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

Webinar, 26 February 2021
# Webinar – Agenda

<table>
<thead>
<tr>
<th>Timing</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:30 – 10:40</td>
<td>Welcome&lt;br&gt; <em>Jean-Luc Dorel, DG Connect, European Commission</em></td>
</tr>
<tr>
<td>10:40 – 10:50</td>
<td>Introduction&lt;br&gt; <em>Alasdair Reid, NGI Trust coordinator, EFIS Centre</em></td>
</tr>
<tr>
<td>10:50 – 11:40</td>
<td>NGI_Trust Funded projects results&lt;br&gt; <em>NGI_Trust Project managers</em></td>
</tr>
<tr>
<td>11:40 – 11:55</td>
<td>Round table discussion and exchange - Q&amp;A&lt;br&gt; <em>All</em></td>
</tr>
<tr>
<td>11:55 – 12:00</td>
<td>Wrap-up and close</td>
</tr>
</tbody>
</table>
Welcome and Introduction: NGI TRUST in a snapshot

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

<table>
<thead>
<tr>
<th>Project partners</th>
<th>Key facts &amp; figures</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFIS</td>
<td>• Duration: December 2018 - November 2021</td>
</tr>
<tr>
<td>GÉANT</td>
<td>• 3 open calls:</td>
</tr>
<tr>
<td></td>
<td>▪ 300 applications;</td>
</tr>
<tr>
<td></td>
<td>▪ 448 applicants;</td>
</tr>
<tr>
<td></td>
<td>▪ 36 countries.</td>
</tr>
<tr>
<td>ebn</td>
<td>• 3rd party funding: €5.6m:</td>
</tr>
<tr>
<td></td>
<td>▪ 57 funded projects;</td>
</tr>
<tr>
<td></td>
<td>▪ 84 funded third parties;</td>
</tr>
<tr>
<td></td>
<td>▪ 20 countries.</td>
</tr>
</tbody>
</table>
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

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
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

<table>
<thead>
<tr>
<th>Project</th>
<th>Third party</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAP-A [Safer Browsing]</td>
<td>FORTH <em>Theodore Patkos and Giorgos Flouris</em></td>
</tr>
<tr>
<td><strong>CCS Cozy Cloud's Shiffremir</strong> [User Control]</td>
<td>Cozy Cloud <em>Benjamin André</em></td>
</tr>
<tr>
<td><strong>CONTEXT - Decentralized messaging</strong> [User Control]</td>
<td>Danube Tech GmbH <em>Markus Sabadello</em></td>
</tr>
<tr>
<td>CryRev [Beyond Password]</td>
<td>Assured AB <em>Jonas Magazinius</em></td>
</tr>
<tr>
<td><strong>TrustedUX</strong> [Human Centric Internet]</td>
<td>Tallinn University <em>Iulia Paramonova</em></td>
</tr>
</tbody>
</table>
CAP-A
FORTH – Theodore Patkos & Giorgos Flouris
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 suite 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
Cozy Cloud’s Shiffremir (CCS)

Project results

CHANGE THE PARADIGM TO CHANGE THE RULES
### 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

<table>
<thead>
<tr>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performances of client-side encryption</strong></td>
</tr>
<tr>
<td>✓ Generic guidelines for client-side encryption in a web environment</td>
</tr>
<tr>
<td>✓ Technical insights on the implementation choices for Cozy Drive</td>
</tr>
<tr>
<td>✓ Benchmarking of Web Crypto API in several devices</td>
</tr>
<tr>
<td><strong>Zero-knowledge server</strong></td>
</tr>
<tr>
<td>✓ Indexing: an original solution mixing deterministic encryption and order-preserving encryption</td>
</tr>
<tr>
<td>✓ Sharing: a decentralized protocol using a proxy re-encryption scheme</td>
</tr>
<tr>
<td><strong>Sustainability through decentralized recovery</strong></td>
</tr>
<tr>
<td>✓ An intuitive protocol combining client-side encryption, decentralized sharing and Shamir’s secret sharing</td>
</tr>
<tr>
<td>✓ Strong focus on UX with user interviews led alongside the technical design</td>
</tr>
</tbody>
</table>

Open-source code: [https://github.com/paultranvan/cozy-drive/tree/crypto](https://github.com/paultranvan/cozy-drive/tree/crypto)

<table>
<thead>
<tr>
<th>Next steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client-side encryption</strong></td>
</tr>
<tr>
<td>➢ In production for passwords, next step for files</td>
</tr>
<tr>
<td><strong>Zero-knowledge sharing</strong></td>
</tr>
<tr>
<td>➢ Current exploration for encrypted password sharing</td>
</tr>
<tr>
<td><strong>Sustainability of client-side encryption to recover user password</strong></td>
</tr>
<tr>
<td>➢ A huge topic itself partly due to UX complexity: funding expected (through customer or NGI?)</td>
</tr>
</tbody>
</table>
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
Results and Next Steps

- **Architecture and Prototype:**

- **Business Deliverables**
  - Market analysis, go-to-market-strategy, business modelling, pricing, IPR
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 parallel signer engines

- Comparison to commercial alternatives

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>SafeNet USB HSM</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA-1024</td>
<td>200</td>
</tr>
<tr>
<td>RSA-2048</td>
<td>60</td>
</tr>
<tr>
<td>ECC P256</td>
<td>49</td>
</tr>
<tr>
<td>ECIES</td>
<td>29</td>
</tr>
<tr>
<td>AES-128CM</td>
<td>70</td>
</tr>
</tbody>
</table>
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
Tallinn University, School of digital technology, the HCI group, http://hci.tlu.ee/
Sonia Sousa, Iuliia Paramonova

2021
Objective
To develop an easy-to-use, user-friendly online tool that enables user researchers, interaction designers, and user experience practitioners to run studies to understand users' trust in digital technologies.

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

- [https://www.trustux.org/](https://www.trustux.org/) Tool that aggregates 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.
Experience and learning from the project – how can the NGI initiative further improve support third-party projects

What’s next: the route to market – or scale-up - what can NGI do to help?

Future NGI: what should we be focusing on in terms of privacy and trust in future initiatives for a human-centric internet?
The NGI_TRUST project has received funding from the European Union’s Horizon 2020 Research and Innovation Programme under Grant Agreement No 825618

More information/contact us

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