International Mutual Recognition

Technical Working Group

(IMRT-WG)

November 28, 2018

InterNational Cyber Security Center of Excellence

(INCS-CoE)

Terms of Reference

This Terms of Reference (ToR) sets out the working arrangement for International Mutual Recognition Technical Working Group (IMRT-WG), such as its purpose, membership and secretary, meeting schedule and expected outcomes.

1. Purpose

Global recognition of trust services (e.g. electronic signature, electronic authentication, electronic timestamp, electronic seal, electronic delivery, web authentication) is an urgent demand for global economy. A global company needs to sign the contract with their partner in overseas electronically, a non-US company wants to use their credential for DoD incident report program in the US, a pharmaceutical company wants to sign the document with same signing key for both European Medicine Agency and US Food and Drug administration, and more. These are possible only if mutual recognition among countries is achieved, often requiring an agreement between the parties (e.g., International agreement). However, such legal agreements need to be supported on a secure technical foundation for mutual trust of the concerned electronic trust services. By bringing together technical experts involved in different trust schemes such as Federal PKI, WebTrust for CA, EU audits under the eIDAS Regulation (EU) 910/2014 which can be based on ETSI standards, and the Japanese Act on Electronic Signature and Certification Business, it is aimed that the IMRT-WG will explore the technical foundations of international mutual recognition of trust services giving full support to the implementation of legal recognition agreements.

2. Term

The ToR is effective from 2018-11-21.

3. Expected outcomes

The below mentioned outcomes are expected at the moment.

Initial outcome 1: Define a common methodology for bilateral recognition by establishing equivalence between trust service policies (e.g. certificate policies) and audit schemes.

Initial outcome 2: Define a common representation scheme for trust in verification (e.g. list of trusted anchors and associated data) under the recognition (e.g. certification/audit/supervision) scheme applied to one or more trust service policies (e.g. certificate policies).

Initial outcome 3: Explore case studies applying outcomes 1 & 2 to example international mutual recognition scenarios.

4. Membership

IMRT-WG is comprised of the following experts:

Satoru Tezuka（Chair）

Project Professor, Graduate School of Media and Governance
Director, Cyber Security Research Center, Keio University

He graduated from the department of Technology, Keio University in 1984, and joined Hitachi Ltd. He has been a Professor of the School of Computer Science, Tokyo University of Technology since 2009. Since April 2016, he is a Project Professor at Keio University.

He received the 2004 IPSJ Best Paper Award, the 2008 IPSJ Best Paper Award, the IEEE-IIHMSP2006 Best Paper Award, and the 2013 Information Security Cultural Award.

In government related organizations, he is a Commissioner of Personal Information Protection Commission, a SIP Sub Program Director of Council for Science, Technology and Innovation, a Committee Member of Critical Infrastructure Advisory in Cybersecurity Strategy Headquarters Information Security Policy Meeting, a Task Force Member of IT Strategy Headquarters Electronic Administration, a Working Group Member of Related Information Infrastructure Technology, a Member of Basic Resident Register Network Research Committee, and a CRYPTREC Member. He is also a Chairperson of the Electronic Signature Law Working Group.

He is the President of the Information Network Law Association, an executive director of the Japan Society of Security Management and a director of the Institute of Digital Forensics.

His books include “Q&A Security Countermeasures for My Number (Seibunsha)”, “Electronic Signature and Authentication using My Number (Nikkei BP) “, ”Enterprise Codes make Japan Strong: Another Type of Individual Number, the “Corporate Number (Nikkei BP)” and “Basic Information Security (Kyoritsu Shuppan)”.

Judith Spencer

Chair, CertiPath Policy Management Authority

Judith Spencer is the Chair, CertiPath Policy Management Authority. She manages the CertiPath Bridge Certification Authority, which provides the federated trust environment for industry, including the Aerospace-Defense community. Previously, Ms. Spencer was Chair of the Federal PKI Policy Authority and co-Chair of the Federal CIO Council's ICAM Subcommittee, building cross-organizational consensus on matters related to identity management and the implementation of HSPD-12. She continues to champion high assurance identity credentials in the federated environment.

David Simonetti

SAFE-BioPharma Association

David has over 30 years of experience in technology development and services including critical infrastructure protection, information security, systems architecture and engineering, and software engineering with customers spanning the U.S. Federal civilian government, the U.S. Department of Defense, and healthcare, financial, payment, and energy industries. His entire career has been focused in the fields of information security (INFOSEC) and communications security (COMSEC) allowing him to gain a broad set of experience in security technologies and processes, data protection, cryptography, key management, identity and access management (logical and physical), network security, and various cloud computing environments. Currently, he leads policy and governance activities for the SAFE-Biopharma high assurance identity trust infrastructure within the Healthcare Information Sharing and Analysis Center (H-ISAC). His previous projects included the implementation of smartcard-based identity systems and federated identity systems for multiple U.S. Federal agencies, and he was a principal contributor to the original CCITT X.509 Authentication Framework and subsequent IETF and U.S. Government initiatives.

Patrick Patterson

President and Chief PKI Architect of Carillon Information Security

Patrick Patterson, as the President and Chief PKI Architect of Carillon Information Security, has been working in area of high value PKI for over 20 years, and is the author of numerous papers and presentations on the subject. He has been one of the lead authors of the PKI and Identity Management specifications at aerospace standards organizations such as the ATA, AEEC, and the TSCP.

Matt King

Director, SAFE-BioPharma Association, LLC

Matt King, Director of SAFE-BioPharma, has 20+ years of cybersecurity expertise, focusing on Identity, Credential, and Access Management for a broad range of commercial and government entities. He served in the role of Senior Policy Analyst and Identity Management Subject Matter Expert for the US Federal Public Key Infrastructure (FPKI) Policy Authority under the US Government's Identity Credential and Access Management Subcommittee (ICAMSC) for more than a decade. He also has worked for Booz Allen Hamilton supporting the National Security Agency's PKI and Biometrics Research initiatives. He holds multiple degrees in Computer Systems Management and Information Systems and a Certificate in Information Resources Management.

Nick Pope

Director of Security & Standards Associates

Nick Pope is a Director of Security & Standards Associates providing consultancy in IT security and the application of standards to the financial, commercial and governmental sectors. He is vice chairman of ETSI technical committee on electronic signatures and trust infrastructures. He has played a leading role in the development of standards under the European eIDAS Regulation 910/2014 and most recently the use of eIDAS Qualified Certificates for secure communications under the payment services Directive 2015/2366.

Dipl. Wirtsch.- Ing. Arno Fiedler

Owner & Managing Director, Nimbus Technologieberatung GmbH

Born in 1963, married, two children,
Located in Germany, Berlin
Diploma as an industrial engineer
2 years german navy
20 years IT Industry
15 year experience in the field of IT-security,
ISO 27001 Lead Auditor [BSI, ICRA]
Architecture and management of Public-Key-Infrastructures,
PKI- and security policies (ETSI, CA/B-Forum, ETSI, eIDAS)
Design of (X.509) Certificates in accordance with data protection laws
Requirement engineering for ID-Card Systems

Olivier Delos

Senior eSecurity & eSolutions consultant, SEALED

Olivier Delos is a senior eSecurity & eSolutions consultant based in Belgium; he has more than 25 years of professional experience. He is a European recognised expert in eSignatures, eProofs, PKI and eID design & consulting, combining technical and business expertise in these matters. Olivier has a M.S. degree in Computer Science Engineering from Université catholique de Louvain (BE), 1991.
In late nineties, Olivier set up and managed the first Belgian Certification (Trust) Service Provider issuing qualified certificates, providing time-stamping services and registered email.
Since 2005, as part of SEALED, Olivier served and continues to serve international and governmental organisations from EU MS and from States beyond EU (North & West Africa, GCC country, Middle East, Asian country) in the context of the set-up of national PKI & related trust services, and their international recognition notably through mapping of legal, business, technical and approval scheme requirements.
Since 2009, He is the technical expert supporting the European Commission (EC) drafting the specifications of the trusted lists first in the legislative context of the Services Directive and then under the secondary legislation of eIDAS Regulation (EU) No 910/2014. He also assisted the EC in having the European cooperation for Accreditation (EA) and ETSI collaborating in setting up an EU accreditation framework on the basis of ISO/IEC 17065 and the ETSI EN 319 403 for CAB confirming the conformity of QTSP/TS against the eIDAS requirements.
He is also active in ETSI standardisation activities regarding eSignatures, trust services and trusted lists. He is a member of the STF 560 in charge with global acceptance of European Trust Services.

Kazuo Noguchi

Senior Researcher, Keio Research Institute at SFC
Senior Manager, Hitachi America, Ltd.

Kazuo Noguchi is a Senior Research at Keio Research Institute at SFC and Sr. Manager, R&D, Global Center for Social Innovation at Hitachi America, developing new go-to-market business strategy and execution with Social Data Infrastructure (SDI). Recently, he became Senior Researcher at Keio Research Institute at SFC, actively involving International Cyber Security Center of Excellence (INCS-CoE). He facilitated a panel discussion as a Chair inviting British, U.S., and Japanese representatives hosted by OASIS at the World Bank in Washington DC.

Currently, he is supporting to launch INCS-CoE, organizing U.S. and British governments, companies, and universities at Keio University. He joined Hitachi Group in 2002 as Chief Consultant and Business Development Manager, initiated M&A and alliance strategies to the Hitachi board.

He is a seasoned strategy and management consultant with over 20 years of experiences in the industry in the US, Canada, and Japan. His expertise includes creating emerging Big Data and Open Data businesses, supporting Information Sharing and Analytics with Cybersecurity, devising and executing IT strategies, post-merger integration, and project management.
Prior to joining Hitachi, he was a Manager at KPMG at the New York office. He managed market entry projects in the financial services industry, e.g. porting U.S. version of 401(k) to Japanese version of 401(k) products, services, and processes, leading the team of KPMG consultants and IBM subject matter experts.

He received MBA from University of Toronto, Master and Bachelor in Management Science from Tokyo University of Science. He was a Rotary Foundation Scholar to study and research at the University of Toronto.

Atsushi Inaba

GMO GlobalSign K.K.

Atsushi Inaba is responsible for PKI related business development at GMO GlobalSign.
He has been engaged in Root CA Certificate embedment, Service Planning and Business Development of Digital Certificate Services for more than 20 years from its dawning age. He has participated in various consortiums and forums, e.g. CA/Browser Forum, Asia PKI Consortium, JANE (Japan Association of New Economy), JIIMA(Japan Image and Information Management Association) etc., and has been taking part in activities to develop guidelines, promote awareness about security and provide recommendations.
Currently he is serving as a member of the Council of Anti-Phishing Japan's management board, and a visiting researcher at JIPDEC (Japan Institute for Promotion of Digital Economy and Community).

Kirk Hall

Director of Policy and Compliance - SSL at Entrust Datacard

Kirk Hall is Director of Policy and Compliance - SSL at Entrust Datacard, a global leader in trusted identities and secure transactions that make the world safe for businesses and consumers to exchange digital information. Hall's responsibilities include Entrust SSL's digital certificate policy and compliance operations as well as regulatory and audit matters. He previously served in similar roles at GeoTrust and Trend Micro, and was a co-founder of certification authority AffirmTrust, which was acquired by Entrust in 2016. Hall was a founder of the CA/Browser Forum in 2005 and Chair from 2016-2018, and was a co-inventor of the Extended Validation SSL server certificate and validation process. He holds an A.B. degree from Harvard College, a Master's degree in economics and resource use from Yale University, and a Juris Doctor. degree from Northwestern School of Law at Lewis and Clark College.

Soshi Hamaguchi（Secretary）

Senior Researcher at Keio Research Institute at SFC

Cosmos Corporation

Visiting Researcher of JIPDEC

Soshi Hamaguchi is a Senior Researcher at Keio Research Institute at SFC, a director of Cosmos Corporation, and a Visiting Researcher of JIPDEC. Ph.D.

2008 – 2009	Temporarily transferred to TÜV Nord AG group in Germany and took the training course including Management, Communication Protocol for Automotive and Common Criteria (ISO/IEC 15408), etc.
April 2011	Provided the audit/certification services for the management systems of certification authorities and time stamping authorities.

Hosted the related seminars and other services as a Japanese representative of TÜV Informationstechnik

GmbH.

April 2013 As a Visiting Researcher at JIPDEC, engaged in research about the latest trend of the trust services in the EU and the U.S.

2015 Engaged in standardization activities as a member of the subcommittee of the ISO/IEC JTC1 SC27 WG3.

2016 Being appointed as the director of Cosmos Corporation and surpervised IT Security business.

Focusing on the trend of European trust services since the draft stage of eIDAS Regulation, provided introduction and explanation of eIDAS regulation to the industry group, governement organizations, etc.

Also being engaged in the research project about FPKI and FICAM in the U.S.

Contributed to establishment of the International Mutual Recognition Technical Working Gourp (IMRT-WG) utilizing own network with the EU and US experts built in these activities.

As a core member of Japan Trust Technology Association(JT2A), being engaged in development of guidelines about remote signature.

As a member of Japan Trust Service Forum (TSF), being engaged in the research project about the European trust services.

5. Roles and Responsibilities

The experts of the IMRT-WG will;

- Attend IMRT-WG meetings unless not possible due to other obligations,
- Foster collaboration,
- Contribute to the IMRT-WG from their expertise.

The secretary of the IMRT-WG will support:

- Communication with the experts,
- Arranging the meeting schedule,
- Sharing information with the experts.

The secretary will be assigned by the Chairman.

The Chairman of the IMRT-WG will be:

- Leading the IMRT-WG activities

The Chairman will be assigned by agreement of the IMRT-WG members.

6. Meetings

All meeting will be chaired by the assigned Chairman, unless he is unable to attend in which case he may assign someone to be a temporary chair.

Meetings will be held as agreed are necessary by the members. It is expected that meetings will be held at least every 3 months.

Meetings will be held mainly by using WebEx system. Some members may attend meetings physically co-located,

Meeting agendas and minutes will be prepared by the secretary.

7. Amendment, Modification or Validation

The ToR may be amended, varied or modified after consultation and agreement by IMRT-WG experts.