NGI POINTER

1st Open Call

Selected NGI Architects:

Project Descriptions

Grant Agreement No.: No 871528
Call: H2020-ICT-2019-2
Topic: ICT-24-2018-2019
Type of action: RIA

1st Open Call

Selected NGI Architects:

Project Descriptions

Index

Intro

1st Open Call

Selected NGI Architects:

Project Descriptions

What is the Next Generation Internet (NGI)

NGI (ngi.eu) is a European Commission funded programme to evolve the Internet, Internet technologies and uses in a more human centric way.
NGI Pointer, NGI Pointer is part of the NGI and seeks brilliant Internet talents – NGI Architects.

Who are NGI Architects?

Historically, the inception of the Internet clearly has key persons behind it. Internet Architects like Vint Cerf, Bob Khan and the inventor of the web Tim Berners-Lee made huge contributions. Technicians, researchers, funders, businesses and policymakers made it happen and scaled it up globally.

However, as the Internet grows in terms of complexity such as technology choices, actors, users and use cases, boundaries become blurred and activities hidden or implicit. Internet governance bodies, such as the Internet Architecture Board and the Internet Engineering Task Force create structure. But it is the people that everyday evolve and change the Internet through ocial and unocial channels, at the core of the architecture or through new applications and uses that are growing rapidly.
These people are NGI Architects.

Who are the proto NGI Architects?

NGI Pointer has found their first batch of NGI Architects. After the first Open Call NGI-Pointer received 159 applications of fiinternet talents interested in joining a community of NGI Architects. After the evaluation of applications, 24 of those 159 fiinternet talentsfl have been invited to join NGI-Pointer as NGI Architects.

NGI POINTER (NGI Program for Open Internet Renovation) has received funding from the European Commission, as part of the Horizon 2020 Research and Innovation Programme, under Grant Agreement No.871528

Some Congestion Experienced

With support from the NGI Pointer program, our goal is to expand SCE high-fidelity congestion control signaling beyond the edge and into core networks and aggregation points. To accomplish this goal, we will develop a new SCE queueing discipline (qdisc) that can operate using a small and fixed number of FIFO queues, for when fair queueing is not available. This new qdisc will provide approximate fairness between SCE, RFC3168 ECN and non-ECN flows, some isolation for latency-sensitive flows, and mitigation for unresponsive flows. Along with the new qdisc, we will develop an expanded suite of tests and tools, addressing an appropriate set of congestion control concerns from RFC5033. Source code and test results will be added to our open source repositories, and a new I-D (Internet Draft) will be submitted, along with any updates to existing Internet Drafts. If possible, the results will be presented to the TSVWG (Transport Area Working Group) in the IETF.

Country: **Germany**

Team: **Center for the Cultivation of Technology gGmbH**

Further information: **https://robur.coop**

Contact: **team@robur.coop**

Deploying MirageOS unikernels

A MirageOS unikernel is a virtual machine that provides a single service. It is written in a statically-typed memory-managed functional language. The language choice avoids several attack vectors, and since a unikernel only contains the required functionality the attack surface is reduced drastically. The resource usage of a MirageOS unikernel is reduced by an order of magnitude compared to a Linux based solution.
Most components are open source under a permissive license (MIT/ISC).
In this project, we will improve and document the deployment story of MirageOS unikernels: establishing a repository of reproducible binary images, enhancing existing MirageOS orchestration tooling, integrate into established orchestration systems, and improve the observability of MirageOS unikernels. We will as well conduct case studies with external organizations and integrate MirageOS unikernels into their existing infrastructure.

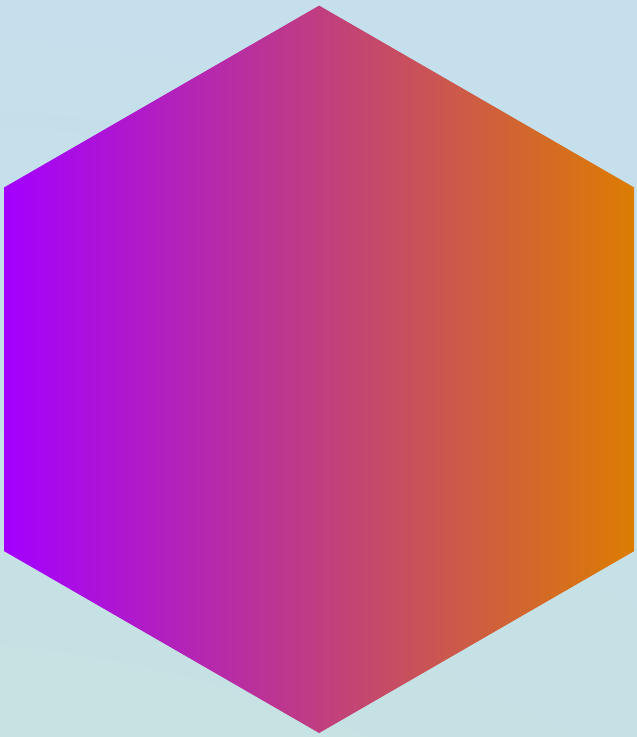
Operators will be able to use MirageOS unikernels instead of relying on commercial cloud solutions. This way they take back control over their data and reduce the carbon footprint.

Country: **Germany**

Team: **Center for the Cultivation of Technology gGmbH**

Further information: **https://robur.coop**

Contact: **team@robur.coop**



WireGuard

WireGuard is a layer 3 secure network tunnel,
originally designed for the Linux kernel, but now making its way into all major operating systems.

It is meant as a more secure replacement for many uses of older protocols like IPsec and OpenVPN, which suffer from countless security design flaws from the 90s.

It uses state of the art cryptography and is designed from the ground up to emphasize a small TCB and defense-in-depth security practices.

WireGuard also aims to be extremely easy to use, having few nobs, and a general notion of being secure by default and misuse resistant. It also has a very small and hardened attack surface, being designed to be placed on the outer-most edge of networks.

Country: **France**

Team: **Jason A. Donenfeld**

Further information: **https://www.wireguard.com**

Contact: **Jason A. Donenfeld**

Ltt.rs - Open Source Email client (JMAP)

Ltt.rs (pronounced "Letters") is a beautiful, user friendly and encrypted by default E-Mail client for Android based on modern standards like JMAP (RFC 8621) and Autocrypt.

Using JMAP instead of IMAP will make the app more maintainable and more reliable on current mobile operating systems due to the build in push capabilities.

Country: **Germany**

Team: **Daniel Gultsch**

Further information: **https://ltt.rs**

Contact: **https://gultsch.de**

Multipath TCP for 5G networks

Multipath TCP was invented in Europe.
It already plays an important role to support Hybrid networks but it will play an even more important one in the Wi-Fi/5G coexistence.

Unfortunately, its deployment remains limited.

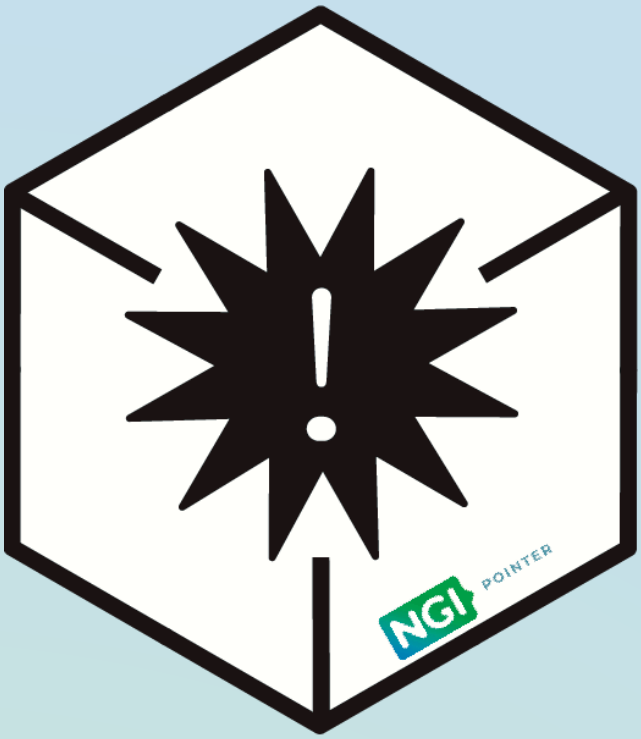
This project will bring
stable and tested open-source implementations that enable vendors of Linux-based user equipments and servers to leverage all the benefits of this new protocol.

Country: **Belgium**

Team: **Tessares S.A.**

Further information: **tessares.net**
twitter.com/TESSARES_SA
linkedin.com/company/tessares
facebook.com/tessares2015/

Contact: **github.com/gdetal**



European Firmware and App Library

Current security research for Internet connected devices (consumer electronics, but also industrial IoT and SCADA systems) happens in a haphazard way.

In reporting many vulnerable devices are missed, leading to underreporting of vulnerabilities and a lack of sense of urgency for vendors to fix devices.

By creating a library of firmware files, with analysis reports and the possiblity to do further analysis on large collections of firmware files and apps it becomes easier to have more complete reports and pro-actively scan and analyze more amounts of devices and apps.

Country: **Belgium**

Team: **Tjaldur Software Governance Solutions ZZP.**

Contact: **https://www.linkedin.com/in/armijnhemel/**

Trust and Authentication for Next Generation Internet (TA4NGI)

TLS-KDH is an evolving standard protocol for high security authentication and transport encryption, which aims at security in a future world of quantum computing. It combines basically three established technologies to reach this aim: Kerberos, TLS, and Diffie-Hellman key agreement protocol.

Since DH and TLS are used together already, the real innovation of TLD-KDH is the integration of the Kerberos protocol, so that a client can authenticate with a Kerberos ticket instead of using an X509 client certificate, which showed to be hard to manage for many users.

This Project will as proof of concept implement TLS-KDH as authentication mechanism in the form of a microservice plugin to the open source software Satosa. Satosa is a multi-protocol authentication and authorization proxy that supports both sides of the SSO protocols SAML and OIDC (Identity Provider/Service provider or OpenID Provider / Relying party).

It will also evaluate it's use as transport encryption in the open source application Corteza.

Country: **Germany**

Team: **DAASI International GmbH**

Further information: **https://daasi.de/de/**
https://twitter.com/DAASI_Int
https://www.facebook.com/daasiinternational
https://www.linkedin.com/company/daasi-international-gmbh/

Contact: **https://www.linkedin.com/in/petergietz/**

Fast prototyping of complex Graph Neural Networks for network optimization (IGNNITION)

Despite being a hot-topic, we -the Internet community- have failed to produce marketable AI products for autonomous network operation and control. The main reason behind this is that state-of-the-art AI techniques can only operate in the same scenarios seen during training. As a result, the vendor needs to train the AI algorithm in each of the production networks where it is planning to deploy it. This strongly limits commercialization since AI training requires using configurations that may break the production network.

Recently, Graph Neural Networks (GNN) emerged as the only AI solution capable of generalizing to unseen networks. This allows a vendor to train a GNN-based AI algorithm and deploy it as is on any operator's network.

However, developing a GNN is a cumbersome task that requires AI experts with deep skills. In this project we aim to address this issue, by allowing the Internet community at large to take advantage of GNN without requiring such skills.

We thus present IGNNITION, a framework for fast prototyping of Graph Neural Networks.

Country: **Spain**

Team: **Universitat Politècnica de Catalunya**

Further information: **Repository: https://github.com/knowledgedefinednetworking/ignnition**
Website: https://bnn.upc.edu/
Twitter: @BNN_UPC

Contact: **https://www.linkedin.com/company/bnn-upc/**

Veri?ed Secure Routing with SCION (Veri?edSCION)

The Next Generation Internet needs to offer a high degree of security to enable trustworthy communication despite omnipresent adversaries.

Since vulnerabilities are extremely difficult to detect during reviews and testing, the NGI must be based on solid foundations: security properties must be certified through formal proofs.

We will demonstrate the feasibility of developing an NGI that is provably secure by formally verifying strong security properties of the SCION inter-domain routing architecture. We will formalize SCION s security guarantees and verify that the protocol main.

Country: **Switzerland**

Team: **Anapaya Systems AG**

Further information: **https://www.pm.inf.ethz.ch/research/veri˚edscion/NGI.html**

Contact: **www.pm.inf.ethz.ch**

Reshaping Linked Data on the Fly (Solid-Shape)

In this project, we aim to implement an open-source registry of linked data shapes and forms so we can identify and resolve problems that still remain unclear about these theoretical concepts.

Because a registry of linked data shapes and forms is an essential part of the Solid ecosystem, the execution of this project will accelerate Solid's adoption.

As the Solid specification is designed to improve data privacy, trust and portability, this open-source project matches to a great extent with the vision of NGI and several European values.

Country: **Belgium**

Team: **Digita BV**

Further information: **https://digita.ai**
https://www.linkedin.com/company/digita-ai

Contact: **https://github.com/digita-ai**

InternetWide Identity through Realm Crossover (id-xover)

A security infrastructure for gaining trust in another realm's identity can be imagined with DNSSEC/DANE and certificates.

Embedding this in actual authentication schemes, with minimal change, is quite a challenge. We found theoretic options in Kerberos and in SASL; the former scales well and the latter offers a migration path for current password users.

Country: **Netherlands**

Team: **OpenFortress BV**

Further information: **http://internetwide.org/**
https://gitlab.com/arpa2

Contact: **https://gitlab.com/arpa2/**

Peergos

Peergos is a private-by-design protocol with a global end-to-end encrypted file system at its foundation.

Designed to bring private and secure applications to the web, Peergos respects user privacy - servers cannot see data like file names, sizes or directory topology or even who is sharing with who.

Peergos also gives users portability of their data - since our servers are trustless, users can mirror their data safely on many storage providers. Finally, Peergos does not depend on DNS or TLS certificate authorities.

With support from NGI-POINTER we will build upon this foundation to offer a social network and several productivity applications with our unique privacy and security features.

Peergos is designed to ensure that each user's social graph remains hidden from the server whilst ensuring that users are able to discover each other and the content they post.

Applications served through Peergos are sandboxed so that they cannot track users or exfiltrate data without permission..

Country: **UK**

Team: **Peergos Ltd.**

Further information: **https://peergos.org**
https://github.com/peergos/peergos
https://twitter.com/peergos

Contact: **https://www.linkedin.com/in/iancpreston**

Linux kernel regression tracking (Linux-Regtracking)

Build and integrate mechanisms into the Linux kernel development processes to track all regressions reported by humans or CI systems.

Together with the existing “no regression” rule this will help to make sure new releases with their improved security techniques work as good as their predecessors.

That's important, as the kernel is at the very heart of many devices that drive the internet or connected to it – but many of those use outdated kernel versions with known vulnerabilities, as vendors and admins fear switching to a later version might break something.

The mechanisms built for tracking Linux kernel regressions will include adapting or writing a servicebot tailored to the specific needs of the kernel developers and their email based workflow. To make sure the solution is practical and accepted in practice the project owner will work it out in close relationship with the maintainers and create procedures on how to use it during development.

The goal is to see the solution properly established to ensure its continued use after this project ends

Country: **Germany**

Team: **Thorsten Leemhuis.**

Further information: **https://linux-regtracking.leemhuis.info/**

Contact: **linux@leemhuis.info**

From Low-level Internet Sockets to High-level Programmable Connectors (Reowolf)

A major obstacle in the further development of the Internet is that improving quality of service relies on non-standard ad-hoc techniques such as deep packet inspection.

The effectiveness of these techniques is thwarted by the uptake of end-to-end socket encryption (partially caused by EU privacy regulation)!

Funded by NLnet/NGI0, Reowolf 1.0 is a first step to solve these problems, demonstrably by a centralized proof-of-concept implementation, but leaves some major challenges out-of-scope. In this project, Reowolf 2.0 tackles remaining challenges: increasing reliability, trust, standardization, and performance.

Reowolf replaces sockets by connectors which support high-level verification, compilation, and optimization techniques.

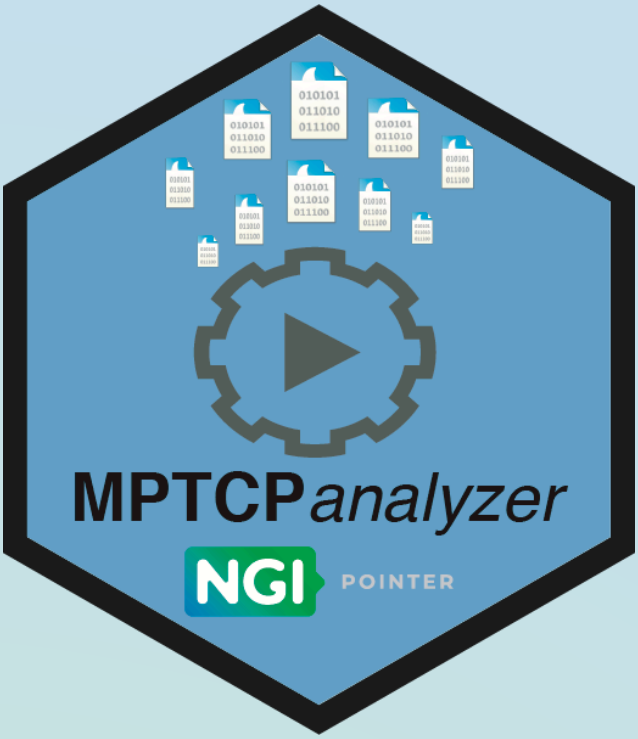
Resilience against service disruption is realized by decentralization; we improve security aspects of confidentiality, integrity, and availability (CIA); we draft Internet standards; and we integrate the middleware into the operating system kernel.

Country: **Germany**

Team: **Stichting Nederlandse Wetenschappelijk Onderzoek Instituten - Institute CWI**

Further information: **Website**
https://reowolf.net
Repository
https://scm.cwi.nl/FM/reowolf

Contact: **reowolf-list@cwi.nl**



Multipath TCP (MPTCP)

Multipath TCP (MPTCP) extends the most widely used transport protocol on the internet (TCP) so that it can use several physical paths (e.g., Wifi, cellular, between multihomed servers).

This allows to speed up transfers, smoothly transition from wifi to cellular when leaving one's house or potentially avoid traffic spying.

While the protocol is proven to work well in certain conditions (the fastest TCP connection ever was using MPTCP), it is configuration-sensitive and can degrade badly under adverse conditions (for instance in heterogeneous networks with small buffers).

The aim of this project is to provide the tool to help analyze the performance of a multipath protocol as well as the software to (auto)configure the system depending on the application objective and network conditions.

Country: **France**

Team: **Matthieu Coudron**

Further information: **https://github.com/ngi-mptcp**

Contact: **http://github.com/teto/**

Wireless Optical Communication System for Urban Environments

KORUZA is a wireless optical communication system for urban environments, based on the FSO technology, designed for last-mile, 5G and IoT applications. It uses an eye-safe collimated beam of IR light for point-to-point data transmission through air.

The solution avoids digging up roads, allowing distances up to 150m with fibre-like speeds 1-10 Gbps.

By utilizing mass-produced parts and open-source standards, KORUZA differentiates itself from the competition by dramatically reducing costs, coming at ¬ 10/meter, 10x cheaper than other FSO and fibre-based solutions.

The low latency and jitter makes it suitable for 5G networks, last mile network

Country: **Slovenia**

Team: **IRNAS – institute for development of advanced applied systems Ltd.**

Further information: **https://www.irnas.eu/**
https://www.facebook.com/instituteirnas/
https://twitter.com/institute_irnas
https://www.linkedin.com/company/institute-for-development-of-advanced-applied-systems/
https://www.instagram.com/institute_irnas/
https://medium.com/@institute_irnas

Contact: **https://www.linkedin.com/in/luka-mustafa/**

Receiver-driven Incoming-tra˚c Management

The goal of RIM is to evolve the Internet's resource management approach to enable receivers to execute congestion control functions, taking an active role in determining how the capacity of incoming

Further information is split among flows. In the current Internet architecture, the distribution of link capacity across multiple flows is determined by the congestion control algorithms running in the senders.

Content consumers play a passive role on the distribution of the capacity of their incoming Further information between flows.

The ambition of the RIM project is to empower end-users to be able to influence the share of capacity that is allocated to different incoming flows according to their preferences.

We propose to achieve this by enabling congestion control functions at the receiver-end of existent transport protocols (TCP/QUIC).

Country: **Spain**

Team: **Universidad Carlos III de Madrid**

Further information: **http://rledbat.netcom.it.uc3m.es/**

Contact: **Marcelo Bagnulo - Associate Professor - Telematics Department University Carlos III of Madrid**

https://www.researchgate.net/scientic-contributions/Marcelo-Bagnulo-9200827

Incentivised Content Dissemination at the Network Edge

DataHop is building a mobile content distribution infrastructure based on smartphone D2D communications.

Content is pushed to source selected mobile users and then hops from device-to-device (D2D) and spreads in the network to destination nodes. Sources and destinations sync through our unique, data-centric connectivity software solution.

Our revolutionary approach guarantees that content spreads independently of the cellular connection, building a content distribution network that works completely at the edge without depending on the network infrastructure.

Therefore, challenged connectivity and data caps are not a barrier to the distribution of large volumes of data, allowing users to share their unused resources (in our case smartphone memory and available battery) to become an active part of the network, instead of just a consumer.

Country: **UK**

Team: **DataHop Labs Ltd.**

Further information: **http://datahop.network**
https://www.linkedin.com/company/datahoplabs/
@datahoplabs
https://github.com/datahop

Contact: **contact@datahop.network**

EDGESec

Internet technologies and current practice does not address security requirements of edge based devices very well. It is a fact that the "admin page" of most routers, wifi devices and webcams is "unsecured". It is perhaps not surprise that a recent Symantec study showed that "Routers account for 75% of infected IOT devices " [1]

The problem is that domain resolution on local Internets and HTTPS certificates do not work well together. Also HTTPS certs assume the private key is secure; how do I do this on a small edge device?

EdgeSEC will define innovative user experience, key distribution, key storage and secure service discovery primitives, to address current security shortcomings and provide a new vision for integrated cloud-edge services.

[1] https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

Country: **Ireland**

Team: **NQMCyber Ltd**

Further information: **Company website: nqmcyber.com**
Git repo for project:
https://github.com/nqminds/EDGESec

Contact: **https://www.linkedin.com/in/nickallott/**

Nyxt Browser

We make Next, a fully extensible power-browser. It enables sophisticated web document manipulation and processing, e.g.:

+ A user can switch between tabs by topic, URL, etc.
+ A user can instantly search all URLs on a page by name, or target.
+ A user can search through all of their bookmarks with compound queries (e.g. (show bookmarks tagged "fish" AND "goldfish" OR "carp")

We wish to extend these capabilities via a number of paradigms/technologies:

+ Strengthen the text and semantic analysis capabilities of Next to allow chaining these operations in workflows for document processing.
+ Graphical, interactive document object model selection and manipulation.

This will allow the user to operate on a set of elements simultaneously, to for example, map a download operation on a set of Further information.

+ Users can persist/retrieve document annotations.
+ "Omni-search" capability allowing users to simultaneously search through their history, notes, and all other sources.

Country: **Germany / France**

Team: **John Mercouris**

Further information: **https://nyxt.atlas.engineer**
https://github.com/atlas-engineer/nyxt

Contact: **http://john.mercouris.online**

Lightmeter (LM)

Lightmeter will make it easy to run email servers large and small by visualising, monitoring, and notifying users of problems and opportunities for improved performance and security.

People will regain control of sensitive communications either directly by running their own mailservers, or indirectly via the increased diversity and trustworthiness of mail hosting services

Country: **Germany, Brazil, Albania**

Team: **Sam Tuke**

Further information: **https://lightmeter.io/**
https://twitter.com/lightmeterio
https://www.linkedin.com/company/lightmeter
https://mastodon.social/@lightmetert

Contact: **@samtuke**

Scuttlebutt - The Gossip Protocol (SSB)

Scuttlebutt (SSB) is an edge computing, peer-to-peer communications protocol.

Originally created by Dominic Tarr in 2015 it is currently developed by an established global community with a variety of implementations, the most wide-spread implementation currently being the main network of ~20,000 nodes.

As one of the frontier protocols in the realms of the Distributed Webs, it shares this space with DAT, IPFS and more.
SSB stands out among its siblings due to its unique network architecture in which data flows opportunistically between nodes and along paths of trust relationships between humans, it is due to this the protocol is called "the gossip protocol", with the network architecture resembling data flows between humans.

Country: **Denmark**

Team: **Scuttlebutt European Collective via IOLA ApS**

The organizational structure behind Scuttlebutt is distributed over several projects globally, in the scale of VC-funded startup apps based on Scuttlebutt to experimental network designs for the Distributed Webs.

Currently all of the Scuttlebutt code base, as developed by different parties, is licensed as MIT and
AGPL

Further information: **https://scuttlebutt.nz/**
https://scuttlebutt.eu/
https://github.com/dominictarr/scuttlebutt

Contact: **@thezelf / @zelf**

DREAM - Distributed Replicable Extensible Agency Machine

DREAM stems from the encounter of P2Pcollab, openEngiadina, and IN COMMON developers through grassroots community events.

Over time they realized the common interest in systems architecture and values they share to sustain local communities and commons initiatives in the respect for human dignity and human rights, freedom, democracy, equality, and the rule of law.

DREAM aims to advance critical infrastructure parts of our common projects to jump start a long time dream – hence the name – to see converge the best of the Social Web (easy UI, Linked Data), with the best of Peer-to-Peer networking architectures (end-to-end encryption, autonomy, replicability, lack of central control, censorship resistance, privacy-by-design and privacy-by-default).

Together we want to explore and bootstrap the next generation of locally-aware, distributed collaborative Internet protocols and applications to empower citizens to act and find agency together, free from alien interference and disinformation.

Country: **Belgium**

Team: **Petites Singularités ASBL**

Further information: **https://dream.public.cat**
https://gitlab.com/public.dream

Contact: **DREAM Team <dream@public.cat>**

Core Internet Application: 3;

Lightmeter - **Email infrastructure reinvented**
Ltt.rs - **Open source email client (JMAP);**
Next - **Fully extensible power-browser.**
Dream - **Distributed Replicable Extensible Agency Machine**

Identity: 1;

Id-xover - **Internet-wide identity through realm crossover.**

Virtualisation: 1;

MirageOS - **Deploying MirageOS unikernels.**

Transport/Network: 7;

MPTCP5G - **Multipath TCP for 5G networks;**
MPTCP - **Multipath TCP;**
RIM - **Receiver-driven Incoming-tra˜c Management.**
IGNNITION - **Fast prototyping of complex Graph Neural Networks for optimisation**
WireGuard - **Secure VPN tunnel for all major operating systems with modern crypto**
TA4NGI - **Trust and Authentication for Next Generation Internet.**
SCE - **Some Congestion Experienced**

Security: 2;

Firmware-lib - **European Firmware and app library.**
EDGESec - **New architecture for local (edge based) routers.**

Tools: 1;

Linux-Regtracking - **Linux kernel regression tracking.**

Privacy-by-Design Communication Protocols: 4;

KORUZA - **Wireless optical communication system for urban environments.**
DATAHOP - **Incentivised content dissemination at the network edge.**
Scuttlebutt - **The Gossip protocol.**
Peergos - **Decentralised, end-to-end encrypted, and trustless protocol.**

New ideas and paradigms: 4;
DREAM - **Distributed Replicable Extensible Agency Machine.**
Reowolf - **From low-level internet sockets to high-level programmable connectors.**
Solid-Shape - **Reshaping linked data on the ˛y.**
Veri?edSCION - **Veri˚ed secure routing with SCION.**