Horizon 2020 Programme
DG CNECT
Next-generation Internet

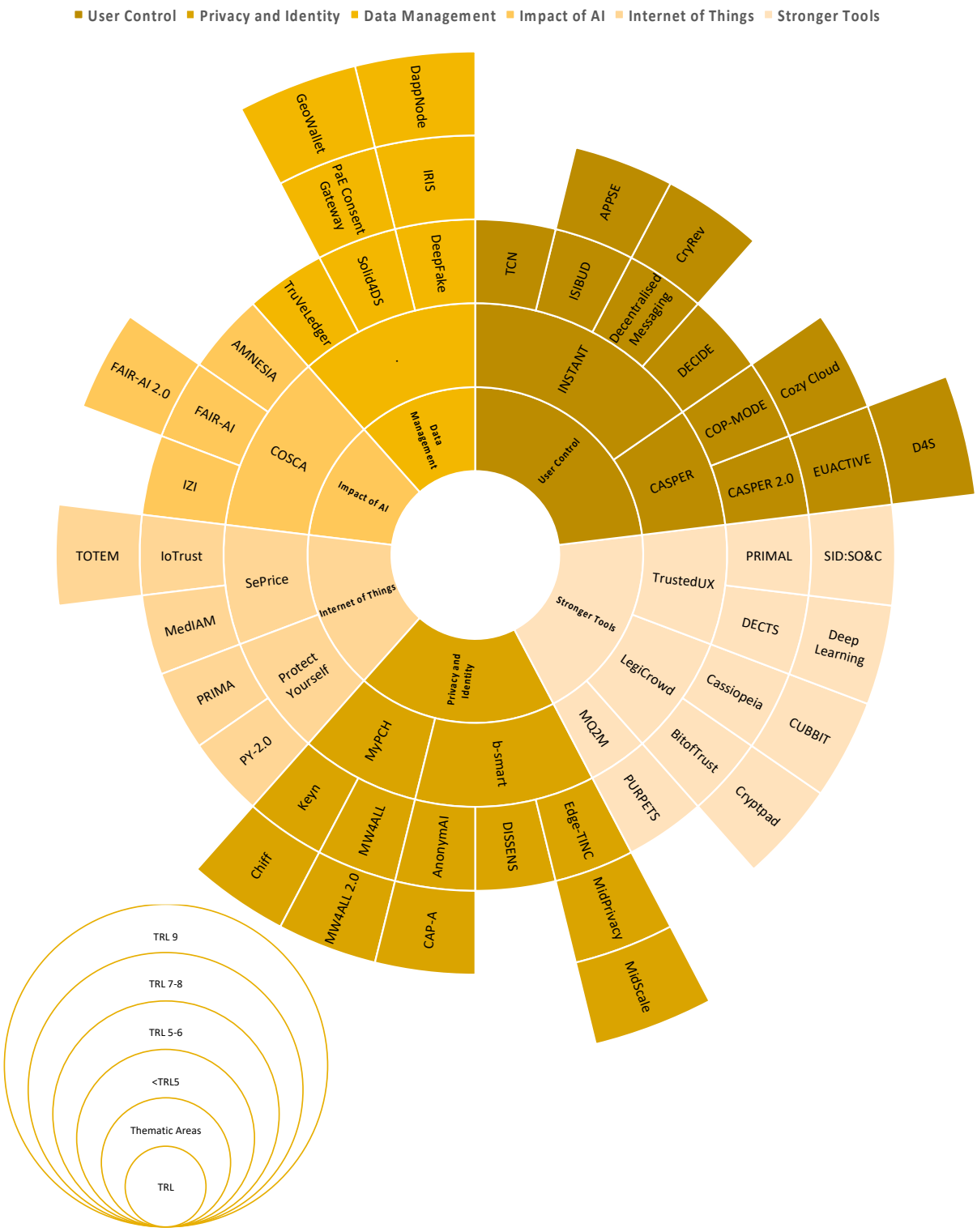
NGI TRUST

"Multi Stakeholder Collaborations for Sustainable Trust and Privacy in the Next Generation Internet"

Catalogue of Projects

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

NGI Trust Projects Ecosystem



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

MAIN TOPICS

User Control: this area focuses on user control to ease the decision making and customisation of settings to give the user a role in their internet. This contributes to solve the increasing complexity and options of a globally connected internet through modern collaborative approaches to UX design.

Privacy and Identity: this area will look at how we can both protect and utilise data, how we deal with managing large amounts of data in the cloud and how we can better support users in understanding the legal issues around consenting to use services. Additionally, it includes the use of digital identity solutions that help users to share, and not share, personally identifiable information.

Data Management: this area looks both at personal data management and data ethics, including projects working to provide users more control of their own data and a better understanding of fundamental principles about data usage and the safety of users based on this data.

Impact of AI: this area looks at systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. Any AI-generated improvements need to be based on rules that safeguard the people's privacy and safety.

Internet of Things: this area will work on securing the Internet of Things and tackling the security and privacy around IoT. They aim at creating more user trust against the Impact of AI and the growing use of smart devices at home, in offices and on the move.

Stronger Tools: this area focuses on mapping human-trust to technical solutions, designing privacy in UX design, security of sensitive data and providing users with stronger tools for daily life, including emerging and novel technologies such as quantum-cryptography.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

TOPICS	<TRL5	TRL5-6	TRL7-8	TRL9
User Control	INSTANT CASPER	CASPER 2.0 COP-MODE DECIDE Decentralised Messaging ISIBUD TCN	APPSE Cozy Cloud CryRev EUACTIVE	D4S
Privacy and Identity	b-smart MyPCH	AnonymAI DISSENS Edge-TINC Keyn MW4ALL	CAP-A Chiff MidPrivacy MW4ALL 2.0	MidScale
Data Management		DeepFake Solid4DS TruVeLedger	IRIS PaE Consent Gateway	DappNode GeoWallet
Impact of AI	COSCA TRUSTRULES	AMNESIA FAIR-AI IZI	FAIR-AI 2.0	
Internet of Things	Protect Yourself SePrice	IoTrust MedIAM PRIMA PY-2.0	TOTEM	
Stronger Tools	LegiCrowd TrustedUX MQ2M	BitofTrust Cassiopeia DECTS PRIMAL PURPETS	Cryptpad CUBBIT Deep Learning SID:SO&C	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

Projects' Information

Project Name: AMNESIA	
Company	ZenaByte s.r.l & Cefriel s.cons.r.l
Country	Italy
Goal	AMNESIA's objective was to assess the fairness of AI-based tools and models available from FAAMG or other companies currently embedded in most of the Future Interactive Technologies (FIT) and suggest mitigation actions of detected unfair behaviours.
Contact	https://www.zenabyte.com/project/project-3/

Project Name: AnonymAI	
Company	CELI & ICT Legal Consulting
Country	Italy
Goal	This project designed and developed a multilingual anonymization service ("AnonymAI") in order to help public and private organizations protect personal data through masking spans of text containing personal identifiers. The prototype system automatically analyses unstructured data or written documents, identifies personal information, and masks them with a label describing the type of masked information such as NAME, SURNAME, DATE OF BIRTH, PLACE, etc.
Contact	https://www.celi.it/en/research/research-projects/anonymai/

Project Name: b-smart	
Company	THINGS
Country	Italy
Goal	The project explored the development of a clear and positive User Experience in setting the privacy controls of connected objects, focusing on a different set of verticals such as Smart City, Smart Retail, Smart Mobility, Smart Home, Smart Wellness, and identified initial pain points related to the increase of IoT devices in our life, resulting in possible touchpoints and personal thoughts on how to define and value privacy in and between each context.
Contact	http://things.is/b-smart/

Project Name: BitOfTrust

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

Company	Open Knowledge & BitOfTrust
Country	Belgium
Goal	The aim of the project was to build & document the workings of a POC that shows how a distributed trust model without Identities could be built to bring a more human aspect of trust and solve some of the issues other 'trust architectures' have. One of the objectives was also to put it into perspective of the proposed W3C Decentralised Identifiers (DID's) standard. Because although DID methods create an interoperability bridge between the worlds of centralized, federated, and decentralized identifiers, we noticed that in the current DID Methods registry the focus of the community working on this is on the Blockchain way of interpreting trust.
Contact	https://bitoftrust.io/

Project Name: CAP-A	
Company	FORTH & IN2
Country	Greece
Goal	A Community-driven Approach to Privacy Awareness (CAP-A)'s objective was to deploy a socio-technical solution based on collective awareness and informed consent, whereby data collection and use by digital products are driven by the expectations and needs of the consumers themselves, through a collaborative participatory process and the configuration of collective privacy norms. The implemented solution creates a new innovation model that will complement existing top-down approaches to data protection, which mainly rely on technical or legal provisions.
Contact	https://cap-a.eu

Project Name: CASPER & CASPER 2.0	
Company	University of Belgrade & O Mundo da Carolina & "S. Cyril and Methodius" University (KINKI)
Country	Serbia & Portugal
Goal	The aim of the project is the implementation of the real smart children-protection software agent (based on AI) on human-computer interaction level that could be easily installed, set-up and delivered to end-users as a software-as-a-service (SaaS) solution. Different types of content are analysed, including text, images, video, and speech & audio, as well as the different types of online threats. The resulting system is meant to be modular, extensible, multi- platform, and compatible with already existing solutions.
Contact	https://www.casper-project.com/

Project Name: Cassiopeia

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

Company	Instituto de Telecomunicações – Aveiro & BCU & Birmingham City University & Gilad Rosner
Country	Portugal, Lithuania & United Kingdom
Goal	The CASSIOPEIA project investigates how open-standard/open-source technologies can be used to create usable and transparent architectures enabling device owners to selectively collect, share and retain data from users, while delegating control of device features to the users from whom data is being obtained. Selective sharing is a critical dimension of privacy: enhancing user choice, autonomy, participation, and trust. It is the technical embodiment of respect for social contexts in information sharing. Moreover, "privacy-by-default and -design" is the law of the land, but there are few examples of what that actually means aside from basic ideas of confidentiality and limited conceptions of transparency. The CASSIOPEIA project will provide a proof-of-concept for policymakers, technologists and the public showing how privacy-by-design can mean enhanced informational control - focusing on sharing rather than hiding data.
Contact	https://www.cassiopeia.id/

Project Name: CCS Cozy Cloud's Shiffremir	
Company	Cozy Cloud
Country	France
Goal	The aim of the CCS project is to enforce data privacy and security in the CozyDrive open-source files management application. Encryption is generally performed on the server side, in such a way that the data is protected at rest. The project argues that the only legitimate places where the data should be accessed are the devices of the user. However, client-side encryption comes with some issues: (a) computational overhead: the user devices are generally less powerful than servers, which can lead to a degradation of the user experience if the cryptographic overhead is too high; (b) loss of advanced features: as the server becomes blind on the stored data, it becomes unable to perform treatments on it, such as indexation, search, AI algorithms, etc. Yet, state-of-the-art techniques are designed for server-side computations and tend to either scale badly or be impractical on the client-side; (c) sustainability: by design, it becomes impossible for the service provider to guarantee the recovery of a lost password and thus the access to the data. Therefore, the objective for this project was to evaluate the feasibility of a complete solution of client-side encryption by tackling these three issues.
Contact	https://cozy.io/en/

Project Name: COP-MODE	
Company	Joao Vilela & Alastair Beresford

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

Country	Portugal
Goal	The main goal of the COP-MODE project is to advance the state-of-the art on privacy protection mechanisms for mobile devices operating in ubiquitous computing environments. The pervasiveness of mobile devices (e.g. smartphones) allows great quantities of data to be collected at all times. This collection can be beneficial for both users and collecting entities, by facilitating user-tailored services. However, much of this data can also be considered private and sensitive, thus requiring privacy protection mechanisms that can provide an adequate trade-off between utility and privacy.
Contact	https://cop-mode.dei.uc.pt/about

Project Name: COSCA	
Company	Università degli Studi di Catania (UNICT) & Consiglio Nazionale delle Ricerche (CNR) & Università degli Studi di Modena e Reggio Emilia (UNIMORE)
Country	Italy
Goal	COSCA produces a conceptual framework for car safety, driver privacy and trust enhancement, thus guiding the Next Generation Internet at its core. The overall objective of COSCA is the conceptual development of a Framework that classifies all relevant elements in support of car security and drivers' privacy.
Contact	https://cosca-project.dmi.unict.it/

Project Name: CryptPad SMC	
Company	Xwiki SAS
Country	France
Goal	CryptPad is a web-based suite of collaborative tools that uses end-to-end encryption to protect users' information from the host of the service. CryptPad was designed from the start with the goal of synchronizing dynamic content across multiple devices while protecting content and metadata to an unrivaled extent. This architecture offers many benefits but is not well-suited to mobile platforms which are often quite constrained in terms of screen space and computing resources. While the ease of deploying software to clients via the web has proven a great way to make privacy a practical option for many users, it also undermines the strengths of our platform since a compromised server could transparently deliver malicious code to clients.
Contact	https://cryptpad.fr/

Project Name: CryRev	
Company	Assured AB
Country	Sweden

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

Goal	The CrypTech project has developed an open-source Hardware Cryptographic Module (HSM) design to meet the needs of high assurance Internet infrastructure systems that use cryptography. This open-source hardware designs are aimed to be of general use to the broad Internet community, covering needs such as securing email, web, DNSSEC, PKIs, etc. Due to the openness and the structuring of the HSM, the design and its parts have proven to be amendable to wide variety of use case, applications, and markets. The outcome of CryRev project is a major revision of the CrypTech designs, an accompanying board design and a test-run of board manufacture. The objectives of the CryRev project included (a) Convert the board design to KiCAD, (b) Implement key handling Including key wrap, master key loading and storing in the FPGA, (c) Implement a master key memory In a Lattice ICE40 FPGA using the open toolchain IceStorm and (d) Develop a new generation of hardware acceleration of RSA and Elliptic Curve operations.
Contact	https://www.assured.se/

Project Name: CUBBIT	
Company	Cubbit s.r.l.
Country	Italy
Goal	Cubbit distributed technology does not only rely on direct end-to-end encryption, but it also embeds privacy keeping at the core of the whole software architecture, which does not force organizations to consign their files to a third party while at the same time guaranteeing a full cloud experience. Cubbit on-premises distributed cloud is able to provide organizations with a data storage technology offering the highest performance, the lowest costs and privacy-by-design.
Contact	www.cubbit.io

Project Name: D4S	
Company	DTU & KADK & Commons Conservancy Foundation & Commons Caretakers b.v.
Country	Denmark
Goal	Let's Connect! is a VPN solution. It also exists under the name eduVPN when targeting the research and education community. The purpose of the solution was to design a service able to provide secure access both to private institutional networks (as in typical corporate solutions) as well as to public networks. D4S relied on user consultation and participative design to make a VPN solution more adapted to end-users. The main outcome of the project is a new design for the apps and its implementation.
Contact	https://www.eduvpn.org/
Project Name: DAppNode	
Company	DAppNode Association
Country	Spain & Switzerland

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

Goal	The DAppNode project was meant to scale DAppNode from a functional user-focused "fat client" for decentralized services, to truly forming the backbone of the decentralized infrastructure. The objectives (linked to Sub-Projects) of DAppInfra include: • The elimination of DAppNode as a centralized party which acts as a gatekeeper of the applications that are available in DAppNode - making DAppNode a truly decentralized, fully Open-Source platform for running any kind of decentralized infrastructure completely permissionless with minimal technical ability. • Implementing the technical basis to be a decentralized platform that acts as the gateway to decentralized systems in DAppNode. • Creation of a tokenomic layer on top of the infrastructure that will allow DAppNode users to deploy a node of any network and be rewarded for operating it.
Contact	https://dappnode.io/

Project Name: Decentralize Messaging	
Company	Danube Tech GmbH
Country	Austria
Goal	The main goal of this project was to showcase the feasibility and potential of distributed applications in which users are not only in full control of their data (user-centric) but can also share identity-related Information to establish trust and, thus, enable peer-to-peer transaction without middlemen.
Contact	https://danubetech.com/

Project Name: DECIDE	
Company	University of Stuttgart (USTUTT)
Country	Germany
Goal	New approaches to identity management based on technologies such as blockchain and distributed ledgers are promoted as a chance to give users full control over their own identity data. Despite being often called the future of digital identity management, Decentralized Identity Management (DIdM) and Self-sovereign Identities (SSI) are still facing a number of challenges, usability being a major one: their concepts are too sophisticated for users and do not fit their mental models. The project DECIDE addresses this by conducting a study that analyses and evaluates the usability and practical applicability of some of the most advanced DIdM solutions.
Contact	https://www.iat.uni-stuttgart.de

Project Name: DECTS	
Company	ownYourData Verein zur Förderung der selbstständigen Nutzung von Daten & MeeCode by Mario Murrent

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

Country	Austria
Goal	Neither industry nor authorities have provided the deaf community (about 1 Mio. in Europe) with up- to-date solutions for communication with control centres. The proposed project will improve emergency chat handling by: • Deploying consent management technology for sensitive data exchange • Allowing purpose base data sharing during an emergency chat • Rolling out the existing solution at the European level Inspired by MyData principles and using current technological advancements in semantics and distributed ledger we want to implement and evaluate a solution that will not only benefit the deaf community but enables everyone to make silent emergency chats (e.g., in hostage situations).
Contact	https://www.dec112.at/dects/

Project Name: Deep-Learning	
Company	SensifAI
Country	Belgium
Goal	The project developed specific deep learning architectures for the smartphone chipsets of most major smartphone manufacturers. With this technology, we can enhance users' images and videos locally on their smartphones without any connection to the internet. This is an on-device, smart- enhance App that can help millions of people enhance their video/image archives while guaranteeing control over their personal data. The project will also add automatic and real time face and vehicle license plate detection/blurring systems in future versions of the app such that users can avoid unwanted violation of other people's privacy in public areas while live broadcasting or sharing images/videos on the internet.
Contact	https://sensifai.com/

Project Name: DeepFake	
Company	Sidekik ou
Country	Lithuania
Goal	The aim of the "Public Deepfake & Cheap fake detection tool" project was the development of a public facing platform for individuals to verify whether a video was artificially generated or not (e.g., development of a user-facing deepfake and cheapfake detection platform). This was building on top of previous work designing and developing a deepfake and cheap fake detection solution used by several government agencies in the EU.
Contact	https://thesentinel.ai
Project Name: DISSENS	
Company	Fraunhofer AISEC & Taler Systems S.A. & Berner Fachhochschule
Country	Germany & Switzerland

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

Goal	The aim of the DISSENS project was to design a technology stack which combines privacy-friendly online payments with self-sovereign personal data management. DISSENS project provides a comprehensive architecture and reference implementation for privacy-preserving identity management that bucks the trend towards centralization present in contemporary proposals. DISSENS integrates a technology stack which combines privacy-friendly online payments with self-sovereign personal data management using a decentralized directory service. This enables users to be in complete control of their digital identity and personal information while at the same time being able to selectively share information necessary to easily use commercial services.
Contact	https://www.aisec.fraunhofer.de/de/das-institut/wissenschaftliche-exzellenz/DISSENS.html

Project Name: Edge-TINC	
Company	Fluentic Networks Ltd
Country	United Kingdom
Goal	The project's aim is to design and implement a proof-of-concept prototype of an edge-network gateway that implements the first generation of In-Network Computing protocols and overcomes the limitations of current cloud-based distributed applications.
Contact	https://fluentic.gitlab.io/solutions/edge-tinc

Project Name: EUACTIVe	
Company	VDP & NHLS & TUV Rheinland AG & Ilionx
Country	Netherlands
Goal	The aim of the EUACTIVE project is to make Consumers aware of the Data Economy that is built on Data Bodies made of Consumers' Personal Data and the necessary steps to take in order to regain Control and next Ownership of this Personal Data. Next step is Control followed by Registration-Ownership. The ultimate goal: A Data Passport.
Contact	https://www.valueme.nl/eu-ngi/

Project Name: FAIR-AI & FAIR-AI 2-0	
Company	University of Cambridge
Country	United Kingdom

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

Goal	The aim of the FAIR-AI project is to endow an AI with the ability to read sentences and decide if the action being described is fair or unfair, without the need for human input or pre-programmed deontic rules. The second phase the project develops further by abstractly mapping the principal components of social relations: harm, and causal outcome. Both of which require the vectorisation of principal abstractions tied to text/visual input. Once completed we can integrate further human values to allow for a comprehensive appraisal of any text. A text that presents a potential or actual human-centred challenge, then assign the legally recognised fundamental rights and responsibilities therein. This will allow for an API to be developed that wishes to integrate this heuristic into currently used Apps. Essentially providing the required digital architecture to assign fairness assessments to problems, documents and data that is converted to a textual format.
Contact	https://www.psychometrics.cam.ac.uk/

Project Name: GeoWallet	
Company	Blocs et Compagnie
Country	France
Goal	GeoWallet is a Graph-based Blockchain - Confidential Computing platform for mobility data management, providing both trust to the service providers and privacy to the users. The aim of the project is to develop a platform allowing users to collect trusted mobility information, manage contracts with third parties and prove them mobility activities without exposing personal mobility data, based on an innovative personal data management architecture
Contact	https://www.blocsetcie.com/geowallet

Project Name: INSTANT	
Company	Virtual Angle BV
Country	Netherlands
Goal	AI and Big Data technologies potentiate an increasing number of personal data applications. It's urgent to increase transparency regarding the usage of personnel data by enterprises and to ensure that users are better compensated for providing others with access to their personal data. INSTANT aims to empower users with a transparent tool to manage the access to their personal data and to support due compensation by its use by third parties.
Contact	https://www.virtualangle.com/instant-project/

Project Name: IoTrust	
Company	Odin Solutions SL & Digital Worx GmbH
Country	Spain

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

Goal	The aim of the IoTrust project is to provide a simple setup and reliable operation of IoT networks in a trusted and secure manner via automated setup of IoT peer-to-peer networks and open-source stacks for worldwide applications. IoTrust implements and validates a trustworthy, open and human-centric solution to setup and maintain IoT networks based on the development and integration of a novel bootstrapping protocol, Peer-to-Peer and Distributed Ledger technologies in order to provide secure initialization of IoT devices, vulnerability detection and software patching/reprogramming. The proposed solution is based on recent standardization and research activities such as "Secure IoT Bootstrapping" draftxiv of IETF (Internet Engineering Task Force) and Peer-to-Peer InterPlanetary File System (IPFS)xv with Distributed Ledger Technology to ensure decentralized IoT networks.
Contact	https://www.odins.es/en/ - https://www.digital-worx.de/en/home/

Project Name: IRIS	
Company	Resonate Cooperative
Country	Ireland
Goal	Resonate is the Stream 2 Own ethical music streaming co-operative, established in 2017, now with a catalogue of some 11,000 tracks and 1800 artists. The co-op relies on trust-based relationships and transactions in the music ecosystem. The IRIS project (Identity for Resonate.IS) will allow artists and listeners to use their digital identities and proofs for access to communities and for co-creation, authorship, ticketing attendance, purchase of rights and many more exciting peer-to-peer music scenarios.
Contact	https://resonate.is/

Project Name: ISIBUD & APPSE	
Company	Better Internet Search Ltd & Edinburgh Napier University
Country	United Kingdom
Goal	The objective is to demonstrate that better internet search can be achieved through the use of user-side personalisation (under the full control of the user) and with no personal data revealed to external third-party services. One essential ingredient of this alternative search engine is there must be no commercial bias in the results and so a second objective is to show the viability of the proposed (non-advertising) revenue model. The Alternative Privacy-Preserving Search Engine (APPSE) project will deliver a unique user-tested and highly secure search engine.
Contact	https://www.betterinternetsearch.com/
Project Name: IZI	
Company	University of Jyväskylä
Country	Finland

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

Goal	The aim of the IZI project was to design and implement an intelligent zero-trust networking solution capable of detecting attacks initiated by both external attackers and smart devices from the inside, adapt detection models under constantly changing network context caused by adding new applications and services or discovering new vulnerabilities and attack vectors, make an optimal set of real-time crisis-action decisions on how the network security policy should be modified in order to reduce the ongoing attack surface and minimize the risk of subsequent attacks in the future.
Contact	http://users.jyu.fi/~mizolotu/research/ngi_trust_izi/

Project Name: Keyn & Chiff	
Company	Keyn B.V. & Content Power
Country	Netherlands
Goal	Keyn is a solution that allows people to log in to websites more easily and more securely using their smartphone. It bridges the gap from password authentication to strong authentication on the web, by creating a uniform user experience for a variety of existing authentication methods. The solution consists of a smartphone application and browser extension, which communicate over an end-to-end encrypted communication channel. All secrets are stored on the smartphone, and the browser extension is required to send a request to the smartphone if it needs to authenticate. The user authorises these requests by authenticating to the phone. The Keyn project aimed to bring this solution to the market by developing a strategy that is focused on explaining the cryptographic trust mechanisms to non- technical users. Additionally, the existing prototype should be developed into a mature and stable version with an intuitive interface. Lastly, a technical feasibility assessment needed to be conducted to discover if it is possible to decentralize the server component to be able to open source the core of the solution. Chiff project aims at helping companies to gradually adopt WebAuthn by offering a business-version of Keyn and offering libraries and support to implement WebAuthn for internal web applications. In this project, we will implement and test the solution with at least five companies and design a scalable strategy for commercialization. To support the shift towards a B2B strategy, we will make the core of Keyn, developed in the first phase, open source and freely available for consumers.
Contact	https://chiff.app/#landing

Project Name: LegiCrowd	
Company	APIL (Association des Professionnels des Industries de la Langue) & NTUA (National Technical Universtity of Athens) & Future Now Business Consultants, Training & Research Ltd
Country	France & Greece

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

Goal	LegiCrowd Onto aims at agreeing upon an ontology of descriptors for ToS to be used both for To SDR annotation and for MyData.org. Undoubtedly, other usages will emerge during the course of the project. It will rely upon the existing ToSdr platform, the Legicrowd Platform, work already performed at NTUA as well as other attempts such as P3P.
Contact	https://tosdr.org

Project Name: MedIAM	
Company	Fabien Imbault
Country	France
Goal	The MedIAM project defined an architecture in order to comply with cyber regulation of medical devices, as well as their integration into the larger e-health ecosystem. The key achievement is that the architecture has been validated by prototyping various protocols and analysing their pros and cons in the field, including feedbacks from professionals. Some of the results have been included in research papers (OID2021) and standards (IETF GNAP, DIF KERI). The aim of the MedIAM project is to analyse how it is possible to embed cyber security requirements into connected medical devices.
Contact	https://fimbault.com/

Project Name: MidPrivacy & MidScale	
Company	Evolveum
Country	Slovakia
Goal	Goal of the midPrivacy project was to develop an open-source privacy-enhancing identity management solution on top of midPoint. MidPoint is a comprehensive open-source identity management and governance solution used by many organizations world-wide. Our ambition is to provide a comprehensive, scalable and open-source platform that can assist organizations of all sizes in their implementation of practical data protection policies. We believe that there is a significant gap in the market offering and midPoint is uniquely positioned to fill that gap. We see this opportunity as a singular chance to transform midPoint into a leading world-class product in the area of identity management, governance and data protection .
Contact	https://evolveum.com/blog/

Project Name: MQ2M	
Company	Technische Universiteit Delft
Country	Netherlands
Goal	Current cybersecurity and cryptography methods used in communications rely on asymmetric public key distribution

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

	protocols that are not future-proof nor quantum resistant. Various Quantum Key Distribution (QKD) protocols that are future-proof exist, and some commercial QKD equipment is already in the market. Nonetheless, widespread adoption has not yet occurred. A next-generation QKD technology, MDI-QKD, which we at QuTech/TUDelft have pioneered, offers considerable advantages over commercial point-to-point QKD, including being intrinsically multi-point-to-multi- point networked and having increased security against attacks. With this technology in hand, along with the European Union's EuroQCI project to develop and deploy a pan-European quantum internet, the MQ2M project sought to investigate the commercial feasibility of MDI-QKD.
Contact	https://qutech.nl/

Project Name: MW4ALL & MW4ALL 2.0	
Company	Least Authority
Country	Germany
Goal	The project assessed the technical and commercial feasibility of a large-scale deployment of Magic Wormhole in order to provide an option for identity-free, secure, and easy file-transfer between two devices. Magic Wormhole allows for data sharing between two parties without either party needing to know each other's identities; it does not require persistent relationships or the use of email addresses or phone numbers. The goal is to achieve easy, private, and ideally also anonymous, file transfer between two devices. The goal of this project is to bring the security and privacy benefits of Magic Wormhole to more people through a sustainable product.
Contact	https://leastauthority.com/

Project Name: MyPCH	
Company	Diabetes Service ApS & Verein zur Forderung der selbststandigen Nutzung von Daten
Country	Denmark & Austria
Goal	The aim of the MyPCH project is that our innovation is a paradigm shift in sharing self-monitoring health data for a Person with Diabetes (PwD). The innovation is open-source and empowers the individual by sharing data in a secure, trusted, auditable, traceable, and consensus-based way inspired by MyData principles.
Contact	https://www.ownyourdata.eu/en/blog/ - https://diabetes.services/about/

Project Name: PaE Consent Gateway	
Company	Trinity College Dublin & Open Consent Network & Birmingham City University, School of Computing and Digital Technology
Country	Ireland & United Kingdom

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

Goal	This proposal will develop an end-to-end, user-centric, comprehensive, open-source solution to managing Consent for Personal Data. It delivers a concept we call Privacy-As-Expected (PaE) by creating, implementing and demonstrating a novel system to make online privacy practices accountable.
Contact	https://privacy-as-expected.org/

Project Name: PRIMA	
Company	Cognitive Innovations
Country	Greece
Goal	The project aims to provide a privacy protocol in order to deploy distributed intelligence in data aggregated by IoT networks. The protocol will rely on FL framework and the data analysis will take place to the fog nodes at the edge of the Internet. Using such a distributed intelligence approach, future Internet users (and especially mobile) will experience new type of services such as augmented reality (AR). AR will provide an intuitive interface to the digital connected world by superimposing virtual information coming from the IoT devices. Our objective is to offer such services by protecting the users too.
Contact	https://www.cogninn.com/

Project Name: PRIMAL	
Company	Tree Technology S.A.
Country	Spain
Goal	The massive increase in data collection worldwide calls for new ways to preserve privacy while still allowing analytics and machine learning among multiple data owners. Today, the lack of trusted and secure environments for data sharing inhibits data economy while legality, privacy, trustworthiness, data value and confidentiality hamper the free flow of data. PRIMAL proposal aims to demonstrate the implementation of a privacy-preserving machine learning approach based on the concept of federated machine learning (FML). This approach alleviates privacy-related data sharing barriers by enabling secure privacy-preserving analytics over decentralized datasets using machine learning algorithms (specifically deep learning). Data is kept in different locations under the control of the data owners with different privacy constraints, but still secure collaborative machine learning processes are enabled without data centralization.
Contact	https://www.treetk.com/en/R&D_PRIMAL.html
Project Name: PURPETS	
Company	CEA - Commissariat à l'Energie Atomique et aux Energies alternatives
Country	France
Goal	The objective is to propose a substantial improvement of a mobile app designed for privacy enhancement which is under

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

	development at CEA. It currently integrates deep learning techniques for visual recognition but not does address the real-life effects of data sharing. The outcome will be a fully functional mobile application which will be released in Android. The code will be open-sourced to increase trust and to allow interested third parties to contribute to it. The creation of a legal entity (NGO) is envisioned in order to support the development of the application in the long run.
Contact	https://www.cea.fr/

Project Name: Protect Yourself & PY 2.0	
Company	PANGA & MyDataBall
Country	France
Goal	PY is a central checkpoint for all connected devices. This overall hardware and software solution aim to inform and protect citizens from the unknown connections and unwanted data flows that automatically start when a device is connected to the internet. Thanks to a user-friendly interface, the system graphically shows the status of all the activities, provides risks assessment and enables user to define their security settings and authorized personal data. The objective of the project is to provide a hardware and software platform as well as a browser extension that will manage and secure the data collected from devices connected at home. PY2.0 introduces a computer server embedded in the home on which the users will be able to load a large number of application like on a smartphone. The idea is to offer a solution in Edge computing mode to give autonomy to Internet users by allowing them to protect their privacy and by limiting the call on the resources of the actors and giants of the NET. This server that we call the HNOS for Home Network Operating Server with PY (protect Yourself software) will support many applications that will be geolocated in home. It will provide security solutions, IoT protection, strong authentication like SSO & Self-Sovereign Identities and others applications.
Contact	www.pyguard.fr

Project Name: SePriCe	
Company	University of Jyvaskyla (JYU)
Country	Finland
Goal	The overall objective of this project is to research the viability of automating compliance checks of requirements stipulated within

	emerging IoT certifications/standards (ETSI, NIST, ENISA IoT) aimed at cybersecurity and privacy (e.g., IoT device decommissioning).
Contact	https://www.jyu.fi/it/en/research/research-projects/international-funding/iot-seprice-auto-poc

Project Name: SID-SO&C	
Company	Kelp.Digital (ex. SENSIO)
Country	Estonia
Goal	The idea behind Sensio is to develop an open-source software that gives content creators (for now, mainly, photographers) a set of tools to manage, protect and license their work. Simple, transparent and secure. The aim of the SID-SO&C project in particular, is to develop and build the distributed open-source software for the digital photography market that empowers content creators by simplifying their workflow and putting them in charge of the images they create and share. Within the scope of SID-SO&C project we were working to create a tool that will help photographers to stay in charge of the photos they share online and their data.
Contact	https://kelp.digital/

Project Name: Solid4DS	
Company	STARTIN'BLOX
Country	France
Goal	SOLID4DS project aimed to give more control to the users on their data when accessing and using services thanks to a privacy-by-design functional component based on Solid web standards. Our experience over the years reveals that privacy and data transparency for end-users are crucial issues in e-society data flow. By the time that one service connected to an "app" assembles a lot of information regarding end-users, the habit of multiple "accounts" inevitably means having a huge amount of personal data in the hands of digital providers. The goal was to enhance the security and privacy of end-users online by giving them the power to easily manage their own data.
Contact	https://startinblox.com/

Project Name: TCN	
Company	Athena Research and Innovation Centre in Information, Communication and Knowledge Technologies & University College London
Country	United Kingdom & Greece

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

Goal	The aim of the TCN project is to provide decentralized trust and security mechanisms for the future Internet. Project focuses on two emerging technologies: the Blockchain and the Information-Centric Networking paradigms. Blockchain technology is employed to create secure, distributed, and immutable databases shared and trusted by all parties in a network, while Information-Centric Networking employs a content- centric communication model, where access to content is mapped to the content itself irrespective of the location where the content is held and departs from the traditional host-centric access paradigm.
Contact	https://www.athena-innovation.gr/

Project Name: TOTEM	
Company	Feron Technologies P.C. (FERON) & ntop di Deri Luca
Country	Greece & Italy
Goal	The main target is to significantly increase the trust in connected homes through the provision of improved information to end users about their home network security status, on a simple, usable, and comprehensible way. This will come with a set of new, open low-cost devices and software tools, which will automate and make accessible to non-experts new technologies for early detection and proper avoidance of malicious misbehaviours from connected home end-points. We aspire to pave the way for democratizing the IoT trust-enhancing technologies and bridge the gap between technological advancements in modern smart homes and their actual uptake by end users.
Contact	https://feron-tech.com/

Project Name: TrustedUX	
Company	Tallinn University
Country	Estonia
Goal	Project's objective was to provide a service that helps UX designers quickly prove the value of using a trust-centric design approach in their organizations/companies and costumers — fostering a change in the UX awareness of trust. TrustedUX project aimed at: • providing a set of tools for where researchers and practitioners reflect, explore and transfer insights on the dimensions of trust experience when one engages with technology; and • developing a user-friendly toolset to support designers in shaping positive experiences and awareness of trust, similar to these services AttrakDiff or Ethical tools for designers.
Contact	http://hci.tlu.ee/portfolio/trustedux/
Project Name: TRUSTRULES	
Company	S.POULIMENOS KAI SYNERGATES IKE (ASN)
Country	Greece
Goal	Many vertical industries are putting AI into use but often they still do not fully comply with the GDPR in this respect. TRUSTRULES

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

	evaluated the possible potential of novel AI technologies to comply to GDPR. Our vision is to increase Trust in the application of recommender technologies by providing a clear description of how a recommendation was reached. This is the main goal of TRUSTRULES, a project that targets trade fair organizers and has as baseline the use case of our customer and trade fair organiser ROTA S.A.
Contact	N/A

Project Name: TruVeLedger	
Company	RISE Research Institutes of Sweden AB
Country	Sweden
Goal	Traffic accidents are large societal problems. Currently, we rely on gathering data about accidents after they have happened. With the emerging technology of Vehicular Ad Hoc Networks (VANETs) comes new possibilities to increase road safety by collecting safety-related data from vehicles as well as providing value added services and applications to users in a human-centric vehicular Internet. The data collected can be sensitive and has the potential to be misused by malicious entities to violate personal integrity of road users and it is important that data can be trusted to be accurate and truthful. By collecting and processing data at the network edge, the system can scale to a much larger size and such a decentralized system will inherently substantially reduce some privacy concerns present in the system, since data is collected and processed locally. It is however still important that an open trusted platform and related mechanisms are available to secure data and the communication of it so that users can rely on having their data in a robust and reliable trusted system. In this project, we apply the emerging Distributed Ledger Technology (DLT) which provide support for trust in systems without strong central entities. By combining VANET and DLT technologies, opportunities for stronger trusted communication in vehicular networks arise, but also challenges that must be addressed.
Contact	https://www.ri.se/en