Funded Projects Call 3

Project Number	Proposal Name	Lead Partner (name)	Partners	Keywords	Abstract
3.108	**MW4ALL 2.0**	Least Authority		identity free file transfer	Currently, in an NGI Trust Type 1 project, we are assessing the technical and commercial viability of Magic Wormhole to be deployed for broader use cases as an option for identity-free, secure and easy file transfer between two computers. This approach allows for data sharing between two parties without either party needing to know each other's identities, does not require persistent relationships, or the use of email or phone number. Magic Wormhole uses SPAKE-2 , a PAKE (password authenticated key exchange), which is a means for two parties that share a password to derive a strong shared key with no risk of disclosing the password. We think that Magic Wormhole could be a solution to the problem that two computers are still unable to easily, let alone privately, exchange a file. For this Type 2 project, we would like to execute on the plans we develop during the Type 1 project, which we are set to complete in July 2020. Although we have not completed our project, we expect that Magic Wormhole will require some development effort to make it (a) more conducive to scaling, (b) establish an independent infrastructure, (c) further differentiation from existing tools and (d) better suited for the identified use case(s). For this project we are proposing to execute on the effort determined necessary in our Type 1 project.
3.110	**DAppNode**	DAppNode Association		personal data management	DAppNode is the self-owned infrastructure layer for a human-centric, data-sovereign, private-by-design internet.
3.10	**GeoWallet** website: https://geowallet.io/	Blocs et Compagnie		gelocation, mobility data, blockchain	A user-centric approach for personal data management providing user with full control over his personal data and the ability to grant selective access to third parties comes with many advantages. Still it does not address the specific case of mobility data and usage-based mobility contracts between user and a third party: usage-based insurance, usage-based fares for public transportation... How to prove a third party that mobility data controlled by a user is authentic, was not forged or partially deleted? How to provide trusted results of queries and analysis authorized by a user on his mobility data to a third party without exposing the detail of the underlying activities and geolocation information? GeoWallet is a user-centric platform for mobility data management providing both trust and privacy. GeoWallet allows users to collect trusted mobility information, manage contracts with third parties and prove them mobility activities without exposing personal mobility data. GeoWallet is a trusted service based on an innovative personal data management architecture: • Graph-based Blockchain for fully anonymized, user-manageable, unforgeable and non- repudiable mobility data storage between asynchronous IoT nodes (mobile app) and online nodes (cloud) • Proofs for geolocation information provided - but not kept - by telecom operators • Transparent and trusted contract management between parties and automatic execution • Queries and analysis performed in enclaves (TEE), as per contract co-signed by user and third party, providing trusted results transparently shared with user and third party • Self-contained and self-protected data format (user Id, mobility information, contract) preserving trust, privacy and functionalities in any environment GeoWallet infrastructure has been fully specified, implemented and successfully tested with two insurance companies and a telecom operator on a limited set of users.
3.12	**Chiff / Keyn 2.0** website: https://chiff.app. Twitter: https://twitter.com/chiff_app.	Keyn B.V.	Content Power	webauthn, authentication	Password authentication has been the primary means of authentication for web applications since the early days of the Internet, but suffers from both security and usability issues. WebAuthn is a promising alternative, but lacks adoption from both end-users and website owners. With support of the first call of NGI_Trust, we have developed a hybrid authenticator (Keyn) that supports various underlying authentication methods in a uniform UI-flow for the user. This lowers the threshold for end-users to start using WebAuthn. This second 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 type 3 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. The current team consists of four people working in two complementary organizations: Keyn and Content Power. Keyn's authenticator and technical knowledge about the WebAuthn standard and Content Power's contacts and project management skills have proven a strong combination. We have had several meetings and developed a first prototype together. With the financial support of NGI_Trust, the team can be expanded with additional expertise in marketing and extra back-end development capacity, which is needed to reach the project goals.

3.21	**TOTEM**	Feron Technologies P.C. (FERON)	ntop	IOT, trusted connected home	The connected home enables the interconnection and interoperability of various types of end-points catering for applications like connectivity/networking, media/entertainment, physical security, energy monitoring, or even healthcare, fitness, wellness, and more recently, given the unprecedented challenges of the COVID-19 outbreak, remote working. From advanced control of previously non-connected devices such as home appliances, to the employment of smart IoT platforms, the connected home end-user enjoys an extraordinary degree of convenience and money-saving capabilities. However, this level of automation comes at a price: every single connected device may act as a potential trojan horse, a backdoor compromising the privacy, the cyber security and even the physical safety of the house. We argue that as more and more connected things are incorporated in our digital environment, there is a need to develop new robust, open, and easy to use tools to help users increase trust and achieve greater control over their devices fleet. Our proposal aims at significantly increasing the trust in connected homes, through simplifying, automating and eventually making accessible to non-expert users all the necessary tools for early detection and proper avoidance of any malicious misbehavior from connected home end-points. To achieve this goal we deliver a set of technological innovations along with open hardware devices and software applications /tools that will enable the holistic monitoring of the connected home network activities, identify and proactively prevent potential security /trust breaches, and even more importantly, increase connected home end-users awareness and familiarization with trust-enhancing technologies. The project will be carried out by FERON and ntop, bringing together and synthesizing an extensive, multi-disciplinary and complementary know-how and rich solutions portfolio on IoT and networking enabling technologies (nEdge, insigh.io). The partners aspire to exploit the project results through embedding the newly developed features to their existing products and jointly designing and developing new commercial offerings.
3.27	**PY - 2.0** www.pyguard.fr	Panga		Home Network Operating Server, IoT, home working	The current pandemic beyond the health disaster, has highlighted a number of society dysfunctions, for example people and businesses were not ready for the remote / home office. Cyber attacks have increased because people have left the corporate world, which has structure and people dedicated to ITC security. The attack surfaces have therefore increased and the doors of entry have multiplied : 600% increase in phishing attempt. The computers have left offices to home where the family , including children, may have to use them and potentially introduce malware or viruses. Isolation factors of certain people were highlighted as well as needs of telemedicine and users want and need for efficient and easy-to-use communication tools Confined people sometimes use NET resources which are not secure and sensitive information can be disseminated there. We believe that the home will evolve very strongly in the future and that it must have its TIC resources by freeing itself from the resources of the NET. The objective of the project is to introduce 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. It will be the first brick in the decentralization of the internet and the re-appropriation of data by users.
3.38	**PRIMA**	Cognitive Innovations		AI, FOG, machine learning	Next generation Internet (NGI) requires a decentralized and distributed intelligence in order to make available a new type of experience to serve the user's interests. Such new services will be enabled by deployment the intelligence over a high volume of IoT devices in a form of privacy protocol. Such a protocol will orchestrate the machine learning (ML) application in order to train the aggregated data available from the IoT devices. The training is not an easy task in such a distributed environment, where the amount of connected IoT devices will scale up and the needs for both privacy and computing are high. In this project, we aim to address both issues by combining two emerging technologies known as edge AI and fog computing. Our solution will aggregate the data collected by the IoT devices into fog nodes and apply edge AI for data analysis at the edge of the infrastructure. In order to provide privacy, federated learning (FL) will be deployed in an end-to-end fashion. FL will be deployed to down scale the necessary training set and reduce the label cost. The criterion of this choice is that we need to train the initial model to the extent that it may roughly measure the uncertainty. Otherwise, the model will not be able to choose more representative IoT data. Another criterion is that we should not over-train the model. Otherwise, there is no significant difference between ML and randomly choosing data. We will explore configurations with massive distribution, where the end-to-end FL protocol implementation will be cascading the model training procedure and the cost of slowing down the training procedure will be guaranteed as well. Our solution will reply on the TensorFlow Federated (TFF) framework and our application scenarios will be considered in a smart city environment with multiple IoT devices.
3.40	**Privacy as Expected: Consent Gateway (PaE: CG)** https://privacy-as-expected.org/	Trinity College Dublin	Open Consent Network, Birmingham City University	personal data management, consent management	This proposal will develop an end-to-end, user-centric, comprehensive, open source solution to managing Consent for Personal Data. We will deliver a concept we call Privacy-As-Expected (PaE) by creating, implementing and demonstrating a novel system to make online privacy practices accountable. The key deliverables are open software, a public demonstrator, real-world trials and publications. Whenever a User accepts a Privacy Notice and starts sharing personal data, they will receive a cryptographic Consent Receipt (based on a secure architecture [2] and open standards [3]) which, with non-repudiation and unforgeability proves, at any time, who-what-how any conditions were accepted. Considering the dynamic nature of the Web, a User will not have to extensively review or re-accept the same Privacy Terms. While creating an infrastructure to manage transparent, usable and accountable Consent, the User will further have access to crowd-reviewed Privacy Notices. As long as the Notice does not change, the User will not have to repeatedly re-accept. This will dramatically improve usability, while improving Transparency. A further key deliverable of this project is to design a Consent Gateway service which, while not keeping any Personal Information, will review, for the User, and notify the User of any changes requiring re- acceptance (while still keeping previous Consent valid). Considering that a key challenge in Online Consent is Usability, this architecture is poised to make dramatic advances for all parties involved in online Consent: Users, Organisations, Data Protection Officers, Institutions and Regulatory Agencies. This proposal is based on existing work from the Open Consent Group (affiliated with the Kantara Initiative) and academic work from Trinity College Dublin and Birmingham City University. To the best of our knowledge, such a framework does not exist anywhere and has not been proposed before despite its urgent need and demand.
3.53	**TruVeLedger**	RISE Research Institutes of Sweden AB		vehicle safety data	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. We will investigate the viability of a trusted communication platform for Vehicular Ad Hoc Networks using Distributed Ledger Technology in order to provide a more robust and reliable system for distributing safety and vehicle-to- vehicle data for reducing traffic accidents and improving road user experiences. A conceptual framework for secure and trusted VANETs will be developed which will be showcased with a usecase and performance evaluations in a simulated environment.

3.56	**MidScale** https://evolveum.com/introducing-midscale/ https://docs.evolveum.com/midpoint/projects/midscale/ Evolveum blog posts https://evolveum.com/tag/midscale/ Evolveum mailing lists https://lists.evolveum.com/mailman/listinfo/ Public on-line workshops /webinars https://docs.evolveum.com/talks/ Evolveum YouTube channel https://www.youtube.com/channel/UCSDs8qBlv7MgRKRLu1rU_FQ Internet2 /InCommon communication channels (selective) NGI_TRUST 9th Results Webinar Releases: https://docs.evolveum.com/midpoint/release/ Source code: https://github.com/Evolveum/midpoint	Evolveum https://evolveum.com/		automated identity management, MidPoint	Automated identity management is a necessary condition for implementing data protection policies in most large organizations. MidPoint is a popular open source identity management and governance platform. Data protection features are added to midPoint as a part of midPrivacy initiative. MidPoint has a potential to become leading data protection platform on the market. However, midPoint was originally designed for medium-size organizations. Limited scalability capabilities of midPoint pose an obstacle for large-scale midPoint deployments. Yet, large populations of identity data about users, citizens, students, scientist, partners and consumers are most likely to benefit from data protection features of midPoint. MidPoint was designed with replaceable data storage components and this design decision allows us to make midPoint scalable. We plan to re-implement midPoint data store mechanisms to support large data sets and take full advantage of PostgreSQL open source database. We also plan improvements such as autoscaling that will make midPoint more at home in cloud environments. Important part of the plan is a focus on stability and quality assurance to make sure that midPoint is ready for large-scale deployments . Our goal is to improve scalability of midPoint at least by one order of magnitude, reaching millions to tens of millions of managed identities . 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-classproduct in the area of identity management, governance and data protection .
3.57	**Anonymai** https://www.celi.it/en/blog/2020/11/anonymai-rd-project-legal-compliant-text-and-voice-anonymization-through-artificial-intelligence/	CELI	ICT Legal Consulting	free text anonyimisation, natural language processing	With the introduction of the Regulation (EU) 2016/679 and the need for companies to comply with ISO/IEC 27001 requirements, privacy enhancing technologies are becoming crucial for several types of enterprises. There is therefore an increasing demand for new and effective anonymizing techniques and their application in different domains with specific requirements. Our main objective is to provide a service that allows the automatic anonymization and protection of user personal data contained in texts and voice transcriptions in compliance with the applicable legal framework. With this aim, we intend to work on a Type 2 project for the technological development of an automated anonymizer prototype for Italian and English, to be firstly applied to two relevant use cases, and then extended to other scenarios (domain adaptation). The use cases will involve the anonymization of 1) free text sections from customer surveys and internal reports analyzed for the evaluation of customer and employee experience; 2) linguistic resources (both written texts and audio recordings) created for companies that develop voice technologies such as STT and ASR. The anonymization process will be carried out by means of both Deep Learning and rule-based Natural Language Processing technologies and will include common data (i.e. proper names, locations, ID numbers, phone numbers and e-mail addresses) and so-called “special categories of personal data”. This combination of technologies will allow for a more precise configuration, the immediate application of user requirements, system scalability to new relevant PII, and service improvement with the gradual collection of new documents. The project will be implemented by CELI, an Italian company with experience in Language Technologies and AI, and ICT Legal Consulting, an international law firm specialized in the fields of ICT, Privacy, Data Protection/Security and Intellectual Property Law.
3.58	**CASPER 2.0**	University of Belgrade – School of electrical engineering	O Mundo da Carolina – Associaçao de Apoio a Crianças e Jovens	online child protection	Our consortium has received a Type 1 grant from NGI_Trust for the CASPER project in 1st open call. The main goal of the project was to identify and apply the potentials of using artificial intelligence to protect children on the Internet. The current events, related to COVID-19 pandemics, show that this kind of protection is more relevant than ever since children are spending much more time online. Different types of content have been analysed, including text, images, video, and audio, as well as different types of online threats. We have also analysed several software architectures to potentially apply in order to develop a high-quality solution with taking care of privacy protection. As a result of numerous developments, analysis, and testing activities, we have defined CASPER software agent architecture and identified optimal algorithms regarding the criteria mentioned previously. We proved the initial concept, that AI can be applied at the Human-Computer Interaction level to protect children on the Internet. The proposed approach was innovative in terms that there are no other solutions working on that level, capable of analysing all major types of content (visual, audio, and textual), able to respond to different types of threats (porn and nudity, cyberbullying, indoctrination, etc.), and capable of overcoming problems related to content encryption. Based on the results achieved in this grant period, we created a CASPER pilot demo that represents the selected algorithms effectiveness and the intended way the solution will work: https://drive.google.com/file/d/1kc3GmRfFTuLKvORYqr1m2pyl16s5wrfO However, despite the results achieved, we identified few major ways that the solution needs to be improved in: 1. Achieving real-time performance; 2. Exploring different deployment models;3. Improving the algorithms effectiveness; 4. Expanding project scope to elderly population; 5. Supporting languages other than English. Therefore, we are proposing the extension of the project and support from the NGI.

3.65	**IoTrust**	Odin Solutions SL https://www.odins.es/en/	Digital Worx Gmbh	IoT bootstrapping and distributed ledger technologies	Internet-of-Things (IoT) enables advanced applications and new business opportunities in global sectors like Industry 4.0, Smart Cities, Precise Agriculture and othersi. However, existing IoT products fail to provide human- centric and trustworthy applications covering security/privacy requirements specified in international legal regulations such as: (1) GDPRii for data privacy and the protection of personal data, (2) NIS Directiveiii for internetwork operations and (3) EU Regulation No 526/2013iv from ENISA for electronic communications, infrastructure and services. Moreover, international studies like “Industrie 4.0 Readiness”v reveal that end-users are not able to setup and maintain easily IoT networks in a secure and trustworthy manner. To setup IoT networks, the first process is secure bootstrapping. This involves authentication, authorization and key management operations that are vital to control network resources and communications. Nevertheless, traditional bootstrapping protocolsvi are not adapted to recent IoT networks vii viii(e.g. NB-IoTix, LoRax, Sigfoxxi, etc) formed by IoT devices with limitations in computing and networking capacities to implement complex security protocols. Moreover, to maintain IoT networks it is required open and trustworthy solutions for detecting vulnerabilities in IoT software/hardware and providing robust update/patching management. However to maintain IoT networks, current solutions xii xiii xiv are complex, closed and non-interoperable what do not permit the end-users to manage their networks with heterogeneous IoT devices in an easy and homogeneous way. To tackle these challenges, IoTrustwill implement and validate 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, vulnerabilities detections and software patching/reprogramming. The proposed solution is based on recent standardization and research activities such as “Secure IoT Bootstrapping” draftxv of IETF (Internet Engineering Task Force) and Peer-to-Peer InterPlanetary File System (IPFS)xvi with Distributed Ledger Technology to ensure decentralized IoT networks. The main expected outcome will be a standards-based solution with open-source stacks for IoT devices and distributed services platform that will be supported by real-world pilot validation.
3.73	**Solid4DS**	STARTIN' BLOX		web decentralisation, personal data management, solid	SOLID4DS project aims to give more control to the user 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 to end-users are crucial issues in e-society data flow. By the time that one service connected to an “app” assembles many information regarding to end-users, the habit of multiple “accounts” inevitably means having a huge amount of personal data in the hands of digital providers. Our goal is to enhance the security and privacy of end-users online by giving them the possibility to easily manage their own data. We believe in the decentralized approach of “Solid” , the latest version of web standards, developed by Tim Berners-Lee and his teams in the W3C, to develop tools centered on the needs and practices of users and bring a more personal, safer and more transparent experience of the web. Solid standards allow better business models by providing applications with more data, enabling superior and more customized services while respecting data privacy . Despite Startin’blox framework is still the only one on the market that fully leverages the power of Solid standards up to the user interface, we never had the chance so far to use time and resources on exploring further the main security issues involved by a Solid environment. The support of SOLID4DS project by NGI Trust would give us the opportunity to work on a privacy-by-design user interface to add to the Startin’blox Solid-based app’s Suite. The main goal of our project is to bridge the gap between our current framework where most security issues in a Solid environment are still to be explored (TRL 6-7) to a privacy-by-design functional component ready-to-plug to the Startin’blox app’s Suite (TRL 8).
3.75	**DeepFake**	Sidekik OU		fake news / information analysis	Sentinel is tackling one of the most serious problems affecting the world today: disinformation. Disinformation, and especially disinformation propagated via synthetic media like deepfakes and cheap fakes is a growing risk to the wellbeing of democracy and economic stability with losses extending upwards of $78 billion annually according to a recent University of Baltimore report. Beyond the economic impact, we are seeing firsthand the chaos and xenophobia disinformation is causing in relation to COVID-19. For example, the Kremlin has currently deployed a large-scale coronavirus disinformation campaign to sow confusion, panic and destroy confidence in the emergency response in the EU. Per an EU report1, they are playing with people's lives, have created public riots in Ukraine through coronavirus disinformation and are subverting European societies from within. The strength of Democratic nations lies in shared values and trust in institutions but this has been continually put to the test, and because of the democratization of the technology underlying disinformation and deepfakes, we are approaching a time when the average person could create many hyper realistic news article or videos of a political figure spreading lies related to response measures against a viral outbreak with minimal effort using open source tools online, causing economic damage and even death. Sentinel has built a best in class deepfake and cheap fake detector utilized by governments and media companies, and now is looking to build out a public facing platform that would enable individuals to check if a video is a deepfake or cheap fake. This is the core product that we are looking for support with for this grant as this product will be more a public good than a commercializable product as we want to enable access to the tool to as many people as possible so that they can independently verify information.
3.82	**FAIR-AI 2.0**	The University of Cambridge		improved AI algorithms	All of the greatest projects on the topic of human-centric AI have one shortcoming. They use humans to consider problems that can arise from the use of the internet and human data. Humans look to see where fundamental rights lie, how they can be infringed upon, and where responsibility towards these rights must be met. Herein lies the problem. They do not use an AI to detect where these assignments or infringements on rights and responsibilities lie. This bottlenecks AI, as well as limits the true capacity of AI to be human centred, since no AI algorithm can carry out such a humane task: That is, cognate the essential core of human values; fairness - to do onto others as one would wish to be done onto themselves. In our first project (Type I) at the University of Cambridge we began to untangle this problem into its constituent factors. The first step was the detection of power between agents in a text, for an auto-assignment of rights and responsibilities. For this (Type II) proposal, we develop this further by abstractly mapping the principle 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. As the AI would have an integrated 'cognition' of fairness, it would protect humans and provide enormous AI power.
3.85	**Cassiopeia**	IT-Av - Instituto de Telecomunicações - Aveiro (affiliated with University of Aveiro)	GR - Gilad Rosner, Birmingham City University	personal data management	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. A human-centric conception of data sovereignty and sharing, allows flexible sharing and delegation arrangements that reflect the dynamics of social relations. More importantly, considering the trend of Amazon and Google becoming gatekeepers to the smart home, there is a real danger that these giants will have tremendous power over the nature of data sharing and device control. Through the use case of a person wanting to rent their home on Airbnb, we will build a technical demonstration that illustrates selective sharing and feature delegation, granular consents, transparency, and non-repudiation. These technical architectures will be built on open standard and open-source technology, enabling a wider range of sharing styles and a more holistic conception of privacy. CASSIOPEIA demonstrates ways of bootstrapping trust at the protocol level by implementing existing and emerging protocols and markup languages. It focuses on trust and reliability by working with technologies that create controls to share data in ways that users actually want, doing so in a secure, transparent manner.
3.90	**MedIAM**	Fabien Imbault		secure medical IOT devices	According to cybercrime magazine, “healthcare suffers 2-3X more cyberattacks than the average amount for other industries”, because the data has more value for hackers. Cyber regulations such as the EU cybersecurity act provide mandatory requirements to protect sensitive information and systems. Beyond traditional clinical systems of electronic health records (EHR), it remains really difficult to extend that line of requirements to connected devices people carry around as part of their treatments. If those medical devices aren’t properly secured, people may unknowingly be broadcasting their health status, as well as many other personal sensitive data, everywhere they go. Or even be directly harmed by hacked devices. Existing protocols available for IoT are unable to meet the complete requirements from regulators. In the current proposal, we provide an opensource pilot implementation on how an equipment vendor should protect the functions and data of their medical IoT devices.

3.94	**IRIS Community Credentials** https://resonate.is/community-credentials/	Resonate Co-operative	Pavilion and Verifiable Credentials Ltd	SSI, ethical music	Resonate is creating a Co-operative Privacy and Trust system for digital dignity across communities: Artists in every field want to collaborate with each other and with their own community-supporting audiences. But trusted collaboration without face to face interaction is difficult. Many of us let the major corporate social platforms manage the majority of our identity information, even if we prefer to work in trusted 'peer-to-peer' circles. Our Community Credentials project helps communities to award simple badge-like credentials that can be proven and recognised across organisations. Assuring safety, confirming identity, but protecting our data and private information. Resonate is partnering with Pavilion co-operative and Professor David Chadwick's VerifiableCredentials Ltd for this project that has won grant funding from the European Union's TRUST programme. The Problem: In 2020 there has been a surge in online community values and greater visibility of cooperatives as a business model (1.2Bn members of co-ops globally) as the global community reels from the effects of Covid-19 on music and the arts. Forums and groups are springing up everywhere to support collective action or help local communities and neighbourhoods. Unfortunately, solutions are often fragmented and don't share information very well, or safely. We end up 'over-sharing' information in an effort to prove things we claim about ourselves. We should only share what we need in order to transact. And we should not have to keep on proving the same information over and over again (copies of utility bills, driver's licenses, etc) when we could do that once, and re-use that 'show me'. We need something like our own wallet, not another bank, central ID provider, Facebook, Google, or some credit reference agency to hold all our cards for us. Our Solution: Open Source Community Credentials provide community-friendly and transparent recognition, award and governance of verifiable credentials as simple badges. Verifiable Credentials are a new web standard for proving things digitally, thanks to some clever cryptography. We are building to be the 'Know Your Co-operator' equivalent of KYC (Know Your Customer for business) for co-op social trust, all without reliance on centralised providers. We're providing an open source 'plugin' solution product, initially for Discourse, the biggest of the community software platforms (over 343m page views/month), reaching out to its active developer community and beyond that to other open source forum software providers. With our solution, members get control over what they choose to share and prove digitally, and don't risk leaking information or being tracked. We use the idea of the 'wallet' (kept in your pocket) and the 'badge' (worn on your shirt) as simple metaphors. Benefits The music streaming ecosystem needs better authentication and digital proof, and with privacy. Credentials are essential for membership, music purchases, music copyrighting and gig ticketing scenarios. Particularly when music is the soundtrack for popular resistance, artists' and listeners' safety, security and privacy must be guaranteed. We shouldn't rely on the global social corporate platforms to do this for us. We're working with our collaborating partners to bring this to you in mid-2021 for the Resonate ecosystem and eventually, for the broader co-op ecosystem. Who are the partners? Resonate - https://resonate.coop - is an ethical music streaming co-operative. Open source and fair trade, it's a place where artists, listeners, and members control the community as voting shareholders. Membership is free and non-exclusive for artists and labels that share music. We are a rapidly growing community of artists, listeners and members who want to Play Fair. For community-building, we are working with Pavilion - https://thepavilion.io/ - a workers co-operative for online communities. Pavilion has a long history of working with open source community software frameworks, and jumped at the chance to be a part of a project that could bridge identity, and foster privacy and trust, between different communities. VerifiableCredentials Ltd is a spin-out from the University of Kent, UK, led by Professor David Chadwick, a co-author of the W3C Verifiable Credentials Data Model Recommendation. David has been a leading researcher in identity management for 20 years, and the verifiable credentials eco-system he has developed is simple to administer, lightweight and standards conforming, supporting: X.509, TLS, WebAuthentication (FIDO2) and Json Web Tokens. It is one of the few verifiable credential eco-systems that does not require non-standard blockchains, zero knowledge proofs or distributed identifiers.
3.13	**APPSE** https://www.betterinternetsearch.com/	Better Internet Search	Partisia ApS	personal data management	The Alternative Privacy-Preserving Search Engine (APPSE) project will deliver a unique user-tested and highly secure search engine. This project builds on the platform built during the successful NGI_Trust Type 1 project ISIBUD, which demonstrated the feasibility of a new user-focused search engine with an alternative ad-free business model. Specifically, this project will advance the technology to a point where a beta version can be released and tested by users in Europe. To achieve this, the users' personal data will need to be encrypted and secure and the monetisation model will need further developed in a way that is equitable and transparent to the users. Thus, the developers of the ISIBUS search platform at Better Internet Search Ltd have teamed up with cryptography and blockchain experts Partisia ApS to deliver the project objectives. The project will create an enhanced search platform where users have total control over their personal data and how it is used. Through zero-knowledge computations personal data remains encrypted but can still be used to perform personalised services that benefit the user. The alternative business model being developed is transparent in showing users where their searches are a cost and where they can generate a revenue. A search credit system has already been developed and will be significantly enhanced during this project through the use of tokenisation and smart contracts for data transactions based on Partisia's commercial Privacy Blockchain (PBC) technology. A beta version of this search engine will be released for users in Europe during Q4 2020.