Center for Digital Trust

www.c4dt.org

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

The Cambridge Analytica scandal, the WannaCry hijacking, the hacking of 1 billion Yahoo accounts,... How much do **you** *trust our digital infrastructure?*

For millennia, humans have developed trust-building mechanisms to facilitate interactions among people, businesses and governments: language, social norms, contracts, legislation, diplomacy...

We are becoming a digital society. Interactions are increasingly mediated by digital technologies. This results in traditional trust-building mechanisms becoming less effective. As a result, low levels of trust discourage us from engaging in new forms of interactions and constrain business opportunities or worse, cooperation might stall altogether if trust erodes further, due to large-scale data breaches by sophisticated criminals or due to nations taking casual approaches to mass surveillance and cyber warfare.

We must reinvent trust for the digital society. The global shift towards a digital society is an opportunity to create a technical, legal and ethical digital-trust framework that delivers stronger guarantees, is universal, and reduces the cost of achieving trust in the digital world.

Vision

A prosperous, cooperative and empowering development of our digital society will come from making it trustworthy. We firmly believe such *digital trust* can be achieved by

- Synergies between existing and emerging technologies, including blockchains, smart contracts, privacy-enhancing technologies, advanced cryptography, software verification and numerous other technologies that researchers and innovators are currently developing;
- Integrating the human, political, and economic implications of digitalization, thus aligning technologies, laws, industry standards, ethics and public perceptions;
- Proposing adequate and pragmatic solutions to enable companies, institutions and citizens worldwide to become *digitally trustworthy* and to create new opportunities.

Mission

The C4DT is a partnership between research, industry, the public sector and the civil society to imagine and realize a common vision for digital trust. Its mission is as follows.

- Identify opportunities. Shape the research agenda. Co-design technologies. Foster mutual learning and offer training. Facilitate meaningful exchanges at the individual level. We call this the C4DT Open Lab to emphasize its first mission as a connector of ideas, people, organizations, and scientific domains.
- Integrate key digital-trust technologies and practices into a high-quality platform. Identify best practices and provide expertise to partners to quickly prototype solutions. We call this the DTOP (Digital-Trust Open Platform).
- Facilitate the identification and setup of bilateral or multilateral application projects, to accelerate the deployment of cutting-edge commercially-viable solutions.

Values

The C4DT will be guided by the following values. And EPFL's experience of knowledge transfer will help maximize benefits for the partners.

- Excellence of research, in the tradition of EPFL: the foundation for an ambitious and long-term vision of digital trust.
- Collaboration in building a cooperative digital-trust infrastructure: supporting a diverse ecosystem of businesses in finance, insurance, and health, as well as the Genève internationale.
- Transparency, resulting from a publicly reviewable DTOP (open-source software): digital-trust solutions that emphasize consent and choice, and a clearly laid-out vision for digital trust.
- Neutrality and Ethics, in the tradition of Swiss institutions that play a global role as a facilitator and mediator.

These organizations support the development of the C4DT

CICR · ELCA · CISCO · CHUV · SICPA · Swissquote · swisscom · Swiss Re

Where next?

A small number of businesses and institutions, with a strong engagement in developing digital trust, will have the opportunity to become Founding Partners of the C4DT. Other partnership options will be made available after the C4DT becomes fully operational. For more information on the Founding Partner status, or the C4DT in general, please write to info@c4dt.org.

Center for Digital Trust — Technology and Research Outlook DTOP Concept

Technological Pillars

The DTOP will be a software platform enabling the development of secure and trustworthy applications. It will offer a test bench to research and demonstrate new digital-trust solutions. The DTOP integrates various technology pillars into a single, easily usable and high-quality platform. The first version of the DTOP will integrate three pillars, and more will be integrated in the future. They represent three fundamental and complementary elements of digital trust: privacy, accountability, and verifiability. Each pillar is guided by a technological vision:

Privacy Protection and Cryptography: Data will be handed to third parties, knowing that it benefits from unbreakable technological privacy guarantees; this extends to data on feature-rich online services such as public clouds. The loss of privacy in data analytics will be protected by similar technological guarantees. Its scope will also be better understood.

Blockchains and Smart Contracts: With higher transaction-processing capacities, lower latencies and no single points of failure, blockchains will become routine repositories for accountable information. Blockchain features will include private-information storage, identity management, and improved smart contracts. Blockchains will not only prevent retroactive modifications, but will offer further trust-related guarantees.

Software Verification: New trust-centric software-engineering processes and tools will make it possible to automatically verify that desired functionalities are maintained under all conditions, and to verify advanced trust-related properties. They will also help to automatically identify potential attack scenarios. The first to benefit from these technologies will be smart contracts and IoT applications with short program codes.

Application Verticals

Application verticals will explore opportunities that arise from using the DTOP. Bilateral projects conducted with partners in connection to application verticals will offer opportunities to use the DTOP to meet business needs and pursue competitive advantages. They will also guide development priorities to ensure that the DTOP remains a practical platform that delivers value to partners. To begin, the C4DT will pursue the five verticals described below. Additional verticals and the concept behind existing ones will evolve in collaboration with partners.

Finance: Cryptocurrencies and smart contracts will be trusted because quantitative models and empirical analysis take into account the underlying technology and the new applications they enable, such as ICOs. These models will influence the technological development of blockchains and smart contracts so that desirable trust and financial properties will be integrated in their technological core.

Critical Infrastructures: The security of critical infrastructures, such as energy grids and transportation infrastructures, will come from tight control of what can be trusted and what cannot. Every action and network access will be authenticated and controlled; access to data will be minimized using privacy-preserving techniques. Technology will include emergency response and post-attack recovery from the start and will also manage cyber-physical interactions.

Digital Information: Digital-trust technologies will become increasingly important for the management of the ever-growing flow of digital information, and to discern authentic-looking "fake" images, videos, messages, etc. Rights management, forgery-detection and classification technologies, and information forensics will help detect and manage malicious-content manipulation, the spread of forged information, and illegal sharing.

Health: Predictive, preventive, personalized, and participatory (P4) medicine will result from a significant change in the ability to produce, share, and to analyze health and genomic data. The judicious application of privacy-protection techniques in highly usable and transparent systems will create a P4 data-sharing ecosystem that stakeholders and patients will trust and that responds to legal requirements (e.g., EU GDPR and US HIPAA).

Democracy and Humanitarian Assistance: Trust in e-voting, in participatory or distributed governance, and in smart services will be guaranteed by technologies designed with democratic or humanitarian values at their core. Information used by democratic institutions, public services and NGOs will be more dependable and reliable. Privacy technologies will better balance the need for national security with that for privacy. Low-resource technologies will ensure universal access, especially in extreme humanitarian situations.

The DTOP's technological design and its application in verticals will be guided by the values and principles explored in the Governance and Ethics pillar.