Trustless Computing Certification Body & Seevik Net

PARTNER TRACTION UPDATE

TRUSTLESS.AI

TCCB Trustless Computing Certification Body

List of current partners of TCCB and Seevik Net
and details of engagements with actively-interested Prospective Partners,
with a special focus on nation-states' ministries, agencies and strategic companies.

(This is a Nov 24th, 2022 version. Request an updated version at rufo@trustlesscomputing.org)

TABLE OF CONTENTS

This Document

Ours is **completely transparent initiative** for the global public good, that seeks to aggregate a critical mass of globally-diverse set of nations, IGOs and NGOs and co-founding and governing partners.

For each prospective partner it is essential to gauge the updated actual interest of like-minded others, to inform their decision to progressively join more actively and formally.

So, this *Traction Update* details List of **current partners** of TCCB and Seevik Net and details of engagements with actively-interested prospective partners, with a special focus on nation-states' ministries, agencies and strategic companies.

References to persons and entities that have shown previous interest are maintained but the fact their interest is no longer active will be clarified.

Please **contact us for corrections**, if you find your name or the name of your institution in this document, and you either: (1) want to update your level of interest; (2) are not actively-interested but instead not interested now and any time in the future; (3) you believe some references are incorrect.

2-PAGER SUMMARY

Partners, Advisors and Activities

Since 2015, we have advanced TCCB and Seevik Net via R&D initiatives and academic papers, together with 35 top R&D partners and 25 top advisors, and a global conference series called **Free and Safe in Cyberspace** with 8 editions held on 3 continents, with over 120 exceptional speakers. In 2019, we created a *spin-in* startup, TRUSTLESS.AI, with a top team and advisors - building initial minimalist TCCB-compliant mobile IT systems and devices - which is bound to be owned by TCCB via a "spin-in" agreement.

Establishment of the TCCB in 2021

Last June 2021, during the 8th Edition of **our** Free and Safe in Cyberspace conference series, held in **Geneva** - after previous editions in **Brussels, Berlin, New York, Geneva and Zurich** - we finalized the Trustless Computing Paradigms, and the statute of the *Trustless Computing Association* (**TCA**) and the *Trustless Computing Certification Body* ("**TCCB**") - together with World-class speakers. Among those top IT security experts, the former top cyber diplomats of the United States and Netherlands, and executives of top EU banks.

Traction Nation States

Over recent years, months and weeks, we attracted the substantial interest of several nations via engagement with top representatives of different relevant departments and ministries, their strategic cyber-only investment entities, or their strategic low-level IT security firms.

Over the last 5 years, very extensive engagements have occurred with **Germany** and **Italy** at all levels. More recently, with **France**, **Netherlands,** and several third nations with high strategic autonomy like **Switzerland, Malta** and **Liechtenstein**. Some interest has been shown by **Romania** and **Poland**. In recent months, following meetings in DC, London, Munich, and Vaduz, we have presented a customized presentation of the opportunity for Germany, and for Liechtenstein and for Middle East nations. Details of those engagements are available on request.

Since 2015, together with global tech leaders in high-assurance open-source low-level IT and ***EOS*** (EU largest IT security industry association), the national IT certification bodies for top secret IT of **Austria** (A-SIT, CIO) and **Italy** (ISTICOM/OCSI), equivalents of the German BSI, have been among our formal governance R&D partners in our 2015-2016 EU funding proposals for TCCB and Seevik Net, to radically improve the transparency, the security levels and the mutual recognition of classified IT certifications.

For each nations, we have engaged one or more of the following:

- (1) their foreign affairs, security, intelligence, or IT certification departments for participation as **governance** partners in TCCB;
- (2) their state-funded or state-controlled VCs or **funding** entities specialized in strategic investments in IT security for joint controlling investment in our startup spin-in;
- (3) their strategic IT security firms specialized on high-assurance open-source low-level IT for **technical partnership**, primarily based on a few open-source derivative designs of the open-source **Sel4** operating system and the open-source **Risc-V** CPU/SoC designs.

Nations' Strategic Investment Entities

In addition to private western VCs, in recent years and months, we had dozens of meetings for over 30 hours with **cyber-only state-funded or state-controlled VC firms** to jointly invest in the association *spin-in* startup TRUSTLESS.AI, which is building initial TCCB-complaint IT systems and will provide initial funding for the TCCB. And maintain active interest with some from **Germany** (eCapital Entrepreneurial Partners), from **Netherlands** (Innovation Quarters), **France** (Cyber Impact Ventures), and the **USA** (Paladin Capital Group). MACH37, the US leading cybersecurity accelerator and investors, for which we were chosen among hundreds in Q4 2021, has accrued rights to 3% of the shares. In early October 2022, the *Agenzia Della Cybersicurezza Nazionale* of **Italy** announced, following program statements from the new majority, that it will also be investing in strategic cybersecurity startups, a first in Italy.

IGOs (Inter-Governmental Organizations)

On the front of IGOs (Inter-governmental Organizations) interested in joining, we recently received substantial top-level interest from UN International Computing Center to develop the TCCB and Seevik Net inside the **United Nations** as per this proposal for the United Nations, via a new "voluntary fund" which is being set up for critical UN IT needs. In recent weeks, we have had increasing interest in several meetings with the **International Committee of the Red Cross.**

United States and Israel

Over the last two years, we held over 9 meetings of intense and detailed dialogue with the former highest-ranking cyber diplomats of both the **US and Israel.** Following such dialogues, we wrote an all-important detailed case as to why **Israel** and the **US** should and will eventually join as governance partners of the Trustless Computing Certification Body - even though they'd need approval by an UN-like resilient, democratic body to intercept an elected official or private citizen from a friendly nation. MACH37, the Virginia-based **US** leading cybersecurity accelerator, for which we were chosen among hundreds in Q4 2021, has accrued rights to 3% of the shares of the startup spin-in.

CURRENT R&D & GOVERNANCE TECHNICAL PARTNERS

Current Governance R&D Partners

The following participated to formal EU He2020 R&D initiatives that we conceived and coordinated since 2015:

- **Federal Chief Information Officer of Austria. (Austria)** Represented by Reinhard Posch, since 2001 it has reported directly to the Austrian Chancellor for directing all Digital Austria and e-government activities in Austria. Led the Digital Austria ICT Board", responsible for creating the legal and technical requirements as well as coordinating the planning and development of eGovernment solutions between the Federal Government, the provinces, and local authorities. It acts as Director general of A-SIT and therefore coordinates Austria's role in SOGIS and the most relevant cybersecurity standardization and certification activities.
- **ISCOM - Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (Italy)** is a General Direction of the Italian Ministry of Economic Development and it runs OCSI, the Italian Scheme for ICT Security Certification. OCSI is the Italian official member within CCRA and SOG-IS MRA. As authorizing member in both agreements it produces ICT security certifications which are recognized in Europe and world-wide. OCSI operates in the context of certification of ICT products and systems for civil use. In addition to OCSI, ISCOM hosts Ce.Va, an evaluation center laboratory for ICT products and systems dealing with classified data.
- **Data Protection Authority of the State of Schleswig-Holstein (Germany).** Unabhängiges Landeszentrum für Datenschutz (ULD, Engl. Independent Centre for Privacy Protection) is the Data Protection Authority of Schleswig-Holstein, the northernmost Federal State of Germany. Its office with 40 employees is located in Kiel, Germany. The Privacy Commissioner of Schleswig-Holstein, Marit Hansen, is head of ULD. ULD is responsible for both freedom of information as well as data protection at private and public sector entities seated in Schleswig-Holstein.
- **Lombardia Informatica. (Italy)** It is a public-capital service company which was constituted in December 1981 as an initiative of the Regional Government of Lombardia (Regione Lombardia). It has around 630 employees and a turnover of about 200 million Euro. Lombardia Informatica's mission is to innovate services and increase the Regional System's productivity through Information Technology, in order to improve Citizens' quality of life and Lombard companies' competitiveness. As the IT partner of Regione Lombardia, Lombardia Informatica designs and implements ICT Systems for the Regional Government and represents the unique interface between Regione Lombardia and the marketplace. The LISPA team has a complete expertise in providing public services. The large experience in complex service and in providing critical privacy and security services in e-Gov and eHealth fields involving citizens and public employees guarantees that it has all the competence needed to manage the pilot site.
- **The Secure Information Technology Center of Austria (Austria)**. A-SIT is the leading IT standardization and certification public body in Austria. It represents public authorities or assists Austrian public authorities in various international and EU bodies (e.g., Council of Europe, ENISA Management Board, Common Criteria Management Board, SOG-IS, OECD, etc.). Its members are the Austrian Federal Ministry of Finance (BMF), the Central Bank of the Republic of Austria (Oesterreichische Nationalbank, OeNB), the Federal Computing Centre of Austria (BRZ), and

Graz University of Technology (TU Graz). Further formal duties are Competent Authority for certifying online collection systems for the European Citizen Initiative (EU Regulation 211/10, art. 6(4)), security assessment of e-voting technical components (student union elections), or expert opinions for the Data Protection Commission. Following a Cabinet Council decision the Austrian federal ministries are asked to call on A-SIT in the cases of research orders or questions corresponding to the A-SIT mission. Thus, A-SIT has the duties of a national ICT security advisory agency, even though not organized as an agency, but as an association.

- **Municipality of Barcelona (Spain)**. It is the capital city of the autonomous community of Catalonia in Spain and Spain's second most populated city, with a population of 1.6 million[5] within its administrative limits. As the capital of the autonomous community of Catalonia, Barcelona is the seat of the Catalan government, known as the Generalitat de Catalunya; of particular note are the executive branch, the parliament, and the Supreme Court of Catalonia. It has historically been an EU leader in government and e-government practices centered on promoting citizens' autonomy.

Current Technical R&D Partners

The following participated to formal EU He2020 R&D initiatives that we conceived and coordinated since 2015:

- **European Organisation for Security (Belgium)**
  A member-supported research, dissemination and strategic organization that represents most leading European IT security providers, researcher entities, universities, clusters and associations[1], including Thales, Almaviva, Atos, CEA, Fraunhofer, Engineering, Airbus, Indra, Saab, STM.
    - Role: contribute to analysis and recommendation from a perspective of large IT industry actors, and networking and dissemination towards the same.
- **COSIC - KU Leuven. (Belgium)** Research group COSIC (Computer Security and Industrial Cryptography) of the Dept. of Electrical Engineering-ESAT ept. Led by Prof. Bart Preneel, the COSIC research group provides world-leading expertise in digital security and strives for innovative security solutions. Their research is applied in a broad range of application domains, such as electronic payments, communications, identity cards, e-voting, protection of e-documents, intelligent home appliances, telematics for the automobile industry and trusted systems.
    - Role: Design the crypto infrastructure of the target architecture; and lead analysis and recommendation of related improved assurance assessment methods and governance.
- **Applus+ Laboratories (LGAI Technological Center S.A) (Spain)**
  Performs testing, inspection, certification, R&D in more than 25 sectors, including ICT technologies. Part of Applus+ is a leading company in testing, inspection, certification and technological services. First Spanish multinational in the certification sector (9th in the world), present in 5 continents and structured in 4 Divisions: Applus+ Laboratories (which will participate in this project), Applus+ IDIADA, Applus+ Auto and Applus Energy & Industry. The annual turnover is around 40M€, and has around 400 employees of high technical skills and different knowledge areas. R&D projects are part of the activities of the entity, and as some of the most representative R&D Projects carried out in the last years are: National: Adv-SCA, Adv-FI, MalpApp, Mobile , Ctless-Tool (internal), NFC-DCC (MICINN-INNPACTO), SINTONIA (CENIT), SMARTCARD (internal),

[1] http://www.eos-eu.com/Middle.aspx?Page=members&tID=175

LI-MASH (MICINN), eCID and TRATAMIENTO 2.0 (MITyC-Plan Avanza), TS-CIMONHET (CATRENE, without funding), IMPACT-EMR (ENIAC, without funding), NET-EMC (Eurostars), COSY3D (Euripides), COOPERS (FP6).
    - Role: Key expert in standard setting and certification processes.

- **TUBITAK BILGEM Cyber Security Institute (SGE) (Turkey).** Cyber Security Institute (SGE) founded in 1997 as a network security department then established as an individual institute in 2012. The institute is one of the six institutes of the governmental research center of TUBITAK BILGEM (Informatics and Information Security Research Center). The Scientific and Technological Research Council of Turkey (TUBITAK) is the leading agency for the management, funding and conduct of research in Turkey. TUBITAK also acts as an advisory agency to the Turkish Government on science, technology and research matters. The Cyber Security Institute (SGE), is a group of researchers working on Systems Security projects, mainly within the public sector. The Institute focuses on applied research where the results can be used with immediate effect and has a strong relationship with both public and private sector stakeholders in Turkey.
    - Role: Strategy, analysis, specification, and implementation contributions as the leading national technical authority on high-assurance IT for public sector organizations.

- **Genode Labs GmbH. (Germany)** It is a German SME specialized in building highly secure operating systems (OS). The company is the driving force behind the Genode OS Framework - an open-source OS technology that aligns highly dynamic workloads with security, robustness, and scalability. It is compatible with seL4 the only formally proven OS/kernel in the world. The combination of seL4, Genode, and the SCuP SoC will represent an unprecedented platform in terms of security, scalability, and confirmability.
  Unlike traditional high-assurance systems, Genode is based on a completely open and transparent development methodology. Since its foundation in 2008, Genode Labs has operated as an independent company solely owned by its founders. The community of users, participants, and customers includes individuals, small and medium sized businesses, governmental institutions, and research groups of multinational corporations alike.
    - Role: Contribute the operating-system foundation to the project and related critical software components

- **DFKI - German Research Centre for Artificial Intelligence[2]. (Germany)**: Deutsches Forschungszentrum für Künstliche Intelligenz, DFKI). Currently it is the largest research center worldwide in the area of Artificial Intelligence and its application in terms of number of employees and the volume of external funds. DFKI shareholders include Deutsche Post, Deutsche Telekom, Google, Microsoft, SAP, BMW, Intel and Daimler.
    - Role: Contribute to analysis, requirements and recommendations from the point of view of critical cyber-physical systems, as well as analyze medium and long-term impact on AI control, safety and security. Will lead the lab validation of the CivicCPS for securing a moveable autonomous system in human environments.

- **SCYTL Secure Electronic Voting S.A. (Spain)** Global leader in e-voting and high-assurance remote deliberations technologies. It is focused on providing electoral modernization solutions with the highest security levels in the market. Scytl cryptographic measures rely on more than 40 international patents which contribute to ensuring the privacy and integrity of sensitive electoral information.
    - Role: prototype of software application layers, other TBD.

[2] http://www.dfki.de/web?set_language=en&cl=en

- **EMAG Institute of Innovative Technologies (Poland)** The Institute of Innovative Technologies EMAG is the R&D leader in many sectors of the market, such as information security management systems, business continuity systems, risk management systems, natural hazards monitoring, and systems for automation and measurement. EMAG Institute employs 138 people, including 42 scientists and 74 engineers and technicians. The Institute has been given almost 500 patents, over 80 protection rights and 6 trademarks and has been granted several hundred awards at different competitions and fairs. The Institute's research team also has knowledge and experience in the development of risk assessment methods and tools for different domains of applications e.g. for critical infrastructures, transport utility.
    - Role: analysis and optimization of certification processes, also through new IT enabled processes.

- **Delft University of Technology** - Parallel and Distributed Systems Group (Netherlands) Delft University of Technology (http://www.tudelft.nl/) is the oldest, largest and most comprehensive technical university in the Netherlands. With over 19,000 students and 2,500 scientists (including 400 professors), it is an establishment of both national importance and significant international standing. The PDS group of TU Delft has a 15-year history in designing, implementing, deploying and analyzing P2P systems. It has created the BitTorrent-based P2P client Tribler that has many added functionalities such as support for video on demand and live streaming, channels, information dissemination protocols, and a reputation system.
    - Role: Design of the P2P and mixed network layer of the target architecture. Lead related analysis and recommendations.

- **Kryptus (Brazil)** Kryptus is a Brazilian company with unique global capabilities in secure hardware design and system integration. It designed the 400,000 voting machines of Brazil, fighter to fighter communications systems, and the Hardware Security Module (HSM) of the core Root CA of the main Brazilian PKI. It developed the first secure general-purpose CPU microprocessor in the Southern Hemisphere, the SCuP, which uniquely provides open and verifiable designs and FLOSS microcode. Runs at 100-300Mhz. It is at the core of CivicIT HW architecture.
    - Role: Design and prototype of critical HW, including CPU and SoC of target architecture; and contribute to related analysis and recommendations for improved assurance assessment methods.

- **TECNALIA Research & Innovation (Spain)** is a private, independent, nonprofit applied research center of international excellence. Tecnalia is the leading private and independent research and technology organization in Spain and one of the largest in Europe, employing 1,319 people (198 PhDs) and with an income of 94 Million € in 2014. Its ICT unit has extensive expertise in assurance and certification of ICT in many domains. In H2020 TECNALIA participated in 87 projects, coordinating 17 of them, up to December 2015. TECNALIA is a member of EARTO and of EUROTECH, linking together the most important research centers in Europe.
    - Role: contribute to collecting and analyzing assurance guidelines and certification schemes.

Prospective CoreTechnical Partners

In addition to our established long-timne technical partners, we have been engaged with technical partners with unique capabilities in open-licensed battled-tested low-level IT from like-minded nations:

Strategic low-level Tech Partners

Over the last few months, we have been engaging 5 C-level executives at Hensoldt Cyber AG, a spin-off of Airbus (and 25% bought by Italian Leonardo), global leaders in open source ultra high security CPU and OSs - as well as companies in US (Galois Inc.), Israel, and Australia (Sel4 Foundation) working the highest level on similar stacks of Sel4 operating system and Risc-V CPU/SoC. Their TrentOS is based on Sel4, and derives from work by US DARPA and is advanced with DARPA and public R&D entities of Australia.

(Details available on qualified request).

National Defense Contractor Partners

We've had one or more meetings with **G&D/Secunet** (DE), **Telsy** (IT), **Leonardo** (IT), **Thales** (FR), **Rhode & Swartz** (DE), **CyOne** (CH), for their interest to become co-exclusive go-to-market partner for deployments for governmental clients and derivative for military use.

(Details available on qualified request).

CYBER-ONLY STATE-CONTROLLED FUNDING ENTITIES & VCS

Given that our initiative involveS a new inter-governmental IT security certification body and a “spin-in” startup that is creating compliant IT systems and services, the most natural engagement channel to nations participation is through special funding entities they have specialized in cybersecurity strategic investments.

Over the last 2 years, months and weeks, we have engaged for over 40 hours of meetings, and dozens of email exchanges with state-controlled or state-close cyber-only investment vehicles or venture firms (or "state cyber VCs") from “like-minded” nations for their interest to participate in a $7m+ Seed round investment in our startup spin-in TRUSTLESS.AI a joint strategic investment with other similar companies jointly acquire majority control of the spin-in startup TRUSTLESS.AI,

- For over 3 years, and with over 15 hours of meetings we've had interest from **Germany**'s eCapital Entrepreneurial Partners through Steffen Reinecke and Hans-Christophe Quelle (former CEO of Secusmart).
- Over the last weeks, we had one meeting with **France**'s Cyber Impact Ventures (AurigaPartners) through William Lecat and Jean-Noel de Galzain.
- Over the last weeks, we had one meeting (and one next week) with **Netherland**'s Innovation Quarter, via Philip Meijer and Martijn van Hoogenhuijze.
- Over the last 5 years, we had over 10 hours with the current Director of **Italy**'s Agenzia Nazionale per la Cybersicurezza, Roberto Baldoni, who last week announced Italy's first program to invest in strategic cyber startups, following the new majority declarations a week before on the need to reinforce EU digital sovereignty primarily supporting cyber startups.
- For 2 years, we've had 2 meetings with the **USA**'s Paladin Capital Group, via Ken Pentimonti and Ciaran Martin. We were selected among hundreds last Q4 2021 to participate in USA Virginia-based MACH37, the US leading cyber accelerator led by Jason Chen, which acquired rights to 3% of the shares of our startup spin-in.
- Not included above are **2 EU and 2 third nations** that have expressed preference to remain confidential at this stage, and 2 UK state cyber VCs whose interest seems to be less current.

In addition, we have a large number of private VCs also interested in investing, awaiting for mortraction from prospective private and governmental end-users.

GERMANY

Summary

In recent months and years, we have been engaging extensively with the leading players in ultra-secure IT for digital communication, **G+D**, **Secunet**, **Hensoldt Cyber**, **eCapital Entrepreneurial Partner** and the **President of BSI,** and the **German Foreign Office**. Given that Germany has shown the most interest in our initiative, we are ready seeking it to have a lead role in our TCCB and Seevik Net initiative, and we are considering moving our company and/or association to Germany, especially Berlin or Munich. (Also, TCA founder's daughters, have been going to Deutsche Schule in Rome since kindergarten.)

Details

In December 2017, our Trustless Computing Association was requested by **Nicolas Heyer,** one of the founders of the German MoD Cyber Innovation Hub for a PoC proposal for use of our solution and certifications in use cases of German military intelligence.

Following such proposal, in May 2018, we held in **Berlin** the 5th edition of the Free and Safe in Cyberspace in Berlin - participated by Mr. Andreas Reisen, head of the Ministry of Interior area for IT security certifications (oversees BSI), and the German DoD Cyber Innovation Hub, and adhered to by Michael Sieber, former *Head of Information Superiority* of European Defence Agency (speaker to our FSC1, top sponsors for years in EDA, now back in German DoD), where we premiered a 50-pager academic Position Paper on TCCB. After a period in Luxembourg, we were based in **Berlin** for 4 months in 2018.

In September 2018 and then September 2019, we met in person 1-to-1 once in Berlin and once invited to HQs by the **President of the German BSI** in Bonn to present our Trustless Computing Certification Body in Bonn. Back then, BSI said it was sympathetic but not ready to join TCCB, as it was pursuing similar certifications via the EU process. To our account, nothing even remotely similar to TCCB has been successfully advanced to date. More recently in July 2022, we received an email on behalf of the President of BSI stating that BSI is not ready to engage since our initiative appears to be "not neutral" (supposedly due to the role of the startup spin-in). We replied with detailed clarifications, clarifying how our project is conceived to be as neutral and democratic as it can be, awaiting an answer.

In October 2020, I was invited to a 1-to-1 dinner in Rome by the ***Deputy Ambassador of Germany in Italy*** to discuss an Italy and Germany joint participation in TCCB, who has shown support and introduction within the German Foreign Office.

In early June 2021, we had a long Zoom with Regine Grienberger, ***Ambassador for Cyber of the German Foreign Service***, interested to participate in Day 2 of the 8th Edition of FSC to discuss possible participation in TCCB. She said she would consult BSI and Mr Sieber. Ultimately, she decided to not participate given the short notice but asked to be updated on follow-up meetings. On Sept 27th, she replied quite enthusiastically to an invitation to her agency to participate in "observer" status to our 9th Edition of Free and Safe in Cyberspace, when originally planned for Washington DC.

Last October 2021, the Head of IT of German Foreign Service, Sven Stephen Egyedy, announced that the IT department was charged with procuring a new **HW-based solution for classified communications of German diplomats and other ministries**, under the guidance of BSI. Later in 2024 to be extended in a Diplo Version whereby “representatives of other countries will be provided with the solution for direct protected communication”, and then for the private market in 2025. The project aims seem extremely in line with what we are building.

In advance of presentation we were asked to give at *Munich Cyber Security Conference* last April, we published a 15-pages blog post - prefaced by a 5-pager summary - which makes a detailed case, of why Germany would stand to benefit more than any other nation by co-leading this initiative - framing our arguments in stated objectives, concerns and initiatives of the current German government, and also **help Germany counter internal neo-nazi tendencies**. Read especially the sections titled: *""Made in Germany" hardware-based secure communications for all?*" and the one titled "*Germany's internal fight against far-right subversion*".

In recent months and years, we have been engaging extensively with the leading players in ultra-secure IT for digital communication, **G+D**, **Secunet**, **Hensoldt Cyber**, **eCapital Entrepreneurial Partner** and the **President of BSI,** and the German **Foreign Office**. Given that Germany has shown the most interest in our initiative, we are ready seeking it to have a lead role in our TCCB and Seevik Net initiative, and we are considering moving our company and/or association to Germany, especially Berlin or Munich. (Also, the main founder's daughters, 12 and 16, have been going to Deutsche Schule in Rome since kindergarten.)

Starting 2015, the Trustless Computing Association - the NGO from which the startup "spin-in" TRUSTLESS.AI was created in 2019 - we conceived and lead three H2020 R&D initiatives for TCCB and Seevik Net with partners including 2 EU member states (the Italian and Australian equivalents of the German BSI), and key German partner technical partners DFKI, KernKonzept and Chair of Mobile Business & Multilateral Security at Goethe University Frankfurt. In 2016, we participated in pre-acceleration at Hardware.co in **Berlin**.

Special Case

In advance of such presentation, we published a 15-pages blog post - prefaced by a 5-pager summary - which makes a detailed case, of **why Germany government would stand to benefit more than any other nation by co-leading the TCCB and Seevik Net initiativ**e - framing our arguments in stated objectives, concerns and initiatives of the current German government, and also help Germany fight internal ultra-nationalist threats. Read especially the sections titled: ""*Made in Germany" hardware-based secure communications for all?*" and the one titled "*Germany's internal fight against far-right subversion*".

Technical & go-to-market partners

As we detail in this recent blog post: "Last April 28th, 2022, we were invited with four members of our advisory boards and several partners attend the Spring Forum 2022 of the Munich Cyber Security Conference (MCSC) to give a slide presentation during the MCSC Roundtable on day 2 of our Trustless Computing Certification Body and Seevik Net initiatives, in front of representatives from industry, government and military from Germany, and several EU and non-EU member states. As a sister initiative of the Munich Security Conference, MCSC it is arguably the leading EU high-level transatlantic and trans-european cybersecurity forum. The Chairman of MCSC is the **Group CEO of the G+D group**, the leading provider of government cybersecurity solutions in Germany, and owner of **Secunet**."

Over the last few months, we have been engaging on1to1 calls or meetings with 5 C-level executives at Hensoldt Cyber AG, a spin-off of Airbus (and 25% bought by Italian Leonardo), global leaders in open source ultra high security CPU and OSs - as well as companies in US (**Galois**), Israel, and Australia (**Sel4 Foundation**) working the highest level on similar stacks (Sel4 and Risc-V). Their TrentOS is based on Sel4, and derives from work by US DARPA and is done with DARPA and public R&D entities of Australia.

LIECHTENSTEIN

Summary

Active interest as governance partner, end-user and strategic investor. Also interested as a channel partner through its largest private bank. Main Contact: Mr **Daniel Batliner**, the First Secretary of the Liechtenstein Mission to the UN in Geneva.

Engagements

In May 2021, we attracted the interest of Mr Pal Erik, the CEO of **Lightrock**, a $2bn ethical investment fund controlled by LGT, a $200 billion AuM private bank, whose CEO is **Prince Max of Liechtenstein**. Following, we had a meeting with a senior executive of Lightrock, Sahib Bhasin, who showed interest for a later stage as they focus on Series A. Mr Bhasin explained how Lightrock is not engineered to support startups of our stage, but that they would explore the possibility of passing the investment opportunity to angel/pre-seed investing entities or persons in their network.

Last June 2021, we were invited to the Lichtenstein Investor Summit. We met personally **Prince Max of Liechtenstein**, for about 30 minutes. We also had a long 1-to-1 meeting with Ms **Simone Frick** in her office in Schann, as a single-point of contact of the Business Angels Club Liechtenstein and as *Head of National Economic Development of Liechtenstein*. We met briefly in Schaan with Mathias Jaeggi, CEO of **SeedX**, the most prominent local pre-seed VC, chaired by Prince Max.

We then engaged with Prince Max of Liechtenstein in multiple email exchanges afterwards over several weeks. He expressed substantial long term interest for strategic channel partnership with LGT and short term interest in helping us close this smaller round.In early November 2021, we had a meeting with Mr **Daniel Batliner**, the *First Secretary of the Liechtenstein Mission to the UN in Geneva*. He showed interest to know more about other interested nations and more details.

Special Case for Liechtenstein and Small Nations

The problem of hacking of their leaders and elected officials is especially dire for smaller countries like Switzerland, Malta and **Liechtenstein** - as well as inter-governmental organizations like the UN or ICRC - because they have **less capacity to control the entire supply chain to build classified mobile systems that they can trust**. So, they find themselves forced even more than others to discuss classified or top-secret matters using commercial smartphone devices, or classified phones reliant on obscure foreign technologies and suppliers. At times, smaller nations have more strategic autonomy and neutrality than larger ones to lead international impactful initiatives for the global public good and for peace, as shown by Liechtenstein led in the UN veto initiative, and Switzerland lead UN agreements for responsible cyber behavior. Plus, they often host significant financial centers that would benefit significantly from globally unique digital confidentiality offerings by their financial institutions, while also preventing its abuse to commit grave financial and other crimes.

Special Case for Liechtenstein

We drafted a special blog post: How Liechtenstein could co-lead in building a global digital infrastructure for positive systemic change.

SWITZERLAND

Summary

Since we moved to Switzerland in 2019, we've had innumerable meetings with IT security experts, NGOs, firms and governmental representatives. We hosted in Switzerland the last 3 editions of Free and Safe in Cyberspace - a conference series centered exclusively on deepening and widening consensus around the TCCB and Seevik Net. Those editions were held the 6th Edition in Geneva, 7th Edition in Zurich and 8th Edition in Geneva again, and were participated by over 25 Swiss prestigious private-sector speakers and partners, in addition to international ones.

In November 2022, we had a meeting call with **Anneick Valleau**, the First Secretary to the **Switzerland UN Mission to the UN in Geneva**. Interest has been shown in the prospect of joining the TCCB and to receive more information on the interest by other nations. As of December 6th, they stated that they prefer to participate with an observer status.

Special Case for Switzerland

The problem of hacking of their leaders and elected officials is especially dire for smaller countries like **Switzerland**, Malta or Liechtenstein - as well as inter-governmental organizations like the UN or ICRC - because they have **less capacity to control the entire supply chain to build classified mobile systems that they can trust**. So, they find themselves forced even more than others to discuss classified or top-secret matters using commercial smartphone devices, or classified phones reliant on obscure foreign technologies and suppliers.

At times, smaller nations have more strategic autonomy and neutrality than larger ones to lead international impactful initiatives for the global public good and for peace, as shown by Liechtenstein led in the UN veto initiative, and Switzerland lead UN agreements for responsible cyber behavior. Plus, they often host significant financial centers that would benefit significantly from globally unique digital confidentiality offerings by their financial institutions, while also preventing its abuse to commit grave financial and other crimes.

Engagements

In September 2018, our *Trustless Computing Association* was selected among hundreds of startups to participate in the **Fintech Fusion**, a leading Swiss Fintech startup accelerator. We quickly realized that Switzerland was the perfect place for us because of its center for neutral inter-governmental organizations like UN agencies, ICRC - and like our *Trustless Computing Certification Body* will be - and because private banks appeared to be great potential clients and channels to help us attract private investments for building Seevik Net, the first TCCB-compliant IT systems.

In June 2019, after the acceleration established in Geneva its startup *spin-in* TRUSTLESS.AI, dedicated to building the IT systems, ecosystem and initial clients of TCCB-compliant systems, bound to be eventually owned by the democratic inter-governmental *Trustless Computing Certification Body.* We moved from Rome to Geneva the headquarters of the Trustless Computing Association and established the Trustless Computing Certification Body in June 2021.

Since then we received quite a bit of interest from Swiss industry and banking associations, very large private banks and the cybersecurity expert community, who engaged as prospective clients and channels, and participated to our Free and Safe in Cyberspace series, which exceptional Swiss and foreign speakers and sponsors, solely dedicated to refining and advancing expert and stakeholders consensus of the Trustless Computing Paradigms and Trustless Computing Certification Body.

A large number of distinguished **Swiss cyber experts and representatives of Swiss institutions participated** in the 6th Edition in Geneva, 7th Edition in Zurich and 8th Edition in Geneva.

During our 8th and latest edition, last June 2021, top world and Swiss cyber personalities participated as speakers to the formal launch and establishment of the Trustless Computing Certification Body, including the former top cyber diplomat of the Obama administration, the former cyber ambassador of Netherlands, former Head of Cybersecurity Centre of the World Economic Forum, the Deputy Secretary General of the Republic of Geneva, and more.

While Switzerland has been a very active and a recognized leader in the area of cyber diplomacy, we were not able to involve any Swiss cyber NGO nor the Swiss Ministry of Foreign Affairs to participate in such 8th Edition of FSC, to meet, or show any interest. That is quite understandable given the complex ongoing political consequences of the Crypto AG and Infoguard AG affairs, starting February 13th 2020, with wide investigations were ongoing and expanding involving high officials from past administrations, and how closely our initiative is in many ways a sort of **post-Cold War version of Crypto AG**, via **new novel and better way** to reconcile privacy and global public safety in secure communication, that gave rise to the Crypto AG affair.

In fact, just 1 month before our 8th Edition in Geneva, the head of Swiss intelligence resigned over Crypto AG related controversies. For the same reasons, about 4 high level Swiss advisors joined our scientific and governance advisory boards, but then quickly resigned without plausible reasons.

Over the years, we have made the case several times in dedicated blog posts as to the huge benefits for the Swiss Federation to join among the *founding nation-state governance partners* of the Trustless Computing Certification Body as governance partner, in May 2019, Sept 2019. Twice we were published in the leading Geneva-based newspaper **Le Temps,** once about us positively and once as authors.

In posts after the Crypto AG affair revelation, in late Feb 2020, in Aug 2020, we emphasized how our initiative would great **increase the trust of foreign governments in the neutral "good offices" of Switzerland**, increase the trust of its own citizens in in **democratic digital sovereignty and democratic institutions**, and the trust of worldwide clients on Swiss made secure digital communication solutions, and increase even more the actual and perceived confidentiality (and accountability) of Swiss digital banking services.

In 2019, we signed 3 small Geneva-based asset managers as proof-of-concept partners to build our Seevik Phone/Pod Functional Proof-of-concept Device as we completed our Fintech Fusion acceleration program in Geneva.

Over the last 3 years, we moved our main operational base from Geneva to Zurich primarily to be able to engage with large private banks, as end-users and channel partners.

Swiss Private Banks

Since 2020, we've deepened our negotiations with **over 15 Group-C and Group-Head executives of 3 of the 4 largest Swiss private banks for a six-figure deal including a limited go-to-market exclusivity**, a proof-of-concept, and a possible strategic investment. This allowed us to advance our Proof-of-concept Device (video) and complete a finely-detailed 60-pager Business Case for Private Banks (available on qualified request). Credit Suisse and UBS participated publicly in our FSC events, live recorded on video, and adhered to our closed-door pre-conference with other leading Swiss public and private organizations.

Recent scandals and revelations about the use by Swiss private banks of encrypted devices (such as Omnisec, and Infoguard, the sister company of

Crypto AG) and secure messaging apps (such as Threema) highlight the need for more secure devices and a better way to reconcile privacy and lawful access.

UBS Group

In Q4 2020, we had 1 to 1 meetings (in-person or online) with Martha Boeckenfeld, UBS Group Head Digital Platforms & Marketplaces, who seems to be in a key role vis-a-vis the new CEO of UBS. Also, I spoke to Andreas Kubli. From Mr Kubli, we were introduced to UBS Group Head of Department Robert Wernli, in charge of UBS mobile device roadmap, with whom we had a detailed discussion about their status and roadmap, and how our product will fit.
Earlier in the year, we met in-person the Head Innovation Solutions & Partnerships UBS Group Chief Digital Officer, Beat Bannwart - following meetings within Q3 and Q4 2019, with his superior Head of Digital Engagement of UBS Group Chief Digital Office, **Veronica Lange**, who lead the UBS 2019 Future of Finance program and event, where UBS invited a dozen startups, including us for a close discussion.
We met Head of Innovation of UBS Global Wealth Management Martin Meyer, and UBS Group Head of Digital Corporate Bank, Christian Maehr. We followed back with a highly detailed Business Case for Private Banks, addressed to UBS business, digital, and security departments. Last August, we received initial interest and detailed questions on our documents from UBS Group Head of Digital Banking, Stefan Brunner. In May 2020, meanwhile, UBS announced a new venture capital fund for hundreds of millions to invest in fintech startups, especially in the area of digital banking and client engagement, similar to what has been done by Credit Suisse Helvetia Capital, whom we are engaging with substantial interest for our next round at the MD level.

Main contact: Veronica Lange

Julius Baer

After a 1st meeting last December with Mr. Nic Dreckmann, Julius Baer Group Chief Operating Officer, and several email exchanges with him, we have been introduced by him to JB Group Head of IT, Andreas Fahrni, whom we met last February. Last week, they reiterated their interest, yet suggested engagement with noticeable Swiss, EU, and global non-governmental institutions as a useful intermediate step, which aligns with our traction with major global NGOs for the TCCB. We had calls and initial interest in our offering and the certification body from JB Executive Director of Public Policy, Frank Wulms, JB Group Head of Innovation, Matthias Plattner after being introduced by Pascal Gentinetta, JB Managing Director and Head of Public Policy, and CEO of VAV-ABG, one of the 2 largest associations of Swiss private banks.

Main contact: Nic Dreckmann

Credit Suisse

We have engaged with Mr. Stephan Hug, Group Security Architect of Credit Suisse, and his subordinate Kai Schramm who participated as a speaker at the 7th edition of a conference series in Zurich on our proposed certification body, and adhere to a closed-door pre-conference reserved for entities to promote our new certification body. Mr. Hug recently stated progress with them would interest and appetite build in other relevant departments. We have had some initial positive feedback via email or Linkedin feedback from others at CS, including Didier Denat, Anke Bridge Haux (who is on the prize board of Swiss Fintech Awards), Thomas Saler, Claudiu Duma, Claude Honegger, Maurice Leimgruber, Thomas Gerber, Christian Katz. We also had a couple of meetings with Rolf Zengaffinen before he recently joined Credit Suisse. We also had 2 top mgmt of CS (Brent McLean, really at CS now at Universal Digital Bank, Thomas Kern, Head of Core Compliance Services Technology (and he was also Vice-President of SICTIC, the largest angel group in CH).

Main contact: Stephan Hug

Credit Suisse - Helvetica Capital

We received statements of interest for the follow-up round from Helvetica Capital ("HC"), the venture capital arm of Credit Suisse, reserved for Swiss startups (a similar VC fund by UBS Group for hundreds of millions of dollars was announced last week, reserved for fintech startups). This week, after a few exchanges and a call, we received a note from one of their four Managing Directors, who wrote to us substantiating a quite substantial interest for the later stage: *"Your concepts and vision are inspiring. However, you are too early on your roadmap for us to consider participating at this time. Your designs and ambitions seem to be very relevant. However, we do not invest in pre-seed, seed or early venture and our investment sweet spot is post POC and growth. I encourage you and your team to continue your interactions with key bank Chief Digital/Information Officers, and (U)HNWI client advisors and wish you luck. We wish you continued success and when you have POC and economic traction and require growth capital please do get back in touch with us*." In 2019, we had a call followed by a full review by Benedict Wollschlaeger who clarified how they are not authorized to invest in startups with less than CHF 500k in revenue, but how they "would appreciate if you reach out to us again once you have an initial customer base and are active in the market as we find your concept really interesting".

Raiffeisen Bank

It is a nice feeling when clients start looking for you, rather than the other way around, as when last week Rub Friedrich, Group CISO of Raiffeisen Bank reached out to me on Linkedin to have a meeting.

ITALY

Summary and Status

The current director of Italy's main cyber agency has shown much active interest over the years. His agency is exploring the possibility to participate in FSC9. Some media attention to the project is emerging. We are yet to receive any reply from the Ministry of Foreign Affairs.

Engagements

The Italian OCSI-ISTICOM (together absorbed by ACN) together with its Austrian equivalent A-SIT (similar to the German BSI or US NIST) has been our formal R&D and governance partner in R&D initiatives sent since 2016 for EU funding in H2020 Horizon program.

Since 2015, we had over 4 meeting for over 10 hours with **Roberto Baldoni**, while in his role as Director of the *CIS Italian leading intelligence and cybersecurity academic unit* and then as Deputy Director of the Italian DIS (intelligence). He is currently the Director General of the new *Agenzia Nazionale della Cybersicurezza*, as sort of new BSI equivalent, in charge of standardization, international cyber relations and more. In 2020, Baldoni gave his availability to join closed-door meetings in Switzerland to discuss with other nations joining TCCB, and also suggested an edition of Free and Safe in Cyberspace could be held in Rome.

Since 2017, the head of the Italian Cyber Command, Adm. **Ruggero Di Biase**, has been our main sponsor since 2017 within Italy MoD, and beyond, for an EDA Cat-B project with Germany.

Since 2019, we met 3 times with **Angelo Tofalo,** the *former deputy Minister of Defense of Italy*, delegated on cybersecurity. In early January, we met the former **Italian Minister of Defense**. And we met for a three times, for cofounder interest, with the **former CTO of TELSY, an "Italian strategic defense" company**, that has been making the mobile device for the most sensitive secret communications of Italy's highest officials.

In January 2022, the **former Minister of Defense of Italy**, Elisabetta Trenta, joined as member of our advisory board.

In Spring 2022, we held one meeting with a member of the newly formed Agenzia della Cybersicurezza Nazionale, headed by Roberto Baldoni.

Last November 2022, a long opinion piece by TCA Director Rufo Guerreschi was published on the leading Italian IT security porta Cybersecurity Italia, titled: Così come centinaia di migliaia di cittadini, primi ministri e diplomatici vengono hackerati sui loro telefonini. Può il problema essere risolto?. (

USA

Special Case for the US

Find here in a long blog post the all-important detailed case as to why Israel and the US will eventually join as governance partners of the Trustless Computing Certification Body - even though they'd need approval from an UN-like neutral democratic body to intercept an elected official, journalist or private citizen from a friendly nation.

Engagements

In 2018, Anthony Ferrante was among our speakers at the Free and Safe in Cyberspace edition in Berlin (but we had to cancel, as we could not afford his travel). Anthony Ferrante was from 2015-2017 the *Director of Cyber-incident Response & Director of Cybersecurity Policy at the US National Security Council of President Barack Obama*. Formerly Chief of Staff of the Cyber Division of the FBI (2014-2015). He was recently hired by Bezos to attribute the famous hack of Amazon CEO. He led in 2020 the FTI Consulting team hired by Jeff Bezos to attribute the famous hacking of his personal communications.

In July 2020, we met the Head of EU for Paladin Capital Group, the EU head of a "**state-close" Washington-based US venture capital fund** with a portfolio of $800 million set up in 2001, focused exclusively on cybersecurity, for their interest to invest in our startup. And then again in early 2021, yet they concluded they'd be interested to invest after we "have gone to market". We met another of their MDs (and former director of GCHQ) in London but focused our discussion on convincing the UK to join a co-lead of the TCCB.

Since April 2021, we met three times online 1to1 with Christopher Painter who also chose to participate as a speaker in our launch of the Trustless Computing Certification Body during the 8th Edition of our Free and Safe in Cyberspace last June 24-25 2021 in Geneva/Zoom. Currently President of The Global Forum on Cyber Expertise Foundation, he was formerly the first and **Acting Cyber Coordinator and Senior Director for Cyber Policy at the US National Security Council under Obama** (2009-2011). And then Coordinator for Cyber Issues at the US State Department (2011-2017).

In early October 2021, our startup and association were selected among hundreds of candidates to join the **Fall 2021 program of the leading cybersecurity accelerator in the USA**, MACH37, 20 minutes from the White House. Based in McLean, Virginia, only a 20-minute drive from the State Department, CIA, Pentagon, DARPA, half a dozen cyber-only VCs, and a 1-hour flight to New York.

With 300 mentors, 20 partners, and 60 one-to-one meetings planned, the 12-week MACH37 program offers unmatched access to hundreds of World-class cybersecurity mentors, talents, clients and investors, while MACH37 acquires a small number of shares.

The only reason we accepted was to increase our engagement with relevant US gov entities in order to convince them that joining the TCCB would bring to the US many more benefits than downsides. Due to covid we could not go there in person, and we had quite low remote engagement and interest with the US governmental entities.

The *Director of the Privacy Panel of the Director of the National Security Agency*, David Hoffman joined for a few weeks as a very active advisor to TCA, and then resigned without stating reason, as we started discussing engaging China as well in the TCCB.

In October 2022, the head of NSA Cybersecurity Collaboration Center, **Morgan Adamski**, connected and asked us to send a formal proposal which we did via email and in the form of a public blog post. Find here a October 2022, blog post

that makes a case for the **NSA Cybersecurity Collaboration Center** and US gov to join the TCCB. A few months ago, the US National Security Agency established the NSA Cybersecurity Collaboration Center, lead by **Morgan Adamski**, which is in charge of promoting both missions by centralizing all unclassified collaboration with private firms, foreign and domestic, as well as participation in standardization initiatives and with standardization partners.

MALTA

Engagements

In November, we met with the **Consul of Malta to San Marino**, Claudio Maria Marciano della Scala, which followed with the invitation to fly to Valletta, Malta capital, within two weeks to meet in person the current Minister of Forign Affairs of Malta, Dr Ian Borg for their potential interest to participate as governance partners of TCCB and end-users of Seevik Net, and as (co)convenors of the upcoming FSC9 and Pre-FSC9 event in Geneva. Malta citizen and professor, Joe Cannataci, and former UN Special Rapporteur of the Rights of Privacy, participated in our 3rd Edition of the Free and Safe in Cyberspace in New York in July 2016.

Special Case for Small Nations

The problem of hacking of their leaders and elected officials is especially dire for smaller countries like Switzerland, Malta and Liechtenstein - as well as inter-governmental organizations like the UN or ICRC - because they have less capacity to control the entire supply chain to build classified mobile systems that they can trust. So, they find themselves forced even more than others to discuss classified or top-secret matters using commercial smartphone devices, or classified phones reliant on obscure foreign technologies and suppliers.

At times, smaller nations have more strategic autonomy and neutrality than larger ones to lead international impactful initiatives for the global public good and for peace, as shown by Liechtenstein led in the UN veto initiative, and Switzerland lead UN agreements for responsible cyber behavior. Plus, they often host significant financial centers that would benefit significantly from globally unique digital confidentiality offerings by their financial institutions, while also preventing its abuse to commit grave financial and other crimes.

ISRAEL

Special Case for Israel

Find here **in a long blog post** the all-important detailed case as to why **Israe**l and the **US** will eventually join as governance partners of the Trustless Computing Certification Body - even though they'd need approval from an UN-like neutral democratic body to intercept an elected official, journalist or private citizen from a friendly nation.

Engagements

In 2017-2018, we connected and met once Nimrod Kozlovski, at the time the *Director Cyber Labs at Jerusalem Venture Partners* (JVP) (2013-2018), is the **largest public/private VC in Israel in the area of cybersecurity**, with investments of $1.3 billion. Mr Kowalski wanted to join as speaker for our 4th FSC edition in Berlin, but in the end could not fit it in his agenda. He introduced us to the University of Tel Aviv to hold an edition of Free and Safe in Cyberspace. Kozlovski invited us to meet him while in Israel. We have also been invited to meet the Head of Israel National CERT while there.

Since September 2019, we have been engaging Rami Efrati, former *Head the Civilian Division of the National Cyber Bureau of Israel Prime Minister's Office*, and sort of de-facto EMEA cyber ambassador, about his interest in our startup and certification body. We met originally in October 2019 in Zurich, at an event where we were both speakers, and then spoke 4 times since, last a few weeks ago. Efrati has invited us to fly to Israel for meetings he'd host to introduce us in-person to local prospective investors, cofounders and possibly gov entities. Because of Covid we postponed. We've reached out to very many in the private and governmental sector in regard to a trip to tel Aviv, where we were invited by Rami Efrati. We had a few calls but no-one was interested to follow up with a meeting in Tel Aviv.

In July 2021, we met the head of the leading Swiss Israeli cyber investor, Cyverse Capital, who also put us in touch with Mr. Pinhas Buchris, founder of Unit 8200.

During our last call a early 2022, Rami Efrati agreed to speak to his US equivalent Mr Christopher Painter (former top US cyber ambassador, speaker at our FSC8, met 3 times) about our Trustless Computing Certification Body and the possibility that Israel may be backing it with other like-minded nations. Yet, the call never materialized.

CHINA

Engagements

During 2019-2020, we extensively engaged with over 4 Swiss and global top executives Huawei as a non-western tech partner and a proxy for China.

In November 2022, we engaged via email and phone with the Secretary of the China Mission to the UN in Geneva in charge of IT standards activities, Ms. SHAO Wu, in regards to their initial interest in joining the TCCB.

UNITED KINGDOM

Engagements

One of 3 of our Exec Committee members of the Trustless Computing Association is a renowned UK citizen researcher, Jon Shamah, who has been leading our R&D initiatives since 2015.

In 2020, we had a call of interest in the Trustless Computing Certification Body by **Ian Levy**, the Technical Director of the UK NCSC, and the mastermind behind the UK lawful access mechanism proposal for secure messaging apps.

In early October 2021, Nick Kelly (our other Exec Committee member, Australian citizen) and I participated in an exclusive 30-ppl post-event dinner reserved for the top-profile speakers of the Tortoise Cyber Summit, and a few VIPs of the UK cyber scene.

During such event and meetings, we had a meeting minutes with the former director of **NCSC**, defense arm of **GCHQ**, Ciaran Martin, about UK participation in TCCB (and MD of the cyber-only US VC Paladin Capital Group) and over 1 hour with the **former director of MI6**. We also met extensively with top mgmt and partners of 3 cyber-only state-close UK VCs, including CyLon, Zetta Venture Partner, and Istari.

AUSTRIA

Engagements

Since 2016, the Austria A-SIT (the equivalent of German BSI in Italy OCSI-ISTICOM) has been our R&D and governance partners since 2016, participating formally in the submission of three EU funding proposals to build TCCB and Seevik Pod.

Since 2015 until 2019, the Chief Information Office of the Austrian Republic for about 20 years, Reinhard Posch, and former head **A-SIT,** has been our greatest sponsor since 2015 till 2019, President of our association scientific advisory board since 2015 until 2019, keynote speaker to three Free and Safe in Cyberspace editions, including the 6th edition in Berlin, held with the German Ministry of Interior and 2 German Dept of Defense.

In March 2019, substantial political changes in Austria led Posch to step down from our advisory board. He is now retired for about 12 months).