TCA Trustless Computing Association

Trustless Computing Certification Body

Can a new international certification body deliver
radically unprecedented IT security for all,
while at once ensuring legitimate lawful access?

Rufo Guerreschi | Exec. Dir. – rufo@trustlesscomputing.org

The *Trustless Computing Certification Body* is an initiative of the *Trustless Computing Association* to create a new cybersecurity certification body. This will be suitable to confidently validate IT services that sustainably deliver levels of **security and privacy that radically exceed current state-of-the-art,** while at once solidly enabling only legitimate and constitutional **lawful access**.

Both will be achieved through uniquely uncompromising “zero trust” security-by-design paradigms down to each critical lifecycle component, including the certification governance itself.

Are meaningful **freedom** and public **safety** really an "*either-or*" **choice**?

Or are they instead "*both-or-neither*" **challenge** that can and must be solved?!

Credits: https://ali-radicali.deviantart.com/art/Safety-or-Freedom-266033539

Free and Safe in Cyberspace?

CHALLENGE A: freedom

What paradigms and certifications can validate IT and AI systems that provide security and privacy that are radically more secure than state-of-the-art?!

CHALLENGE B: freedom + safety

How can we achieve such *ultra-high* assurance IT while enabling legitimate and constitutional – no more, no less – lawful access? so it does not get abused or outlawed?


Public Sphere
Private Sphere
street
squares
Home
church
Party branch
Public Sphere
Private Sphere

“Among EU member states, it’s hilarious: they claim digital sovereignty but they rely mostly on Chinese hardware, on US American software, and they need a famous Russian to reveal the vulnerabilities"

Stated by Michael Sieber, former Head of Information Superiority of the European Defence Agency, and current Director at BAAINBw , at our 1st Free and Safe in Cyberspace in 2015

How bad is digital freedom tody?

1983: Promises for all

2013: Reality for nearly all

Is public safety a big problem?

- Worry about lightning, bees OR Islamic terrorism?
- Popular support for ISIS
- Ultra-nationalism on the rise
- Corruption by top politicians, heads of state, and judiciary
- Luxleaks and Panama Papers financial fraud and immorality.

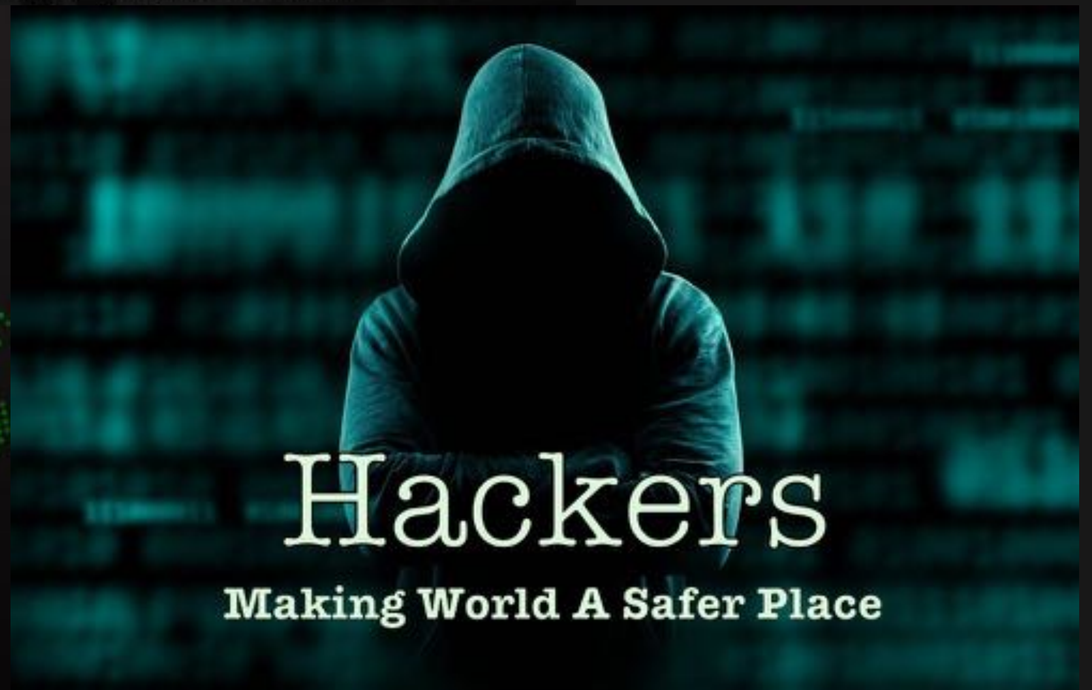
CHALLENGE A: freedom

What paradigms and certifications can validate IT and AI systems that provide security and privacy that are radically more secure than state-of-the-art?!

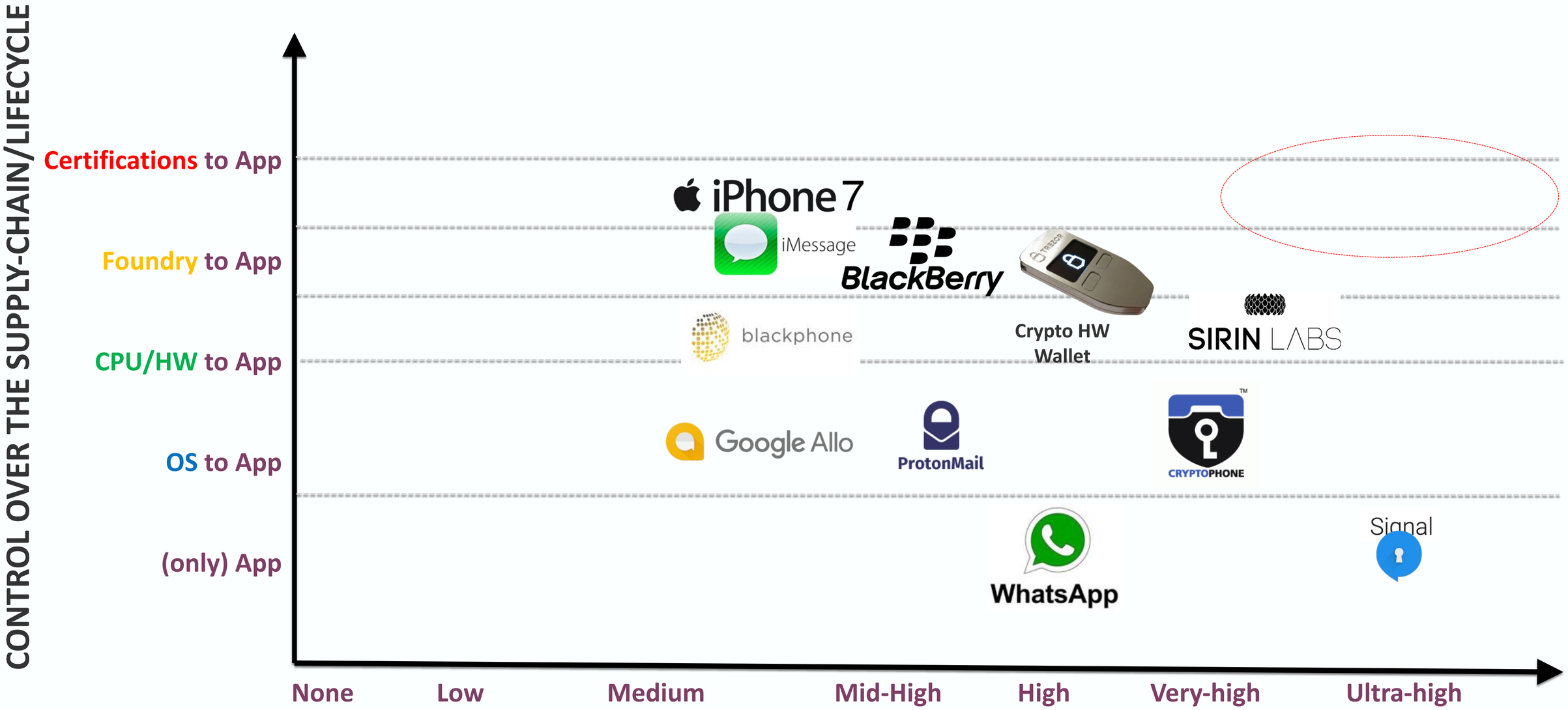
World as a Hacker Republic

Malicious hackers

Ethical hackers



Why? Black Boxes Everywhere



Why? HW Design & Fabrication

Michael Sieber, former Head of Information Superiority of the European Defence Agency stated at our 1st Free and Safe in Cyberspace (2015): "*Among EU member states, it's hilarious: they claim digital sovereignty but they rely mostly on Chinese hardware, on US American software, and they need a famous Russian to reveal the vulnerabilities*"

Bruce Schneier (2014): "From what we've learned, we should assume all mainstream CPUs to be compromised"

US Defense Science Board (2005): "Trust cannot be added to integrated circuits after fabrication"

Problem with current IT solutions

IT

AI

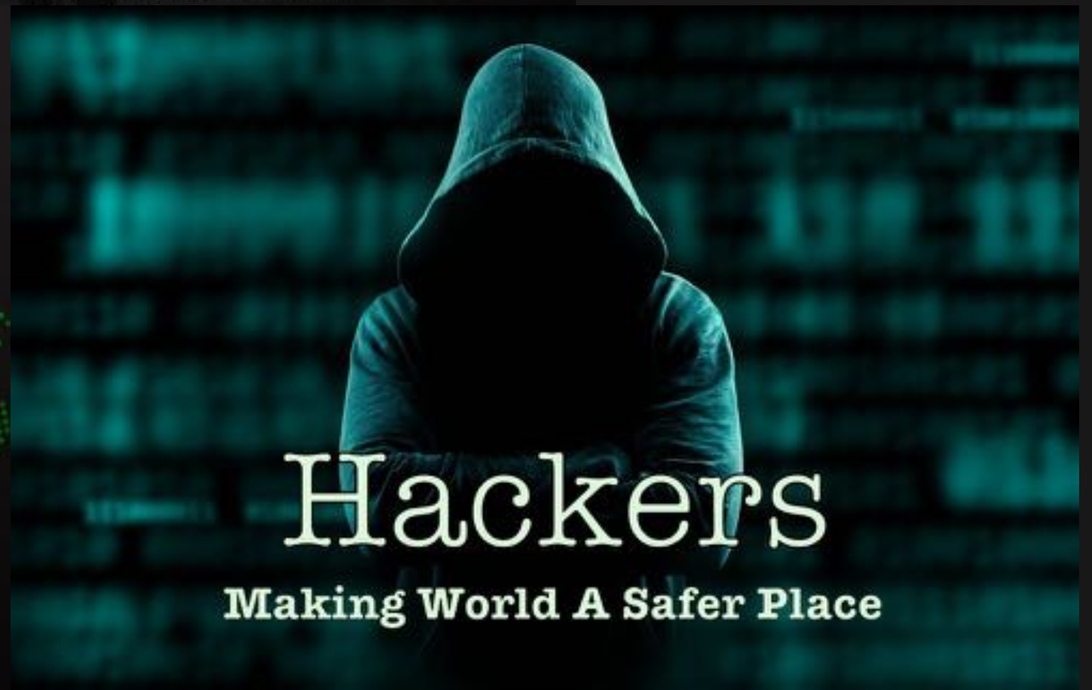
Superintelligence or Singularity

processes?

World as a Hacker Republic

Malicious hackers

Ethical hackers



Why? IT security certifications today

Whether state-driven (i.e. ETSI, CEN, CENELEC, Common Criteria, FIPS, etc.) or industry-driven (i.e. Trusted Computing Group, Global Platform, ETSI, etc.). All of them have one or more of the following shortcomings:

1. do not certify any complete end-2-end computing experience and device service and lifecycle, but just parts of devices, server-side service stacks or components;
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 devices that - are embedded or are critically 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. **(ultimately) they are developed in opaque ways by standard organizational processes that are only very indirectly (and inadequately) user- or citizen-accountable**, and subject to various pressures of undetermined provenance;

EU Cybersecurity Strategy (2013)

- "*.... promote cyberspace as an area of freedom and fundamental rights. Expanding access to the Internet should advance democratic reform and its promotion worldwide. Increased global connectivity should not be accompanied by censorship or mass surveillance.*"
- "*The need for requirements for transparency, accountability and security is becoming more and more prominent*".
- *"The* ***same laws and norms that apply in other areas of our day-to-day lives apply also in the cyber domain***. Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in *the Charter of Fundamental Rights of the European Union* and EU core values. Reciprocally, individuals' rights cannot be secured without safe networks and systems".
- "*..., as well as possibly establish voluntary EU-wide* ***certification schemes*** *building on existing schemes in the EU and internationally.*"
- "*The EU will place a renewed emphasis on dialogue with* ***third countries****, with a special focus on like-minded partners that share EU values."*.
- "*There is a risk that Europe not only becomes excessively dependent on ICT produced elsewhere, but also on security solutions developed outside its frontiers. It is key to ensure that* ***hardware and software components*** *produced in the EU and in third countries that are used in critical services and infrastructure and increasingly in mobile devices are trustworthy, secure and guarantee the protection of personal data."*

EU Defense Goals and Challenges

- **EU Cyber Defence Policy Framework** states: "*So it will be crucial to maintain close cooperation with the private sector, ... It is also important to foster an assured and competitive European industrial cyber security supply chain by supporting the development of a robust European cybersecurity sector including through involvement with SMEs". "Contribute to develop further and adapt public sector cyber security and defence organisational and technical standards for use in the defence and security sector. Where necessary, build on the ongoing work of ENISA and EDA".*
- **EU Digital Agenda Commissioner** Oettinger recently stated "*There are some who do not respect privacy of our citizens. Some do not want to play on fair terms with our businesses. We need to safeguard our values and interests. It is in the interest of all citizens that we ensure a prosperous and a secure European digital future. That means that we have to be leaders in these technologies and support international standardization efforts that ensure high levels of security, proven by certification where necessary.*"
- **EDA Head of Information Superiority,** Michael Sieber, stated (m3.37) at our Free and Safe in Cyberspace: *"Among EU member states, it's hilarious: they claim digital sovereignty but they rely mostly on **Chinese** hardware, on US **American** software, and they need a famous **Russian** to reveal the vulnerabilities"*

CHALLENGE B: freedom + safety

How can we achieve such *ultra-high* assurance IT while enabling legitimate and constitutional – no more, no less – lawful access? so it does not get abused or outlawed?

Are meaningful freedom and public safety
an "*either-or*" choice,
or a **solvable** "*both-or-neither*" challenge?!

Busting some myths about lawful hacking

1) Lawful cracking is hugely problematic but inevitable. Mostly legal and increasingly so in US and EU, **(B)** all nations are greatly increasing investments EU (Zitis, etc.). Very unlikely that it will be made illegal**,** because (a) need to pursue criminals (b) all other states are developing those capabilities (c) essential to improve cyberdefense. **But** they have great problems of highly scalable abuse, even if perfectly regulated, and to promote criminal vulnerability market

2) Most current "lawful cracking" access systems are plausibly cracked. Plausibly extremely prone to abuse by third parties, especially private ones. No adequate standards at all. The 1st of such private system, from the 80's (**Promis by Inslaw**) was developed by Mossad former agents and adopted by CIA to be sold to tens of governments worldwide so that they could spy and interfere with their most sensitive intel actions.

3) Nations are not really about to or really intentioned to "outlaw crypto" or mandating a new "Clipper Chip", or is it smoke in the eyes? Outlawing crypto or mandating all device implement technical requirements that enable state remote access through due legal process would present unacceptable risks for privacy (Clipper Chip), be hugely costly and useless (steganography?! Status quo is fine for security agencies . They pretend to go dark to preserve and extend their authorities, as it is in their mission.

SO?! We should be on the offensive and not defending what we don't have (i.e. meaningful privacy) and see if the same radical safeguards need for ultra-high security can deliver accountable lawful access.

A new certification body?!

Key & unique concepts: (1) Complete verifiability, extreme compartmentation and minimization and sufficiently extreme verification relative to complexity of all critical HW&SW; (2) Citizen/peer-witness oversight of all *critical* service components, including ICs fabrication, and server-room access, including for lawful access requests; (3) Very high tech proficiency & citizen-accountabily of governance.

Overcoming Privacy/Safety Dichotomy & Reaching Critical Mass: provides unique extreme safeguards for transparently reconciling lawful access and personal confidentiality, which is crucial for legal sustainability of a critical mass of dual-use investments for create a EU-domestic "*trustworthy computing base*".

Strategy: Kick-start an extremely open and resilient **ecosystem**, a **certification body**, and a **complete critical SW/HW stack** for an wide-market end-2-end computing platform, for basic voice & text communications, that is devoid of the need or assumption of trust in anyone or anything; except in the intrinsic resilience of all socio-technical organizational processes *critically* involved in the entire lifecycle (from standards setting to fabrication oversight) against decisive attacks of up to tens of millions of euros, as assessable by an informed and moderately educated citizen.

Trustless Computing Paradigms (1 to 5)

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, and strongly minimizes use of non-Free/Open-source software and firmware.

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.

Trustless Computing Paradigms (6 of 8)

6. *includes* only highly-redundant hardware and/or software **cryptosystems**, whose protocols, algorithms and implementations are **open**, **long-standing**, **extensively-verified and endorsed**, and with significant and scalable post-quantum resistance levels.

7. *is continuously certified by* an **extremely technically-proficient and user-accountable independent standard/certification body governance**.

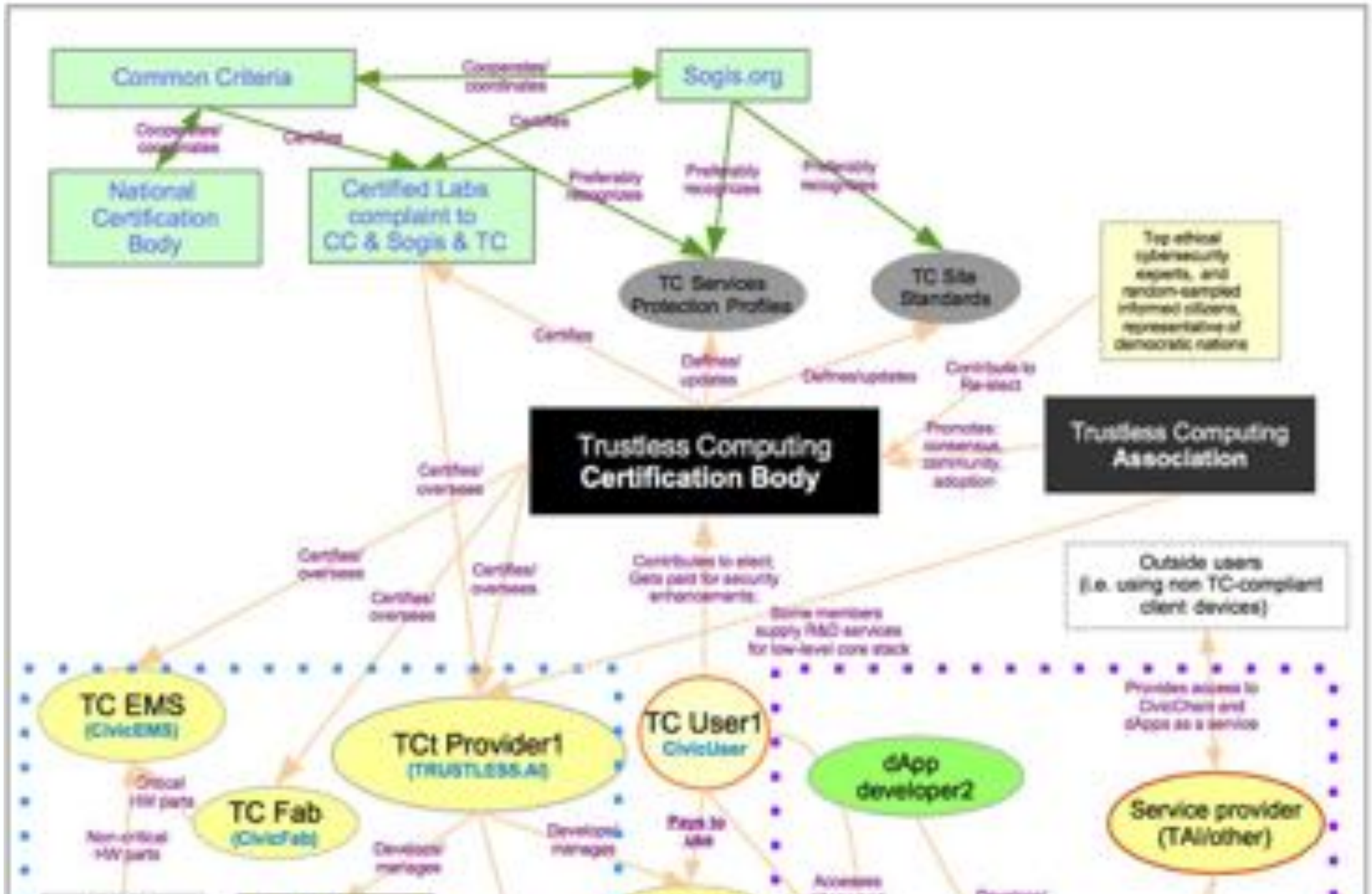
8. *will* provide an **in-person offline key or data recovery function**, to benefit of (1) end-users, in case of loss of death or loss passcodes, and (2) to enable a voluntary (i.e. in addition to current law requirements) compliance to legitimate lawful access requests:

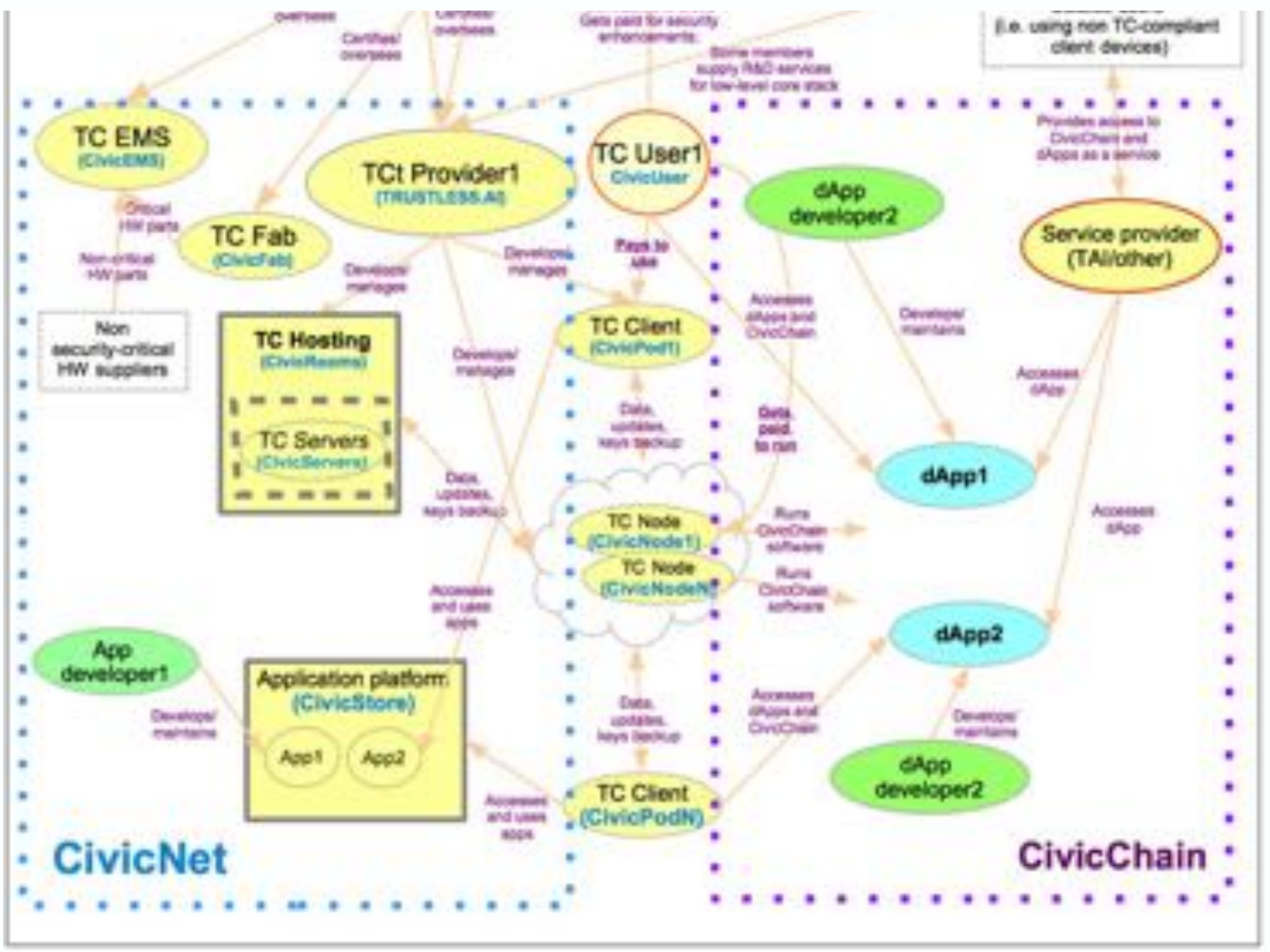
   a) This function will rely on setups and management process of **multiple hosting rooms in multiple jurisdictions** that implement unprecedented safeguards.

   b) In addition to state-of-the-art security, these will utilize only **TC-compliant endpoints and door locking mechanisms**.

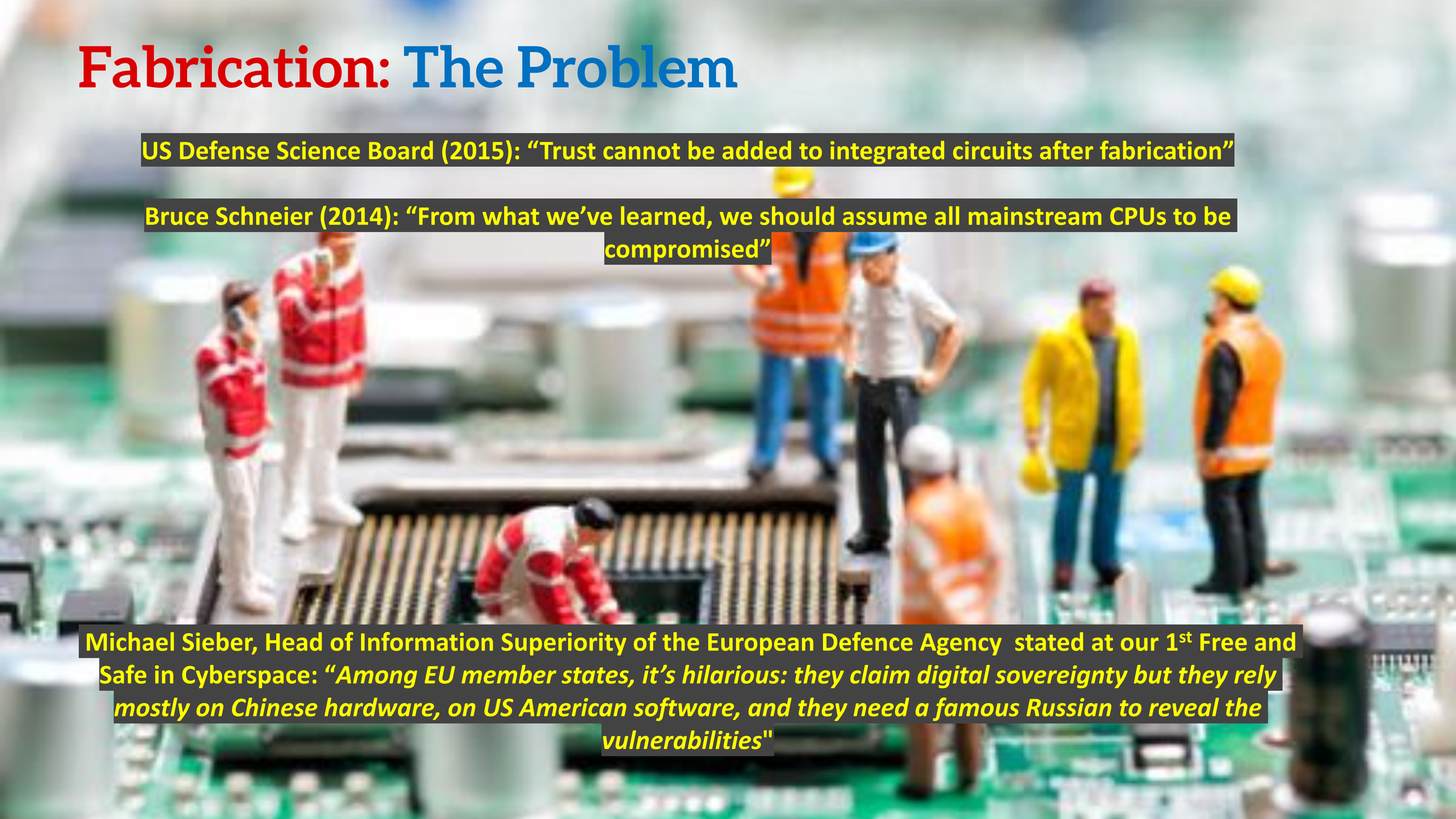
   c) Access to such rooms for any reason, always requires the express approval of an attorney and 5 trained citizen-jurors, that are managed and accountable to the Certification Body - that will assess the compliance of the requests to national law, constitution and EU Charter of Human Rights. Any kind of remote access is physically disabled.

TCCB & CivicNet Architecture (1 of 2)




TC EMS
(CivicEMS)
TCt Provider1
(TRUSTLESS.AI)
TC User1
CivicUser
dApp developer2
Service provider (TAI/other)
TC Fab
(CivicFab)
TC Hosting
(CivicRooms)
TC Servers
(CivicServers)
TC Client
(CivicPodT)
Non security-critical HW suppliers
dApp1
TC Node
(CivicNode1)
TC Node
(CivicNodeN)
dApp2
App developer1
Application platform
(CivicStore)
App1
App2
TC Client
(CivicPodN)
dApp developer2
CivicNet
CivicChain

Fabrication: The Problem



US Defense Science Board (2015): “Trust cannot be added to integrated circuits after fabrication”

Bruce Schneier (2014): “From what we’ve learned, we should assume all mainstream CPUs to be compromised”

Michael Sieber, Head of Information Superiority of the European Defence Agency stated at our 1st Free and Safe in Cyberspace: “*Among EU member states, it’s hilarious: they claim digital sovereignty but they rely mostly on Chinese hardware, on US American software, and they need a famous Russian to reveal the vulnerabilities*"

TrustlessSite Process

But how do we prevent abuse by criminals?!

JUN 18, 2013 @ 02:23 PM 70,906 VIEWS The Little Black Book of Billion

NSA Implementing 'Two-Person' Rule To Stop The Next Edward Snowden

At the **service** level.

TRUSTLESS.AI will provide **key recovery service** to all its customers, in case of user death or loss of password, as well as a way to comply to legal AND constitutional lawful access requests. Although the architecture is decentralized, partial temporary encryption keys are mandatorily saved daily into a redundant set of **TrustlessRooms**, whose physical access is under the direct management, certification and oversight of an international *Trustless Computing Certification Body* (TCCB). **The validity of civilian court orders AND absence of blatant unconstitutionality will be evaluated on-site by trained citizen-jury-like body assisted by legal counsels**. Its radically unprecedented technical and organizational safeguards will guarantee both users' rights and the crucial needs of the public security agencies.

At the **fabrication** level.

The public availability of all TRUSTLESS.AI critical SW & HW source designs **could enable criminal actors to produce their own CivicDevices for malevolent use**. Such threat will be extremely and sufficiently reduced by a combination of: (A) IP cores tied to specific, capital intensive fabrication processes, naturally not available on mini scale prototyping fabrication facilities and foundries; (B) current inability of malevolent states or groups to fully and truly control a suitable semiconductor foundry. (C) In the rare case in which terrorist groups may attempt to enter in agreements with suitable foundries, current Allied intelligence capabilities can make sure to either forcefully prevent it or, better, insert vulnerabilities in their fabrication processes to acquire in the future extremely valuable intelligence.

CivicNet: a TC-compliant Open **Computing Base**

A groups of **globally-rare or unique open high assurance IT supplier partners along the entire critical supply-chain stack** that have previously signed formal detailed IP & non-compete clauses for the creation of TRUSTLESS.AI Offering and the Trustless Computing Certification Body. Including:

World's largest Artificial Intelligence R&D center, a partner in our unique *CivicFab* **FOUNDRY OVERSIGHT** process. (*Germany*)

Maker of **World's 1st general-purpose CPU with publicly reviewable HW/SW designs.** *(Brazil)*

Leading free/open source high assurance **microkernel/OS L4re** with less than 11K lines of source code. Deployed for over 8 years in civilian and military domains. (*Germany*)

EU leading **CRYPTO** R&D center, lead by the most renowned EU cryptologist and IT security expert, Bart Preneel (*Belgium*)

A 200mm 110nm EU-based **FOUNDRY**, fully validated economic feasibility of our *CivicFab* oversight processes. (*Italy*)

CivicNet: a TC-compliant IT Service

CivicPod

2mm-thin ultra-secure device:

1. **Messaging** with other Pods
2. **Text co-editing** for contacts
3. **E-banking** with partner bank
4. **Cryptocurrency** HW wallet
5. **Blockchain** client

CivicDock

CivicPod docking station:

1. **Charger for phone &Pod**
2. **Anonymization and blockchain node**
2. **HDMI-switch** for long-form text editing.

(3d renderings)

Play our 2-minute product video at: www.TRUSTLESS.AI

TRUSTLESS.AI: a TC-compliant **Provider**

Seamlessly delivering **radically unprecedented endpoint cybersecurity**

to **(A)** the most critical human communications and transactions,

and then **(B)** to the *root-of-trusts* of safety-critical AIs.

Rufo Guerreschi | CEO – rufo@trustless.ai

Scale Up

Once market proven for use through a 2mm-thin device attachable to the back of any phone:

(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** autonomous/AI systems.

AI security, safety, privacy, and human control

If hacker can make one self-driving car remotely crash, it can likely do the same for thousands of units concurrently

Drone pilot arrested for dropping leaflets over 2 NFL stadiums, including Seahawks game

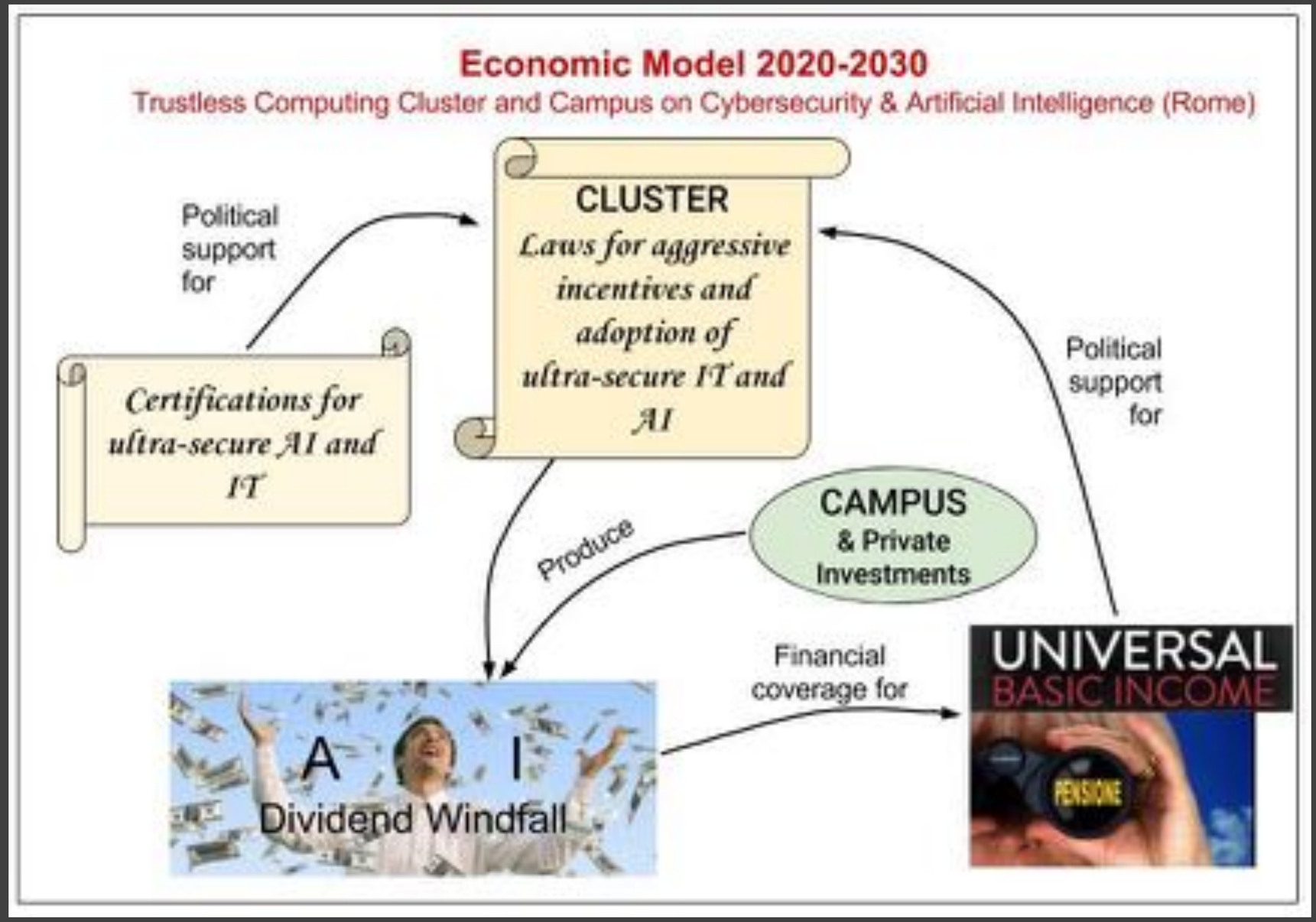
Why *deterministic* IT is key for AI security?

Makers of high-volume safety-critical civilian autonomous systems (robots, drones, self-driving cars) are **seeking to lower by 1-2 orders of magnitude the risk of concurrent remote critical hacking of thousands of product units during operation**, to achieve and sustain wide-market funding, uptake and legal authorization for mass-scale deployment in dense human environments.

TCCB will certify an open low-level computing base, lifecycle and certification governance processes - for their most critical deterministic sub-systems od security critical AIs- that radically exceed the state-of-the-art in resistance to malicious or accidental remotely exploitable critical vulnerabilities, by ensuring extreme levels of expert ethical inspection relative to complexity of ALL hardware and software components critically involved

AI Security and Control: the good case scenario

A Socio-Economic Model of Trustless Computing



Massive Dual-use Exploitation

- **SHORT-TERM**: It will cater to the most critical civilian and military **strategic communications**, and downward-compatible to mainstream military (EU/NATO SECRET) and civilian (eIDAS “high”) standards.
- **MID-TERM**: The guaranteed low royalty fees, open ecosystem, and highly-portable client-side form factor will support deployment in the **tens of millions** in the corporate, e-banking, government. The low-royalty regime, the addition of functional features, and reduction of unit cost at scale support wide scale consumer roll out in the tens of millions.
  Military: Added support for high-availability scenarios will enable to cater to such as: critical infrastructure, cyber-physical systems, **autonomous and semi-autonomous IT systems**, fixed and moveable, command & control systems for military missions. **Help EU/EDA lead within NATO in the development of a strategic and emerging niche of foundational IT capabilities**.
- **MID/LONG-TERM**: Make such new “EU trustworthy computing base” the global leading standard, with the consequent huge societal, economical and geostrategic benefits. Derivative of the results will spur ever more trustworthy IT systems in numerous domains and wide market applications. AI?! The platform and ecosystem will evolve to constitute a low-level computing base, standard and a governance model that is sufficiently trustworthy for large democratically-accountable advanced narrow and strong AI projects and systems, in critical sectors for the economy and society, to substantially increase their safety, robustness and “value alignment”.

Global Democratization & Security

TCA
Trustless
Computing
Association

International Atomic Energy Agency
IAEA

OPCW
Organisation for
the Prohibition of
Chemical Weapons

EVENTS

A Global Cyber-Attribution Organization – Thinking it through

TCA Trustless Computing Association

Trustless Computing Certification Body

Can a new international certification body deliver
radically unprecedented IT security for all,
while at once ensuring legitimate lawful access?

Rufo Guerreschi | Exec. Dir. – rufo@trustlesscomputing.org