Trustless Computing Association
Rue Fendt 1,1201 Genève, Switzerland (HQs) --- Via Francesco Vettori, 39, Rome, Italy
info@trustlesscomputing.org

EXECUTIVE SUMMARY

(Revision of October 26th, 2023)

Offer to like-minded States, Intergovernmental Organizations and neutral INGOs to join as cofounder or governance partners of the Trustless Computing Certification Body and Seevik Net initiative

1. INTRO 2-PAGER

The Trustless Computing Certification Body and Seevik Net Initiative ("Initiative") is a proposal for new intergovernmental agency for secure communications and control systems for part frontier AIs and other critical societal systems. While standalone, TCCB is one of the three agencies proposed by our Harnessing AI Risk Initiative to manage AI and digital communications for the global public good.

The Initiative is aggregating a critical mass of globally-diverse states, intergovernmental organizations and neutral INGOs to build new open, neutral and participatory intergovernmental organizations to develop and certify radically more trustworthy, widely trusted and accountable end-to-end IT systems, for use in (1) confidential and diplomatic communications (Seevik Net) and (2) control subsystems for critical AIs, social media and other critical systems (Seevik Controls) - while enabling legitimate lawful access, national and international.

How: Key to achieving such trustworthiness is the application of the Trustless Computing Paradigms to ensure: (1) much higher transparency of technical designs and processes; (2) much more expert and varied security reviews in relation to complexity, (3) trustworthy procedural in-person legitimate lawful access mechanisms, and most importantly (4) higher global participation and neutrality in the standardization and certification governance processes.

Progress & Traction: As detailed 25-pages Traction Update, in addition to **nine states** and **three IGOs** interested to join the Initiative, high officials of **six states** from Africa, Asia and South America, including three Permanent Representatives of their Missions to the UN in Geneva, have signed up to participate as prospective partners in the 9th and 10th editions of the Free and Safe in Cyberspace event series we held in Geneva in Q2 2023.

So far, we've built the high-level technical, socio-technical and governance details of the certification body, and launched it in 2021 at the presence of prestigious personalities. We built a proof-of-concept device of a TCCB-compliant mobile client-side endpoint devices (video). We have designed a large part of the supply chain and ecosystem, while the rest will be completed with strategic firms from participating states.

Solution: The Initiative entails the creation, via participatory and neutral processes, of a new intergovernmental IT security certification and governance body, TCCB, and a set of initial infrastructure and ecosystems complaint with it based on battle-tested and open systems:

- a new **cloud infrastructure** and **supply chain ecosystem,** multinational, neutral and redundant
- a new **modular endpoint platform**, for use as client, server and control system for use in two domains:
    - *Seevik Net*, a **2mm-thin ultra-secure mobile device**, carried in custom leather wallets or embedded in the back of Android, iOS or Harmony smartphones (proof-of-concept device video). Via such form factor, it will initially be running alongside current hegemonic mobile devices, apps and cloud services, instead of trying to replace them.
    - *Seevik Controls*, a **base control system endpoint platform**, suitable for critical functions related to compliance systems, access controls, security monitoring, firmware upgrade and AI value systems.

Roadmap: We'll be holding several preparatory meetings leading up to the 1st Harnesing AI Risk Summit and 12th Edition of the Free and Safe in Cyberspace, in Geneva next June, 12-13th 2024. By mid 2024, we aim to select a limited number globally-diverse states, IGOs and NGOs to become the initial cofounder partners (CHF 2,000,000) of such open intergovernmental joint-venture to build and govern the 1st global democratic digital communications infrastructure. A few more will be selected to join as mere governance partners (CHF 20,000/year).

Neutrality: Given how central **neutrality** is to our Initiative, the current cyber superpowers of the **USA, China and Israel** are very highly welcome to join the Initiative as *cofounder* or *governance partners* and join FSC12 but their application will be held in suspension until all three of them will have applied (as you can read in chapter 13 of our Executive Summary, or here on our site).

The Problem with Control Systems of Advanced AIs and Social Media: Minimized and ultra-secure technical and socio-technical IT systems and standards, referred to as **high-assurance**, are utilized today to maximize the security, privacy, safety and accountability of control subsystems of critical infrastructure that are society-critical and inherently complex, such as **advanced AIs** and **social media systems**, such as firmware upgrade, access controls, security monitoring, compliance systems and values/constitution systems. While there has been an enormous increase in the foreseen global cost of failures of those systems due to accident, hacking or misuse, standards have not kept up. Even top national security agencies have shown to be unable to safeguard their most critical data, as shown by the Shadow Brokers, OPM and Vault 7 hacks.

The Problem with Sensitive Digital Communications: Heads of states, ministers, diplomats, elected officials, journalists and top scientists do not have access to interoperable computing devices and services that enable them to meaningfully protect the confidentiality of their sensitive and off-the-record communications against abuse by innumerable state and non-state hacking entities. They are therefore forced to rely only or mostly on in-person meetings to further global cooperation and diplomatic initiatives. Seevik Net Initiative aims to foster the wide availability of mobile IT systems with **radically unprecedented levels of privacy, security and accountability** of the mobile sensitive (non-classified or low-classified) human-to-human and human-to-AI communications of millions of sensitive law-abiding citizens and officials that are most targeted for profit and political reasons, from prime ministers to diplomats, from elected officials to businessmen, from journalists to activists.

Why and How Lawful Access?: Since the commercial availability of those levels of security have consistently and structurally proven to be incompatible with global public safety, the same extreme safeguards that ensure radically higher trustworthiness will be applied to applied to ensure sufficiently secure mechanisms for their **in-person procedural legitimate lawful access**, national and international, within the confines of current national and international laws.

2. TABLE OF CONTENTS

3. BRIEFING 15-PAGER

3.1. About Us

We are a project-driven NGO, based in Geneva, Switzerland, dedicated to the radical increase of the safety, liberty and democratic accountability of digital communications and AI.

Since our foundation our sole focus has been the Trustless Computing Certification Body and Seevik Net Initiative (TCCB & Seevik Net), aimed at catalyzing the creation of new open, neutral and participatory **intergovernmental organizations** to develop and certify radically more trustworthy and widely trusted end-to-end IT systems, for use in **confidential and diplomatic communications**, as well as **control subsystems for critical AIs** and other society-critical infrastructure like as social media - via battle-tested and time-proven trustless technical, socio-technical and governance systems, as specified in the Trustless Computing Paradigms.

In 2015, we started advancing TCCB & Seevik Net via a series of research initiatives and publications, and the holding of the 1st Edition of the Free and Safe in Cyberspace conference series in Brussels.

In 2019, a startup *spin-in* called TRUSTLESS.AI which attracted private investments to build initial architecture, ecosystems, proof-of-concepts and systems compliant the TCCB (closed in September 2023).

In 2021, the *Trustless Computing Certification Body and Seevik Net Initiative* was launched and established in Geneva during the 8th Edition of the Free and Safe in Cyberspace, in its preliminary form, at the presence top partners and personalities.

By Spring 2023, we held eleven editions of the Free and Safe in Cyberspace (in Geneva, Zurich, Brussels, New York and Berlin) with over 120 outstanding public and private participants. We aggregated world-class advisors and research partners, evolved the *Trustless Computing Paradigms*. Over 15 nation states and 3 IGOs have engaged in our events and constituent processes, or stated their interest for the Initiative.

On June 28th 2023, a reckoning of the **immense risks and opportunities of AI** lead us to expand our scope presenting (to the *Community of Democracies* at the UN) a Harnessing AI Risk proposal for creation of **three new global intergovernmental organizations** and participatory constituent processes leading up to them, to wholly govern AI and digital communications, one of which is the Trustless Computing Certification Body.

On October 18th 2023, we issued a call for the convening of an *Open Transnational Constituent Assembly for AI and Digital Communications* inviting a critical mass of globally-diverse nations to democratically and inclusively build such new organizations.

Next March 2024, we'll be aggregating a critical mass of pioneering nations, IGOs and vision-align entities to jump-start the constituent process of such organizations during the 12th edition of Free and Safe in Cyberspace, in Geneva.

3.2. The Problem for Elected Officials, Ministers, Diplomats and Citizens

Last November, it was revealed that the then foreign minister of the UK, Liz Truss, was spied on for months on her communications with colleagues, friends and foreign diplomats. A few days later, Ignazio Cassis, the president and foreign minister of Switzerland, the political editor of the BBC, and 100 other personalities, were revealed to have been victims of hacking-for-hire by Indian hacker gangs, via UK legal firms, via unknowns.

They are in good company. Last year alone, the sitting prime ministers of Spain and of Finland, the son of the new prime minister of Israel, the head of opposition of Greece and of Poland, in what the Rapporteur of the EU Parliament 48-strong Committee on Spyware referred to as "much, much worse than Watergate".

Same fate was suffered by the editor of the Financial Times, who suffered similar total unchecked spying. And that's just the hacks that were discovered and disclosed by the victims! Even the president of the US runs the same risks, as detailed in 2017 by the New York Times.

Such spyware are undetectable, often leave no trace, take full control of the device, by being able to read all information, and turn on the microphone at will. Not only they are spied on and blackmailed, but state and non-state hackers, domestic and foreign, but in an attempt to reduce their risk they are forced to renounce to communications and self-censor themselves, causing huge inefficiencies in their professional and private lives.

3.3. The Root Source of the Problem

Are hackers just too good? Can't those phones be made more secure?

If you are to believe mainstream media, the reason why any and all client device available on the open commercial market, including the iPhone - even with the best protection software and hardware, and managed in the most careful ways - remain so highly vulnerable to so many actors has to do with the fact that, while companies like Apple do their best, state and non-state hackers becoming are beating them at the security game.

But every year, Apple, top Android phone makers, and cybersecurity protection suite makers, introduce new security improvements. Like a mirage, decent security is never attained.

Why is that? Sure, state and non-state hackers keep significantly increasing their investments. Yet, we can make IT devices that are both reliably secure against the most advanced attackers and accessible to interception only to intended entities - as argued in this detailed academic paper by

the Trustless Computing Association, and as shown in practice by Crypto AG, the Swiss-based western standard devices for secure diplomatic communications in the Cold War.

Two are the real root causes. First, hyper-complexity and obscurity are demanded by competition for rich entertainment performance features that are required of top-end smartphones. Second, the unconfessed need to surreptitiously ensure that several powerful states can hack them at any time to prevent terrorist, enemy or adversary states.

In addition, carrying an **extra device** may be acceptable for the most targeted persons but too cumbersome for their many sensitive non-classified interlocutors.

Even the best secure messaging apps **cannot be more secure than the device** they run on, while **all smartphones and IT standards and certifications are hyper-complex** and **systematically and surreptitiously weakened by powerful states** to retain their capability to pursue criminals and adversary states, as we've learned from Snowden onwards.

Even worse, these structural processes' **surreptitious nature** and "plausible deniability" causes innumerable other entities to discover, buy, steal, or just rent access to those hacking capabilities.

3.4. The Scale of the Problem

The number of those hacked or at risk is not easy to quantify or even approximate, and this is not coincidental. Security agencies go to great lengths to **ensure that a large number of criminals and terrorists over-estimate the security of secure mobile solutions** so that they can continue their legitimate interception of them. Meanwhile, spyware and secure IT companies like Apple play along, for profit reasons.

But once in a while, some hard evidence comes around. The NSO Group, just one of a dozen spyware firms in Israel alone, testified last June to the 42-strong EU Parliament Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware that over 12,000 citizens each year are hacked via their Pegasus system. The lawsuit that Facebook has against NSO Group provides details and proofs of 1400 WhatsApp hacked worldwide in the course of just 2 weeks.

That's just the tip of the iceberg because those numbers (1) do not include dozens of other similar spyware companies that rent or sell to states and private groups; (2) nor do they include those hacked by security agencies of powerful states like the US, China and Russia; (3) nor hundreds or thousands of other entities to **discover, buy, steal, or just rent access to illegitimately hacking of high-profile users**, as shown by Shadow Brokers and Vault 7 scandals, as consequence of the surreptitious way in which powerful states ensure their "backdoor" access.

Furthermore, a vast majority of these cyber crimes go **undiscovered** for years, if ever, as they often leave no trace, as outlined above. When discovered, they are nearly always kept secret as both victims and attackers gain from keeping them **unreported**. Victims are not required to disclose. Hacking of state officials is often classified as **state secret**.

The New York Times reported in 2018 about NSO Group: "*Clients could then pay more to target additional users, saving as they spy with bulk discounts: $800,000 for an additional 100 phones.*", which brings the price to €8,000 per target (Though the price is apparently higher nowadays). And that's for the Rolls-Royce of hacking tools!

From the above, we can therefore estimate that **the number of victims are in the many hundreds of thousands** every year, while **those at risk are in several millions** world-wide.

3.5. The Initiative

The *Trustless Computing Certification Body and Seevik Net* initiative is both (1) an **intergovernmental cyber diplomacy** initiative to radically or substantially increase the confidentiality, accountability and convenience of the sensitive non-classified mobile communications among diplomats, elected officials, prime ministers, and law-abiding citizens, within and across participating states and any state; as well as (2) an **intergovernmental cybersecurity capacity-building** initiative that is bringing together a critical mass of states, IGOs and neutral INGOs to build and govern a new global digital infrastructure for sensitive non-classified mobile computing, and mechanisms for their national and international *legitimate* lawful access.

3.5.1. Components

The Initiative entails the ongoing creation of: (1) the *Trustless Computing Certification Body* (TCCB), a new **intergovernmental IT security standards-setting, certification and governance body** established in Geneva last June 2021, and (2) *Seevik Net*, an initial set of TCCB-compliant mobile IT systems, ecosystems and solutions, based on uncompromising transparency, neutrality, multilateralism; and on open source, battle-tested, globally-supported, low-level IT platforms, based on **Sel4** operating systems and **Risc-V** processors.

3.5.2. Seevik Net

Seevik Net will include a multinational TCCB-compliant set of hosting rooms, messaging apps for mainstream mobile stores, and **2mm-thin mobile devices carried initially in custom leather wallets and later embedded in the back of global commercial smartphones**. Such a new mobile form factor and product class enables such systems to **conveniently complement today's hegemonic mobile devices**, apps and services that we've all grown dependent on, instead of trying to outright replace them.

3.5.3. Unique Security Paradigms

TCCB and Seevik Net will achieve radically-unprecedented levels of trustworthiness and ensure *legitimate* national and international lawful access (A) by applying to both **extreme, battle-tested, and open socio-technical safeguards, and checks and balances,** the Trustless Computing Paradigms, that are applied to all technologies and processes critically involved in the entire life-cycle - down to fabrication oversight (TCCB Fab), CPU design and hosting room access (TCCB Cloud) and (B) via a governance model and statute that highly maximizes global **democratic accountability**, socio-technical competency, and resiliency from state pressures.

3.5.4. Precedents

There are many successful precedents of intergovernmental joint ventures or consortiums - among more than 7 states - to build and operate shared telecommunication or digital infrastructure, and not only standards, including. the European Conference of Postal and Telecommunications Administrations, (1959-, 48 states), the Commonwealth Telecommunications Organisation (1979-, 52 countries), the African Telecommunications Union (1995-, 55 countries), the Asia-Pacific Telecommunity, APT (1979-, 20 countries), the International Mobile Satellite Organization, IMSO (1982-, 150 countries), the International Telecommunications Satellite Consortium, INTELSAT (1964-, 149 countries), South American Telecommunications Network, SATNET (1988-, 8 countries). On May 3rd, 2023, several EU countries and firms, and the EU announced they'll be jointly building and managing building a low-orbit satellite internet infrastructure for sovereign communications.

Our initiative aims to realize **a sort of "2.0, multi-governmental, mobile and ultra-secure" version of the Minitel**, the digital platform created by the French government in the 80's, that became a bigger success than similar EU initiatives, constituting by 1988 a digital ecosystem with 3 million users of Minitel terminals, a dozens of private and public compliant terminal makers, and thousands of private and public services and apps.

In a way, we are building **a sort of "post-Cold War version of Crypto AG"**, the de-facto global standard and state-of-the art for secret and diplomatic digital communications during the Cold War, that turned out to be controlled by only two states. As opposed to the original one, this one will be based on open democratic multilateralism, uncompromising transparency, and an ultra-resilient

procedural front-door instead of Crypto AG **technical back-door** model.

More importantly, our model stands in contrast to the current "**bug-door**" model, whereby even the most targeted law-abiding individuals like heads of states are forced, for their sensitive non-classified communications, to rely on hegemonic mobile devices like iPhones and Android devices and the strongest IT security standards that are "somehow" always chronically vulnerable to hacking by innumerable entities via widely available state-grade hacking tools.

What about precedents of important inter-governmental initiatives that have been early on NGO-driven? A few decades ago a number of NGOs had a key role in the creation of the **International Criminal Court** through the Coalition for the International Criminal Court, and especially the World Federalist Movement as the Convenor of such a coalition. The Rome Statute was signed in Rome, the city where our initiative was born and where our operations are mostly based.

3.5.5. Funding so far & Control of TCA and its startup spin-in TRUSTLESS.AI

The Spin-in Model: relationship among TCA and its startup spin-in

TCA is currently controlled by TCA founder and Exec. Director Rufo Guerreschi (Italian), Roberto Savio, and Davide Cova. An expansion of the board is foreseen in the end of 2023, with the addition of a globally representative spiritual/religious representatives of all the world's most common faiths and creeds, including atheists and agnostics.

As stated in the current its statute, TCA will be rename itself into TCCB, and enact a **permanent intergovernmental democratic governance** as specified, "*within three months after the TCA have received funding in excess of CHF 150,000 or its startup spin-in TRUSTLESS.AI will have received in excess of CHF 700,000*", - and once 7 states will have joined as cofounder partners of the TCCB and Seevik Net Initiative.

While TCA has been building the TCCB, its startup *spin-in* TRUSTLESS.AI has been building Seevik Net. As specified in *spin-in* agreement among the two organizations, once TCA/TCCB has moved to its permanent governance it acquires an option to buy 100% of the spin-in shares at the price of CHF 20 million. This spin-in model has enabled the leveraging of private sector innovation, while **ensuring a highly democratic multi-national long-term control** (see precedents in the German DoD BWI project).

Funding and Control so far, and exit of private

Since its inception, funding for the Initiative, TCA and the startup spin-in, have come from cash and "sweat-equity" contributed by a number of entities. A total of € 50,000 over 3 years came from the European Union digital innovation promotion agency EIT Digital. About CHF 350,000 and 6 unpaid man-years were contributed by Rufo Guerreschi. A number of advisors, angel investors, a Swiss startup cofounder, advisors and team members have invested over 4 man-years of "sweat equity"

and over CHF 250,000 in cash. Rufo Guerreschi owns 100% of the shares of the startup spin-in, while about 35% of the share rights have accrued to those other contributors.

As per the intention of the majority of shareholders of TRUSTLESS.AI, to be formalized in MoU with cofoudner partners of the Initiative, all of its shares and shares rights holders will be "bought out" by TCA, all at once, for CHF 6 million, via funds that will be contributed by the next 3 states that will join as full *state partners* after the initial 7 *state cofounder partners*, so as to **remove any long-term private influence**, and give completion to the spin-in model. Rufo Guerreschi will remain as honorary chairman of the Initiative for 2 years, without a decision-making role.

3.6. Use Case 1: Diplomats, Ministers and Parliamentarians

Increasingly states and IGO, such as the Spanish, German and EU parliaments - for their **internal** low-classification or non-classified (but sensitive) communications - mandate their staff to use specific **enterprise/state** secure messaging apps and hosting (e.g. Element/Matrix, Wire, Threema, Wickr), and/or protective software like Crowdstrike, and in some cases "secured" commercial phones - for **external** non-classified but sensitive communications they are increasingly suggested or mandated to use specific **consumer** secure messaging apps (e.g. Signal or Telegram).
Yet, as we've learned, no app **can be more secure than the device it runs on**, and protective software has been proven to be very insufficient, as shown by recent hacks of Finnish diplomats.
Seevik Net will especially benefit officials and staff of **prime ministers, parliaments, and ministries of foreign affairs and defence** as these are struggling with the huge scale and pervasiveness of illegal hacking of their personal smartphones, when the overwhelming majority of those **professional and personal associates** need to speak to about sensitive (albeit non-classified) matters do not have their classified phones or apps, or have incompatible ones. In such use cases, high-level and sensitive governmental officials and their closest professional and personal associates will be mandated to use Seevik Net devices.

3.7. Use Case 2: Private Organizations and Citizens

Seevik Net will initially be targeted to the **sensitive mobile communications of millions of law-abiding citizens**, elected officials, diplomats, businessmen journalists - and their institutions and organizations - that are most targeted for profit or political reasons. Their hacking is of great detriment to democracy and national security and the economy. But our aim is for nearly everyone to be able to afford a TCCB compliant device as it reaches mass scale and per unit costs go down as much as $200. Private market demand is very significant. Pre-Covid surveys by UBS and by Northern Trust showed that the 16 million wealthiest persons in the World regard **cybersecurity as their n.2 concern** and family offices, the small banks of the super rich, consider it their n.1 concern.

3.8. Lawful Access Requests: National and International

The ***TCCB Cloud*** is a set of holistic socio-technical system, supply chain and operational requirements for a **private cloud system**, primarily consisting of a mix of nodes running in a multi-national network of *TCCB Hosting Rooms* as well as on TCCB-compliant client devices.

It is an integral and essential part of the Trustless Computing Paradigms, the binding socio-technical requirements of IT systems complaint to the TCCB, that complements client-side requirements that a given IT systems ensures **radically unprecedented levels of confidentiality and integrity,** while concurrently ensuring prompt, safe, in-person and secure ***legitimate*** **lawful access, national and international**.

The ***Seevik Cloud*** is instead the name of an initial private cloud compliant to TCCB Cloud requirements, that will be built and enacted as part of *Seevik Net* by TCA and the Cofounder Partners of the TCCB and Seevik Net Initiative, comprised of no more than 7 globally-diverse states, 2 IGOs and 2 neutral INGOs.

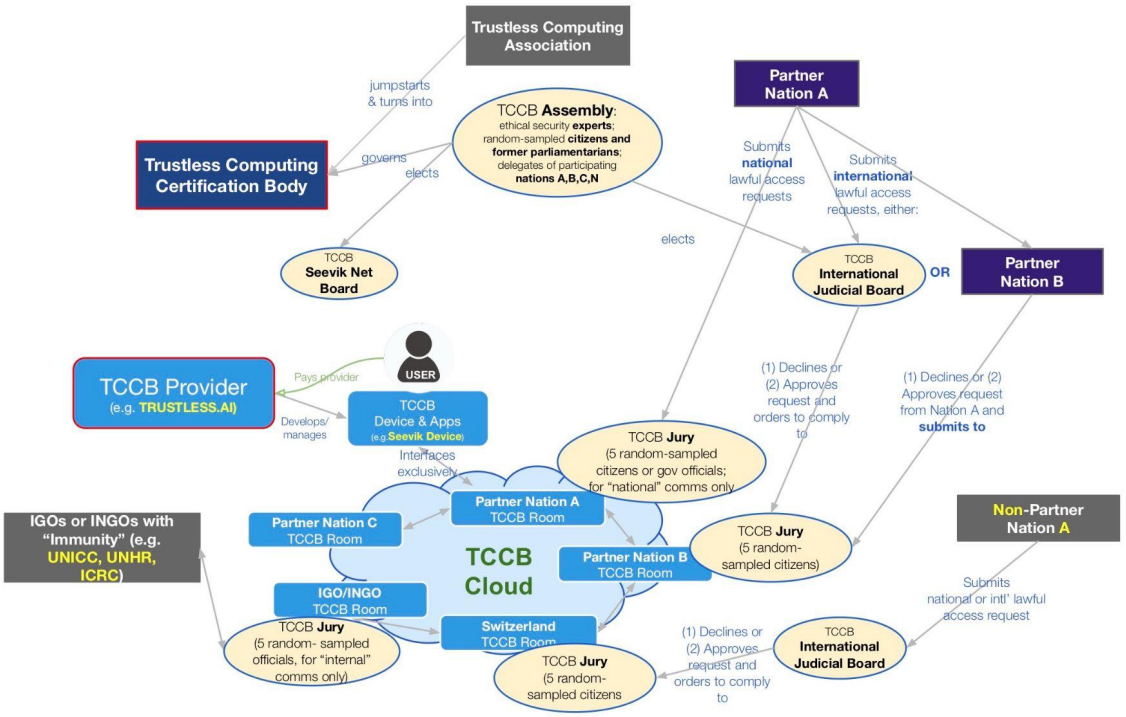
While extensively implementing open source and battle-tested decentralized, peer-to-peer and **end-to-end** protocols and technologies, all Providers of TCCB-compliant IT systems will be required to mandatorily store all sensitive user data and code in such a TCCB-compliant private cloud system, which will be comprised of at least 4 TCCB hosting rooms, that will:

- (A) be located in at **least 4 different states that are Cofounder Partners of the TCCB and Seevik Net Initiative and are part of at least 2 different military/intelligence alliances**, one of which include the (somewhat) neutral state that will be hosting the headquarters of TCCB.
- (B) deploy state-of-the art technologies and human processes, substantially exceeding the highest military, civilian and banking international standards and practices;
- (C) use only TCCB-compliant endpoints for its servers' hardware and software, and for their physical access management systems and devices;
- (D) are accessible only physically, and after the explicit approval of **5 or more random-sampled citizens** of the host country and a local attorney, to manage for national and international lawful access requests.

While TCCB and one TCCB Hosting Room the will be subject to the laws of **Switzerland** (or possibly other hosting state that will offer more protection, autonomy and possibly some immunity status) each TCCB Hosting Room will be (of course) subject to the laws of the states where they'll be located. In some cases, this will mean having to comply with governmental executive decisions without any meaningful judicial oversight.

States that join as *Cofounder Partners* may choose to locate a TCCB Hosting Room in their territory and, together with *Governance Partners*, are guaranteed the ability to submit a lawful access request directly their local TCCB Hosting Room (for "local" requests) or to the TCCB (for "international" requests). These will be processed according to the TCCB Cloud requirements, as overseen by the TCCB and the host states, as follows:

1. If the access request is by the local government - and it is in reference to (a) personal computing of one of their citizens, or (b) communications between their citizens, or (c) between foreign citizens while both present in their territory - then such request will be:
    1. vetted by a **TCCB Jury** in their respect of judicial "due process" (not in the evidence) which will act as both *citizen-jury* and *citizen-witnesses*. The jury will be made of 5 or more local random-sampled citizens (and 2 possibly random-sampled parliamentarians), plus a vetted local attorney. Every 3 months, 15 are sampled and instructed. When the need arises, 10 are randomly called, as soon as 5 arrive, the process can begin.
    2. If the request is approved by the TCCB Jury, a specific process will be followed to allow access to specific users' data and/or keys according to the approved part of the request.
    3. For requests that are for communications among certain level of state officials of a certain high levels, it is faculty of the host states to specify in full autonomy a different process that may include, for example, 5-random sampled state officials or elected officials (or even 5 members of the ruling royal family) and just communicate it to TCCB.
2. If the access request is by a foreign government, - and its is **not** in reference to (a) personal computing of a local citizen, or (b) communications between local citizens, or (c) between foreign citizens while both present in their territory - then such request will be:
    1. vetted by a **TCCB Judicial Board**, made of 15 recognized experts in international law, civil rights, and public security, who have been, sometime in the past, elected or appointed to high offices, such as a leading international court or the highest court of a large democratic nation. Deliberation by such members will happen remotely using TCCB-compliant devices to provide the utmost confidentiality safeguard of the submitted evidence being analyzed. The Board decision will assess the "*legitimacy"* for each request by evaluating the provided and autonomously-acquired evidence to determine to what extent the request (A) complies with the national legislation where TCCB is based (Switzerland currently), and (B) it maximizes:
        1. Compliance to and promotion of international civil rights and civil rights norms.
        2. Promotion and protection of international security and safety.
        3. Complies to laws and constitutions of the jurisdiction of the requesting state or international institution, and that of the user that is the target of the request.
    2. If the request is approved in full or in part by the TCCB Judicial Board, then the TCCB Jury will be instructed and ordered to allow access to specific users' data and/or keys according to the approved part of the request.



More details on the TCCB Cloud are available on a dedicated page on our website at the chapter *"Detailed TCCB Cloud Requirements"*.

3.9. Our Offer to states, IGOs and neutral INGOs

We are selecting **no more than 7 globally-diverse states, 2 IGOs** (e.g., EU, UN agencies, Arab League) **and neutral and neutral INGOs** (e.g. ICRC, Amnesty International) to become *cofounder partners* of the TCCB and Seevik Net initiative.

Cofounder partners will fund the entire initiative, via an investment of **€2 million** each in order **take full joint intergovernmental control of the entire initiative**, including the TCA/TCCB, the startup spin-in TRUSTLESS.AI, the Seevik Net infrastructure, and receive several limited-time exclusive rights and privileges, except for committing to later invite other states on equal terms and with aim at maximizing global-diversity. Participating INGO's and IGOs receive a 50% discount.

Cofounder partners will enjoy temporary special privileges, including:

1. **receive 900 TCCB-compliant mobile device units,** in the Seevik Wallet form factor.

2. be able to establish a TCCB-compliant **hosting room in their territory** for the lawful access of domestic communications of Seevik Net users.

3. **participate in the development rather than just oversight** of Seevik Net, with their own national experts, firms and agencies ("*Trust cannot be added to integrated circuits after fabrication*" wrote the US Defense Science Board in 2005. As an old say goes, you have to "*be there when the sausage is made*")

4. **participate in the initial TCCB constituent governance** that will give shape to TCCB and Seevik net statute, and the first operational version of the *Trustless Computing Paradigms*;

5. private and public **entities headquartered in their territory will have exclusivity** for the first 12 months to (a) purchase TCCB-compliant IT systems and (b) submit IT services for TCCB certification.

We are also selecting no more than 5 states as *Governance Partners*, at the cost of **CHF 20,000** with full right to participate in the TCCB governance, but none of the other rights lesser rights and privileges. Up to 3 states will be selected as *observer state partners* at the cost of **CHF 10,000** per year.

For more read below the "*OUR OFFER for States, IGOs and Neutral INGOs*" chapter below.

3.9.1. Engagements Steps

For Cofounder Partners

- 1) Signs *Terms of Participation to the FSC10 workshops in Geneva in May 2023*
    - States the level of interest, and sets the confidentiality terms.
    - Fees: ***free-of charge***
- 2) Signs *MoU of Option to Join as Cofounder Partner of TCCB & Seevik Net*
    - Reserves an option for until the date whereby 11 entities will have signed MoUs for cofounder or governance partnership.
    - Fees: **CHF 20,000**, "one-off", to be paid within 2 weeks of when 3 others have signed the same or similar. The first state to sign the *Cofounder Partneship MoU* receives a 50% discount on such a fee, while the 2nd and 3rd receive a 25% discount.
- 3) Co-signs a non-binding *Preliminary TCCB & Seevik Net Governance Partners and Cofounders Accord*.
    - The status as *Cofounder Partner* is formalized, with to-be-determined clearly-specified decision-making rights states in revised Initiative statutes.
    - Fees: **CHF 2,000,000**, "one-off", to be paid within 6 weeks of when notified that 3 other *governance or cofounder partners* will have signed the same or similar Accord. Eventual future financial contributions, in whatever form, by partner states will be partly adjusted in respect to GDP, so that the state with the largest GDP will contribute 2 times as much as the state with the lowest, while the amount contributed by the states in between will be determined through *linear interpolation* between those amount.

For Governance Partners

- 1) Signs *Terms of Participation to the FSC10 workshops*.

    - States the level of interest, and sets the confidentiality terms.
    - Fees: **free-of charge**
- 2) Signs *MoU as Option to join as Cofounder Partner of TCCB & Seevik Net*
    - Reserves an option for until the date whereby 11 entities will have signed MoUs for cofounder or governance partnership.
    - Fees: **CHF 5,000,** "one-off", to be paid within 2 weeks of when 3 others have signed the same or similar. The first state to sign the *Governance Partneship MoU* receives a 50% discount on such a fee, while the 2nd and 3rd receive a 25% discount.
- 3) Co-signs a non-binding, preliminary *Cofounder and Governance Partners Accord*.
    - The status as *Governance Partner* is formalized, with to-be-determined clearly-specified decision-making rights states in revised Initiative statutes.
    - Fees: **CHF 20,000**, per year, to be paid within 1 week of when notified that 3 other *governance or cofounder partners* will have signed the same or similar Accord. (Fee will be CHF 10,000 instead for *Observer Governance Partners*)

3.9.2. Join our Events to Learn about the Initiative

To learn more, help us improve it, join other interested prospective partners in preparatory meetings and workshops we'll hold during the 11th Edition of the Free and Safe in Cyberspace, in our headquarters in **Geneva/Zoom next May 18th, 24th and 31st (15-17)** for *FSC11 Preparatory Meeting* and for the FSC11 Main Workshops (9-12 and 14-18) on **June 7th, 2023**, as well as 1 to 1 meetings in Geneva on the same days,

3.10 Value Proposition for States

1. The participant state would radically increase both (A) the **protection of legal communications** and (B) the **accountability of illegal communications** for its most sensitive law-abiding citizens and organizations, including elected officials, journalists, business leaders, activists, as well as their reference organizations. It will radically increase protection from politically-motivated extortion, blackmail, manipulation, or profit-motivated extortion, ransomware and trade secret spying.

2. The participant state would **increase the certainty, integrity, and attribution capability of your security agencies' when investigating users of TCCB-compliant systems, foreign and domestic, as opposed to other IT systems**.

    In fact, while their security agencies would "by definition" lose the arbitrary capability to hack into TCCB-compliant systems (which will be designed with the stated purpose of being impregnable to such acts) - when legitimately authorized - they will: (A) have higher assurance of prompt access, without the risk of "going dark" or being unable to hack, and independently from the availability to assist of other states or firms; and (B) obtain more solid

and forensic-friendly evidence that is much more reliable, and that will be accepted by the highest state courts, unlike that obtained via targeted hacking which does not stand in the highest courts in Germany and France

3. The participant state would **be recognized by other states as a leader in promoting peace and fair and effective global cooperation** by participating in building nothing less that a post-Cold War version of Crypto AG, the de-facto global state-of-the art for sensitive and diplomatic digital communications during the Cold War, that turned out to be controlled by only two states.

   As opposed to the original one, it is based on open democratic **multilateralism**, uncompromising **transparency**, and an ultra-resilient **procedural front-door** instead of a technical back-door - and available to all in a highly convenient way. Beyond diplomats, it'll be available to millions of targeted law-abiding persons and organizations with portability and convenience via 2mm-thin standalone devices, carried inside custom leather wallets or in the back of future smartphones, and then other form factors.

4. By leveraging **unique levels of transparency and intergovernmental cooperation** at all levels and stages - the initiative aims to (1) achieve radically unprecedented levels of actual and perceived trustworthiness in personal mobile computing and communications of citizens and elected officials anywhere in the World; (2) advance **digital sovereignty radically and concurrently at the state, international and citizens' levels** and (3) enable and foster **confidential, fair and effective global dialogue** within and among states.

3.10.1. Special Advantages for Mini, Small and Medium-sized States

The problem of hacking of their leaders and elected officials is especially dire for smaller countries like **Switzerland, Malta or Liechtenstein** - as well as intergovernmental 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 states 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 confidentiality offerings by their financial institutions, while also preventing its abuse to commit grave financial and other crimes.

Micro, small and medium-sized states would especially benefit from participation via a **decisive boost in their cybersecurity capacity-building** for their most critical IT systems. As opposed to a

handful of states, they are not able to build and control within their territory, or even with regional allies, complete systems and their supply-chains when IT security is defined as that of the weakest link. In particular, capabilities to control the design and manufacturing of the critical low-level systems, like CPUs, operating systems, and the manufacturing of the integrated circuits, makes it impossible to autonomously ever achieve digital sovereignty.

By being able to involve their our IT and cybersecurity experts in all phases of the architecting, design, testing and certification of the solutions - and the use of open-licensed and patent-unencumbered critical technologies - they'd be able to expand they **greatly expand over the next few years their internal national knowledge base and talent pool**, in order to be able to create derivative systems and certification schemes for their own internal national needs, for non-classified as well as classified systems.

3.10.2. Special Advantages for the EU and/or EU Member States

Our TCCB is meant to inspire amendments or extensions to new regulations that have been proposed to regulate spyware and to created certifications to ensure much more secure devices - in the EU, EU states and around the World - and **fill the gap** in the meantime, while planning to be "downward compatible" with them.

Our initiative aims to complement the *EU Cyber Resilience Act* and *EU Media Freedom Acts* to cover the need of the sensitive (yet non-classified) personal computing of the 1% most targeted law-abiding citizens and elected officials - and their close personal and professional associates - such as those hundreds of thousands hacked and hackable by NSO Group and similar tools.

For participating EU states, TCCB and Seevik Net will allow them to **move ahead decisively and without hesitation** to (1) adequately protect the security, privacy, accountability and democratic nature of the sensitive communications and social interactions of their most sensitive officials, institutions and citizens; while at once (2) **leading by example** to positively influence the debate of newly proposed EU Regulations and Acts that are supposed to solve the same problem (e.g., EU Cyber Resilience Act, EU Media Freedom Act, EU Cybersecurity Act).

3.11. Our Vision 2030

Increasingly, with growing scale, TCCB-compliant mobile IT systems and mobile device will be made more powerful, secure, cheaper, and with more 3rd party apps, so as to be affordable to any ordinary citizen, and become **embedded in governmental Kiosks placed in public offices and pharmacies** for the offering of digital public services in ways complaint to national and international requirements (e.g. EU eIDAS2) while largely exceeding those requirements.

Seevik devices can also become citizens' **personal trust hub and interface** , wearables, VR headset, and advanced AI services. TCCB will gradually be extended to cover other critical societal

systems, starting from social media feed systems, conversational AIs like ChatGPT, and beyond. Read more about our vision and mission on our website.

3.12. More Information

A **40-page *Executive Summary*** follows below details the benefits, the terms and conditions, a list of current public and private R&D partners. A *Milestones and Partners* chapter, below, summarizes **the interest shown so far by multiple prospective states, IGOs and neutral INGOS**, **including over 14 states**. After NDA it is also possible to access a confidential 25-page *Detailed Traction Update* detailing of our engagements with those prospects. A more graphic 33-page ***Slide Deck*** is available for download here.

4. MORE ON THE SCALE OF THE PROBLEM

The number of those hacked or at risk is not easy to quantify or even approximate, by design. Security agencies go to great lengths to **ensure that a large number of criminals and terrorists over-estimate the security of secure mobile solutions** so that they can continue their legitimate interception, while spyware and secure IT companies like Apple play along, for profit reasons.

But once in a while, some hard verified data comes around. The lawsuit that Facebook has against NSO Group provides details and proofs of 1400 WhatsApp hacked worldwide in the course of just 2 weeks. The NSO Group, just one of a dozen spyware firms in Israel alone, testified last June to the 42-strong EU Parliament Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware that over 12,000 citizens each year are hacked via their Pegasus system.

But those numbers (1) do not include dozens of other similar spyware companies that rent or sell to states and private groups; (2) nor do they include those hacked by security agencies of powerful states like the US, China and Russia; (3) nor hundreds or thousands of other entities to **discover, buy, steal, or just rent access to illegitimately hacking of high-profile users**, as shown by Shadow Brokers and Vault 7 scandals, as consequence of the surreptitious way in which powerful states ensure their "backdoor" access.

Last October Kaspersky declared it had found and “fully deconstructed” the most advanced German and UK spyware, FinFisher, enabling them to fully re-use it. The same could have been done by others. Already ten years ago powerful state security agencies like, and to a lesser extent some semi-private spyware companies, had capabilities to turn targeted surveillance into a scalable enterprise via systems and programs like the NSA FoxAcid and NSA Turbine.

Furthermore, a vast majority of these cyber crimes go **undiscovered** for years, if ever, as they often leave no trace, as outlined above. When discovered, they are nearly always kept secret as both victims and attackers gain from keeping them **unreported**. Victims are not required to disclose. Hacking of state officials is often classified as **state secret**.

Apple declared in 2021 that the attacks should not worry because exploits: “*cost millions of dollars to develop, often have a short shelf life, and are used to target specific individuals. While that means they are not a threat to the overwhelming majority of our users,the overwhelming majority of our users*”. Their use of the term “overwhelming” is compatible with hundreds of thousands of devices hacked, which would amount to 0.01% of the 1.5 billion iPhones out there.

The New York Times reported in 2018 about NSO Group: “*Clients could then pay more to target additional users, saving as they spy with bulk discounts: $800,000 for an additional 100 phones.*”, which brings the price to €8,000 per target (Though the price is apparently higher nowadays). And that’s for the Rolls-Royce of hacking tools!

From the above, we can therefore estimate that **the number of victims are in the many hundreds of thousands** every year, while **those at risk are in several millions** world-wide.

As opposed to what security agencies, smartphone makers and uncritical media want us to believe **those most at risk have known the truth for some time now**. Pre-Covid surveys by UBS and by Northern Trust showed that the **16 million wealthiest persons in the World and family offices regard cybersecurity as their n.2 or their n.1 concern**, respectively. There is nothing money can buy.

Paradoxically, on the other hand, legitimately authorized judiciary of democratic states are often unable to enforce legal intercept orders on such smartphone - as it happened with the deleted encrypted messages of US president's secret service detail on Jan 6th 2021 and leaders of a top swiss private bank - because the best spyware is unavailable to them, or is limited in use forstate security cases - while criminals may have acquired such evidence before its deletion for use in blackmail.

It is nothing short of a **public security and democratic emergency,** as well as a huge market demand.

5. PROPOSED SOLUTIONS: Why neither single states, nor the EU or the UN can solve it alone.

More than any other governmental institution around the World, the EU is attempting to solve this huge problem by **regulating spyware** and **setting requirements and certification for more secure mobile devices**. Yet, the current approaches and EU's own institutional constraints make it very unlikely it'll be able to truly tackle this problem. A recent draft report by the EU Parliament PEGA Committee on Spyware, in line with recommendations by leading human rights neutral INGOs, calls for urgent national and EU **regulation of spyware**.

This is needed and useful, but will inevitably have very limited effect. Due to the huge technical, operational and jurisdictional complexities of spyware - and the hyper-complexity and chronic vulnerability of even the most secure smartphones - such regulations (a) would be very hard to enforce, (b) attribution of hacks would remain extremely difficult, and (c) law-abiding officials and citizens would anyhow remain hackable by innumerable entities located outside the regulators' jurisdiction, while law enforcement and intelligence would loose a critical tool to fight crimes and terrorists.

The recently announced EU Cyber Resilience Act is not going to even remotely protect millions of highly targeted individuals because:

1) It does not require full **transparency** of source designs, and **extreme levels of security review in relation to complexity** of all critical processes, even down to chip fabrication oversight ("security is the weakest link"!)
2) It does not face the "elephant in the room", i.e. the needs of **legitimate lawful access**, by having a transparent international “in-person” procedural mechanism to manage requests by security agencies,state, EU, allied and beyond.
3) High and ultra-high levels of assurance **cannot be certified ex-post**, i.e. without assessing all assess technology, process and persons critically-involved **ex-ante** in the supply chain and lifecycle, so as to estimate the probability of undetected willful or accidental vulnerabilities - as well as the training and incentive placed on end-users.

In addition, the EU Council has already suggested changes to enable EU states to make devices that are too secure illegal on "national security" grounds. The *EU Media Freedom Act* that is also not remotely going to protect journalists in the EU as pointed out recently by the EDPS.

Hopefully, EU member states and parliamentarians will succeed in amending the Cyber Resilience Act to add much more stringent security **requirements for the most vulnerable users**, in a mandatory or voluntary way. But unfortunately, the EU unanimity decision-making, combined with the lobbying power of Big Tech and powerful states, will likely obstruct such efforts, as we've seen before for privacy Acts.

Since, as discussed above, states, the EU and the UN cannot solve this problem, we propose - as a fail-safe initiative to be brought forward concurrently with policy efforts within those institutions - that some EU member states, parties and parliamentarians - while trying to get the needed amendments approved - move ahead together with non-EU globally-diverse like-minded to **build and govern the certifications and compliant IT that are needed** to shape a fair, safe, effective and participatory global digital sphere for elected officials, diplomats and all citizens.

6. OUR SOLUTION: The Trustless Computing Certification Body and Seevik Net Initiative.

This section assumes you have read the 5-page Summary at the start of the document.

Last June 2021, in Geneva, we established the *Trustless Computing Certification Body,* **a new intergovernmental democratic IT security certification body** to guarantee both radically-unprecedented security and privacy as well as “in-person” procedural *legitimate* lawful access for sensitive yet non-classified communications.

Concurrently, via its startup spin-in, TRUSTLESS.AI, since 2019, we are building an initial TCCB-complaint private cloud, mainstream mobile app and **2mm-thin mobile device** - embedded in custom leather wallets (video animation) or in the back of Android smartphone (video of the Seevik

Phone Proof-of-concept device) - that aims to far outcompete in both security, convenience and accountability even the best-protected iPhones and the best commercial *cryptophones*.

We achieve radically-unprecedented levels of trustworthiness by (A) applying to both **extreme, battle-tested, and open** (technical and organizational) **socio-technical safeguards, and checks and balances** - the Trustless Computing Paradigms - that are applied to all technologies and processes critically involved in the entire life-cycle - down to fabrication oversight, CPU design and hosting room access and via (B) a governance model and statute that highly maximizes global **democratic accountability**, socio-technical competency, and resiliency from state pressures.

The initial version of Seevik Net will derive from the **hardening and integration of battle-tested open-source IT** stacks, via a resilient consortium of carefully-vetted technical partners in suitable states, which will include (a) seamlessly **portable 2mm-thin client devices**, carried in custom leather wallets (video) or embedded in the back of smartphones (video), with special 3rd party apps; (b) **interoperable messaging and social apps** for mainstream stores, (c) a **custom private cloud**, made up of decentralized nodes running on TCCB client devices, and multi-national network of hosting rooms according to our TCCB Cloud process.

TCCB Cloud process requires that all sensitive data and code is stored in **4 TCCB hosting rooms in states part of at least two different military/intelligence alliances**, and approval by a ***TCCB Jury* of 5 random-sampled citizens** - for a local lawful access request - and by such jury executing decision by an international ***TCCB Judicial Board*** - for international ones. The initiative will eventually be opened for joining by all states on a fair and equal basis.

TCCB is a new standards-setting and certification body that will certify IT services for human communications aimed to ensure both (1) **radically-unprecedented levels of confidentiality, integrity and democratic control** and concurrently (2) safe “in person” international ***legitimate* lawful access** mechanism. Meanwhile, via our *spin-in* we are building an initial set of IT systems - minimal but complete and mandatorily interoperable - that will constitute **Seevik Net**, a global democratic human computing sphere and platform, alongside existing dominant platforms.

TCCB aims to create and regulate a **new global democratic digital public sphere** - with apps, cloud, and devices, that run parallel to mainstream ones and over the open Internet. TCCB and Seevik Net will **radically increase** citizens’ **privacy, security, and democratic control** of their sensitive digital lives; **defend democratic institutions** from the rise of authoritarianism, at home and abroad, inside and outside institutions; and **foster fair and effective dialogue and understanding, within and across states**.

6.1. The Spin-in Model: a Uniquely Democratic Innovation Model

An initial set of open-licensed TCCB-compliant systems, devices and services, Seevik Net, is being built through the startup "spin-in" TRUSTLESS.AI that the Trustless Computing Association, created

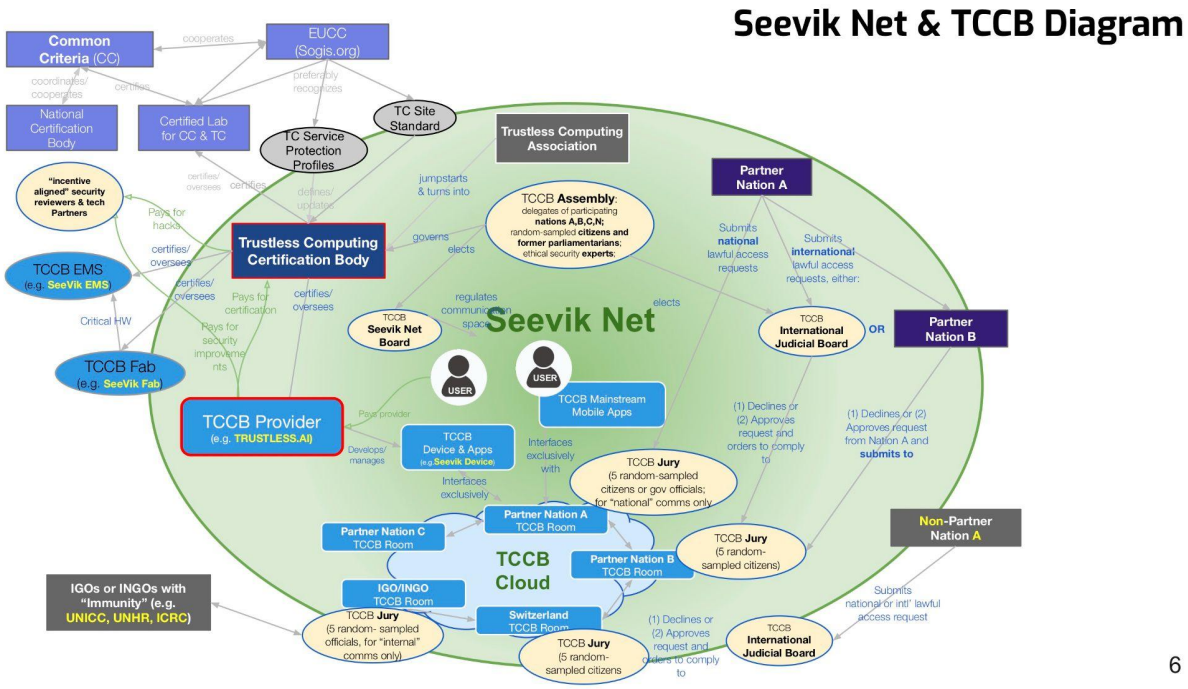
in 2019. According to the spin-in model, a signed agreement between the two entities ensures that the **startup spin-in TRUSTLESS.AI and Seevik Net will be mandatorily owned and controlled by the TCCB** - via an option by TCCB to buy 100% of its shares at precisely-set non-speculative conditions - to leverage private sector innovation while ensuring a highly democratic and multi-national long-term control of such a sensitive transnational democratic infrastructure, such as the BWI project of the German defense ministry, but multi-national.

6.2. Holistic Architecture: Ecosystem, Governance, Lawful Access

The initial version of Seevik Net will derive from the **hardening and integration of battle-tested open-source IT stacks**, via a resilient consortium of carefully-vetted technical partners in suitable states, which will include:

- (a) seamlessly **portable 2mm-thin client devices**, carried in custom leather wallets (video) or embedded in the back of smartphones (video), with special 3rd party apps;
- (b) **interoperable messaging and social apps for mainstream stores**;
- (c) a custom private cloud, made up of decentralized nodes running on TCCB client devices, and a multi-national network of hosting rooms according to our TCCB Cloud process.

TCCB Cloud process requires that all sensitive data and code is stored in **at least 4 TCCB hosting rooms in participant states part of at least two different military/intelligence alliances**, and approval by a TCCB **Jury made of 5 random-sampled citizens** of the host state - for a state lawful access request - and by such jury executing decision by an international ***TCCB Judicial Board*** - for international lawful access requests.



6.3. Relationship to other International & EU Standards

The TCCB initially conflates the standards setting, certification and certification assessment in a single body. By operational launch, estimated in early 2024, the TCCB governance (ultimately accountable to its Assembly) will govern a TCCB Standards Setting Body, a TCCB Certifications Setting Body, and license several Common Criteria labs for independent certification of TCCB compliant IT systems and services.

TCCB will certify systems that at once comply with the highest assurance levels of the EU digital identity and transaction standard, **eIDAS 2.0 High**, while offering levels of confidentiality and integrity of human computing radically beyond state-of-the-art. TCCB will start as a high-level but binding certification framework, and quickly move towards a thoroughly detailed certification scheme akin to **Common Criteria**.

While free-standing as an intergovernmental initiative for voluntary certifications, TCCB will be complementary, synergistic, and inspirational for existing, upcoming and future EU and UN promoted cybersecurity certifications.

To that end, it will also be proposed as a “schema” within the **EU Cybersecurity Certification Framework** and as a new initiative under **UN International Telecommunication Union** (ITU-T) processes. It will also promote future downward compatibility in respect to EU Secret and **Common Criteria EAL4-6** for future use in advanced governmental sectors.

Initial TCCB target domain will be that of human transactions and communications that are non-classified from sensitive to ultra-high requirements of confidentiality and integrity. Initially, the target users of TCCB-compliant IT services will be millions of law-abiding highly-targeted and politically-exposed persons and organizations, such as investigative journalists and news organizations, politicians and political parties, private banks, family offices, exposed enterprises, and neutral INGOs. At a later stage, it will expand to use cases requiring also *high* and *ultra-high availability*, including critical governmental communications, AI, and cyber-physical systems.

7. OUR SECURITY APPROACH: the Trustless Computing Paradigms

TCCB and Seevik Net will achieve radically-unprecedented levels of trustworthiness by (A) applying to both **extreme, battle-tested, and open** (technical and organizational) **socio-technical safeguards, and checks and balances,** the Trustless Computing Paradigms, that are applied to all technologies and processes critically involved in the entire life-cycle - down to fabrication oversight, CPU design and hosting room access and via (B) a governance model and statute that highly maximizes global **democratic accountability**, socio-technical competency, and resiliency from state pressures.

The Trustless Computing Paradigms describes a novel IT security approach - and a new IT security certification model for IT systems to be labeled "Trustless Computing" - that is centered on (a) **uncompromising transparency** of source designs and **extreme security-review in relation to complexity of all critical components and processes in the entire lifecycle**, and on (b) **democratic, time-tested, and decentralized governance, certification and oversight processes**.

7.1. Basic Principles Of "Trustless Computing"

- *Trustless Computing* is a novel approach to IT security and the name of an IT system certified by the Trustless Computing Certification Body that aims and claims to achieve **radically-unprecedented levels of confidentiality and integrity for sensitive human computing and communication** while ensuring **improved "in-person" national and international *legitimate* lawful access**, without requiring any legislative changes anywhere.

- *Trustless Computing* can be conceived as an extreme uncompromising version of the security-by-design approach to IT security, which expands "security design" and early-on deep verification to all critical technologies, supply chain processes and organizational processes critically-involved.

- *Trustless Computing* is centered on (a) **transparency of source designs** and **extreme security-review in relation to complexity** of all critical components and processes in the entire lifecycle, and on (b) **democratic, time-tested, and decentralized governance,** certification and oversight processes.

- *Trustless Computing* is a novel approach to IT security whereby actual and perceived confidentiality and integrity for an IT systems, service and experience - just as that of **electoral processes** in a resilient mature democracies - is not a technical problem but ultimately 100% the **by-product of the accountability and transparency of the design of the organizations and human processes** critically-involved in the entire lifecycle, as can be

assessed by moderately educated and informed citizens.

- *Trustless Computing* **renounces the need or assumption of any upfront unverified trust** in any organization, technology and person. *Trustless Computing* is not based on **distributed ledger technologies or blockchain** systems, while it may include them. Trustless Computing is different from **zero trust**, while it fully embeds its principles. Trustless Computing can be construed as an extreme deeper version of the **security-by-design.**

- Trustless Computing acknowledges that if only one our 16 million commercial airliner fights results in an accident, whereby every smartphone produced is hacked but a innumerable entities, it is not due to the fact that IT is harder, but **because all IT and IT standards are structurally weakened and surreptitiously compromised by nations** due to their failure to reconcile the needs of personal privacy with that of national security. Just as leaving "keys under a doormat", bug-doors are and will always be in all systems until a new mechanism ensures both the utmost system security and privacy and a safe-enough front-door access.

- *Trustless Computing* fully includes and embeds in its paradigms and certification processes the **zero trust** approach to IT security, yet it extend its "*never trust, always verify*" concept and an extreme "security-by-design" approach to the (a) technical and organizational "checkpoint" components that exercise Zero Trust functions in the Zero Trust architecture applied to the target system; as well as (b) the underlying target system in their entire supply chain and lifecycle. (See more in this recent post).

- *Trustless Computing* is **not** an IT security approach based on the **distributed ledger technologies or blockchain system or standard**, while a Trustless Computing IT system that satis it may include them. Many in its ecosystem have referred to their domain or specific solutions as "trustless systems". We challenge the claims that DLT/blockchains constitute a "trustless" system as well as a *standalone* trustworthy system because it requires the user - in varying degrees - to **blindly trust** (a) that several key actors in the power structure of a given blockchain will not act maliciously or collude to do so; (b) their hardware "crypto" wallet for integrity, and their software wallets and clients device for integrity and confidentiality. Conceptually, their flaw comes from thinking that digital **decentralization that is not democratically governed** and a server-side infrastructure without client devices, can alone deliver trustworthiness of sensitive IT systems beyond a digital speculation mechanism, like Bitcoin.

More on our Trustless Computing Paradigms web page.

8. OUR DETAILED OFFER to States, IGOs and Neutral INGOs

(Continues from Chapter 3.9 above)

8.1. How will the CHF 18 million from cofounder partners be utilized?

While a detailed work plan is available on qualified request, in summary, the **CHF 18 million** contributed by the cofounders will be dedicated to:

- (1) Making the TCCB operational, including a separation of standards-setting and certification requirements and processes, as derived from future versions of the Trustless Computing Paradigms, and licensing of a few "highly neutral" Common Criteria certification labs for TCCB certifications.
- (2) Finalizing the supply chain, architecture and design, and executing testing and production of Seevik Net, including 15,000 units of TCCB-compliant mobile client devices, in the *Seevik Wallet* form factors and finalize 2 production-ready prototypes of *Seevik Phones*, together with two different global high-premium smartphone brands or producers (one running Android and the other on Harmony) headquartered in states part of 2 different military/intelligence alliances
- (3) Creating one TCCB-compliant Hosting Room, to be located in the (somewhat) neutral state where TCCB will be headquartered, realized starting from prefabricated "containerized" hosting room (or "data center") units with military-grade levels and compliance with the highest international security standards.
- (4) Assisting cofounder partners in the localization, integration and customization of one or more TCCB Hosting Room, that they may decide to realize in their territory, to concurrently ensure compliance to local laws and local government desiderata, while remaining TCCB-compliant. In fact, having TCCB Hosting Rooms in their territory/premises is one of the optional privileges for *Cofounder Partners*. The cost of building and operating such hosting rooms will be borne by such cofounder entities, except for the above-mentioned assistance by TCCB.

8.2. Rights and Obligations of Cofounder Partners

More in detail, a *Cofounder Partner* will:

1) **Acquire full joint control of TCA, TCCB, the startup spin-in and Seevik Net**
    a) Acquire 5.6% of voting power in the TCA/TCCB Assembly, which will amount collectively to 51%. Such collective voting rights share will be reduced to 30% as foreseen decision making entities will be activated.

b) Acquire 5,6% of the shares of the startup spin-in and 11.1% of the voting rights, which will amount collectively to 51% of shares, and 100% of the share voting rights.

2) **Receive 900 TCCB-compliant mobile client device units and user-seats**;

a) Acquisition of 900 user-seats and client units of Seevik Net (either Seevik Wallet or Seevik Phone) for officials of their organizations, plus a 30% discount on up to 300 additional units for close personal or professional associates, depending on availability;

3) **Participate in shaping the statute of TCCB and *Trustless Computing Paradigms,*** on which 100% of the trustworthiness of TCCB-certified systems will rest.

4) **Local firms can purchase, resale and certify TCCB systems, exclusively for 1 year;**

a) local private and state cybersecurity startups, VCs, IT firms, defense firms, will be able to build and certify compliant systems and sell them abroad, with major economic development.

5) **Participate via local to the paid development of Seevik Net**;

a) Right for their strategic tech firms specialized in high-assurance low-level open IT to participate and be paid for in the consortium building Seevik. the architecture, development, and/or oversight of both TCCB and Seevik Net so as to increase their confidence in the outcomes, and position their firms to benefit economically in the TCCB ecosystem.

b) Right to participate as strategic investors **-** via their state-controlled cybersecurity funding or VC entities - in the startup spin-in of TCCB, TRUSTLESS.AI with other founders. As per a spin-in agreement, the startup is bound to accept acquisition offers by the TCCB at precisely-set non-speculative prices.

6) **Receive the right and full assistance to establish local TCCB-compliant hosting rooms**;

a) Acquire the right to host one or more state TCCB hosting rooms on their territory, or in their headquarters for neutral INGOs with international immunity like ICRC, UN and EU.

b) Such a hosting room will host an encrypted copy of all communications of users that are their citizens or foreign users using TCCB client devices in their territory. Exception to the above will be communications that involve foreign users physically located outside their territory which will instead be stored either in (i) another partner

states' TCCB hosting rooms or (ii) in a set of 3 TCCB-managed TCCB hosting rooms located in 3 neutral globally-diverse states, whose lawful access requires the request to be approved by the TCCB judicial Board.

c) Such state TCCB hosting rooms will be set up and managed in compliance with the TCCB Cloud which includes the physical in-person approval of all lawful access requests by a jury-like group of five random-sampled citizens, according to local laws.

7) **Enjoy special publicity and event-hosting rights**.
   a) Such rights will apply to TCCB and Seevik Net main documents, communications and events, and include the right to submit their candidacy to host a future edition of the Free and Safe in Cyberspace conference series.

8) **Commit to actively participate in good faith in the decision making of the TCCB organs**;

9) **Commit to share with TCCB any vulnerabilities found TCCB-compliant systems**;
   a) Commit to exert their "best effort" to ensure that all governmental and private firms agencies based in their territory will share with TCCB, and only with TCCB, any information the come in possession about actual or potential technical or organizational vulnerabilities in TCCB-certified IT, or TCCB organs or organizational infrastructure as well as tools and methods to exploit such vulnerabilities, and evidence of crimes by or against any members of the TCCB organs. Sustained and grave failures in such efforts, regardless of maliciousness, can result in suspension or revocation of TCCB partner status.

9. PRIVATE MARKET DEMAND

To say that private market demand is very (very) significant, would be an understatement. Pre-Covid surveys by UBS and by Northern Trust show that even the 16 million wealthiest persons in the World and family offices regard **cybersecurity as their n.2 or their n.1 concern**, respectively. There is nothing money can buy. Even the richest have nowhere to hide, not to mention journalists, executives and activists.

Participating states could promote significant economic development by acquiring a limited-exclusivity for their firms and financial institutions in offering TCCB-complaint systems. Several banking and SME associations have shown initial interest in TCCB and Seevik Net for their members and for their members' clients.

10. PERMANENT GOVERNANCE of TCCB & SEEVIK NET

Decision making power will reside in the **TCCB and Seevik Net General Assembly**, except that the Assembly will not be able to impede any nation to join on equal terms, starting 12 months after the initial founding states have joined. The General Assembly will be composed of 75-85 members, to be compensated at 200% of their going market rate according to their expertise and profile, for the time they'll be required to serve. The composition of such Assembly - subject to revision will be divided as follows:

- **30%: Globally-diverse nations and inter-governmental organizations.**
    - We are selecting no more than 7 globally-diverse nations and 5 neutral INGOs (e.g. consumer, industry or human rights orgs) or IGOs (e.g. the EU, UN agencies, Arab League, and African Union) to join as founding governance partners to give final shape to the governance of the Trustless Computing Certification Body and its Paradigms.
        - The global-representativity of participating nations will be maximized via the initial selection of nations and IGOs, and by weighting of the voting to maximize global-representativity in respect to political regimes, continents, population size, religion and other key determinants.
        - Voting will be per country, except it will be weighted according to a to-be-determined coefficient based on population size, GDP per capita, and other metrics, as will membership fees.
        - Special terms apply to the current global cybersecurity superpowers, **USA, China and Israel**, if and when they'll join. First, they can only join together so as to avoid the Initiative to become or be perceived as unipolar. Second, they will have, for the first 2 years, 50% higher decision-making power than other countries with similar metrics. Why? Simply because of the need to find a "realpolitik" compromise to get an ambitious workable global cooperation agreement in place in domains that are highly sensitive for national and global security.

- **15%: Assembly of Global Random-sampled Citizens**
    - *Global citizens will be* selected, and their vote weighted, such that via scientific methods it will maximize global representativity of all major differentiating human factors, such as gender, race, religion, political orientation, and it will be further weighted by 20% according to the size of the members' nations population.
    - Their selection and review will greatly minimize their risk of being subject to corruption, threat, or blackmail by powerful entities. (Logistic and scientific collaboration will the sought with the *Global Citizens' Assembly for COP26,* and

Stanford University Center for Deliberative Democracy)

- **15%: Assembly of a Global Random-sampled Set of Former Parliamentarians.**
  - Members from all nations will be able to join and will need to be globally-representative. The selection of such members will minimize their risk of being subject to corruption, threat, or blackmail by powerful entities.
  - Members' vote will be weighted via scientific methods to maximize global representativity of all major differentiating human factors, such as gender, race, religion, political orientation, and it will be further weighted by 20% according to the size of the members' nations population, and by 20% on the relative "democratic effectiveness" of their parliamentary elections.
  - Members will be selected half from defense, interior, or intelligence oversight committees, and another half from privacy and civil rights committees. (*Logistic and scientific* collaboration will the sought with the *Climate Parliament and Parliamentarians for Global Action*)

- **15%: Scientific & Ethical Advisory Board.**
  Initially composed of the Trustless Computing Association scientific advisory board, with some addition and removals. Chosen according to technical proficiency, proven record of altruism and ethical stands, and resiliency from external legal and illegal pressures (blackmail, bribes, etc).

- **7%: End-user industry associations or human rights NGOs.**
  E.g. IT security industry associations, SME associations, consumer associations,
- **7%: Non-Partner Organizational and Individuals End-Users.**
  E.g. social and political organizations, member-based NGOs, private companies, and individual world citizens
- **6%: Critical Technologies Partners.**
  E.g. Partner firms specialized in targeted open high-assurance battle-tested low-level IT systems and components, especially Sel4 and Risc-V and a specific subset of their derivatives.

10.1. Rationale for Approximating Global-Representativity

- To achieve its aims, TCCB governance has, from its origins, sought to maximize democratic accountability, competency, and resiliency from nations' pressures. Consequently, for its nation-member component, it should maximize global representativity in respect to population size, political regimes, religion. Some hard choices and balancing will need to be done, as no perfect solution exists.

- Which nations should be allowed to participate in the TCCB governance? How should their decision-making be weighted? Firstly, we tackle such an issue by reserving 30% of decision-making to global citizens themselves. Plus another 30% of former parliamentarians should be mostly free from pressures from their nations' executives.
- Some hard choices and balancing will need to be done to ensure over time and during the constituent process of TCCB, a **maximization of global democratic representativity**, in addition to competence and resiliency from powerful nations' pressure.
- How are we to weigh the voting of a country like China - with 1.5 billion citizens and widely considered a dictatorship, technically an "authoritarian electoral single-party social democracy", and self-defined "socialist democracy" - or Israel - with only 6 million citizens and outsized cyber and geopolitical power due to historical and capabilities of its culture?
- Key to our TCCB and Seevik Net mission is to create a **global** digital public sphere for all World citizens, and not merely a **transnational** one limited within "western or liberal'' democracies, because it wants to be a means by which citizens within and across nations, and geopolitical blocks, communicate securely and safely, on the basis of the principles of liberty and democracy. We want to contribute to **structural democratic global cooperation,** via democratic global or open widely-transnational empowered global federal governance systems, which is the only way humanity can hope to successfully tackle the global challenges of climate change, nuclear and digital disruption.
- Also, limiting the governance to a single military/intelligence alliance would reduce the trustworthiness of TCCB even to the citizens of such alliance because in times of global crisis nations and blocks tend to fall prey to the "not on my watch syndrome" and trample on civil rights, which in turn degenerates democracy, and then also national security.
- So therefore TCCB strives for a more "democratic" governance model, also in its representation of nations, while also being globally representative, and **acting as a means to unite and not divide the World citizens, peoples and cultures**.
- Also, nations tend to claim an unequivocal **high-ground of democracy**, self-defining their models "liberal democracy" (US) or "socialist democracy" (China), or just democracy (EU). We'll take a neutral, fact-based approach to such claims.
- Although the initial governance of the Trustless Computing Certification Body (TCCB) does not necessarily require direct nation-state participation - as it relies on random sampled global citizens and parliamentarian - it highly welcomes it to increase even more its actual and perceived democratic accountability, and to ensure it will most efficiently take into consideration global public safety in its decisions.

11. TRACTION WITH PROSPECTIVE PARTNERS

So far, **five states** have signed up to our Free and Safe in Cyberspace 9th Edition and 10th Edition, held in Geneva and Zoom, between March and May 2023, as interested prospects in becoming

governance or cofounder partners. We are not authorized to divulge their names, but include one from South America, one Asia, two from Africa and one from Europe.

Over recent years, months and weeks, we received substantial interest from several states, including **Germany, France, Italy and the Netherlands** - but also the US and Israel, and some smaller third states with high strategic autonomy like **Switzerland, Malta and Liechtenstein**. Such interest includes dozens of hours of engagements by relevant high-level current and former government representatives (foreign affairs, security agency, minister level, parliamentarians), and by suitable low-level tech firms from the same states, and many dozens of hours of engagements with **six state-close/controlled cyber-only venture capital firms** interested to co-invest with other private and public counterparts in the startup-spin-in.

We held over nine meetings with **former highest-ranking cyber diplomats of the US and Israel**, following which 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 McLean-based **United States** leading cybersecurity accelerator, chose us among hundreds of candidates for their program in Q4 2021 and accrued rights to 3% of the start spin-in shares. (In early October, the Agenzia Della Cybersicurezza Nazionale of Italy announced investments in strategic cybersecurity startups).

We have engaged with some interest with several top executives of **Huawei** global and Swiss in 2019-2020, as one of two smartphone partners (one western and one non-western) for building initial mobile device and system complaint to the TCCB Seevik Phone, and as a proxy for engaging with the **Chinese government**. We made some attempts to engage China, over the years, without success. But last November, we initially engaged **a *Secretary of the China Mission to the UN in Geneva*,** in charge of activities at the UN ITU for IT standards, and we are looking forward to a 1 to 1 or joint meeting soon.

For more information, we have available on qualified request a **Detailed Traction PDF, a 25-pager deck PDF profiling our current R&D and governance partners** of TCA, TCCB and Seevik Net, as well as the extensive interest shown so far by several countries - through their relevant ministry, strategic IT security companies, and cyber-only funding vehicles - with a 2-pager summary on top.

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

11.1. Current Advisors and State R&D Partners

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, advisors, and investors, building initial minimalist TCCB-compliant IT systems - which is bound to be re-owned by TCCB via a “spin-in” agreement.

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.

11.2. Prospective Partnership with States

While no written agreement is in place yet - except R&D ones with Italy and Austria - over recent years, months and weeks, we have 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. For each, 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.

Over the last few 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, Qatar**, 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 in a 25 pager document.

11.3. Prospective Partnership with intergovernmental Organizations

While no written agreement is in place yet, on the front of IGOs (intergovernmental 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.**

11.4. Prospective Partnership with Global Cyber Powers

Initial participation by **global cyber superpowers**, like the US, China and Israel would be welcome but not required, and incentivized via higher temporary influence for those that join earlier rather than later.

While no written agreement is in place yet, over the last two years, we held over nine 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 spin-in TRUSTLESS.AI.

When and if the US and/Israel will decide to participate, we believe it would be crucial that China participated as well because it would make TCCB, Seevik Net and TCCB-compliant IT (1) more equally trusted worldwide, to **enable the fair and effective global dialogue,** at all levels, to promote **peace and joint tackling of global challenges;** and (2) substantially **more trusted even by western citizens, elected officials, diplomats**, and even prime ministers, given the experience of programs like Crypto AG, NSO Group, the iPhone, and past overreach of western security agencies.

We made some attempts to engage China, over the years, without success. Last November, we initially engaged a **Secretary of the China Mission to the UN in Geneva**, in charge of IT standards at the UN, and we are looking forward to a 1 to 1 or joint meeting soon. We have engaged with some interest with several top executives of **Huawei** global and Swiss in 2019-2020, as one of two smartphone partners (one western and one non-western) for the Seevik Phone, and a proxy for engaging with the Chinese government.

11.5. Prospective Partnership with State's Strategic Investment Arms and IT Firms

While no written agreement is in place yet, 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). (In October 2022, **Italy** announced a program to invest in strategic cybersecurity startups). MACH37, the US leading cybersecurity startup

accelerator, in Washington DC, for which we were chosen among hundreds in Q4 2021, has accrued rights to 3% of the share rights (not yet the shares). We are actively seeking for a similar participation by a **Chinese** entity to counterbalance such participation.

In recent months, we've been engaging intensely with (global and national strategic) tech firms specialized in the co-development of **multi-national open-source high-assurance battle-tested CPUs and OSs**, from the same countries, based on **Risc-V** and **Sel4**. These include especially *Hensoldt Cyber* (**Germany**, but indirectly invested by **Italy** and **France**), but also Galois Inc. (**US**), Technolution (**Netherlands**) and the global **Sel4 Foundation**, for their participation as technical partners. These will make it so that participating nations - and all nations and the general public - will have full and transparent access to the TCCB standards, initial complaint IT and its architecture, throughout its lifecycle, from its inception, maximizing actual and perceived trust in the resulting tech by nations and all citizens. Seeking further engagement with strategic firms from **China** and non-aligned countries.

11.6. More Details on Prospective Partners

Available after qualified request, and a signed NDA or signed Terms of Participation agreement: a *Detailed Traction Update*, a 25-pager deck PDF profiling our current R&D and governance partners of TCA, TCCB and Seevik Net, as well as the extensive interest shown so far by several countries - through their relevant ministry, strategic IT security companies, and cyber-only funding vehicles - with a 2-pager summary on top.

12. ROADMAP & NEXT STEPS

To learn more, help us improve it, join other interested prospective partners in preparatory meetings and workshops we'll hold during the 12th Edition of the Free and Safe in Cyberspace, next March in Geneva. FSC12 will seek to consolidate and expand the interest, engagement or commitment of an initial group of cofounder entities, capped at 7 states, 2 IGOs and 3 neutral INGOs.

By **mid 2024**, we aim to have co-founder states on-boarded - via LoI or binding agreement or at least engaged in a "TCCB founding process" via closed-door and public meetings online and offline - that will revise the current TCCB statute/governance and the Trustless Computing Paradigms. After six months, TCCB will be **open to participation to all states on a fair and equal basis**. TCCB is bound by statute to strive to achieve a very high global representativity already as it reaches 20 member states, also via weighted voting.

By **Q1 2026**, we plan to become operational with TCCB issuing certifications and to ship initial TCCB-compliant mobile IT systems/services, including a batch of 15,000 mobile client device units

reserved for our initial limited-exclusive partnering states, neutral INGOs and IGOs, and a few select private entities.

13. VALUE PROPOSITION FOR THE US, ISRAEL AND CHINA

Our Offer to like-minded states, IGOs and neutral INGOs to join as *governance partners* or *cofounder partners* of the Initiative apply to the **current de-facto cyber superpowers**: the **USA, China and Israel** as well, with one exception.

Given how central **neutrality** is to our Initiative - while they are each individually welcome to apply to join the Initiative and join our upcoming 10th Edition of the Free and Safe in Cyberspace **workshops** in Geneva - **their partner status will become operational only when and if the other two also join.**

To incentivize each to apply early, the first one of them that applies will enjoy a **30% higher decision-making power** relative to the other two in the Initiative for the first 18 months, although such decision-making power will be suspended until all three cyber superpowers will have joined.

As you can read in our TCCB Governance Page, special terms apply to them in terms of decision making power in the TCCB general assembly. **They will each have, for the first 2 years, 50% higher decision-making power than other countries with similar metrics.** Why? **Simply because of the need for some "realpolitik" compromise to get an ambitious global cooperation agreement in place in domains that are highly sensitive for national security.**

Why should they join? While being entrenched as the global dominant cyber superpowers, we have detailed arguments as to why - as **counterintuitive as it may seem -** they would overall greatly benefit from joining and supporting the Initiative. That said their participation is highly welcome but not required.

The problem with the status quo

The current model by which western states reconcile the need for **sensitive non-classified mobile** privacy and security with the need for international *legitimate* lawful access is causing **increasingly unacceptable collateral damages in terms of civil freedoms and democratic sovereignty** in EU member states, of the EU, the world over, and just as much within the US and Israel, with even parliamentarians and the former prime ministers vulnerable.

Even heads of state and head of opposition, and their close associates, were hacked on their smartphones last year, as shown in Spain, in Greece and in Israel, in Finland, in UK, in Switzerland, among those we got to know about.

The problem has long turned also in a crucial state **security threat,** even in the US and Israel, as it increasingly exposes our leaders, elected officials and journalists to spying and blackmail - by enemies foreign and domestic - and mines the appeal of our democracies to our fellow citizens and towards third states, whose "hearts and minds" we need to prevail over fast rising appeal authoritarian countries and of authoritarianism.

Why the US, China and Israel benefit the status quo

It may seem that the US and Israel, would not have an interested in maintaining the status quo in the market, because they **undoubtedly have an "informational superiority upper hand" in the current model**, via their overwhelming control of leading secure devices (e.g. iPhone, Android), spyware (e.g. NSO Group) and endpoint security firms (Crowdstrike, Koolspan, etc).

Due to their control over the leading and globally-hegemonic private IT security firms, the US and Israel have an apparent distinct advantage, via their ability to access better protections, better espionage capabilities, and better espionage countermeasures. **Similar powers over the security and insecurity of mobile infrastructure is exercised, increasingly, by China**, via its control of nearly all mobile phones except iPhones, and leadership in 5G networks, and increasingly with platforms like WeChat, TikTok and the new mobile operating system Harmony.

Why the US, China and Israel are also greatly damaged by the status quo

Yet, the current model and hegemony comes with **huge and mounting inefficiencies, collateral damages, and a "boomerang effect"** for those leading states, so it may be worth exploring it there may be a better alternative model, like ours, that would eliminate or radically mitigate those effects, and overall be **most convenient for such states and also for the narrower goals of their security agencies**.

Even though they have the upper hand in the current scenario, they are suffering from huge collateral damages mining their own democratic systems. Involuntarily, **they have ended up weakening the technologies, procedural safeguards and oversight processes of the IT systems that are most critical in sustaining democratic society**, such as (a) the mobile devices used by even their top elected officials, parliamentarians, ministers, as well as (b) the targeted hacking systems used to by the police.

This has become even more evident when even the son of the prime minister of Israel Netanyau was reportedly hacked, with no way to know if and by who he was, in a cascade of accusations, severe divisions in society, and further **loss of trust in democratic institutions**. It has become clear that **every elected official or citizen not only abroad but also in their country is hackable by who knows who,** inside or outside their institutions. In addition, sometimes they "go dark" and the evidence they acquire is often unreliable, and not accepted by their highest courts.

Even the president of the US runs very similar risks, as detailed in 2017 by the New York Times. Just as concerning, current smartphones enable users to reliably delete evidence of crimes to evade criminal accountability, as shown by investigations on the US president's secret service detail, while others may have acquired such evidence before its deletion for use in politically-motivated blackmail.

For these reasons, and more detailed below, we believe they will eventually join as governance partners of the TCCB, **even though they'll need approval from an UN-like neutral democratic body to intercept an elected official, journalist or private citizen from a friendly nation**. While nearly every state would be welcome to join such an initiative, none is necessary. That said, it would be highly advantageous that a few states that have a key role in current and future global cybersecurity architecture - like the US, Israel and/or China - would join sooner or later.

Interest show so far by the US, China and Israel

Over the last two years, we held over nine meetings of intense and detailed dialogue with the former highest-ranking cyber diplomats of both the **US and Israel.** Following such dialogues, we wrote a blog post on 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 spin-in TRUSTLESS.AI.

We have engaged with some interest with several top executives of **Huawei** global and Swiss in 2019-2020, as one of two smartphone partners (one western and one non-western) for building initial mobile device and system complaint to the TCCB Seevik Phone, and as a proxy for engaging with the Chinese government. We made some attempts to engage China, over the years, without success. But last November, we initially engaged a **Secretary of the China Mission to the UN in Geneva**, in charge of IT standards at the UN.

Why should cyber superpowers ideally join TCCB together rather than singularly?

As we wrote above, given how central **neutrality** is to our Initiative, the current cyber superpowers US, China and Israel are all individually welcome to join the FSC9 and FSC10 workshops and following ones but, while welcome to join the Initiative, will be accepted only when they do so concurrently.

When and if the US and/Israel decide to participate, we believe it would be crucial to ensure that China also participated or that it would be ensured that it can join later, and the other way around. That's because it would make TCCB, Seevik Net and TCCB-compliant IT: (1) more equally trusted worldwide, to **enable the fair and effective global dialogue,** at all levels, to promote **peace and joint tackling of global challenges;** and (2) substantially **more trusted even by western citizens, elected officials, diplomats**, and even prime ministers, given the experience of programs like Crypto AG, NSO Group, the iPhone, and past overreach of western security agencies.

Eight detailed key arguments as to why the US and/or Israel (and partly China) would benefit from joining the TCCB and Seevik Net Initiative

Let me list below **eight key arguments** why Israel or US, counterintuitively, would greatly benefit overall by joining and co-leading the Trustless Computing Certification Body and Seevik Net as opposed to relying **only** on the current failed model.

- First, they would ensure a **much higher certainty, integrity, attribution capability when investigating users of TCCB-compliant systems**, foreign and domestic, **than they currently have when investigating current IT systems with the current model**.
    - In fact, while their security agencies would "by definition" lose the arbitrary capability to hack into TCCB-compliant systems (which will be designed with the state purpose of being impregnable to such acts) - when legitimately authorized - they will:

      (A) have certainty of prompt access, without the risk of "going dark" or being unable to hack, and independently from the availability to assist of other nations or firms; and

      (B) obtain more solid and forensic-friendly evidence that is much more reliable and that will be accepted by the highest national courts, unlike that obtained via targeted hacking which does not stand in court in Germany, Italy and France.
- Second, they would **expand and improve existing multilateral and bilateral agreements whereby Israel and US, as other friend nations, ask each other's permission to allied host nations** when having to spy on targets that are citizens of an ally country via an obscure complex web of agreements that are oral, software-coded or written, such as MLATs, Club of Berne, 5-9-15 eyes.
    - For example, we recently learned there are "rules" in place for at least a few years that technically prevent any nation-state client of the NSO Group to hack target users with a US number or while they are on US territory. Following the scandals in October 2021, such rule was extended to Israel, the United States, Canada, Australia, New Zealand and the United Kingdom, and France. To be fair and coherent, following the same rationale should be extended to other allied, friend and non-adversarial nations, both for NSO and other "private" spyware as well as state hacking capabilities.
- Third, they would radically mitigate the problem whereby their **current target hacking capability, direct and through private firms, produces unreliable and untrustworthy evidence**, since client devices could have been hacked by others and do not support forensic, as it was highlighted by Rami Efrati, former Head of Cyber Division of the Prime Minister Office of Israel, during a recent university lecture (min 9.35).
    - In fact, evidence so acquired via state trojan is structurally contested by highest civilian courts in Germany and France, as well as in Italy. Often parallel construction is used to mitigate such problems, but creates big others of its own. Requests to TCCB instead are approved even in 1-2 hours, if urgent, and produce much cleaner evidence.
- Fourth, they would **radically increase both the protection of legal communications and the accountability of illegal communications for their most sensitive law-abiding**

citizens and organizations, including elected officials, journalists, business leaders, activists, as well as their reference organizations.

- TCCB would radically increase protection from politically-motivated extortion, blackmail, manipulation, or profit-motivated extortion, ransomware and trade secret spying.
- Provided that key elected and appointed officials, and their close personal and professional associates, are mandated to use such devices, TCCB could serve as a way to better exercise accountability and national and investigative powers over grave activities aimed at subverting the democratic constitution, as we've seem happen in Germany and the US recently. as we outline in this post under "*Germany's internal fight against far-right subversion*".
- They would radically mitigate the problem of their own elected officials being spied on and blackmail by who knows who.
- Over the last decade, in an unforeseen huge "boomerang effect" **those same weaknesses and vulnerabilities in the Internet infrastructure** have been used by adversary nations, and internal authoritarian forces to wreak havoc, compromising democratic stability and national security.
- Any **US or Israeli parliamentarian and their close associates** - and even the son of Israel prime minister or a US presidential candidate - can be hacked undetectably for months or years on hand. Even worse, the fact that this is often not be discovered, non detectable, and **when discovered it is nearly impossible to ascertain who did it**, fosters deep division and mistrust with their societies where everyone is an accuser and victim, and mines citizens' trust in the democratic institutions citizen, creating an untenable situation that could lead Israel down the similar paths as the US democracy**.**

- Fifth, they would mitigate the **huge collateral damage of unwittingly fostering a huge cyber crime business, by fostering a billion dollars zero-days market for vulnerabilities**, and creating the conditions for leaks like Vault 7 and Shadow Brokers, whereby state-grade hacking tools end up in the Dark Web.
  - Even the most sophisticated state-grade malware, protected with multiple sophisticated layer of "obfuscation" ends up being "decompiled" by state and non-state actors - as it happened to Finfisher last year - that find them in a victim device, enabling non-state entities of all kinds to re-use them, often leaving no trace afterwards, and with no way to assess the scale of their hacking, and who did it, creating a real **Wild West**.
- Sixth, they would **retain the threat visibility and influence that they currently have on third and allied nations** through their undue control over the dominant mobile device, platforms, cybersecurity solution and spyware - especially for Israel towards Middle East governments to reduce terrorist and Iran threats - via the careful governance and

socio-technical design of our new **trustworthy international body**, the Trustless Computing Certification Body.

- For threat visibility, the TCCB would radically minimize the risk that legitimate cyber-investigations - that one of those nations deem needed, legal and proportionate - will not be approved by the TCCB International Judicial Board, or impossible to exercise for any reasons, even those involving international communications of a nation's leader.
    - For the influence, US and Israel could benefit from moving from a position of deceitful "hard cyber power" over their allies and third-nations to a new model of "soft cyber power". Move from providing third-nations the ability to hack indiscriminately to giving them the ability to protect legitimate communication and make accountable illegitimate ones.
- Seventh, they **would repair and relaunch their reputation, trustworthiness and leadership towards allied and third nations** - especially after the US NSA revelations of 2013 and the **NSO revelations** of the last few years - about large-scale unwarranted abuse of nation state clients of NSO Group to spy on journalists and even prime ministers of allied countries, and for making us all (through their bug-door model) more exposed to cyber criminals of all kinds that somehow gain access to the most powerful hacking capabilities.
    - Leadership by example rather than coercion. A leadership among nations with equal dignity. More carrots and less sticks. Affirm a model whereby advancing diplomatic, geopolitical and economic interests can be done while also promoting peace, freedom, democracy and safety.
    - They would **increase their ability to counter the rise of authoritarianism at home and abroad**, by having more democratic investigative visibility into internal subversive activities, as well as more coherently project a leadership by example of a model of digital society that is coherent with western democratic values.

      They would **be recognized by other nations as co-leaders in promoting peace and fair and effective global cooperation**- within and across alliances, participating in building nothing less than the **new de-facto global standard state-of-the art for sensitive and diplomatic digital communications**.
- Eight, they would join an initiative that aligns as natural development of the very complex history of attempts by the US to find a solution to this conundrum. It was 1991 when a young **Joe Biden,** as Chairman of the Senate Judiciary Committee, introduced a bill called the Comprehensive Counter-Terrorism Act, that stated aspirational goals for a front-door access mechanism: "*It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law.*"
    - In such a bill proposal, however, **Joe Biden did not specify "how"** those providers should "*shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately*

authorized by law."

Yet, the overly generic nature of such provisions, and the prevailing draft implementations of such bill, lead a group of digital rights experts and activists to foresee that ill-thought implementations of such law would have curtailed the freedoms they had just gained for themselves and all citizens with such new encryption protocols and software while doing nothing to stop criminals.

- It was Biden's bill, and the looming threat that this newly-found strong encryption would be outlawed, that **Phil Zimmermann** wrote at the time "*led me to publish PGP electronically for free that year*.". This open technological solution suddenly enabled anyone in the world to communicate securely, even from US remote interception.

  Those fears of those digital rights experts and activists proved to be exactly right. As the use of algorithmically unbreakable encryption kept spreading, in 1993, the Clinton Administration developed a system hardware component, the Clipper Chip, that was promoted and encouraged to be inserted (initially on a voluntary basis) in US human electronic communication devices and systems, to ensure remote access by the government, when authorized by *due legal process*.
- The wide availability of open source algorithmically unbreakable encryption software forced a shift in the western security community whereby they had to move on to break all IT and IT standards to retain the interception capabilities that they had back when they could break all encryption in transit.
- Last October 2020, the US, UK, Australia, New Zealand, Japan, and India, published a joint International Statement: End-To-End Encryption and Public Safety, issuing a call to IT providers, NGOs, and stakeholders to find a solution to the problem of encryption technologies hindering law enforcement and security agencies from detecting and preventing grave crimes by individuals and nation-states. In the following November, a Draft Resolution of the Council of European Union was revealed, which was very similar to such a Statement, and literally identical to it in key provisions, called on civil society, industry and academia to find a solution that enables lawful access requests that are **not only legal, but also "*necessary and proportionate, and is subject to strong safeguards and oversight*."** adding key requirements that were missing in the original bill by US President **Joe Biden** in 1991.

  This novelty raises hopes that new mechanisms, standards, certifications, and bodies could be created - reserved for IT systems for human communications conceived for the highest levels of security - that apply such new stringent requirements to mechanisms that can **both** ensure *legitimate* lawful access as well as radically raise the level of security and privacy of those systems.

- Ninth, they would be able to affirm a new leadership based on the **principles of democracy and fair and effective international relations, communications and cooperation,** via win-win solutions whereby **national security is increased while and by advancing our democratic and liberal societal values.**

For all these reasons, we believe that by co-leading other nations to build the TCCB and Seevik Net, the US or Israel could lead to enact a new **model of democratic digital society** that is finally coherent with their liberty and democratic principles, creating an healthy constructive competition with China, and other fast rising autocracies, for the **hearts and minds of world citizens**, and promote therefore security, peace, democracy and freedom, at home and abroad.

A sort of post-Cold War Crypto AG: multilateral, transparent, for peace, for all and mobile?

In a way, we are building what could be conceived as **a "post-Cold War version of Crypto AG",** the de-facto global standard and state-of-the-art for sensitive and diplomatic digital communications during the Cold War, that turned out in 2020 to have been controlled by only two nations.

As opposed to the original one, the TCCB and Seevik Net initiative will be based on open democratic **multilateralism**, uncompromising **transparency,** and an ultra-resilient **procedural front-door** instead of a technical back-door.

Beyond diplomats, it'll be available to all with utmost portability and convenience via **2mm-thin standalone devices**, carried inside custom leather wallets or in the back of their future smartphones - to finally enable **secure, fair, and efficient digital communications and dialogue,** within and among nations.

The original Crypto AG provided over 100 nations enormous value in terms of internal and external remote communications reliably secure against interception by any state or non-state actor, albeit at the (witting or unwitting) cost of interception by top security agencies of two nations. Ultimately, Crypto AG was one of the most successful and impactful intelligence operations of the last century, playing a crucial role to make sure that **a more democratic geopolitical block prevailed over a lesser one**.

The original Crypto AG program also proved that digital communications can be made to resist even the most powerful state-grade attackers at relatively moderate R&D costs. Even more relevant, it proved that 3rd-party access to encrypted data and communications can be reliably restricted to intended parties - albeit solely for such ultra-secure IT systems and at moderate scale - contradicting widely shared expert ideas about the impossibility in all cases of a secure-enough "front-door" socio-technical mechanism.

15. MORE INFO & DOCUMENTS

- Executive Summary - Opportunity for States, IGOs and neutral INGOs, (**This Document**!) a 40-page A4 PDF, preceded by a 5-page Summary, detailing our offer to join as *cofounder partners*.
- Introduction Slide Deck, a 40-pager intro deck PDF on our association, partners, advisors, and the Initiative.
- Trustless Computing Paradigms, (latest version online, exported pdf)
    - The TCCB Fab (latest version online, exported pdf)
    - The TCCB Cloud (latest version online, exported pdf)
- TCCB Governance (latest version online, exported pdf)
    - TCA/TCCB Statute
- Available after qualified request, and a signed NDA or signed FSC Terms of Participation agreement: a *Detailed Traction Update*, a 25-pager deck PDF profiling our current R&D and governance partners of TCA, TCCB and Seevik Net, as well as the extensive interest shown so far by several countries - through their relevant ministry, strategic IT security companies, and cyber-only funding vehicles - with a 2-pager summary on top.

16. CONTACTS

Trustless Computing Association
www.trustlesscomputing.org — info@trustlesscomputing.org
Headquarters: Rue Fendt 1 - 1201, Geneve, Switzerland
Main Office: Via Francesco Vettori 39 - 00164, Rome, Italy
Landline +41225483778

Main Contact:
Rufo Guerreschi, Founder and Executive Director - rufo@trustlesscomputing.org
Mobile/WhatsApp/Signal +41799137280 --- Mobile +393289376075