NGI

Partnership for innovative technological solutions to ensure privacy & enhance trust for the human-centric Internet

Webinar, 26 February 2021

NGI TRUST

Webinar – Agenda

Timing	Topic
10:30 – 10:40	Welcome *Jean-Luc Dorel, DG Connect, European Commission*
10:40 – 10:50	Introduction *Alasdair Reid, NGI Trust coordinator, EFIS Centre*
10:50 – 11:40	NGI_Trust Funded projects results *NGI_Trust Project managers*
11:40 – 11:55	Round table discussion and exchange - Q&A *All*
11:55 – 12:00	Wrap-up and close

NGI TRUST

Welcome and Introduction: NGI TRUST in a snapshot

Jean-Luc Dorel, DG Connect & Alasdair Reid, EFIS Centre

Project partners

Key facts & figures

- Duration: December 2018 - November 2021
- 3 open calls :
  - 300 applications;
  - 448 applicants;
  - 36 countries.
- 3rd party funding: €5.6m:
  - 57 funded projects;
  - 84 funded third parties;
  - 20 countries.

NGI TRUST objectives

1. Reinforce, structure and develop the community of researchers, innovators and technology developers in the field of privacy and trust enhancing technologies
2. Build on the state of the art in privacy and trust enhancing technologies by focusing support for third-party projects in a limited number of priority topics
3. Improve user trust and acceptance of emerging technologies by focusing on applications and solutions that develop a more open, robust and dependable Internet and strengthen Internet Governance
4. Foster the exploitation and commercialisation of the results of selected third-party projects through a tailored process of coaching and mentoring

NGI TRUST

NGI TRUST

57 PROJECTS FUNDED
12 THEMATIC AREAS

BEYOND PASSWORDS

BETTER PRIVACY

SAFER BROWSING

USER CONTROL

IMPACT OF AI

HUMAN-CENTRIC INTERNET

STRONGER TOOLS

EFFECTIVE IDENTITY

PERSONAL DATA MANAGEMENT

DATA ETHICS

SECURING THE INTERNET OF THINGS

ADVANCING IDENTITY

TETRA SCALE-UP BOOTCAMP

ONLINE, MARCH 16-18

Applications due this weekend!

business.ngi.eu
info@tetraproject.eu

WHAT DO YOU GET WITH TETRA?

3 days of trainings and coaching on team management and performance growth, startup & scaleup financing, IP in open source services, investor relations, business modeling

20 hours of 1-on-1 mentoring and matchmaking events for most promising teams attending to the bootcamps

A personalised master plan with guidelines for teams successfully exiting the bootcamps

Access to additional trainings, materials and contacts for hands-on business development

UPCOMING EVENTS

24 Feb: Webinar on IP and software code management
Register HERE.

28 Feb: Due date for #1 Scale-up bootcamp (16-18 March)
Intensive trainings and mentoring for teams aiming to scale their business.

Register at www.f6s.com/ngitetrascale-upbootcampmarch2021/apply.

Mar 3: Webinar on IP research tools Register HERE.

TBA: #2 Build-up bootcamp (May 2021)
Intensive trainings and mentoring for teams aiming to build an idea into a business.

TBA: #2 open call for Tenderio Plus subscription
Apply to get easy access to public tenders at business.ngi.eu/join-now/open-call

Applications for March bootcamp due Feb 28

See more at business.ngi.eu

CONTACT US AT

INFO@TETRAPROJECT.EU

The NGITETRA project has received funding
from the European Union's Horizon 2020 Research and Innovation
Programme under Grant Agreement No 825147

NGI TRUST Funded projects results

Project	Third party
CAP-A [Safer Browsing]	FORTH *Theodore Patkos and Giorgos Flouris*
CCS Cozy Cloud's Shiffremir [User Control]	Cozy Cloud *Benjamin André*
CONTEXT - Decentralized messaging [User Control]	Danube Tech GmbH *Markus Sabadello*
CryRev [Beyond Password]	Assured AB *Jonas Magazinius*
TrustedUX [Human Centric Internet]	Tallinn University *Iuliia Paramonova*

NGI TRUST

CAP-A

FORTH – Theodore Patkos & Giorgos Flouris

CAP-A PROJECT

A Community-driven Approach to Privacy Awareness

FORTH INSTITUTE OF COMPUTER SCIENCE

I N 2

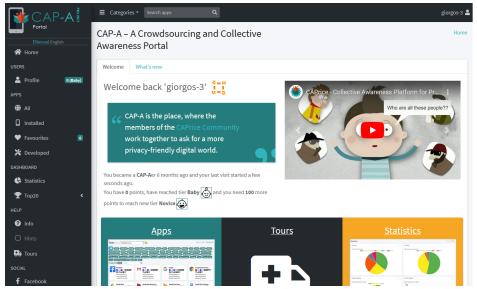
This project has received funding from the European Union's Horizon 2020 research and innovation programme under the NGI_TRUST grant agreement no 825618

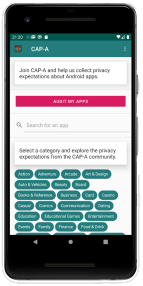
NGI TRUST

Objectives & Contributions

- **Privacy** and **anonymity** in the digital world are becoming increasingly difficult to achieve.
- Solid legal regulations and technical countermeasures are not always sufficient to achieve society-wide impact;
  - **Data protection can also be powered by the society itself**
- CAP-A is offering socio-technical tools to promote **collective awareness** and **informed consent**
- Data collection and use by digital products are driven by the **expectations and needs** of the consumers themselves

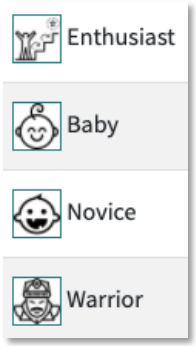
Results & Next Steps

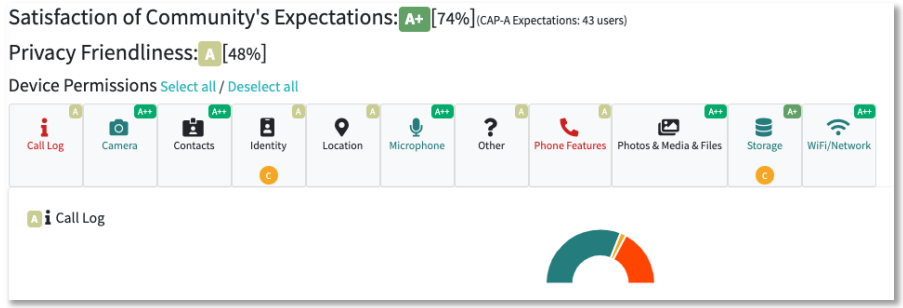


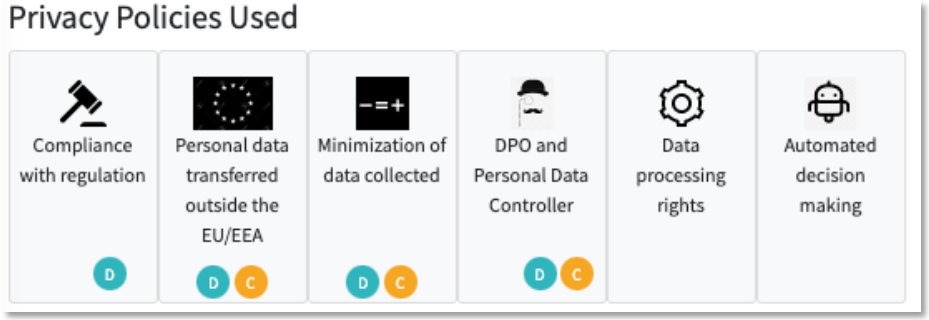


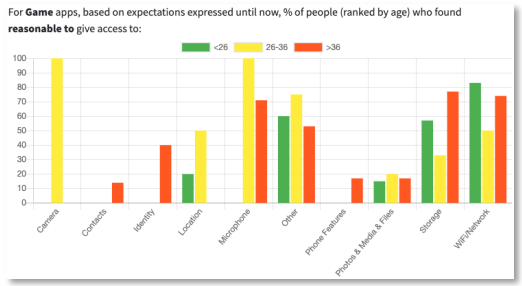
A **web-portal** and a **mobile app** offering a suit of tools to motivate user participation in privacy-related tasks, such as

- App rating
- Expression of expectations
- Privacy Policy annotation
- User rewards policy









Organization of **thematic events** & generation of users **privacy norms**

Up next: Preparatory work towards the establishment of a Non-Profit Organisation (NPO)

Contact: *Theodore Patkos (patkos@ics.forth.gr)*
Giorgos Flouris (fgeo@ics.forth.gr)
Video: *https://tinyurl.com/5ebpjslp*

CCS Cozy Cloud's Shiffremir

Cozy Cloud – Benjamin André

CCS project – Project results

Objectives and Contributions

Objectives

- As one of the most powerful leverage for a real privacy enforcement, the CCS project focuses on **data encryption**.
- Today's traditional approaches are vulnerable and mostly rely on untrusted and centralized servers. Our approach is radically different and considers the **users devices as the only legitimate places for data access and encryption.**

Contributions

- Evaluate the performance impact of a **full client-side encryption** system in a web file management app
- Define technical solutions to enable a **zero-knowledge server on data indexing and sharing**
- Enforce sustainability through an **intuitive and decentralized recovery mechanism** to recover user password.

CCS project – Project results

Results

Performances of client-side encryption

- ✓ Generic guidelines for client-side encryption in a web environement
- ✓ Technical insights on the implementation choices for Cozy Drive
- ✓ Benchmarking of Web Crypto API in several devices

Zero-knowledge server

- ✓ Indexing: an original solution mixing deterministic encryption and order-preserving encryption
- ✓ Sharing : a decentralized protocol using a proxy re-encryption scheme

Sustainability through decentralized recovery

- ✓ An intuitive protocol combining client-side encryption, decentralized sharing and Shamir's secret sharing
- ✓ Strong focus on UX with user interviews led alongisde the technical design

Blog post : https://blog.cozy.io/en/cozy-cloud-how-to-encrypt-web-application/
Open-source code: https://github.com/paultranvan/cozy-drive/tree/crypto

Next steps

Client-side encryption

- ➢ In production for passwords, next step for files

Zero-knowledge sharing

- ➢ Current exploration for encrypted password sharing

Sustainability of client-side encryption to recover user password

- ➢ A huge topic itself partly due to UX complexity: funding expected (through customer or NGI?)

CONTEXT - Decentralized Messaging

Danube Tech – Markus Sabadello

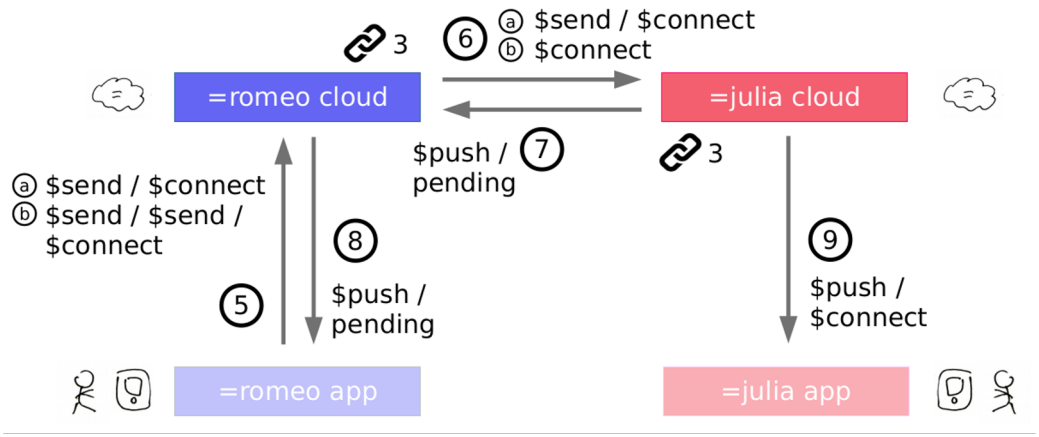
Objectives and Contributions

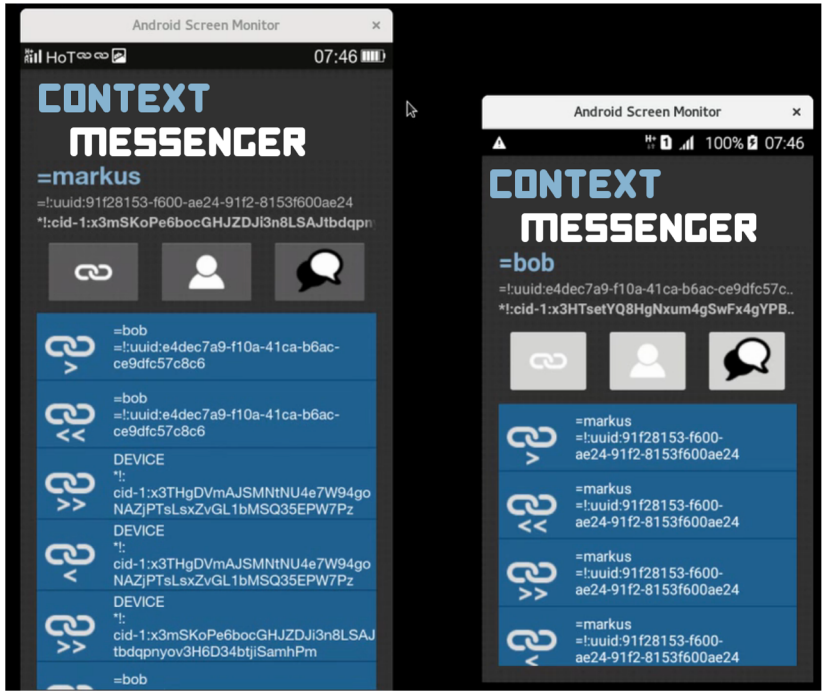
- Project **“Context”**
- Area 1: Digital Identity:
  - DIDs, Verifiable Credentials, JWT, OIDC, Solid, CHAPI, etc.
- Area 2: Decentralized Messaging:
  - SMTP, XMPP, ActivityPub, JWM, DIDComm, OStatus, etc.
- **Objective:** Combine identity and messaging into a single data model and protocol
- Conception of Architecture, Conception of Cryptography, Application Design, Security Risk Assessment, Prototype Implementation

DANUBE TECH GMBH

Results and Next Steps

Architecture and Prototype:





Business Deliverables

- Market analysis, go-to-market-strategy, business modelling, pricing, IPR

DANUBE TECH GMBH

CryRev

Assured – Jonas Magazinius

CryRev

CrypTech Revision

NGI Trust 2021-02-26

ASSURED

SECURITY CONSULTANTS

The CrypTech Project

- Develop an open Hardware Security Module
  - Open hardware, software design
  - Support Applications such as:
    - DNSSEC
    - RPKI
    - TOR Consensus
    - Let's Encrypt CA
- First complete machine
  - The CrypTech Alpha

The CryRev project

- CryRev – CrypTech Revision
- Develop a new revision of the Alpha, improving:
  - Openness: Convert PCB design to KiCAD
  - Security 1: Move master key storage to FPGA with ns tamper response and key zeroisation
  - Security 2: Move att key related processing into the FPGA
  - Performance: Develop advanced RSA acceleration

- *”A more open and trustworthy CrypTech HSM that provides competitive security and performance”*

Delivered results

- Official release of CrypTech 4.0 – ”Way faster”
  - New high speed ModExpNG core with CRT and RSA blinding factor support
  - Clock FPGA synchronously from FMC bus with multipliers, to eliminate clock domain crossing bottlenecks
  - New AES-keywrap core with direct connection to master key memory
  - AES performance improvements
  - SHA-2 timing fixes to support higher clock rates
  - Redesign EC cores, adding support for ECDH (P-256 & P-384) and Ed25519
  - Support for hash-based post-quantum safe signatures
  - I/O speedups on FMC bus
  - Faster prime generation algorithm (RSA key generation)

https://cryptech.is/2020/09/cryptech-releases-version-4-0/

CrypTech 4.0 RSA-2048 performance

- General version: 95 RSA signatures per second
- Specialized signer version (without ECDSA support):
  - 130+ signatures per second
  - 7 parallell signer engines

- Comparison to commercial alternatives

Algorithm	SafeNet USB HSM
RSA-1024	200
RSA-2048	60
ECC P256	40
ECIES	20
AES-GCM	70

Industry needs

- Identified needs
  - Trusted root, trusted storage, key management
  - Environment adapted solutions
    - New FPGAs for Automotive, ICS, Space from Xilinx
  - Performance, power, cost optimized
  - Reduced attack/problem surface
- CrypTech advantage
  - Highly flexible, modular design, both toolbox and platform
  - High single engine performance
  - Core for wrapping and at-rest protection of secrets (keys)

Additional application areas

- Automotive
  - Projects HoliSec and CyRev identified need for in-vehicle key management
  - Secure onboard/offboard communication – ISO26262 / ISO21434
- Maritime
  - NIS directive
- IoT and ICS
  - Wireless sensor networks
  - Distributed Control Loop

More information and contact

- CrypTech website: http://cryptech.is/

- Joachim Strömbergson
  - joachim@assured.se
  - +46 733 759 702

- Jonas Magazinius, PhD – CEO Assured AB
  - jonas@assured.se
  - +46 732 530 530

TrustedUX

Tallinn University – Sonia Sousa & Iuliia Paramonova

TrustedUX

Tallinn University,

School of digital technology, the HCI group, http://hci.tlu.ee/

Sonia Sousa, Iuliia Paramonova

2021

Objectives and Contributions

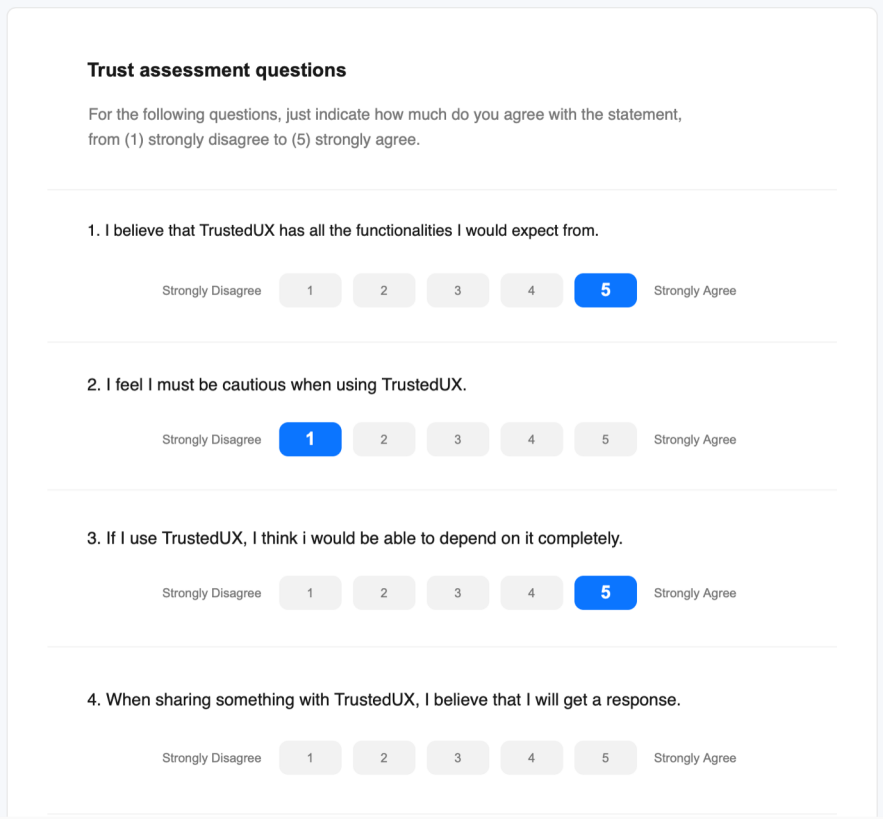
TrustedUX

Objective

To develop a easy to use, user friendly **online tool** that enable user researchers, interaction designers and user experience practitioners run studies **to understand users trust in digital technologies**.

Contributions

- Validated toolset for design trusted interactive systems
- Analytics and visualization mechanisms for rate system experiences and awareness of trust.
- Support digital materials (e.g. how-to videos).
- Guidelines and templates for reporting and present design recommendations.



Results and Next Steps

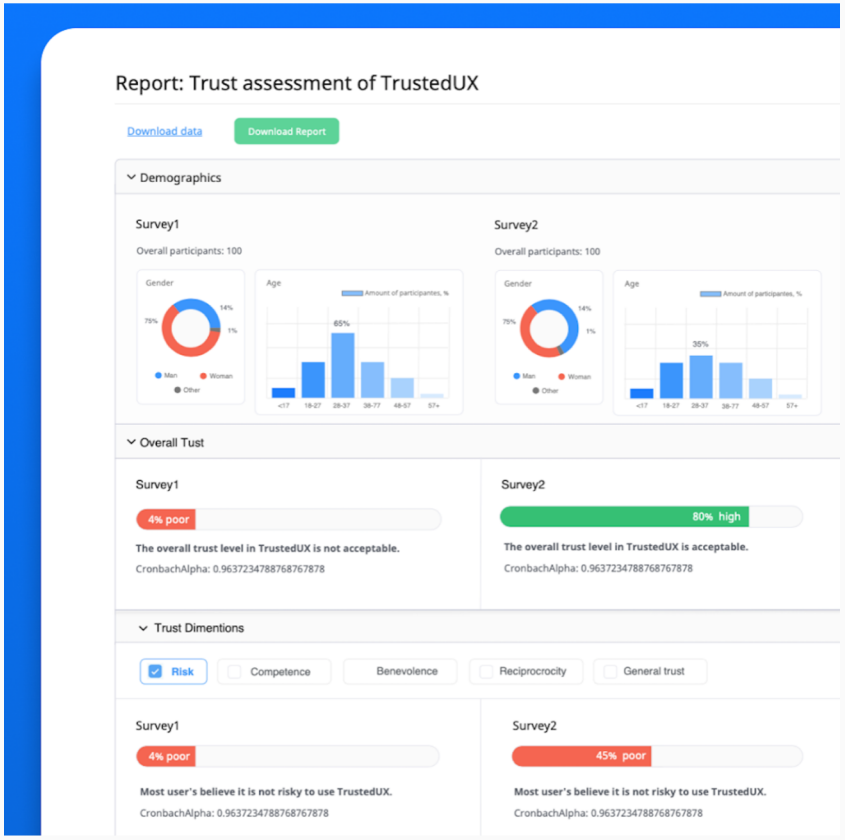
TrustedUX

Results

- https://www.trustux.org/ Tool that aggregate measure of trust and decomposes the indicator in its components;
- Landing and tool Design and graphical resources;
- User evaluation of the system (personas, CJM);
- TrustedUX theoretical framework (Trust Model);
- Videos and guidelines on ways to use TrustedUX;
- The source code of the service

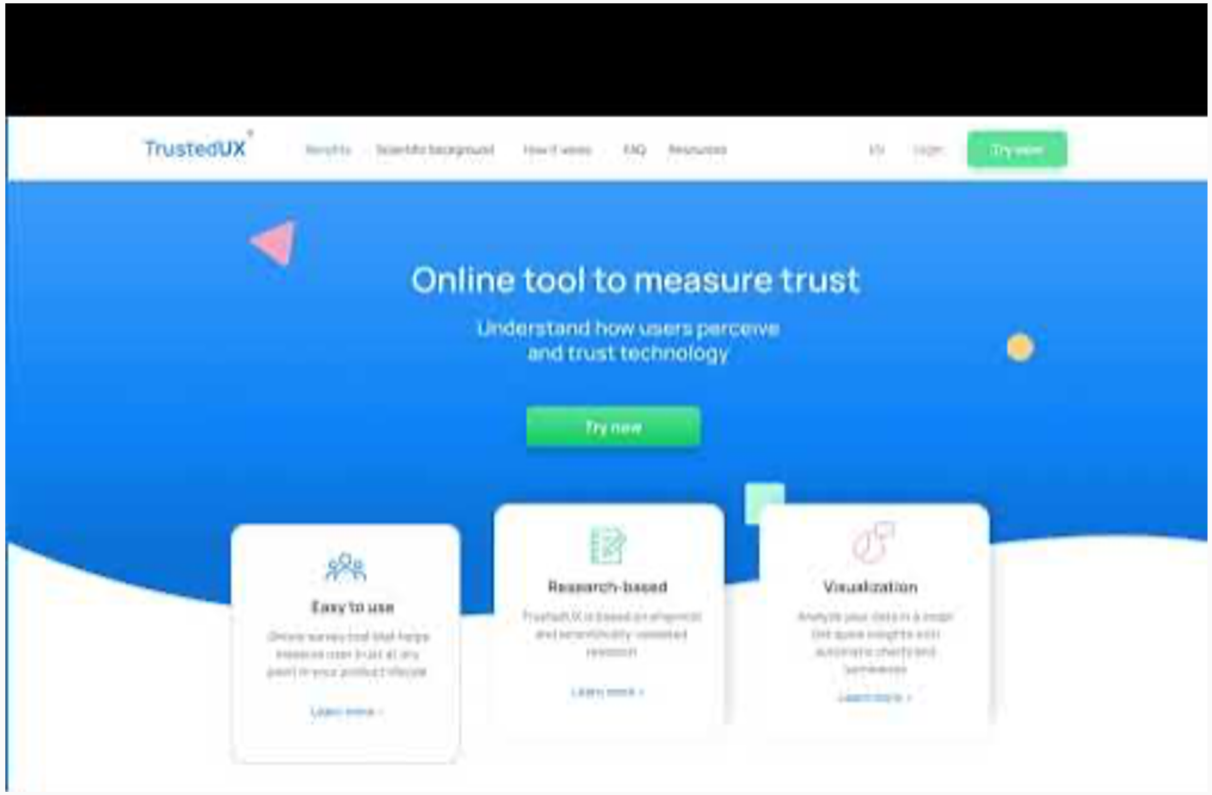
Next Steps

- Front-end updates
- Provide further customisation, consulting and support services
- Promoting (educational context, European research projects, e.g. AI-Mind and SEEDS)
- Exploring trust persona archetypes across gender and culture
- Developing methodological framework on how to design trustworthy human-trust interactions.



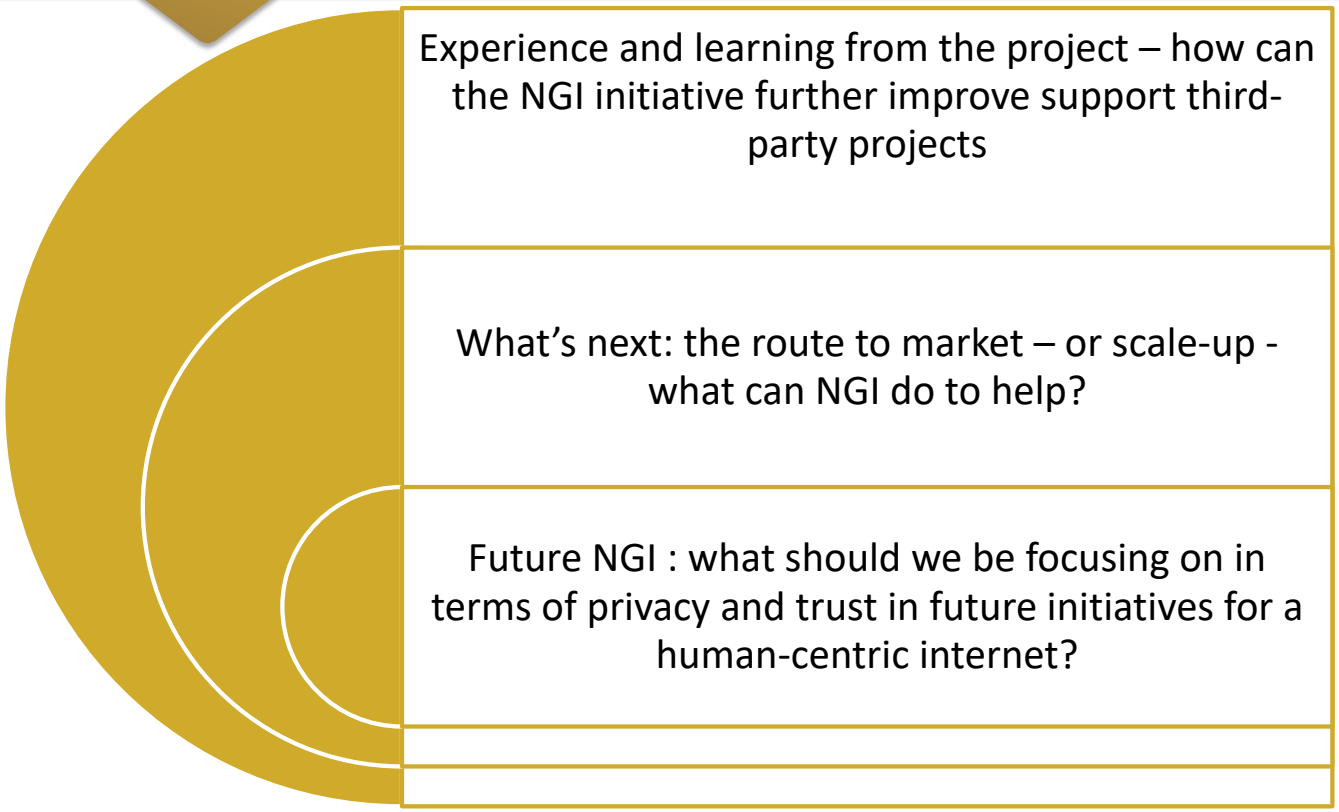
https://www.trustux.org/

TrustedUX



https://www.youtube.com/watch?v=aw-Fsn7WLB0

Round table discussion and exchange - Q&A



NGI TRUST

More information/contact us

- Project coordinator : Mr Alasdair Reid @ EFIS Centre - www.efiscentre.eu
- Email : NGI-Trust-support@lists.geant.org
- Twitter: @NgiTrust
- NGI_TRUST wiki : https://wiki.geant.org/display/NGITrust
- NGI.eu website : https://www.ngi.eu/about/

The NGI_TRUST project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 825618