**OpenSSL FIPS Module Validation Project** (S23a) Tim Hudson, CTO and Technical Director, Cryptsoft Pty, Australia; Ashit Vora, Acumen Security
16:00	**Panel Discussion: FIPS and Common Criteria– How They Play Together** (R23b) Moderator: Steve Weingart, Aruba, a Hewlett Packard Enterprise company, Panelists: Joshua Brickman, Security Evaluations Oracle; Erin Connor, EWA-Canada; Alan Kaye, Fortinet; Laurie Mack, Gemalto `[60 min]`	**China and Crypto Open Source Projects** (S23b) Paul Yang, Architect, BaishanCloud
16:30		**LibreSSL** (S23c) Brent Cook, OpenBSD
17:00	**Cryptographic Module Game Program** (Ottawa Salon 213, 215)	

Friday, May 11

Conference Track Sessions

08:00	**Coffee** (Rideau Canal Atrium)	
	 **Certification Programs** Ottawa Salon 210	 **Advanced Technology** Ottawa Salon 209
		DARKMATTER Track Sponsor
09:00	**A Look Back to a Decade of Security Certification, and a Look Forward the New Landscape in Europe** (C30a) Miguel Banon, DEKRA	**Advanced Technology Track Keynote: Lightweight Post-Quantum Crypto: An Oxymoron** (A30a) Victor Mateu, Crypto Developer, DarkMatter
09:30	**Building Certification Bodies** (C30b) Wouter Slegers, Your Creative Solutions	**Permutation-Based Cryptography** (A30b) Guido Bertoni, Security Pattern
10:00	**O-TTPS Certification as a Companion to CMVP and Common Criteria** (C30c) Teresa MacArthur, EWA-Canada	**Sizing Up the Threshold: Challenges and Opportunities in the Standardization of Threshold Schemes for Cryptographic Primitives** (A30c) Apostol Vassilev, NIST
10:30	**Networking Break** (Rideau Canal Atrium)	
10:45	**CAVP/CMVP Requirements from 800-90B** (C31a) Mary Baish, NIAP; Michael Cooper, IT Specialist, NIST; Allen Roginsky NIST	**Panel Discussion: The Future of HSMs and New Technology for Hardware Based Security Solutions** (A31a) Tony Cox, Cryptsoft; Thorsten Groetker CTO, Utimaco; Tim Hudson, Cryptsoft; Todd Moore, Gemalto; Robert Burns, Thales `[60 min]`
11:15	**TOO MANY CERTIFICATIONS!** (C31b) Ken Fuchs, Motorola Solutions	
11:45	**IG Updates: Chasing the Moving Target** (C31c) Swapneela Unkule, atsec information security	**The Role of Product Platforms in Information Security: Building on the Success of Cryptographic Modules** (A31c) Lawrence Dobranski, Catalone IT Security
12:15	**CMUF Monthly Meeting – May** (Ottawa Salon 210) Open to all.	
12:45	**Lunch** (Rideau Canal Atrium)	
	 **Industry Perspectives** Ottawa Salon 210	 **Advanced Technology** `[Cont'd]` Ottawa Salon 209
13:30	**Reducing Conflict of Interest in Third Party Security Testing Validations/Certifications** (Y32a) Carol Cantlon, EWA-Canada	**Efficient Side-Channel Testing Using TVLA** (A32a) Gilbert Goodwill, Rambus – Cryptography Research; Gary Kenworthy, Rambus – Cryptography Research
14:00	**Brexit, and What It Means for Product Evaluations in the UK and Europe** (Y32b) Simon Milford, DNV GL	**Breaking Symmetric White-Box Algorithms Using CPA and DFA** (A32b) Gabriel Goller, R&D Specialist Cryptology, G+D Mobile Security
14:30	**The EU Cybersecurity Act: Is This the First Tangible Evidence of the Balkanization of Common Criteria?** (Y32c) Joshua Brickman, Oracle; Elaine Newton, Oracle	**Campfire Stories: Test to Break or Test to Verify?** (A32c) Bart Jan Koning, Riscure; Erwin in 't Veld, Product Manager, Riscure
15:00	**Networking Break** (Rideau Canal Atrium)	

(See next page for Closing Remarks, Summary Panel Discussion)

08:00	**Coffee** (Rideau Canal Atrium)	
	 **End-User Experience** Ottawa Salon 211	 **Open-Source Crypto** Ottawa Salon 212
09:00	**End-User Experience Track Keynote: Building Composed Security Solutions for Multinational and Interagency Operations** (U30a) Alex MacPherson, National Defense/Government of Canada	**TLS 1.3 and NSS** (S30a) Robert Relyea, Red Hat
09:30	**The FIPS 140-2 CM Overall Rating: What's (Not) in It For Me?** (U30b) Sridhar Balasubramanian, NetApp; Mike Scanlin, NetApp `[60 min]`	**TLS Panel Discussion** (S30b) Moderator: Tim Hudson, Cryptsoft Pty; Panelists: Brent Cook, OpenBSD; David Hook, Crypto Workshop; Rich Salz, Akamai Technologies & Member, OpenSSL Dev Team `[60 min]`
10:30	**Networking Break** (Rideau Canal Atrium)	
10:45	**A Quantum of Safety—Rooting Trust in a Quantum World** (U31a) Mike Brown, ISARA	**A Case Study on Certification and Audit of Open Source Security Software** (S31a) Tomas Gustavsson, CTO, PrimeKey Solutions AB
11:45	**Towards A Crowd-Sourced Cryptographic Knowledge Base** (U31b) Debra Baker, Cisco; Seth Nielson, Johns Hopkins University	**Proving the Correctness of Amazon's s2n TLS Library** (S31b) Aaron Tomb, Galois
11:45	**Keys, Hollywood, and History: The Truth About ICANN and the DNSSEC Root Key** (U31c) Richard Lamb, Self-Employed	**Do You Really Know Where Your Crypto is Executing?** (S31c) Kelvin Desplanque, Cisco Systems; Barry Fussell, Cisco Systems
12:15	**CMUF Monthly Meeting – May** (Ottawa Salon 210) Open to all.	
12:45	**Lunch** (Rideau Canal Atrium)	
13:30	**Update from the "Security Policy" Working Group** (U32a) Ryan Thomas, Acumen Security	**The Linux Kernel Self-Protection Project** (S32a) Gustavo A. R. Silva, Linux Foundation's Core Infrastructure Initiative
14:00	**We Feel Your Pain! Getting Ready for Certification** (U32b) Alan Kaye, Fortinet; Brad Proffitt, Lightship Security	**Reproducible Builds on NetBSD** (S32b) Christos Zoulas, NetBSD
14:30	**Planning Ahead: Certificate Maintenance** (U32c) Abdullah Abubshait, Cygnacom Solutions	**Security in the Zephyr Project** (S32c) David Brown, Linaro
15:00	**Networking Break** (Rideau Canal Atrium)	
15:15	**Closing Remarks, Summary Panel Discussion** (Ottawa Salon 210) **Can Certification Keep Up With the Pace of Modern Development?** (P33) Moderator: Steve Weingart, Aruba, a Hewlett Packard Enterprise company, Panelists: Mary Baish, NIAP; Tony Busciglio, Acumen Security; Michael Cooper, NIST; Shawn Geddis, Inc.; Brian Wood, Samsung Research America	
16:15	**Adjourn**	

Take a Break Thursday Evening

17:00-17:45 (Ottawa 213, 215)

Cryptographic Module Game Program

Your Host: Nick Goble

Come watch three experienced contestants test their FIPS knowledge at the Cryptographic Module Game Program (CMGP). The CMGP covers FIPS validation trivia related to algorithms, derived testing requirements, entropy, implementation guidance and more. A few members from the audience will be selected to assist the contestants on specific questions and be eligible to win prizes.

WiFi Access

WiFi service is available to conference registrants in the public areas of the facility.

Instructions:

1. Search the available wireless networks with your device and connect to the "FREEMAN AV WIFI" network
2. Once connected, open your preferred web browser. You will automatically be re-directed to a login page
3. Select the "Access code" as the method of payment. The access code changes daily: Tuesday: ICMC18TU, Wednesday: ICMC18WE, Thursday: ICMC18TH, Friday: ICMC18FR
4. Please be sure to use ALL CAPS

Thanks to our student volunteers.

Join Your Colleagues: Dine-Around Ottawa

Sign up at the registration desk. Depart Wed, May 9 at 18:45.

On the evening of Wednesday, May 9, you can enjoy an informal, on-your-own group dinner at one of Arlington's best restaurants with your ICMC colleagues. Select a restaurant, reserve your seat and enjoy a prix-fixe dinner at a group table in the company of other professionals. Reserve early—seating is limited.

Restaurant	Price	Type of Food
Blue Cactus Bar & Grill	US$38	Contemporary cuisine with an upscale casual ambiance
Lowertown Brewery Ottawa	US$35	Enjoy a 3 course Brew Masters Dinner with beer tasting.
Cornerstone	US$25	Eclectic, casual restaurant with a nice outdoor dining area

All restaurants are within walking distance. Meet Wednesday at 18:20 at the registration desk and depart from there.

Speakers

Speaker biographies are online at www.ICMConference.org

Dr. Najwa Aaraj

Independent Consultant

E11a

King Ables

Senior Consultant, atsec information security corporation

R21b

Abdullah Abubshait

Cygnacom Solutions

U32c

Tim Anderson

Program Manager, WWPS Security & Compliance Business Acceleration Team, Amazon

C12a

Roland Atoui

Red Alert Labs

E11c

Reza Azarderakhsh

Assistant Professor, Florida Atlantic University and PQSecure Technologies

Q13a

Junghyum Francis Baik

EYL Inc.

E13a

Mary Baish

Deputy Director, NIAP

C20a, C31a, P33

Debra Baker

Cybersecurity Evangelist, Cisco

U31b

Sridhar Balasubramanian

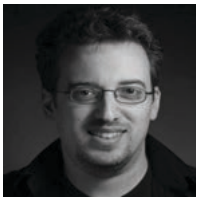
Principal Product Security Architect, NetApp

U30b

Miguel Bañón

Global Technology Leader for Cyber Security DEKRA

C30a



Daniel J. Bernstein

Research Professor, University of Illinois at Chicago

Q12b

Guido Bertoni

Co-Founder and CEO, Security Pattern

A30b

Jeffrey Blank

Technical Director, Endpoint Solutions, NSA Cybersecurity

C11a

John Boggie

Director, Head of Product Certification, NXP Semiconductors

R20b

Harold Booth

Computer Scientist, NIST

C12a, C22a, C22b

Tony Boswell

Senior Principal Consultant, DNV GL

R20c

Joshua Brickman

Director, Security Evaluations, Oracle

R23b, Y32c & Program Committee

David Brown

Senior SW Engineer, Linaro

S32c

Mike Brown

CTO, ISARA Corporation

U31a

Robert Burns

CSO, Thales e-Security

A31a

Tony Busciglio

Co-founder & Laboratory Director, Acumen Security

P33

Carol Cantlon

Senior IT Security Evaluator, EWA-Canada

Y32a

Lily Chen

Mathematician NIST

Q12a

Jeong Woon Choi

Quantum Technology Lab, SK Telecom

Q21a

Cory Clark

IT Security Specialist, CSEC

R21a

Chris Conlon

Software Engineer, wolfSSL

G13b

Erin Connor

Director, EWA-Canada

R23b & Program Committee

Brent Cook

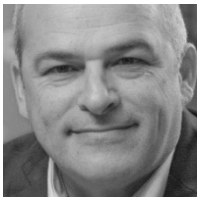
Open BSD

S23c, S30b

Michael Cooper

IT Specialist, NIST

C13a, C13c



Bruno Couillard

President & CEO, Crypto4A, Canada

G11a

Tony Cox

VP Partners, Alliances and Standards, Cryptsoft Pty Ltd.

G23c, A31a

Joan Daemon

Principal Cryptographer, STMicroelectronics

A30b

Isaac Dangana

Red Alert Labs

E11c

Ellie Daw

Software Engineer, Common Security Modules, Cisco Systems

C23a

Fabien Deboyser

Certification Engineer, Thales e-Security

C20b

Kelvin Desplanque

Security Certification Engineer, Cisco Systems

S31c

Terrie Diaz

Product Certification Engineer, Cisco Systems

C13a

Lawrence Dobranski

Managing Principal Engineer, Catalone IT Security

A31c

Valerie Fenwick

Director of Software Engineering, Intel

G11b, Program Committee

Ahmed Ferozpuri

George Mason University

G12a

Carolyn French

Manager, Cryptographic Module Validation Program

C11b, C20b

Ken Fuchs

Science Advisory Board Associate, Motorola Solutions

C31b

Barry Fussell

Software Technical Leader, Cisco Systems

C12a, C23a

Shawn Geddis

Security & Certifications Engineer, Apple Inc.

C12a, C22b, P33, Program Committee

Vlad Gheorghiu

Researcher, Institute for Quantum Computing

Q13c

Nick Goble

Technical Marketing Engineer, Cisco

P24

Gabriel Goller

R&D Specialist Cryptology, G+D Mobile Security

A32b

Alan Gornall

Principal Consultant, Rycombe Consulting

G13a

Quentin Gouchet

IT Security Consultant, atsec information security

C23c

Jon Green

VP and Chief Technologist for Security at Aruba, a Hewlett Packard Enterprise company

W00a

Tammy Green

Senior Principal Security Architect, Symantec

W01b, Program Committee

Michael Grimm

Senior Program Manager, Microsoft

R20a

Thorsten Groetker

CTO, Utimaco

R20a

Jose Ruiz Gualda

Co-founder, jtsec Beyond IT Security

R22c

Chris Guo

Ultra Electronics, 3eTI

E12c

Tomas Gustavsson

CTO, PrimeKey Solutions

S31a

Dianne Hale

NIAP

C11c, C13a, Q21b

Shai Halevi

Principal Research Staff Member, IBM T. J. Watson Research Center

S22a

Ibrahim Halil Kırmızı

Common Criteria Certification Specialist, Turkish Standards Institution, Turkey

R22a

Ian Hall

Certification Architect, Symantec

W01b

Jason Hart

CTO Data Protection, Gemalto

P10a

Joshua Hill

Information Security Scientist, UL

G11c

Ryan Hill

Community Outreach Manager, atsec information services

Program Committee

David Hook

Director/Consultant, Crypto Workshop

S22b & S30b

Tim Hudson

CTO and Technical Director, Cryptsoft Pty Ltd.

S23a, S30b, A31a, Program Committee

Bruno Huttner

Quantum Safe Product Management, ID Quantique SA

Q20a

Erwin in 't Veld

Product Manager, Riscure

A32c

Bart Jan Koning

Business Development Manager, Riscure

A32c

Scott Jones

Assistant Deputy Minister, Information Technology Security, CSE

A31a

Alan Kaye

Director, Compliance Management, Fortinet

R23b, U32b

Matt Keller

Senior Program Manager, Corsec

C13a

Gary Kenworthy

Technical Director, Rambus - Cryptography Research

A32a

Leo Kool

Senior Security Evaluator, BrightSight

R22b

Richard Lamb

Self-Employed

R22b

Tanja Lange

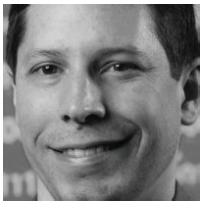
Technische Universiteit Eindhoven

Q11a

Malcolm Levy

Certification Manager, Check Point Software Technologies

R23a



Patrick Longa

Cryptographic Researcher, Microsoft Research, USA

Q12c

Yuan Ma

Director of Security Testing Lab, Institute of Information Engineering , Chinese Academy of Sciences

C21a & C30b

Teresa MacArthur

Manager, Certification Documentation Services, EWA-Canada

C30c

Laurie Mack

Director Security & Certifications, Gemalto

R23b, Program Committee

Alex Macpherson

Cyber Security Engineering & Architecture, National Defense/Government of Canada

U30a

Rumman Mahmud

Compliance Engineer, Cisco Systems

G22b

Yi Mao

VP and Lab Director, atsec USA

C20c

Victor Mateu

Crypto Developer, DarkMatter

A30a

David Mcgrew

Cisco Fellow, Cisco Systems

Q20b

Greg McLearn

Technical Director, Lightship Security

C21b

Simon Milford

Head of Cyber Security, DNV GL

Y32b

Mark Minncoh

Co-Founder, KeyPair Consulting

E11b

Dustin Moody

Mathematician, NIST

Q12a

Bradley Moore

NIST

Todd Moore

Senior Vice President, Encryption Products, Gemalto

A31a

Edward Morris

Co-Founder, Gossamer Security Solutions

C13a, Program Committee

Michele Mosca

University Research Chair & Co-Founder, Institute for Quantum Computing, University of Waterloo; Co-Founder & CEO, evolutionQ

Q11b, Q21b, Program Committee

Tomas Mraz

Senior SW Engineer, Red Hat

G21a, G21b

Stephan Mueller

Principal Consultant and Evaluator, atsec information security

C21c, C22b

Tomislav Nad

Chief Security Architect and Cryptographer, InfoSec Global

W01a

Sae Woo Nam

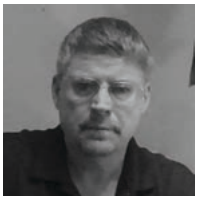
NIST

Q21b

Elaine Newton

Senior Director, Oracle

Y32c



Arthur Nicewick

SalusSec LLC

W00c & E13b

Dr. Seth James Nielson

Director of Advanced Research Projects, Johns Hopkins University Information Security Institute (JHUISI)

U31b

Renaudt Nunez

IT Security Consultant, atsec Information Security

G12c

Martin Oczko

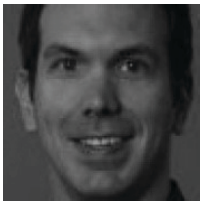
Head of Appliance Technologies, PrimeKey Labs GmbH

G23a

Mike Ounsworth

Software Developer, Entrust Datacard

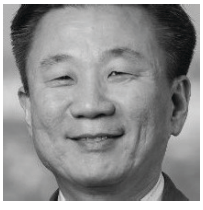
G22a



Christian Paquin

Principal Program Manager, Microsoft

Q13b



Jongwon "JP" Park

Chief Strategy Officer, EYL

E13a

Dayanandini Pathmanathan

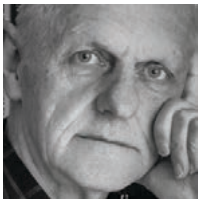
Common Criteria Evaluator, CygnaCom Solutions

C22b

Mark Pecen

CEO, Approach Infinity & COO, ISARA

Q11c, Program Committee



John Petro

Senior Cryptographer, Envieta Systems

G13c

Isaac Potoczny-Jones

CEO, Tozny, LLC

G22c

Brad Proffitt

Business Director, Lightship Security

W01b & U32b

Nithya Rachamadugu

Director, Cygnacom

C13a, G21b, Program Committee

Robert Relyea

Principal, Red Hat

C21a & S30a

Bertrand Reulet

Professor, Université de Sherbrooke, Canada

Q21b

Jose Emilio Rico

Lab Technical Manager, DEKRA

E13c

Allen Roginsky

Mathematician, NIST

G23b & C31a

Bill Rutledge

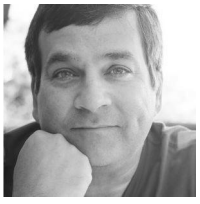
Project Director, ICMC

Program Committee

David Sabourin

Director, Cryptographic Client Services and Operations

Q21b



Rich Salz

Senior Architect, Akamai Technologies; Member, OpenSSL Dev Team

S22c & S30b

William Sandberg-Maitland

Principal Scientist, SPYRUS

E12b

Mike Scanlin

Information Assurance Program Manager, NetApp

U30b

Steven Schmalz

Principal Systems Engineer, RSA—the Security Division of EMC

G20c & G21b

Loren Shade

VP Marketing, Allegro Software

E12a & Program Committee

Gustavo A.R. Silva

Linux Kernel Engineer, Linux Foundation's Core Infrastructure Initiative

S32a

Kirill Sinitski

Common Criteria Lab Manager, CygnaCom

G22a

Wouter Slegers

CEO, Your Creative Solutions

R21c & C30b

Vladimir Soukharev

Chief Post-Quantum Researcher & Cryptographer, InfoSec Global Inc.

Q20c & w01a

Alicia Squires

Global Certifications Team – Manager, FIPS/Common Criteria, Cisco Systems

C22b

Ryan Thomas

Laboratory Manager, Acumen Security

C20b & U32a

Aaron Tomb

Research Lead, Software Correctness, Galois

S31b

Beverly Trapnell

NIST

C11b

Lachlan Turner

Principal Consultant, Lightship Security

W01c & Program Committee

Swapneela Unkule

atsec information security

C31c

Olivier Van Nieuwenhuyze

Board Member and Security Task Force Chair, GlobalPlatform

G12b

Apostol Vassilev

Research Lead–STVM, Computer Security Division, NIST

C12a, A30c

Ashit Vora

Co-Founder & Lab Director, Acumen Security

S23a & Program Committee

Richard Wang

FIPS Laboratory Manager, Gossamer

G22b

Steve Weingart

Manager of Public Sector Certifications, Aruba, an HP Enterprise Company

G20a, R23b, P31d, Program Committee

Steve Weymann

Co-Founder, KeyPair Consulting Inc

C23b

Chuck White

CTO, Fornetix

G23c

Brian Wood

Device Security Certification Manager, Samsung Research America

P33

Paul Yang

Architect, BaishanCloud

S23b

Fangyu Zheng

Chief Engineer of Security Testing Lab, Institute of Information Engineering , Chinese Academy of Sciences

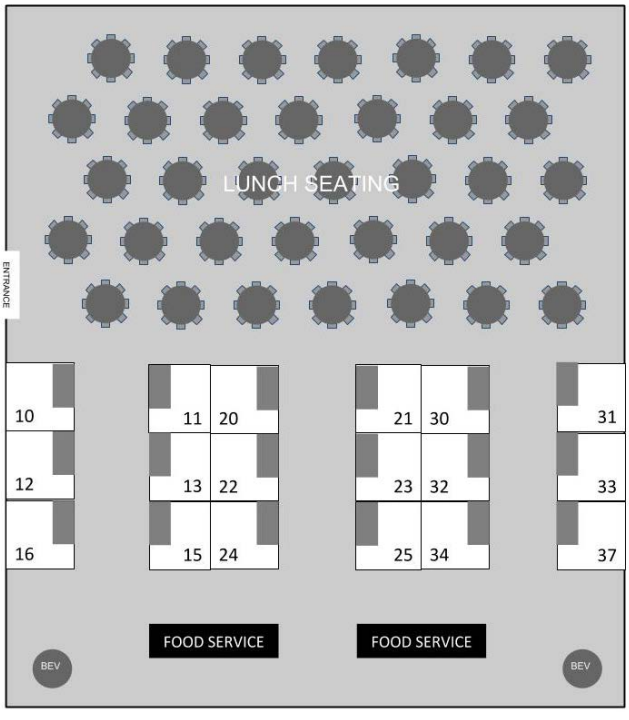
G20b & G21b

Christos Zoulas

Secretary, NetBSD

S32b

Exhibit Floor Plan



Exhibitors

10. atsec information security
11. Cryptsoft
12. Rhode & Schwarz, Cybersecurity GmbH
13. WolfSSL
15. ISARA
16. DNV-GL
20. Allegro Software
21. PrimeKey Solutions
22. EYL
23. InfoSec Global
24. Ultra Electronics, 3eTI
25. NewAE Technology
30. Red Alert Labs
31. Rambus Cryptography Research
33. Riscure
34. EWA Canada
37. DEKRA

Table Top Sponsor

CygnaCom Solutions

Sponsors & Exhibitors

Event Sponsor

Acumen Security

www.acumensecurity.net

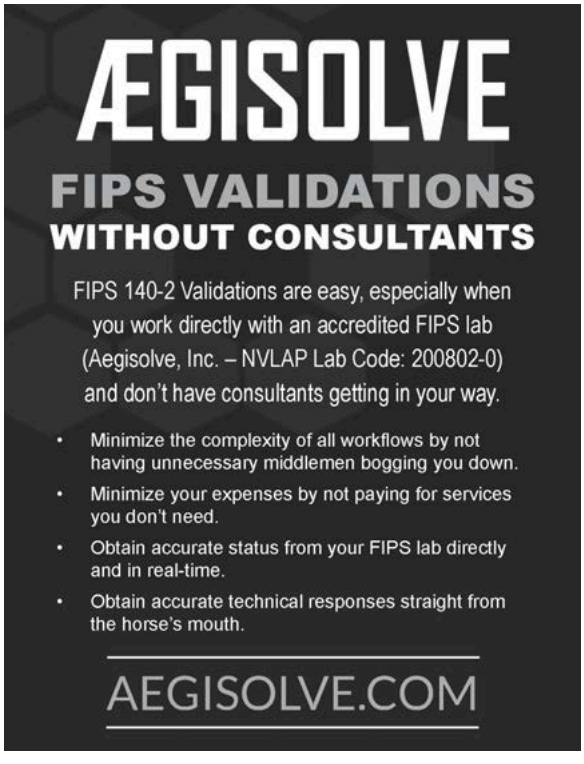
Acumen Security is your one stop shop to certify your products and get into the hands of your government customers ASAP. We aim to not only certify your products, but also do so in the easiest, fastest and cheapest way possible while maintaining the integrity of the certification efforts. That means not cutting corners but working smartly. It means being able to understand your worldview so that we can adapt to your needs. It means being available when you need us. Most of all it means being a partner in your certification journey rather than running parallel.

Event Sponsor

AEGISOLVE

www.aegisolve.com

AEGISOLVE Cyber Security Laboratories accelerates your time to market with proven security analysis and testing processes. Headquartered in Silicon Valley, California, AEGISOLVE is an accredited industry leader, providing FIPS 140-2 validations for nearly a decade.



Silver Sponsor, Booth 20

Allegro Software Development

www.allegrosoft.com

Secure Software for the Internet of Things – Allegro Software is a leading provider of embedded Internet software toolkits to product developers

worldwide. Field proven in 200,000,000+ devices, our solutions enable manufacturers of hardware, software and digital products in the Military, Energy, Healthcare, Enterprise and Consumer markets to create connected secure devices using TLS, Suite B, FIPS 140-2 capabilities and more.

Platinum Sponsor, Booth 10

atsec information security

www.atsec.com

atsec information security is an independent, privately owned company that focuses on providing laboratory and consulting services for information security. We address commercial and government sectors around the world. Our consultants are expert in a variety of technologies including operating systems, databases, and network devices. Our laboratories specialise in evaluating and testing commercial products, using international standards to help provide assurance to end-users about the products they buy and use. We focus on assisting organizations, large and small, achieve compliance with standards such as Common Criteria, FIPS 140-2, O-TTPS, PCI, ISO/IEC 27001 and FISMA and offer a variety of services that complement that goal.

Event Sponsor

Brightsight

www.brightsight.com

Brightsight is the number one security lab in the world. We offer security evaluations to developers/manufacturers of security products, such as terminals, IoT products, smart cards and software solutions. We have over 30 years of experience in evaluating security products against a variety of requirements. As a security evaluation specialist with many years of experience, our holistic approach includes consultancy services, training and unique analysis tools. We ensure a precise preparation for the comprehensive product approval process. Close collaboration during the development phase enables us to understand each customer's individual security needs. Our customers include international financial institutions, developers of IT products, the IT and automotive industries, and governments. The results of our evaluations are used by major international organizations such as EMVCo, MasterCard, PCI-PTS and Visa and by nation-specific certification schemes. Brightsight is the only lab in the world accredited by five Common Criteria Schemes (Germany, Japan, the Netherlands, Turkey and Norway).

Gold Sponsor, Booth 11

CrypytSoft

www.cryptsoft.com

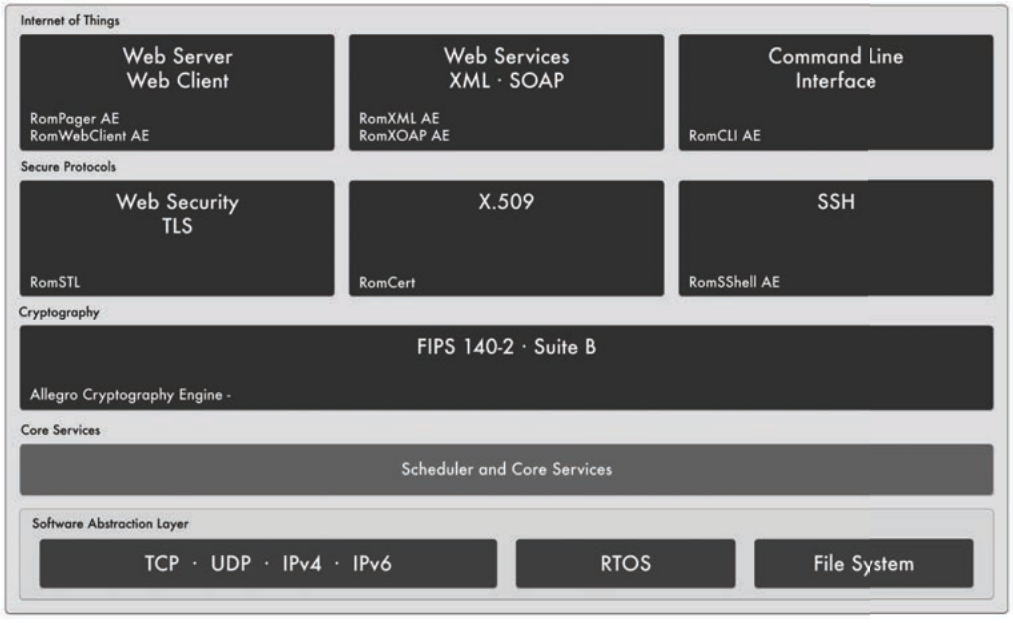
Cryptsoft is a privately held Australian company that operates worldwide in the enterprise key management security market. Cryptsoft's Key Management Interoperability Protocol (KMIP) software development kits (SDKs) are the market's preferred OEM solutions. Cryptsoft's solutions have been selected by prominent global companies for interoperable enterprise key management and encryption technology in their storage, security and cloud products. Cryptsoft is an OASIS Foundational Sponsor, SNIA and SSIF Voting Member. The Cryptsoft Quality Management System was initially certified to ISO 9001:2008 in 2010 and is formally certified to ISO 9001:2015. Refer to the current ISO 9001 certification certificate.

SECURE SOFTWARE FOR THE INTERNET OF THINGS

INTEGRATED DEVICE MANAGEMENT WITH FIPS VALIDATED CRYPTOGRAPHY AND SUITE B

Seamlessly incorporate security and advanced web based device management into your next application. The Allegro AE framework of device management products are pre-integrated with Allegro's FIPS validated cryptography module with multiple layers of security services for protecting sensitive application data.

To learn more at ICMC 2018 visit Booth #20 and explore how Allegro's FIPS validated solutions deliver time to market and reduce risk for your specific application.



Proven • Portable • Pervasive

Allegro

www.allegrosoft.com/ICMC2018

Table 1

CygnaCom Solutions

www.cygnacom.com

CygnaCom Solutions Inc. specializes in information assurance and product certification. We offer a full range of security certification, testing and consultancy services enabling our clients to meet the standards required by many government and regulatory bodies. Our staff of highly qualified professionals will guide your team through evaluations, validations, certifications, and assessments to ensure on time and within budget procurement eligibility and compliance. CygnaCom Solutions laboratories are accredited to conduct FIPS 140-2 cryptographic module (CMVP) and algorithm testing and Common Criteria evaluations in US (NIAP), Canada (CSE) and Turkey (TSE). Contact: Nithya@cygnacom.com

Association Sponsor

Common Criteria User Forum

www.ccusersforum.org

The Common Criteria Users Forum's mission is to provide a voice and communications channel amongst the CC community. The CCUF promotes the CC and provides an open forum for various CC topics to be discussed without favoring anyone group and supports international Technical Communities and technical working groups in a number of ways. The CCUF is independent of any government or certification body and membership is open to all interested in the CC.

Association Sponsor

Cryptographic Module User Forum

www.cmuf.org

The Cryptographic Module User Forum (CMUF) provides a voice and communications channel between the community of unclassified cryptographic module (CM) and unclassified cryptographic algorithm developers, vendors, test labs and other interested parties, and the various national, international, and multi-lateral organizational committees, schemes, and policy makers. Join the Forum at cmuf.org.

Opening Reception, Advance Technology Track Sponsor

DarkMatter

www.darkmatter.ae

With head offices in the UAE and serving regional and global customers, DarkMatter is a team of cyber security specialists dedicated to providing secure, trusted and integrated protection services. As a trusted partner to the UAE government, we have the proven integrity, intelligence and cyber security capability to safeguard a nation. Technology has changed the world beyond measure. Digital progress has made lives easier and businesses more efficient. However, with technological progress comes many threats to Government, Enterprise and Individuals. We are transforming the cyber security landscape through a complete range of state of the art services and solutions for government security agencies all the way to businesses and individuals.

Silver Sponsor, Booth 16

DNV-GL

www.dnvgl.com

DNV GL is a world-leading provider of digital solutions for managing risk and improving safety and asset performance for ships, pipelines,

processing plants, offshore structures, electric grids, smart cities and more. Our open industry platform Veracity, cyber security and software solutions support business-critical activities across many industries, including maritime, energy and healthcare. We are your trustworthy, independent advisor on cyber security for critical infrastructure within maritime, oil & gas, energy, health, finance and manufacturing. We use our cross-industry experience helping you to fully assess and understand your cyber security risk picture, its impact on your business and to take the necessary steps you need to accomplish to secure full compliance, an acceptable risk level and improved business performance.

Booth 37

DEKRA

www.dekra-product-safety.com

DEKRA has been active in the field of safety for more than 90 years and is one of the world's leading expert organizations in testing, inspection and certification. Our qualified and independent experts work for safety on the road, at work and at home. Among other things, they test and certify consumer, industrial, automotive and ICT products, as well as medical devices and products used in explosive atmospheres for worldwide markets. Our smart combination of safety and connectivity testing gives you the edge in a world where products need to work with everything else. It's what makes DEKRA your partner for a safe connected world. www.dekra-product-safety.com

Booth 34

EWA - Canada

www.ewa-canada.com

EWA-Canada was incorporated and has been in operation since June 1988. We are recognized as Canada's premiere provider of information and communications technology (ICT) security and assurance services and a global centre of excellence in security engineering and test and evaluation innovation. Our solutions are based on the vast expertise of our personnel, a structured system engineering approach, and vendor-neutral selection and implementation of appropriate technologies. Our commitment is to provide excellence to our clients. EWA-Canada provides experienced, qualified resources, and company expertise in all facets of security program development and assessments, product test, evaluation and certification, security architecture design and development, identification token and credential issuance, security incident response, computer forensics and training.

Booth 22

Korea

www.eylpartners.com

EYL has developed first generation of entropy chip (5mmx5mm) in 2015. We are now developing a smaller (2mmx2mm), thinner second generation entropy chip in 2017. We are also working on ultralight chip encryptor and thin film type quantum random number generator. Our core technology, a novel solution for loT security at affordable price, will be a gamechanger. Our products can dramatically improve security of all loT devices because they can provide more secure encryption powered by entropy chip.

Badge Sponsor

Gemalto

www.gemalto.com

Gemalto is a global leader in digital security, bringing trust to an increasingly connected world. We deliver a vast range of technologies and services to businesses, governments and other organizations, protecting identities and data so they're kept safe wherever they're found: in personal devices, connected objects, the network, the cloud and in between. Our solutions are at the heart of modern digital life, from payments and the cloud to big data and the Internet of Things. They encrypt data and authenticate people and things – enabling our clients to deliver secure, innovative services for

Booth 15

ISARA

www.isara.com

ISARA is the largest organization in the world focused solely on developing quantum-safe cryptographic solutions for integration into commercial products to protect against emerging security threats. As businesses and governments around the world seek to protect themselves from emerging cybersecurity threats, they are making long-term strategic bets on emerging technologies to address their future business needs. ISARA's mission is to help our customers take important steps to address the next generation of privacy and security concerns in the quantum age. The ISARA Radiate Security Solution Suite is the first commercial offering of a high-quality implementation of quantum resistant algorithms and related integration tools built for developers. It allows organizations and OEMs to integrate critical, quantum-safe security measures into commercial products and networks today, and facilitates the transition to crypto agility in enterprise security.

Booth 25

NewAE Technologies

newae.com

NewAE Technology Inc. has designed the revolutionary ChipWhisperer, the first complete open-source toolchain (hardware and software) that performs power-analysis and glitching attacks on embedded systems. NewAE provides hardware, software support, and training to help customers understand how these attacks apply to their system, so they can build more secure systems.

Silver Sponsor, Booth 21

PrimeKey Solutions

www.PrimeKey.com

One of the world's leading companies for PKI solutions, PrimeKey has developed successful technologies such as EJBCA Enterprise, SignServer Enterprise and PrimeKey PKI Appliance. PrimeKey is a pioneer in open source security software that provides businesses and organizations around the world with the ability to implement security solutions such as e-ID, e-Passports, authentication,

digital signatures, unified digital identities and validation.

Booth 31

Rambus Cryptography Research

www.rambus.com/security

The Rambus Cryptography Research division specializes in embedded security solutions to combat the worldwide threat to data integrity. Our innovative technologies span areas including tamper resistance, content protection, network security, media and payment and transaction services. Nearly nine billion security products are made annually with our security technology, and systems designed by our scientists and engineers protect billions of dollars in revenue every year. Additional information is available at rambus.com/security.

Booth 30

Red Alert Labs

www.redalertlabs.com

Red Alert Labs is bringing trust to the IoT by providing consulting and certification services to organizations developing and integrating IoT solutions. We act as the security partner helping these organizations create, reach and maintain their IoT security goals. Our partners turn to us at any stage of the IoT solution life-cycle to benefit from our special expertise in IoT security and full mastering of compliance and regulations.

Booth 33

Riscure

www.riscure.com

Riscure is an international and independent security test laboratory founded in 2001 by Marc Witteman, with labs in the USA and in The Netherlands. Riscure is an accredited lab for EMVco security testing, DPA lock testing and various Pay TV schemes. Riscure specializes in evaluating and testing the security of embedded devices that are designed to operate securely in any environment and under all circumstances. Besides offering these services, Riscure develops and maintains security test tools for organizations and companies that want to perform in-house security testing, such as side channel analysis or fault injection.

Booth 12

Rohde & Schwarz Cybersecurity GmbH

www.cybersecurity.rohde-schwarz.com

Rohde & Schwarz Cybersecurity is an European IT security company that protects companies and public institutions around the world against cyberattacks. The company develops and produces technologically leading solutions for information and network security, including highly secure encryption solutions, cloud security, next generation firewalls and endpoint security. The portfolio also includes vulnerability scanners and firewalls for business-critical web applications and web services.The award-winning and certified IT security solutions range from compact, all-in-one products to customized solutions for critical infrastructures. To prevent cyberattacks proactively, rather than reactively, our trusted IT solutions are developed according to the security-by-design approach. More than 500 people are employed at locations in Germany, France and Spain.

Conference Bag Sponsor

SafeLogic

www.SafeLogic.com

SafeLogic's product line is focused on standards-based cryptographic engines designed for use in mobile, Cloud, server, wearable, IoT, workstation, and appliance environments. SafeLogic modules

include RapidCert, the industry's only FIPS 140-2 validation service that provides a certificate in the customer's name, while drastically accelerating the timeline, requiring no additional engineering effort, zero interaction with testing labs, and at a fixed cost. SafeLogic was established in 2012, is privately held, and is headquartered in Palo Alto, California..

Booth 24

Ultra 3eTI

www.ultra-3eti.com

Ultra Electronics, 3eTI is a leading cyber-physical technology company with solutions that connect and protect critical information and infrastructure systems. Our products and services reduce the risk of cyber threats causing physical harm by providing certified assurance that operational technology networks and devices are operating when expected, as expected and under the control of legitimate users. Since 1995, Ultra 3eTI has been a trusted supplier for the defense, government, energy and industrial automation markets worldwide through advanced cybersecurity, secure wireless, perimeter management, and security services. These organizations rely on our highly secure, military-grade platforms to communicate and protect critical assets. Our experience and tested performance in some of the most demanding and harsh environments make 3eTI an obvious choice.

Booth 13

WolfSSL

www.wolfssl.com

The wolfSSL embedded SSL library is a lightweight, portable, C-language-based SSL/TLS library targeted at IoT, embedded, and RTOS environments primarily because of its size, speed, and feature set. It works seamlessly in desktop, enterprise, and cloud environments as well. wolfSSL supports industry standards up to the current TLS 1.3 and DTLS 1.2, is up to 20 times smaller than OpenSSL, offers a simple API, an OpenSSL compatibility layer, OCSP and CRL support, is backed by the robust wolfCrypt cryptography library, and much more. The CMVP has issued FIPS 140-2 Certificate #2425 for the wolfCrypt Module.

ARE YOU READY FOR THE DIGITAL DISRUPTION?

JOIN JASON HART, CTO, GEMALTO, FOR THE PLENARY KEYNOTE ADDRESS WHERE YOU WILL LEARN:

- What is the digital disruption and why is security fundamental to the success of the digital transformation revolution?
- How to develop more efficient ways of interacting with customers and producing new services
- Build security into the digital strategies
- What does this mean for traditional Information Security Controls and Standards? Are we going to see disruption in the Cryptography world?

KEYNOTE ADDRESS:
"DIGITAL DISRUPTION AND THE IMPLICATIONS FOR CYBERSECURITY AND CRYPTOGRAPHY (P10A)"

09 MAY 2018
09:20–09:50
OTTAWA SALON 213-215

gemalto

www.gemalto.com

Your Conference Badge is a Digital Business Card

Badge Sponsor

gemalto
security to be free

Use any smart phone or pad QR code scanning app to retrieve complete contact information

Many free QR code scanning apps are available. The following app is highly rated in many app stores:
ScanLife by ScanBuy Inc. on Android, iOS, BlackBerry, Nokia Ovi, Windows Phone
We make no representations or warranties regarding the functionality or performance of any third party software

Certified InfoSec CONFERENCE

The Global Forum for Professionals in Certified Enterprise IT Security

October 9-10, 2018 ★ Washington, DC ★ www.CertInfoSec.org

The year's leading event for professionals focused on certified IT security

Connect with colleagues at networking events and a special showcase exhibition

Located in Washington, DC, with easy local and international access

Join Your Colleagues at the Global Forum for Certified ISMS

This year's Certified InfoSec Conference will be held October 9-10 at the Westin Tyson's Corner in the Washington DC area. Now in its fourth year, the Certified InfoSec Conference will bring together professionals focused on the most widely-implemented enterprise security standards: ISO 27001, ISO 22301, CSA STAR, FISMA/FedRAMP, SOC, and PCI. It's the leading forum for the global certified enterprise security community, including those who develop, assess, specify, support, and implement these standards. In the face of multiplying security threats, organizations are increasingly required to maintain audited proof of management control over cyber security. Whether you're focused on one standard or several, the Certified InfoSec Conference is the place to learn about the current standards and future path for these standards.

Who Should Attend

CISC is a learning forum for ISMS professionals who develop, assess, specify, support, and implement certified information security, including Security Professionals, Network and Computer Systems Administrators, Penetration Testers, Incident Handlers, System Analysts, Security Auditors, Risk Assurance Personnel, Vulnerability Assessment Personnel, Security Operations Center (SOC) Personnel, or Chief Information Security Officers.

Presented by Industry Leaders Lead Sponsors

The Certified InfoSec Conference is presented by Cnxtd Event Media Services with program development support from Emagine IT, BSI Group, and DNV-GL.

Lead Sponsors

emagine it believe it. bsi. DNV·GL

Conference exhibit and sponsorship marketing opportunities are available. Contact Bill Rutledge, +1 212-866-2169, bill@CertInfoSec.org

30 October-1 November 2018 | Hilton Amsterdam | www.iccconference.org

The year's leading event for professionals focused on common criteria

Connect with colleagues at networking events and a special showcase exhibition

Now in the Hilton, Amsterdam, with easy local and international access

Setting the Global Agenda for Common Criteria

Reserve your seat at the 17th ICCC, the leading forum for the community of professionals involved in Common Criteria (CC), the widest available mutual recognition of secure IT products. ICCC is a high-level technical conference, a forum for discussion on the policy and application of CC, and a professional networking opportunity for those in charge of specification, development, evaluation, certification and approval with regard to the IT security of products and systems. The three day conference program will feature government and industry experts from across the international Common Criteria community.

Who Should Attend

This important event brings together hundreds of participants from around the globe: Certification Bodies, Evaluation Laboratories, Researchers, Evaluators, Policy Makers, Product Developers, Sellers and Buyers interested in the specification, development, evaluation, and certification of IT security.

Conference Tracks Include

Advances in the Use of Common Criteria; Meeting Customer Requirements; Updates from Schemes and ITCs.

Presented by Industry Leaders

The International Common Criteria Conference is produced by Cnxtd Inc. Event Media Services and presented with the support of the Common Criteria Users' Forum. The CCUF provides a voice and communications channel between the CC community and the Common Criteria organizational committees, CCRA member organizations (national schemes), and policy makers.

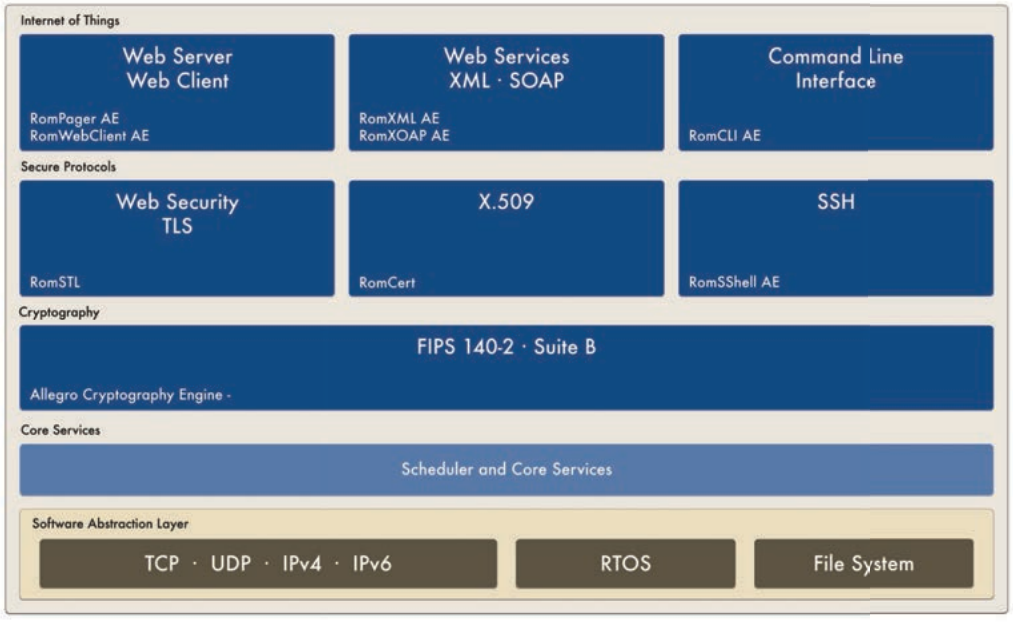
Conference exhibit and sponsorship marketing opportunities are available.
Contact Bill Rutledge, +1 212-866-2169, bill.rutledge@iccconference.org

SECURE SOFTWARE FOR THE INTERNET OF THINGS

INTEGRATED DEVICE MANAGEMENT WITH FIPS VALIDATED CRYPTOGRAPHY AND SUITE B

Seamlessly incorporate security and advanced web based device management into your next application. The Allegro AE framework of device management products are pre-integrated with Allegro's FIPS validated cryptography module with multiple layers of security services for protecting sensitive application data.

To learn more at ICMC 2018 visit Booth #20 and explore how Allegro's FIPS validated solutions deliver time to market and reduce risk for your specific application.



Proven • Portable • Pervasive

Allegro

www.allegrosoft.com/ICMC2018

FOUNDATION SECURITY TECHNOLOGIES
TRUSTED² | EMBEDDED | INTEROPERABLE

CRYPTSOFT®

THE TRUSTED SECURITY PROVIDER TO YOUR TRUSTED SECURITY PROVIDER

Cryptsoft is a privately held Australian company that operates worldwide in the enterprise key management security market. Cryptsoft's Key Management Interoperability Protocol (KMIP) and PKCS#11 software development kits (SDKs) are the market's preferred OEM solutions.

Cryptsoft's solutions have been selected by prominent global companies for interoperable enterprise key management and encryption technology in their storage, infrastructure & security and cloud products. Cryptsoft is committed to the development of standards based security software and is an OASIS Foundational Sponsor.

Products

Cryptsoft produces a wide range of Server and Client based SDKs which provide OEM vendors worldwide to quickly and cost effectively implement OASIS KMIP and PKCS#11 compliant applications.

Server SDK Products

- KMIP C & Java Server SDKs
- KMIP C & Java Server SDKs SGX Module
- KMIP Server Administration Interface - C & Java
- KMIP C Server Integration Modules (PKCS11, HSM, RNG)
- KMIP C Server Integration Modules (HSM, RNG) SGX Module
- KMIP C Server OTP Server Module
- PKCS#11 C Provider SDK SGX Module
- PKCS#11 C Consumer SDK SGX Module
- SQLite3 SDK SGX Module
- Object Store SDK SGX Module

Client SDK Products

- KMIP C, C++, C#, Java & Python Client SDKs
- KMIP C, C++ Client SDKs SGX Module
- KMIP C Client Layered Protocol SDKs for Proprietary Protocols
- KMIP C Client PKCS11 Adapter
- KMIP RKM/DPM C Client SDK
- KMIP C Client Oracle TDE & Microsoft BitLocker
- KMIP C Client Layered Protocol SDK
- KMIP C Interoperability Test Suite
- KMIP Java Interoperability Test Suite
- Online Test Service (XML/JSON)

Customers

Cryptsoft's valued Customers include:

BDT, COHESITY, DATASTAX, DELL, DELL EMC, ebay, FORNETIX, Hewlett Packard Enterprise, HUAWEI, HYTRUST Cloud Under Control, InterSystems Health | Business | Government, MarkLogic, MICRO FOCUS, NetApp, netskope, nimble storage a Hewlett Packard Enterprise company, reduxio, SPECTRA, StorMagic, THALES, TREND MICRO, U.S. ARMY, Vormetric Data Security

SALES@CRYPTSOFT.COM +61 7 3103 0321 | US +1 650 918 4362 WWW.CRYPTSOFT.COM