



# FREE AND SAFE IN CYBERSPACE **8TH EDITION**

JUNE 24-25TH, **2021**

 **Hybrid Online/Offline - Geneva and ZOOM**

# The Impossible choice and trade-off





+



# Building our Democratic Digital Sphere.

We are building a highly **democratic**, competent, resilient, and independent **Trustless Computing Certification Body**, that will standardize, certify and regulate **interoperable** hardware and software systems for human communications and their resulting digital sphere, **Seevik Net**.

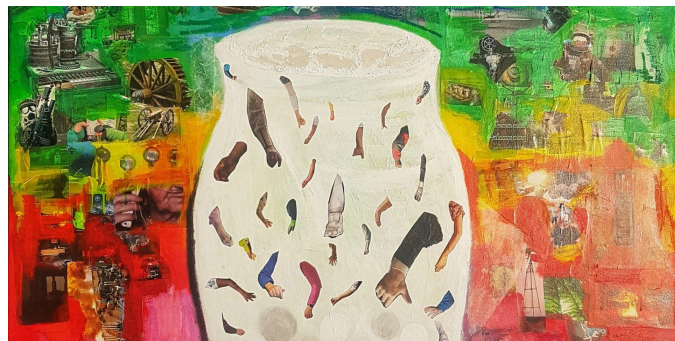
They jointly aim to achieve **radically-unprecedented levels of confidentiality, integrity, and democratic control for our digital lives**, while concurrently ensuring *legitimate* lawful access.

**On Nov 21st, 2017. Levi's Stadium, Santa Clara, California.**

*A recreational drone drops thousands of leaflets, and then again on another nearby stadium.*



# VULNERABLE WORLD HYPOTHESIS



**Jan 22th, 2020.** Bezos reported hacks via WhatsApp. The *New York Times* states: **“For the ultrarich and influential, the Bezos hack should be a terrifying revelation”**



Hacked

Hacked

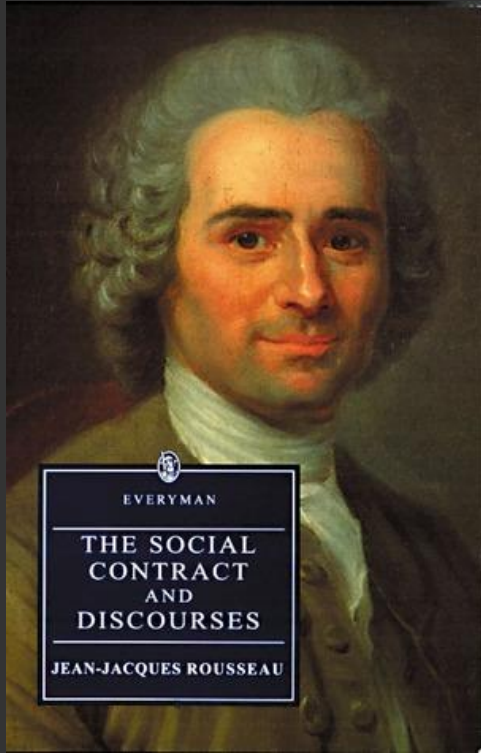
# The Impossible Choice



# Three Ideas whose time has come

1. Meaningful **personal freedom and public safety in cyberspace** are not a “trade-off” in a zero sum game choice, but **“both or neither” challenge fundamental to retain liberty and democracy**; and realize the opportunities of the upcoming Age of AI, and stave off the bad scenarios.
2. This challenge can be solved by **applying to both IT systems and lawful access mechanisms the same extreme battle-tested time-proven technical and organizational safeguards** - as used for decades for nuclear safety and electoral processes - and subjecting the to an **ultra-resilient democratic global governance entity**.
3. Most experts believe that cybersecurity is a technical problem, that will be solved via technical innovations. **Cybersecurity of critical systems is not a technical problem but 100% one of organizational design.**





"Man is born free and everywhere he is in chains."

absolute freedom of  
speech

absolute freedom of  
self defense

absolute freedom of  
X and Y

confers  
**theoretical**  
freedom



receives back **10x**  
**actual** freedom

Social contract

**no zero-sum** but **positive feedback loops**

civil  
freedoms

defense and  
safety

other  
freedoms



As more of our life moved to a global cyberspace, we are **back at square one**, without a social contract.

# Trustless Computing Association

- Established in 2015 in Italy
- Swiss entity, in **Geneva**, since May 2021
- 3 EU **R&D** Initiatives for TCCB and Seevik Pod
- 25 World-class R&D **partners & advisors**
- A Swiss **spinoff startup** since 2019 to fundraise for TCCB and build 1st TCCB-compliant open base and IT service
- **8 Editions** of Free and Safe in Cyberspace about TCCB  
(Brussels, Iguazu, New York,, Berlin, Geneva, Zurich, and Geneva)
- Research **publications**

# Executive Committee



RUFO GUERRESCHI



NICK KELLY



JOHN SHAMAH

# TCA Governance Advisory Board

Include top professors from **Stanford** and **Princeton**, former senior officials from **EU Commission**, **EUROPOL**, and senior top executives from **top banks** and IT giants like **Huawei**, **Barclays Bank**, **Erste Group**.



DANIELE ARCHIBUGI



RICHARD FALK



JAMES S. FISHKIN



PAUL NEMITZ



CHRISTIAN D'CUNHA



STEPHANE DUGUIN



PAOLO LEZZI



NICK KELLY



ANA CHUBINIDZE



MIKA LAUHDE



ELIZABETH FERGUSON



GIOVANI SPAGNOLO



TOUFI SALIBA

# TCA Scientific Advisory Board

Include senior cyber security industry leaders from **PwC**, **Telecom Italia**, **Facebook**, **ETH Zurich**, Chairman of the Board of **World Economic Forum**, **Unisys**, **Centre for Cybersecurity** and **Raiffeisen International Bank** among others.



JOVAN GOLIC



ROBERTO GALLO



SUNIL ABRAHAM



KOEN MARIS



JAWAD HAJ-YAHYA



ADAM BURNS



TROLES OERTING



GERHARD KNECHT



KAI RANNENBERG



ROMAN YAMPOLSKIY



PIERLUIGI PAGANINI



REINHOLD WOCHNER



PAMELA GUPTA

# Global R&D Partners

Two EU nation states, a EU foundry, leading open ultra-secure CPU makers, the largest EU cybersecurity industry association, the largest AI R&D center in the world:





# Biden, Trustlessness and Current IT Security Standards

1. Biden after his Geneva meeting with Putin: "***This is not about trust, this is about self-interest and verification of self-interest.***  
>>> Not "trust but verify" but "trust or verify"
2. Last month, Biden's Deputy National Security Advisor, Anne Neuberger, announcing a new **executive order** to mandate new standards for critical systems: "***If you or I are going out to buy network management software like SolarWinds and we want to buy the software that is most secure, we have no way of assessing which that is***"  
>>> Current standards are not just bad but useless for critical systems.
3. Last May 2020, when asked if NSA compromised RSA encryption standards she declined to confirm.



# Free and Safe - Editions 1-4th



On September 22nd-23rd 2016, the [4th Edition 2016](#) held in **Brussels** gathered experts, including the CIO of Austria, the Vice-Chair of the EU Parliament LIBE Committee, Paul Nemitz, Director of Fundamental Rights and Union citizenship in the DG Justice of the European Commission, and more. See the [Programme](#), [Videos](#) and [Slides](#).

[Read more >>](#)



On July 21st, 2016, a [3rd Edition](#) was held in **New York** with amazing speakers, including Joe Cannataci, the UN Special Rapporteur on the Right to Privacy, and Max Schrems, the Austrian privacy activist behind the overhaul of Safe Harbor Agreement. See the [report](#).

[Read more >>](#)



On Oct 16th, 2015, the [2nd Edition](#) was held during the largest South American free software conference in **Iguaçu, Brazil**, and gathered distinguished minister of IT of Brazil, Marcos Mazoni, Rogerio Winter, a high-ranking official of the Brazilian Cyber Command, the CEO of the most advanced crypto company in Brazil, Kryptus, and more experts.

[Read more >>](#)



On Sept 24-25th 2015, the [1st Edition 2018](#) was held in **Brussels**, with a high-level set of speakers, including recognized IT security experts such as Bruce Schneier and Bart Preneel, and from the IT security institutions, such as the Head of Information Superiority of the European Defence Agency, and more. See the [report](#).

[Read more >>](#)

# Free and Safe - Editions 5-7th



On **January 29th 2020**, the **7th Edition** was held in **Zurich**. A closed-door Pre-Conference was held on the same day of the **7th Edition** in **Zurich**, reserved to entities actively interested to join as founding members of the main concrete initiative grown out of **previous editions**, the **Trustless Computing Certification Body**, which was adhered by **Digital Switzerland, Swiss Ministry of Finance, Credit Suisse, Sberbank, Accenture, InfoGuard, ETH, SATW, Kryptus, ElectroSuisse**, and others.

[Read more >>](#)



On **April 9-10th 2019**, the **6th Edition** was held in **Geneva**. The 2 day the conference revolved around the classic Free and Safe 4 Challenges, but emphasized the challenges and opportunities posed by IT confidentiality and integrity on the client-side, in particular in the sector of private banks. As usual, a roster of top local and international speaker honoured us of their presence.

[Read more >>](#)



On **May 4th 2018**, the **5th Edition 2018** was held in **Berlin**. High profiles joined, including **Reinhard Posch**, Chief Information Officer for Austria, **Andreas Reisen**, Head of Division “IT and Cyber Security in Critical Infrastructures and the Private Sector, Secure Information Technology” of the German Federal Ministry of the Interior, and more.

[Read more >>](#)

# Free and Safe - Supported By



FREE SOFTWARE  
FOUNDATION



POFF TENERIAS LINK



# Free and Safe - Previous Speakers (1/2)

**Michael Sieber** – Head of Information Superiority at the **European Defence Agency**. (2012-2016)

**Joseph Cannataci** – **UN** Special Rapporteur on the Right of Privacy.

**Reinhard Posch** – Chief Information Officer of the Federal Republic of **Austria**. Formerly Chairman of the Board of ENISA

**Wojciech Wiewiórowski** – **Deputy European Data Protection Supervisor**

**Achim Klabunde** – Head of Sector IT Policy at European Data Protection Supervisor

**Thomas J. Ackermann** – Strategy & Rapid Innovation-KdoCIR-**German Federal Armed Forces**

**Andreas Wild** – Former Executive Director at **ECSEL JU**, the largest EU R&D public funding program for microelectronics (150M€/ year)

**Jan Philipp Albrecht** – Former Vice-Chair of the Committee on Civil Liberties, Justice and Home Affairs (**LIBE**) of the **EU Parliament**

**Marit Hansen** – Data Protection Supervisor of the State of Schleswig-Holstein, Federal Republic of **Germany**

**Bart Preneel** – Former President at International Association for Cryptologic Research. Director at **COSIC KU Leuven**. Arguably EU's most peer-recognized IT security expert and researcher

**William R. Pace** – Executive Director, World Federalist Movement-Institute for Global Policy (WFM-IGP). Convener of the Coalition for the International Criminal Court (CICC) since 1995.

**Andreas Reisen** – Head of IR security standardization programs at **German Federal Ministry of the Interior**.

**Jovan Golic** – Former Privacy, Security and Trust Action Line Leader of EIT Digital

**Marcos Vinicius Mazoni** – President of SERPRO, the main Brazilian IT Public Agency, delegated by Rouseff to counter NSA spying.

**Pierre Chastanet** – Senior Policy Analyst at EU Parliament Science and Technology Options Assessment unit (STOA) and the EU Parliament LIBE Committee Secretariat

**Renaud Sirdey** – Director of Research at Commissariat à l'Énergie Atomique, **French Department of Energy**

# Free and Safe - Previous Speakers (2/2)

**Bruce Schneier** – Arguably the **world's most-renowned IT security expert**. Board Member at Electronic Frontier Foundation, OSI and EPIC. CTO at Resilient Systems, IBM. Fellow at Harvard Law School

**Yvo Desmedt** – World-renowned cryptographer, and pioneer of threshold cryptography

**Richard Stallman** – President of the **Free Software Foundation**. Founder of the Free Software movement

**Roberto Gallo** – CEO and Chief Scientist at KRYPTUS. Coordinator of the Cybersecurity Committee at the Brazilian Defense Industry.

**John Calian** – **Head of the Telekom Innovation Laboratories**

**Eric Drexler** – Senior Visiting Fellow at the Oxford Martin School, Oxford University, and Researcher and Internal Advisor to the **Future of Humanity Institute (FHI)**, led by Prof. Nick Bostrom, nanotechnology pioneer and AI security expert

**Paul Nemitz** – **Director for Fundamental Rights and Union Citizenship in the EU Commission's Directorate-General for Justice and Consumers**

**Steven Bellovin** – IT Security Professor at **Columbia University**. Co-author of foundational papers on state attempts to reconcile cyber-investigation and privacy ([1997](#), [2013](#))

**Bjoern Rupp** – CEO of **GSMK Cryptophone**, leading mobile device security provider

**Koen Maris** – CTO at **ATOS**. Former CSO at Telecom Luxembourg

**Melle Van Den Berg** – Managing Consultant at **CapGemini** Cyber Security Consulting.

**Max Schrems** – Leading **Austrian privacy activist**. Initiated a lawsuit questioning the compliance of the Safe Harbor agreement between EU and US

**John C. Havens** – Executive Director of the IEEE Global Initiative for Ethical Considerations in the Design of AI Autonomous Systems

**Roman Yampolskiy** – World-renowned AI superintelligence safety expert and professor. Author of the book “Artificial Superintelligence”

**Kai Rannenberg** – Chair at Deutsche Telekom, Chair of Multilateral Security at Goethe University



+



We are building a highly **democratic**, competent, resilient, and independent **Trustless Computing Certification Body** (TCCB). It will standardize, certify and regulate **interoperable** digital systems for human communications and their resulting digital sphere, **Seevik Net**, which aims to achieve **radically-unprecedented levels of confidentiality, integrity, and democratic control**, while concurrently ensuring *legitimate* lawful access.

## Year 1940s

- Huge advances during WW2 in cryptology and cryptanalysis, which fast becomes central for geopolitical predominance.



## Year 1993

- Biden proposes draft lawful access law
- US proposes voluntary Clipper Chip
- “Unbreakable” Encryption widely available
- Start of “Crypto Wars”
- Governments start breaking all IT and standards to prevent “going dark”

Year **2000**.  
The Promise of the Internet  
for Freedom, and Democracy.



Year **2021**.  
The Promise was  
turned on its head.

# Year 2020: A World ruled by state and non-state hackers

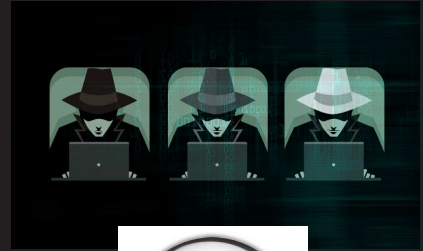
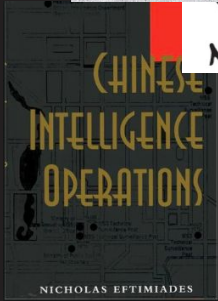
State

6\$

trillion

Non-state

mostly unreported or  
undiscovered



AI

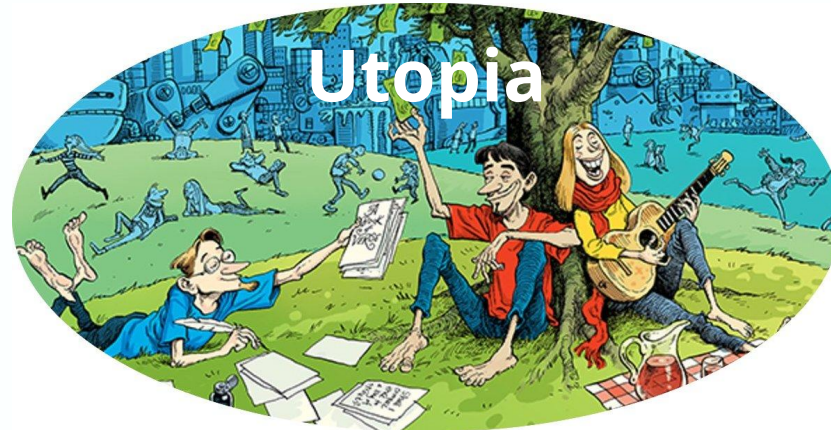
# Year 2020-2021: Covid-19 & Tech Boom



Years **2040, 2060, 2100**

**Catastrophic  
Risk**

**Existential  
Risk**



# Huge Latent Demand for Much Higher IT Security



Cybersecurity is the 2nd greatest **concern** of high net-worth individuals, after “their country politics”  
(source: UBS poll)

US citizens **fear** cybercrime twice more than any other crime  
(source: Gallup poll)

By 2022, yearly IT security sales will be \$250 billion while cybercrime cost will hit **\$2 trillion**  
(source: Accenture)

=

Nothing money can buy: a huge unmet demand.

**Like rain and lightnings**



# Literal Source of the Problem

**Hyper-complexity** of systems and supply-chains.


**Obscurity** in hardware and software design, and fabrication.

**Unverified Trust** in organization, people and systems.



# Ultimate Source of the Problem

But then is it really a technical problem?

 <b>Federal Aviation Administration</b>	One accident every 16 million flights ✓
<b>IAEA</b> International Atomic Energy Agency	17 nuclear nations. We are still alive! ✓
<b>1.6bn</b> phones made every year	Each one hackable by a teenage hacker. ✗

=

Everything is broken, by design, at birth, by powerful nations to retain legitimate investigation capabilities to prevent grave crimes



# Are Standards and Certifications Broken **By Design**?

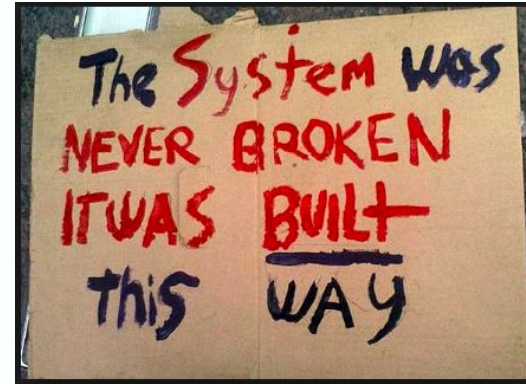
Aviation



Nuclear



IT



Since 9/11, given a stark choice between privacy and safety, western citizens voted for safety.

# The Impossible Choice



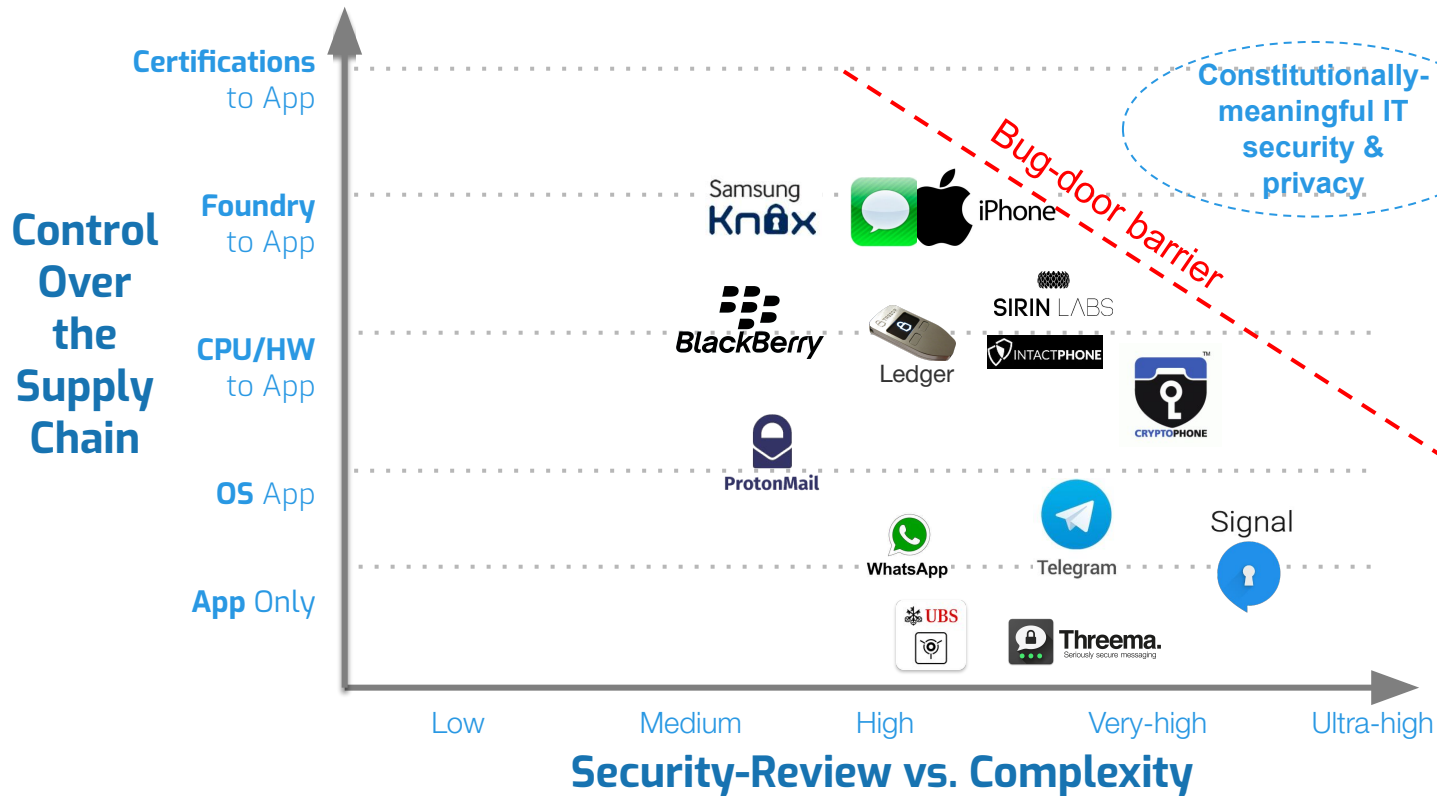
# Inadequacy of Current IT Security Certifications

**Current standards are broken and non-comprehensive by design, with plausible deniability, in order to enable lawful access.**

(e.g. ETSI, CENELEC, Common Criteria, FIPS, Trusted Computing Group, Global Platform):

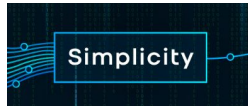
1. **do not certify a complete end-2-end computing experience** over its **entire lifecycle**.
2. **do not include all critical hardware design and fabrication phases**, or with insufficient requirements;
3. **require dubious crypto standards, such “national crypto standards”**, including custom elliptic cryptographic curves, that leave substantial doubts about the ability of advanced threat actors to bypass them;
4. **certify components that are critically dependent or connected** to other devices that are not subject to the same certification processes;
5. **have very slow and costly certification processes**, due to various organizational inefficiencies and to the fact that they mostly certify large (and often new) proprietary target architectures, rather than an extension of certified and open ones.
6. (!) are **developed in opaque ways and processes**, are only **very indirectly and inadequately citizen-accountable**, and **vulnerable to various pressures** from governments and commercial interested;

# Inadequacy of Current Client IT solutions



- Over-the-Top Endpoint Security Solutions:**
- Crowdstrike
  - Symantec
  - Trend Micro
  - Sophos
  - McAfee
  - Kaspersky
  - Palo Alto Networks
  - Fortinet
  - Panda Security
  - Fireeye
  - F-Secure
  - Check Point
  - SentinelOne
  - Cylance

# Solution: TCCB Four Unique Safeguards



## 1. Unique **Transparency:**

All critically-involved hardware and software publicly-inspectable in their source designs.

## 2. Unique **Review vs. Complexity:**

Extreme levels of security-review in relations to complexity by independent “ethically aligned” experts

## 3. Unique **Oversight:**

Including citizen-witness for chip fabrication, and citizens-juries for hosting room access, also for **legitimate lawful access.**

## 4. Unique **New Certifications:**

with an **holistic zero-trust** approach and with extreme technical-proficiency, citizen-accountability, ethics and resiliency against government pressures..

# SOLUTION: TCCB & Seevik Net

## TCCB

Trustless  
Computing  
Certification  
Body



**TCCB**  
**Level-B Client Apps**  
**(mainstream stores)**

iOS Harmony OS android

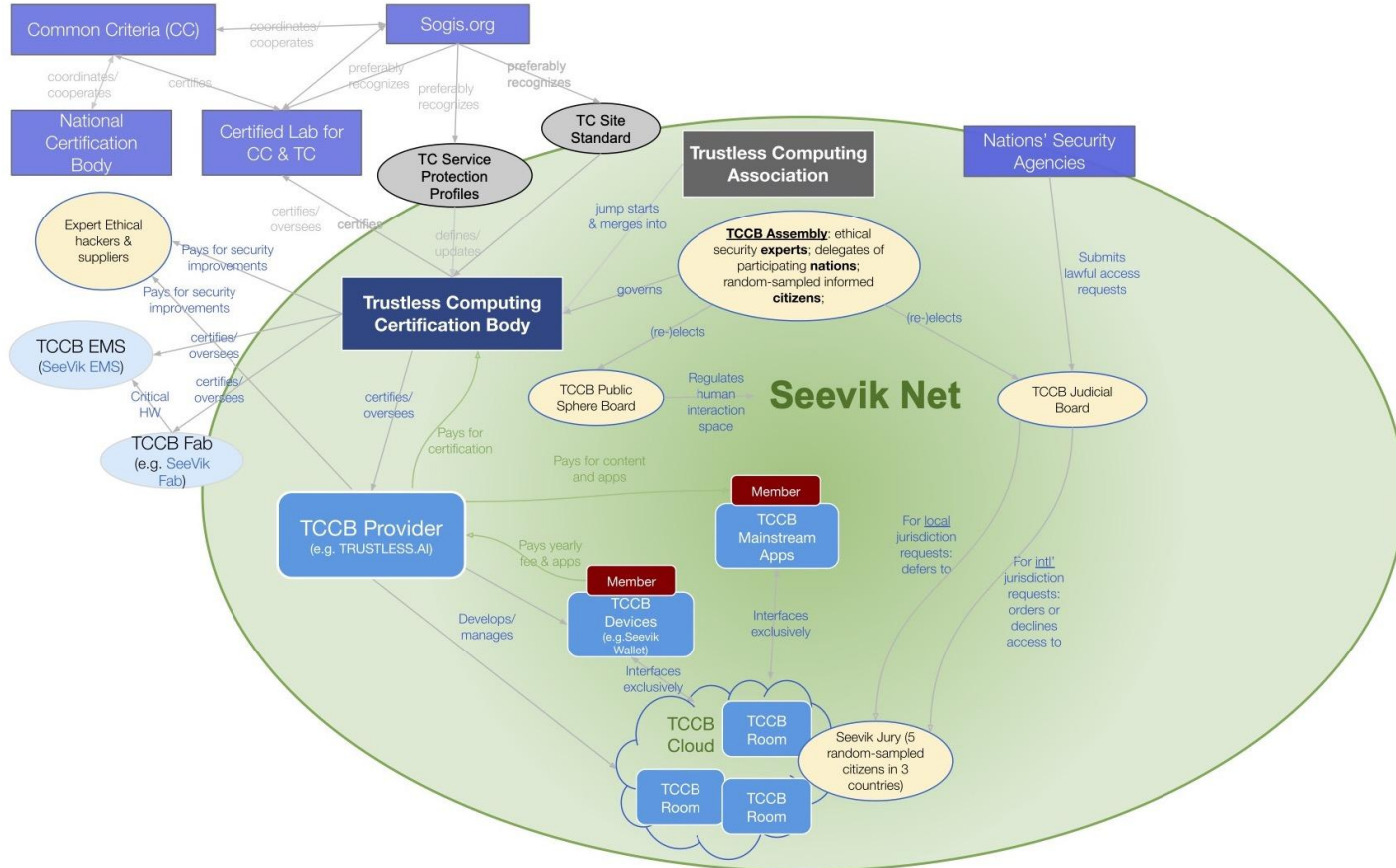
**Seevik Net**

**LFoundry** **TRUSTLESS AI**  
**KU LEUVEN** **DEK**  
**CONFIDENTIAL** **kryptus**  
**TCA** Trustless Computing Association **CONFIDENTIAL** **JRC**

**TCCB**  
**Devices & Level A**  
**Clients Apps**

**Ruffi Our**  
See trustless computing for info and inspiration on the wallet casing

# Solution Holistic Diagram





# TCCB: Ultimately it is all about **Governance!!**

## Governance aims are to maximize:

- Global democratic accountability
- Technical proficiency
- Resilience against undue pressures
- Altruism/selflessness

## TCCB Assembly:

- **25%: Scientific & Ethical Advisory Board.**
- **30%: Global Citizens' Assembly.**
- **30%: Current and Past Parliamentarians of Democratic Nation-states.**
- **10% Other:**
  - 3%: Organizational Users,
  - 3%: Individuals Users,
  - 3%: Technical Partners of TCCB-compliant IT services
  - 6% TCCB Member NGOs.
- **Later:** when at least 8 “more” **democratic nations** from 3 continents join, they will share 30% of voting rights, diluting others.

# TCCB: Trustless Computing Paradigms (1 /2)

1. *assumes* that extremely-skilled attackers are willing to devote even **tens of millions of Euros to compromise** the supply chain or lifecycle, through legal and illegal subversion of all kinds, including economic pressures.
2. *provides* extremely user-accountable and technically-proficient **oversight** of all hardware, software and organizational processes *critically* involved in the entire lifecycle and supply chains;
3. *provides* **extreme levels of security review intensity relative to system complexity**, for all *critical* components; and includes only publicly verifiable components
4. *includes* only open innovations with **clear and low long-term royalties** (<15% of end-user cost) from patent and licensing fees, to prevent undue intellectual property right holders' pressures, lock-ins, patent vetoes and ensure low-costs affordable to ordinary citizens;
5. *includes* only critical components that are **publicly inspectable in their source designs**, and strongly minimizes the use of **non-Free/Open-source software** and firmware, especially in critical components.
6. is subject to **standards-setting and certification institutions** conceived with the utmost care to maximize the likelihood that its governance will be and sustainably remain, highly citizens-accountable, **technically-proficient, effective, independent, ethical, and resilient** to undue processes from powerful state and non-state actors.
7. ensures that the **staff, management and shareholders of the Provider** of TCCB-compliant IT service, and its suppliers, who are in a position to significantly influence the security of the Service - while distrusted by default, as per the other TCCB paradigms - will be deeply vetted, background-checked and KYCed (know-your-customer) to estimate the likelihood that they may decide to, or be induced to, maliciously introduce backdoors or bug-doors for profit, extortion, political reasons, etc.

# TCCB: Trustless Computing Paradigms (2/2)

8. *will* provide an **in-person offline key and data recovery function**, to benefit end-users in case of loss of death or loss passcodes, and enable a voluntary (i.e., in addition to current law requirements) compliance to only *legitimate* international lawful access requests. This function will rely on the setups and management process of hosting rooms in multiple jurisdictions that implement unprecedented safeguards. All sensitive data and keys are stored in “secret-sharing” architecture” in **3 hosting rooms in 3 different nations, part of different military/intelligence alliances**.
- The legality and constitutionality of local-jurisdiction lawful access requests civilian court orders and absence of blatant unconstitutionality of other supposed legal authority or executive order will be ensured by inherently requiring that **physical access by anyone to such hosting rooms is conditional on the physical presence and approval of at least 5 randomly-selected citizen-jury-like body**, in addition to system administrators and an expert legal counsel, that will assess the compliance of the requests to national law, constitution and the *UN Universal Declaration of Human Rights*.
  - For foreign-jurisdiction requests, then such request will be vetted by a **TCCB Judicial Board**, made of 15 recognized experts in international law, civil rights, and public security, who have been elected or appointed to high offices, such as a leading international court, the highest court of a large democratic nation. If approved, such a Board instructs the TCCB Jury as to what data should be conceded to the requesting public authority.

TCCB Cloud, detail of the lawful access mechanism: <https://www.trustlesscomputing.org/tccb-cloud>

Trustless Computing Paradigms: <https://www.trustlesscomputing.org/paradigms>

Academic Detailed Case: <https://www.trustlesscomputing.org/position-paper>

# No one wants to carry an extra device: the **Form Factor**

Translucent Casing



Translucent Casing

**2mm-thin  
TCCB-device**

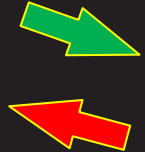


**5-6mm thin  
Android phone**



# New Technologies: for good or for bad?

AI



Security and  
Privacy of the User

Blockchains



Quantum  
Computing



# Milestones



**Seevik Phone PoC Device, with 3 Partners,** and Fusion Accelerator in Geneva.



Spinoff raised **CHF 180k** from 4 external EU and Swiss angels and startpers



Nominated among top 5 for **2020 Swiss Fintech Awards** and **PwC Cybersecurity Days**.

2016

Aggregated over 20 high-assurance CPU, OS, foundry partners, and 2 EU nations, in 3 **R&D initiatives** for TCCB and Seevik Pod. Produced a binding **consortium**, 350 pages of technical docs, and low-level initial prototyping.



2017

Held **7 editions of the Free and Safe in Cyberspace** conference series in Brussels, NYC, Berlin, Geneva, Zurich. to promote TCCB with top speakers and partners.



2019

Engaged at top execs in **2 of top 4 global phone makers**, for strategic partnership for Seevik Phone and TCCB.



2020

Evolved our PoC Device and offering while negotiating a 6-figures go-to-market deal with 15+ top executives of **3 of top 4 Swiss private banks** & top TCCB prospects.



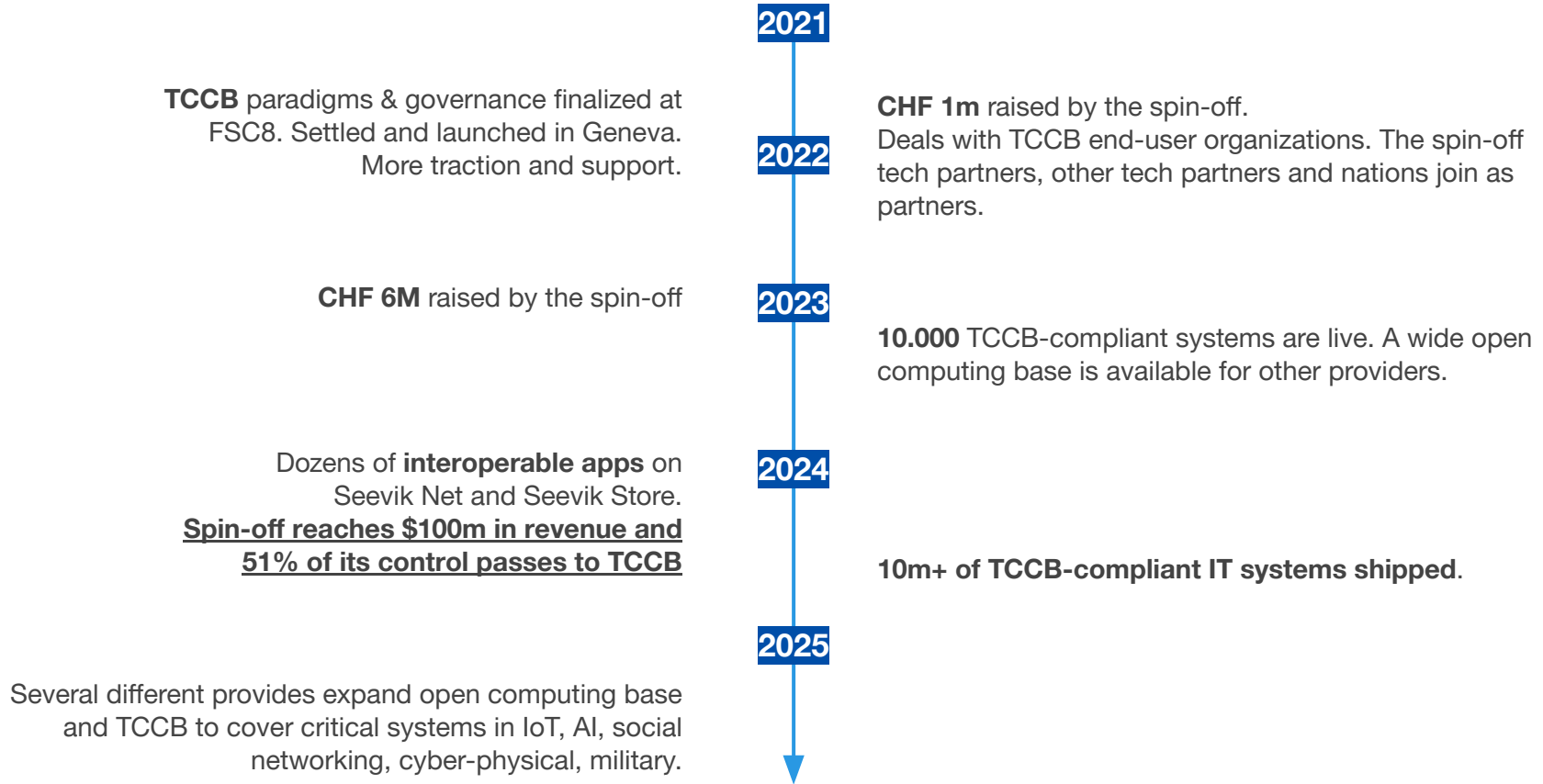
2021



Seevik Phone Demo

1.46 minutes

# Roadmap





# Vision

Once the TCCB and an initial TCCB-complaint systems have been **proven** for the most high-risk human communications, it will be:

(A) Embedded as sort of "ultra-secure smart backscreen" in the back of **hundred of millions of commercial phones.**

(B) Deployed as standard **root-of-trust for the most privacy-sensitive or safety-critical** cyber-physical and autonomous/AI systems, civilian and military.



# TCCB Strategic Positioning

**TCCB**

Trustless  
Computing  
Certification  
Body

Initially complies to:



3+

Submitted through:



Submitted through:

EU Cybersecurity  
Certification Framework



# TCCB: as basis for global institutions for Peace and Democracy



International Atomic Energy Agency

**IAEA**

**TCA**

Trustless  
Computing  
Association



**A Global Cyber-Attribution  
Organization – Thinking it  
through**

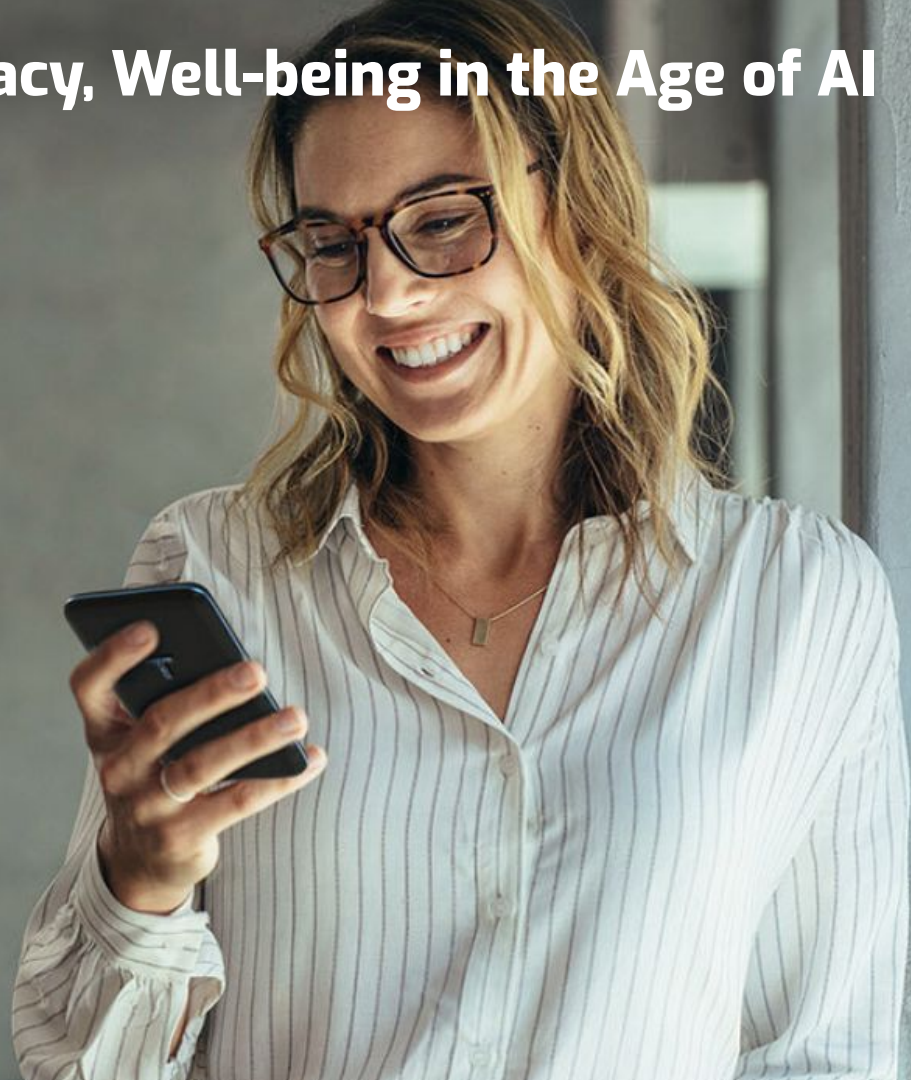


**OPCW**

Organisation for  
the Prohibition of  
Chemical Weapons

*Cour  
Pénale  
Internationale  
International  
Criminal  
Court*

# Freedom, Democracy, Well-being in the Age of AI





+



We are building a highly **democratic**, competent, resilient, and independent **Trustless Computing Certification Body**, that will standardize, certify and regulate **interoperable** hardware and software systems for human communications and their resulting digital sphere, **Seevik Net**.

They jointly aim to achieve **radically-unprecedented levels of confidentiality, integrity, and democratic control for our digital lives**, while concurrently ensuring *legitimate* lawful access.



# FREE AND SAFE IN CYBERSPACE 8TH EDITION

JUNE 24-25TH, 2021

📍 Hybrid Online/Offline - Geneva and ZOOM