15 de julio de 2021

Estimados amigos:

A través de este nuevo boletín informativo, os hacemos llegar las últimas novedades del

Clúster 3: Seguridad civil para la sociedad

- **Publicadas las grabaciones de la jornada informativa Europea de la convocatoria 2021 del Clúster 3 + 2 workshops que tuvieron lugar los días 30 de junio y 1 de julio**:

  Horizon Europe Civil Security for Society Infoday and Brokerage Event - Presentations & recordings (b2match.io)

  Os recordamos que el Marketplace de dichas **jornadas seguirá abierto hasta finales de noviembre de 2021** para facilitar la preparación de consorcios e identificación de socios.

- **NUEVA PÁGINA WEB de CERIS (Community of Users for Research and Innovation in Security):** https://ec.europa.eu/home-affairs/CERIS

  Os recordamos que, para recibir noticias y estar actualizado sobre las actividades de CERIS, es imprescindible estar inscrito a través de: Stay tuned (europa.eu)

- **Información de interés para la convocatoria HORIZON-CL3-2021-INFRA:** conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf

- **Publicada la "Horizon Europe Programme Guide"** : programme-guide_horizon_en.pdf (europa.eu)
  Factsheet: Joint Cyber Unit | Shaping Europe's digital future (europa.eu)

- **Propuesta de la Comisión Europea para la creación de una "Joint Cyber unit":** Daily News 23 / 06 / 2021 (europa.eu)

- **Situación de las entidades Suizas que participen en la convocatoria 2021 del Clúster 3 (información no vinculante).**

  *Legal entities **established in Switzerland** are currently **not** automatically **eligible for funding** in Horizon Europe. Negotiations regarding the association of Switzerland to the next generation of EU programmes are currently on hold,*

therefore Switzerland is considered as a non-associated third country, and remains eligible for Horizon Europe participations under the conditions applicable to non-associated third countries. As a matter of consequences, legal entities established in Switzerland are not eligible for funding, ***except if*** *provided for in the specific call conditions, or if their participation is considered essential for implementing the action by the granting authority, for example in view of their outstanding competence/expertise, access to particular research infrastructures, access to particular geographical environments or access to particular data. Therefore, and if not exceptionally eligible for funding, legal entities established in Switzerland would participate* ***as associated partners*** *instead and would not be eligible to declare costs in EU grants.*
All relevant information on the eligibility of CH entities, in a form of an FAQ, is available in the EC's Funding and Tender Portal.

- **Búsquedas de socios convocatoria 2021 Clúster 3:**

  - **PYME de Estonia interesada en participar en propuestas de los topics siguientes:**

    - CL3-2021-FCT-01-02 Lawful interception using new and emerging technologies (5G & beyond, quantum computing and encryption)
    - CL3-2021-FCT-01-03 Disinformation and fake news are combated and trust in the digital world is raised
    - CL3-2021-BM-01-01 Enhanced security and management of borders, maritime environment, activities and transport, by increased surveillance capability, including high altitude, long endurance aerial support
    - CL3-2021-INFRA-01-01 European infrastructures and their autonomy safeguarded against systemic risks
    - CL3-2021-CS-01-02 Improved security in open-source and open-specification hardware for connected devices

    Ver Anexo 1.

  - **Entidad Lituana interesada en participar en los topics siguientes:**
    - **HORIZON-CL3-2021-CS-01-01;**
    - **HORIZON-CL3-2021-CS-01-02;**
    - **HORIZON-CL3-2021-CS-01-03 ;**

- **HORIZON-CL3-2021-CS-01-04.**

  Ver Anexo 2.

- **Entidad británica interesada en participar en el topic: Horizon Europe CL3 - 2021 FCT-01-12 Online identity theft is countered**

  Ver Anexo 3

- **Entidad británica interesada en participar en los topics siguientes: DRS 01-01, DRS -01-02 and DRS-01-03**

  Ver Anexo 4

- **Entidad británica interesada en participar en los topics siguientes: BM-010-02, BM-01-03 and BM-01-04.**

  Ver Anexo 5

- **Entidades israelíes interesadas en participar en la convocatoria 2021 del Clúster 3:**

Contact Name	Institute / company name		Email	Call Topic ID	Link to one-pager
Moshe Ziv	ATLAS -LTA Advance Technology	Company	info@atlas-lta.com	**Horizon-CL3-2021-BM-01-01 (coordinator)**	Atlas here
Ayelet Sapir	Bar Ilan University - smart cities center	Academia	Ayelet@pangeard.com ;eyal.yniv@gmail.com	**HORIZON-CL3-2021-DRS-01-02**	Smart cities here
Prof. Galit NAHARI	Bar Ilan University	Academia	galit.nahari@biu.ac.il	**HORIZON-CL3-2021-FCT-01-01**	Galit here
Ayelet Sapir	Bar Ilan University - smart cities center	Academia	Ayelet@pangeard.com ;eyal.yniv@gmail.com	**HORIZON-CL3-2021-FCT-01-03**	Smart cities here
Prof. Galit NAHARI	Bar Ilan University	Academia	galit.nahari@biu.ac.il	**HORIZON-CL3-2021-FCT-01-03**	Galit here
Ayelet Sapir	Bar Ilan University - smart cities center	Academia	Ayelet@pangeard.com ;eyal.yniv@gmail.com	**HORIZON-CL3-2021-FCT-01-04**	Smart cities here

Anat BEN-PORAT	Bar Ilan University	Academia	anat.ben-port@biu.ac.il	**HORIZON-CL3-2021-FCT-01-06**	Anat here
Prof. Galit NAHARI	Bar Ilan University	Academia	galit.nahari@biu.ac.il	**HORIZON-CL3-2021-FCT-01-06**	Galit here
Prof. Galit NAHARI	Bar Ilan University	Academia	galit.nahari@biu.ac.il	**HORIZON-CL3-2021-FCT-01-08**	Galit here
Prof. Galit NAHARI	Bar Ilan University	Academia	galit.nahari@biu.ac.il	**HORIZON-CL3-2021-FCT-01-09**	Galit here
Prof. Galit NAHARI	Bar Ilan University	Academia	galit.nahari@biu.ac.il	**HORIZON-CL3-2021-FCT-01-10**	Galit here
Prof. Galit NAHARI	Bar Ilan University	Academia	galit.nahari@biu.ac.il	**HORIZON-CL3-2021-FCT-01-12**	Galit here
Dr. Udi Ganani,	EIS council	Research	udi.ganani@eiscouncil.org	**HORIZON-CL3-2021-INFRA-01-01**	EIS here

- **El "Israel National Cyberdirectorate" está interesado en participar en los siguientes topics de la convocatoria 2021:**
  - Horizon-CL3 -2021 -BM-01-01: Enhanced security and management of borders, maritime environment, activities and transport by increased surveillance capability, including high altitude, long endurance aerial support
  - Horizon-CL3 -2021-CS-01-01: Dynamic business continuity and recovery methodologies cased on models and prediction for multi-level cyber security
  - Horizon-CL3-2021-CS-01-02: Improved security in open source and open specification hardware for connected devices
  - Horizon-CL3 -2021 -CS-01-03: AI for cybersecurity reinforcement

  Ver Anexo 6

- **Entidad británica interesada en participar en el topic siguiente: DS-01-04: Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data**

  Ver Anexo 7

- **Entidad británica interesada en participar en el topic siguiente: HORIZON-CL3-2021-BM-01-01: Enhanced security and management of borders,**

maritime environment, activities and transport, by increased surveillance capability, including high altitude, long endurance aerial support

Ver Anexo 8

Esperamos que esta información os resulte de interés.

Un cordial saludo,

Maite Boyero Egido

Representante y Punto de Contacto Nacional Clúster 3

Departamento de Retos Sociales. Dirección de Programas Europeos y Cooperación Territorial

Centro para el Desarrollo Tecnológico Industrial, E.P.E.

C/Cid, 4. 28001 Madrid

maite.boyero@cdti.es, +34 91 581 55 62

Manifestation of interest in Horizon Europe CL3/CL4

SKUDO (www.skudo.tech) is a young and vibrant start-up based in Tallinn/Estonia. We work with hardware-based encryption solutions for space and drone applications and we are now seeking for the right partners in Europe for applying to selected Horizon Europe (CL3 and CL4) funding projects. Our core expertise lies in the combination of FPGA technology with specific space protocol implementations (e.g. CCSDS) and security architectures, for embedded applications.

At SKUDO we foresee a world where all data communication (especially those in the critical infrastructures, space, drones and government applications) are protected, encrypted and safe. We also strongly believe that at least within Europe we must use European-made cyber security technologies and especially encryption/authentication.

We have developed our own FPGA chip (implementing an HSM). We designed and implemented all the functions within the chip entirely in Verilog without the need for any extra layers of software (firmware) nor using third party ready module cores. This allows SKUDO to be able to port our HSM modules to any FPGA from any manufacturer, thus allowing to implement it in any space grade FPGA chip. On the research side we are also looking into PQC (Post Quantum Cryptography) and Quantum resistant algorithms to be added to our FPGA solution.

It is our mission to design, develop, build and assemble all our solutions entirely in Europe to ensure the absolute safety of our products and reduce the risks of backdoors.

We have recently (July 2021) successfully completed our first ESA contract. Within that, we designed and developed two new Extended Procedures which modify the CCSDS SDLS TM/TC standard by adding asymmetric cryptography, digital certificates (X.509), mutual authentication, and a PKI. Everything is integrated in the same solution, relying on our HSM/FPGA chip for all the crypto primitives and demoed via a VHF (144.8 MHz) data packet modem link. With our new upcoming ESA contract (Q3-2021), we agreed to expand on the above and get space validation by using the orbiting OPS-SAT satellite providing end2end hardware encrypted data link to the ESOC.

As part of our IPR, we have various Verilog cores. Symmetric encryption: Camellia, Camellia-CBC, Camellia-CTR, AES-GCM (fast version up to 1.4 Gbps and compact version), AES-CBC, AES-CTR. Asymmetric: Elliptic Curve25519 (ECDH), Ed25519 (signature and verification). Hashing: Skein, SHA3-512 (Keccak) and SHA512. True Random Number Generator (TRNG): FIGARO. Other cores are on the making (e.g. PQC). All crypto functions are embedded and running in our custom FPGA chip (without OS, bare-metal) without the use of third-party libraries and brand independent.

We are looking forward to cooperate with other European companies, research centers or Universities with the aim to build a consortium and bid on those Horizon Europe projects.

Additional links:

Article on ZDnet: https://www.zdnet.com/article/from-encryption-to-iot-this-regions-startups-are-forging-new-frontiers-with-space-technology/

Kryptor PCB on CrowdSupply: www.skudo.tech/kryptor

BCCS
INNOVATE. DEVELOP. INTEGRATE

Contacts
Email: vytenis.kazanavicius@bccs.tech
Web: https://bccs.tech

BCCS Cluster

BCCS cluster is a collaboration of private and public organizations created to boost the development of innovative products and services. Our core expertise is in Blockchain, Cybersecurity, Software Development, Legal and Compliance areas. This is possible by combining the knowledge, experience, business relations of BCCS Cluster ecosystem. For Horizon Europe calls we can provide the following experience and expertise in:

Blockchain

BCCS can identify use cases suitable for blockchain application and implement them using cryptographic, blockchain and distributed ledger technologies. Capacity includes R&D&I, development of Smart Contracts, Blockchains and Applications.

Cybersecurity

BCCS can cover the development of cybersecurity solutions. Application and system security for software, hardware and IoT. Process and organizational measures: Processes Management, Application Security Management, Information Security (ISMS), Risk Management (ISRM).

Software Development

BCCS can provide development of web and mobile applications, custom software, AI, Machine Learning, Big Data, Enterprise Automatization solutions.

Legal and Compliance

BCCS experts would be able to provide consulting and legal assistance in project implementation, evaluation, legal aspects and revision of drafted project proposals and submission of applications. EU regulation of privacy and data protection with adoption of local rules and various agreements and rules according new GDPR requirements.

Scientific Research

BCCS can cover scientific research needs of these calls as we have one of the largest universities in Lithuania as our cluster member. Which have Horizon EU dedicated teams ready to participate for these calls and are experienced as partners and coordinators due to several years of experience with Horizon 2020. Research priorities include, but are not limited to:

- Blockchain Application
- A.I and Computational Linguistics
- Economics and Management
- Personality and Social Behavior
- Risk and Reliability Analysis Methods

Horizon Europe Topics of interest

Health

HORIZON-HLTH-2021-TOOL-06-03

Culture, creativity and inclusive society

HORIZON-CL2-2021-TRANSFORMATIONS-01-05

Climate, Energy and Mobility

HORIZON-CL5-2021-D3-01-01
HORIZON-CL5-2021-D3-02-07
HORIZON-CL5-2021-D3-02-11

Food, Bioeconomy, Natural Resources, Agriculture and Environment

HORIZON-CL6-2021-FARM2FORK-01-07

Civil Security for Society

HORIZON-CL3-2021-CS-01-01
HORIZON-CL3-2021-CS-01-02
HORIZON-CL3-2021-CS-01-03
HORIZON-CL3-2021-CS-01-04

Digital, Industry and Space

HORIZON-CL4-2021-HUMAN-01-01
HORIZON-CL4-2021-HUMAN-01-03
HORIZON-CL4-2021-HUMAN-01-04
HORIZON-CL4-2021-HUMAN-01-25
HORIZON-CL4-2021-DATA-01-05
HORIZON-EUSPA-2021-SPACE-02-52
HORIZON-CL4-2021-RESILIENCE-01-10
HORIZON-EUSPA-2021-SPACE-02-53
HORIZON-CL4-2021-TWIN-TRANSITION-01-08

Horizon Europe Work Programme

Countering Online Identity Theft

Introduction

Civil Security for Society is a European Commission-backed Work Programme designed to shape EU policies related to security (including cyber security) as well as disaster resilience.

We are a UK technology company about to launch a revolutionary new human authentication system (Shayype™) which will raise the bar over existing authentication technologies, by removing the 'stealable' elements (such as fixed login codes or personal information such as mobile numbers) which hackers have traditionally used to gain access.

A key part of this initiative is the Horizon Europe CL3 -2021 FCT-01-12 *Online identity theft is countered* project, which invites interested consortia to apply for up to €3m of funding for research and innovation (designed to create systems with a TRL of 5-6). Shayype Global Limited is interested in assisting such consortia with their work.

The aim of this project is to protect citizens in Europe from hacking, identity theft and other kinds of criminal activity online, and to create enhanced perception by citizens that Europe is an area of freedom, justice, and security.

The problem

Online crime has been allowed to flourish because it has been so easy for criminals to adopt false identities. (This problem is not unique to the online world – it also hampers law enforcement efforts in the physical world, when for instance a person stopped by an officer may create confusion by providing false details.)

However, criminals' ability to create 'deep-fakes' has made possible a raft of additional undesirable or illegal activities, including spreading misinformation about individuals or companies, implanting celebrities' faces into existing pornographic materials, or even creating 'personalised' child abuse material.

The solution

We believe the introduction of strong authentication for humans, as well as for machines and even objects (e.g. product packaging & validation) could be a game changer.

Shayype technology will strengthen any project designed to combat online crime by enabling honest citizens to

authenticate themselves quickly and easily and in so doing will block or 'weed out' criminals.

Unlike conventional authentication technology Shayype has no stealable element which hackers can capture and re-use. In addition, users can prove authentication or authorisation without giving away any personal details. These two attributes make our proposition unique.

We would be interested in working with existing authentication databases, including those operating in the fields of big data or financial services, as well as governmental and law-enforcement (e.g., the U.K.'s PNC [Police National Computer]).

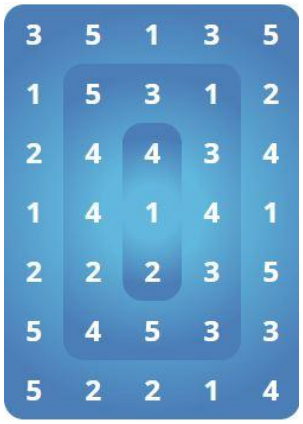
Users could set up authentication accounts which they could use whenever they are required to strongly prove their identities. Such an alliance with existing databases would enable citizens to go about their daily lives, secure in the knowledge that they will be able to prove who they are (or that they have authorisation to perform an action) in a way which cannot be used against them (thieves cannot capture, replicate, or reverse engineer users' Shayype 'secrets').

For example, teaming Shayype with one or more 'know your customer' (KYC) databases, could reduce activities such as online grooming. A teenager could for instance be reassured that he/she is talking to someone of the same age (and not a much older person). Such a system would allow users to control which 'attributes' they want to be revealed (e.g., age, nationality etc) without having to give out 'personal' details like names etc.

What is Shayype?

Shayype is a unique and much-needed new (patent protected) technology designed to allow users to authenticate themselves (or prove their authorisation) via one-time passcodes (OTPs) received without the need for additional hardware.

OTPs in authentication are not new – but with Shayype these can for the first time be delivered more securely and conveniently via the screens of whatever devices are in use. In other words, Shayype can replace all fixed codes (passwords, PINs etc.) as well as 2/mfa systems.

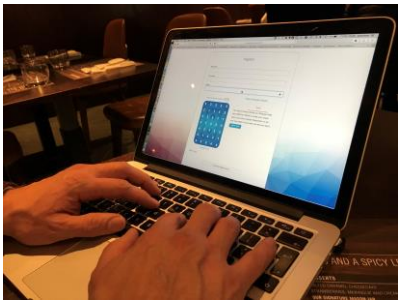


Users simply extract random sets of digits from a randomly numbered on-screen grid to create new OTPs on the fly. All the user requires is a pre-set pattern or shape which tells them which numbers to read off.

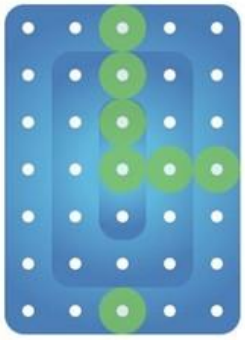
Because each digit is repeated several times on the grid, it's extremely difficult for an attacker to reverse engineer the user's secret (the pattern). We have also added in a number of other systems which make it near impossible to

discern user's patterns using methods such as screen-capture, shoulder-surfing etc.

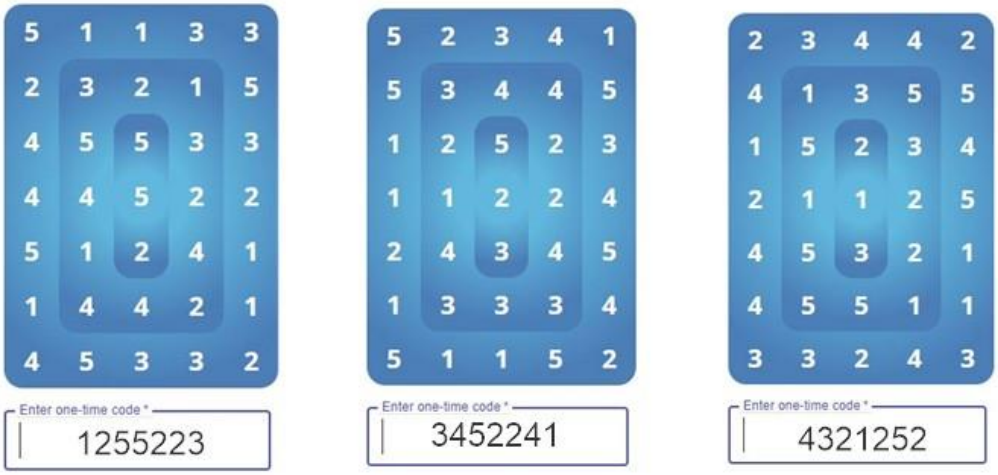
Shayype is powered by an extremely secure backend which we believe is practically unhackable (it uses 'secret sharing' to split up crucial information into sections – only part of which needs to be used to authenticate the user). In other words a hacker, even if he/she managed to break into the database, would not find enough information to reproduce the user's pattern.



Shayype is available in prototype form fronting (via our own API) IBM/RedHat's powerful and adaptable Keycloak IAM (identity and access management) system. (We have used Keycloak as a starting point, but others such as ForgeRock, OKTA, One-Login etc may be used in future with tailored versions of our API.)



Simple on-screen pattern or shape indicates numbers to read off, giving different one-time pass-code (OTP) every time without a device.



Shayype's main attributes are: -

- No stealable elements which can help hackers to break in
- Users can authenticate or prove their authorisation without giving any details.

Note: While we feel Shayype could help with consortia hoping to apply for funding under the Horizon Europe CL3 -2021 FCT-01-12 *Online identity theft is countered* call, we would be interested in working with projects aimed at addressing other 2021-22 projects.

Shayype Global Limited T +44 (0)843 320 9869 F +44 (0)843 320 5347 E info@shayype.com W www.shayype.com Registered Office 1 Ramsay Court, Kingfisher Way, Hinchingbrooke Business Park, Huntingdon, Cambs PE29 6FY, UK. Company Registration Number 8624252. Registered in England and Wales

Anexo 4

Large Scale Evacuation & Community Resilience

Fire Safety Engineering Group (FSEG)

University of Greenwich (UOG)

Seeking to join a consortium in the following Horizon Europe Civil Security for Society calls

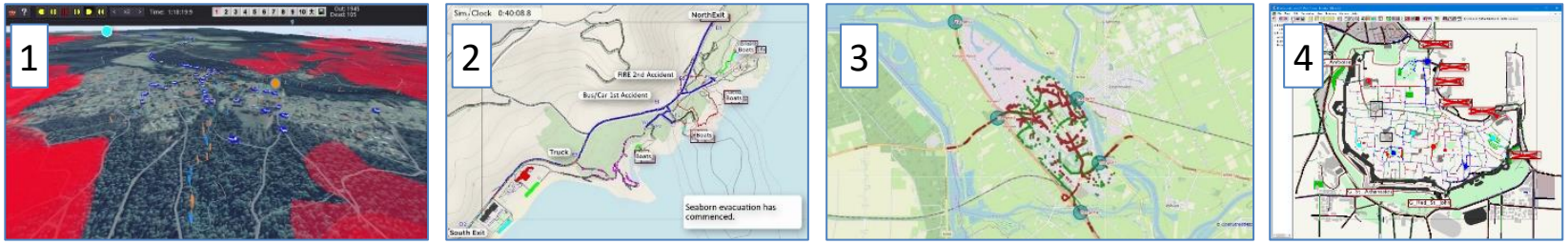
- **HORIZON-CL3-2021-DRS-01-01**:
  Improved understanding of risk exposure and its public awareness in areas exposed to multi-hazards
- **HORIZON-CL3-2021-DRS-01-02**:
  Integrated Disaster Risk Reduction for extreme climate events: from early warning systems to long term adaptation and resilience building
- **HORIZON-CL3-2021-DRS-01-03**
  Enhanced assessment of disaster risks, adaptive capabilities and scenario building based on available historical data and projections

Our expertise

FSEG expertise and specialisation is in research and software development for **fire/hazards** and **evacuation** modelling, **human behaviour**, large-scale evacuation dynamics, developing **operational tools** solving practical, safety and security problems for over 25 years including over **15 successful EU projects** since Framework 4.

FSEG provides the large-scale **urbanEXODUS** evacuation framework to support crisis managers (a) during **preparedness**, aiding in the formulation of engineering-based plans, (b) during **response**, allowing for **informed decisions** to be made and **resource management** and, (c) for developing **educational programs** for **improving community resilience** during disasters. The proposed **TRL is 7.**

FSEG has a **successful track record** in undertaking **large-scale trials** to collect **human-factors** using a variety of methods that include interviews, surveys, designing/monitoring/recording of trials, data extraction and analysis to better understand human behaviour (e.g., Framework 7 EU project SAFEGUARD with over 5000 participants, interviewing WTC survivors).



Large-scale evacuations due to wildfire (1 and 2), flood waters (3), and tsunami (4)

Co-funded by the Horizon 2020 Framework Programme of the European Union

Topics of interest

HORIZON-CL3-2021-DRS-01-01: Improved understanding of risk exposure and its public awareness in areas exposed to multi-hazards
HORIZON-CL3-2021-DRS-01-02: Integrated Disaster Risk Reduction for extreme climate events: from early warning systems to long term adaptation and resilience building
HORIZON-CL3-2021-DRS-01-03: Enhanced assessment of disaster risks, adaptive capabilities and scenario building based on available historical data and projections

Keywords: agent-based models | multi-modal evacuation modelling | human behaviour | community resilience | disaster planning mitigation and response | training | trial protocols

Relevant and direct previous experience:

- H2020 IN-PREP (https://cordis.europa.eu/project/id/740627)
- H2020 GEO-SAFE (https://cordis.europa.eu/project/id/691161)
- Framework 7 IDIRA (https://cordis.europa.eu/project/id/261726)

Co-funded by the Horizon 2020 Framework Programme of the European Union

Contact us!

Lazaros Filippidis

L.Filippidis@gre.ac.uk

Fire Safety Engineering Group

University of Greenwich

UK based academic institution

Co-funded by the Horizon 2020 Framework Programme of the European Union

Anexo 5

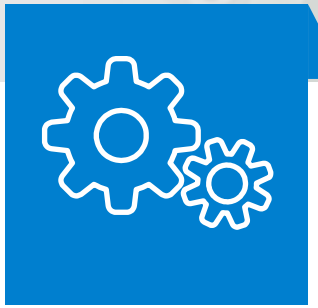
SysElek

Syselek is looking to join consortia on Horizon Europe Civil Security for Society – Destination 2 Border Management

- **HORIZON-CL3-2021-BM-01-02**: Increased safety, security, performance of the European Border and Coast Guard and of European customs authorities
- **HORIZON-CL3-2021-BM-01-03**: Improved border checks for travel facilitation across external borders and improved experiences for both passengers and border authorities' staff
- **HORIZON-CL3-2021-BM-01-04**: Advanced detection of threats and illicit goods in postal and express courier flows

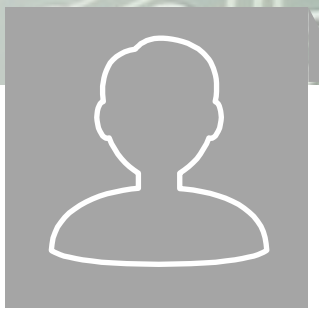
WE HELP PEOPLE

AUTOMATE AND OPTIMISE...



WHAT WE DO

- We develop technologies and tools for high integrity, automated systems



WHO WE ARE

- SME (10 people) with 100+ years experience in research and engineering

HIGH CALIBRE

- We collaborate closely with leading research institutions to develop new technology IP

PRESENCE

- We are located in Warwick, UK, with an international outreach www.syselek.com

Collaboration

SysElek

- We are passionate about international collaboration
- Prior EU-funded R&D contributions:
  - Improved safety of highly automated systems with data analytics and complex system engineering, along with security assessments
  - Reduced environmental impact of transport with secure embedded systems design and connected analytics for vehicles

- We work with many UK agencies and universities

UK governmental departments	UK universities

Department for Transport

HM Revenue & Customs

Border Force

THE UNIVERSITY of EDINBURGH

Imperial College London

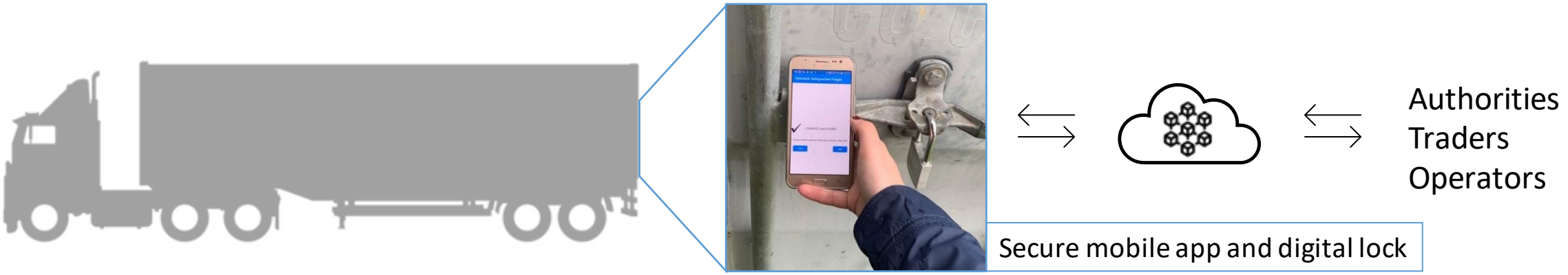
UNIVERSITY OF LINCOLN

Loughborough University

WARWICK
THE UNIVERSITY OF WARWICK

UWE Bristol | University of the West of England

Secure Border-Ready Freight



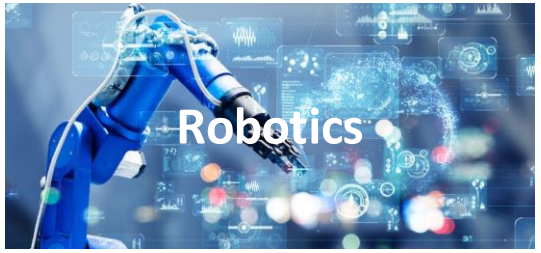
- Secure border-ready freight tracks, controls and secures freight across external borders and customs territories.

- Better situational awareness supporting decision-making systems and communication.
- Transferrable and adaptable technologies to further passenger and goods applications.

Specialist areas

SysElek

Areas	Specialisms



- Our specialist areas and key expertise offers specific support to:
  - Better situational awareness supporting decision-making systems of European border, maritime and customs authorities, with technological security and safety solutions, advanced communication systems, advanced human interface devices and sensors. (01-02)
  - Improved border checks and experiences for both passengers and border authorities' staff while maintaining security and reliability, passengers/vehicles/luggage identification, document/information checks (e.g. customs declarations), portable integrated systems with secure and reliable backend services providing immediate info to field officers. (01-03)
  - Advanced detection of threats and illicit goods in postal and express courier flows crossing external borders and internal shipping, with improved quality/availability/integration/interpretability of data. (01-04)

Contacts

Dr. Bo Gao, Engineering Director

Dr. Bo Gao is a Chartered Engineer and a Fellow of IMechE. He has over 20 years of industry experience in both product development and advanced research. His main areas of interest include software, control, complex systems and automation. Dr. Gao has held various engineering leadership roles. He received his PhD degree in Mechanical Engineering from the University of Bath, sponsored by Jaguar Land Rover. Dr. Gao has co-authored more than 40 patents and refereed technical publications.

bo.gao@syselek.com

Dr. Alan Walker, Business Director

Dr. Alan Walker has 20 years' experience in complex electronics systems engineering, including many years' experience in public funded collaborative research and development at both UK national and European level, with developing new products at Tier 1 supplier and technology consultancy levels. He received his PhD degree from Imperial College London, and MBA from London Business School. Dr. Walker is a Fellow of the IET and has co-authored more than 20 patents and refereed technical publications.

alan.walker@syselek.com

Israel National Cyber Directorate
Consortium Participation Cluster 3- "Civil Security for Society"

The Israel National Cyber Directorate (INCD) is a **government agency** tasked with the protection of the Israeli civilian cyberspace and the building of Israel's long-term capacities to deal with cyber threats. The Economy and Growth Center within the INCD's Strategy Division is looking to participate in the R&D&I Consortium under the Horizon Europe Cluster 3 "Civil Security for Society" calls.

The Economy and Growth Center works to establish and reinforce the cyber science-and-technology base by developing high-quality human capital, support advanced academic research, engage in deep technological R&D, and international collaborations.

The INCD wishes to join as partners to project proposals, to the following call topics:

2021:

- **Horizon-CL3-2021-BM-01-01**: Enhanced security and management of borders, maritime environment, activities and transport by increased surveillance capability, including high altitude, long endurance aerial support
- **Horizon-CL3-2021-CS-01-01**: Dynamic business continuity and recovery methodologies cased on models and prediction for multi-level cyber security
- **Horizon-CL3-2021-CS-01-02**: Improved security in open source and open specification hardware for connected devices
- **Horizon-CL3-2021-CS-01-03**: AI for cybersecurity reinforcement

2022:

- **Horizon-CL3-2022-CS-01-01**: Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures
- **Horizon-CL3-2022-CS-01-02:** Trustworthy methodologies, tools and data security "by design" for dynamic testing of potentially vulnerable, insecure hardware and software components

Capacities & Skills:

The INCD may contribute to such consortiums with the following long gained professional skills and capacities:

1. Design Partner Contribution to the development processes and technical requirements.
2. Collaboration and data sharing between different security actors.
3. Testing and validation of daily tasks, tools and methods from end use perspective
4. Technological, policy, operational, regulatory, ethical and legal consulting from the national government perspective
5. Providing appropriate data sets and feeding different information structures.
6. Assisting user training actions and evaluation activities, including **simulation facilities**.
7. Develop knowledge in novel cybersecurity fields

PoC: **Ms. Yaara Sabzerou**, Head of Cyber Industry, Economy and Growth Center, Israel National Cyber Directorate, yaaras@cyber.gov.il

Anexo 7

mydex

A personal data platform and utility that delivers social value

alex@mydex.org

Mydex is a social enterprise with a mission

Our mission is to help every individual in the world to realise the value of their own data in their lives.

We want to enable individuals to collect, store, handle, share and use their data to make their lives better.

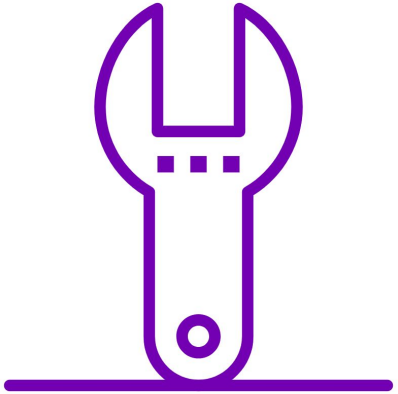
mydex

What Mydex does

Mydex provides individuals with safe, secure personal data stores that enable them to build up banks of data about themselves independently of the organisations they deal with.

Mydex enables individuals to safely share chosen portions of this data with bona fide service providers under their control.

Mydex empowers individuals with their data, helping them realise its value for themselves. Its services are GDPR compliant by default.



Mydex empowers citizens in many ways

Build up a **portfolio** of verified shareable information about themselves	Safely and easily **connect** with service providers, avoiding both sign-in hassles and privacy/data leakage	Upload, collect, receive and store data (including secure **digital tokens** of 'verified attributes)	Use these verified attributes to **prove their identity** when doing anything online
Gain **insights** on behaviour from this data	**Share** their own data under their own control	Manage **consent** with third parties	Maximise the **benefits** they get from their data

Mydex CIC is designed to be trustworthy

As a **Community Interest Company** Mydex is a mission and legally asset-locked social enterprise.

- Its assets cannot be sold to another party, unless that party has the same, legal mission (to empower individuals with their own data)
- 65% of any profits made must be reinvested in pursuit of its mission

Mydex is built to last, not for an exit (IPO or trade sale)

Mydex is designed for security and privacy

Data held in Mydex personal data stores is encrypted in motion and at rest. The Mydex platform is **independently certified for data security** under ISO 27001.

Each personal data store is **individually encrypted**, with each individual holding their own encryption key: data held by Mydex is dispersed and does not act as a honeypot for hackers.

Mydex works on a **zero knowledge** basis. It cannot see data held in individuals' personal data stores.

Use-cases of the Mydex platform

mydex

Social Impact Categories

Employment Training & Education | Housing & Local Facilities | Income & Financial Inclusion | Mental Health and Well-being | Physical Health | Arts, Heritage, Sport & Faith | Family, Friends & Relationships | Citizenship Community | Conservation of the Natural Environment

Mydex: A data utility for social value

Personal Digital ID

- Enables individuals to build up a battery of secure digital tokens verifying different aspects of their lives
- Provides benefits of social sign-in but without data leakage

Personal Data Services

- Enables individuals to collect, receive and share data
- Storage of Verified and self asserted attributes
- Organisation of data across all aspects of life
- Analysis of rich and broad data sets

Data Sharing and Exchange

- Data sharing agreement protects individuals' privacy
- Secure Data Exchange
- Consent receipts ensure all data sharing is permissioned
- Authorisation Management

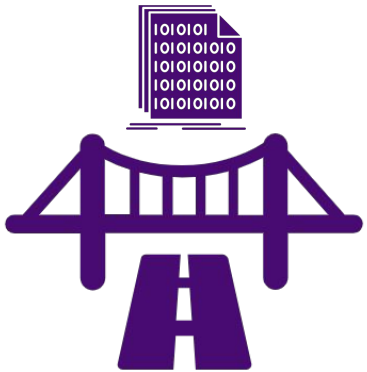
Provides individuals with **end-to-end encrypted personal data stores** that only they can access, where the data remains under their control and which enables **seamless permissioned data sharing** with organisations.

Mydex's infrastructure is neutral and enabling

Mydex's business model is designed so that it has **no financial incentive to seek control** of individuals' data. Organisations pay Mydex a connection fee to enable data sharing relationships with individuals.

Mydex acts as a **neutral infrastructure layer** for safe data sharing. It does not favour any organisations participating in its data sharing network.

As a new layer of connecting infrastructure, Mydex CIC does not require organisations to radically change their systems in order to participate.

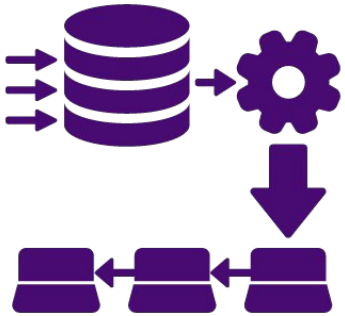


Mydex infrastructure is live and operational

Mydex CIC was 14 years old in March 2021.

Its platform is live, working and operational and listed on the UK Government's G-Cloud platform for the procurement of public services.

It is working on multiple projects to better manage chronic health conditions, access debt advice, improve independent assisted living, assure identities, involve citizens in designing service and to improve access to the value of public services.



Mydex helps service providers in many ways

Access and use verified information they can trust **cheaper and quicker**	**Reduce risks** relating to data security and GDPR compliance	Build **trust** with customers and users	**Assure identities** of users at lower costs
Enrich **insights** on customers and users via improved data sharing	**Streamline** data-driven decisions and **speed up** service delivery	Manage **consent** processes more efficiently and to deliver better user experience	**Reduce costs** of data management processes and regulatory compliance

Examples of Mydex projects

Mydex CIC is working on the front line of social impact

Supporting neighbourhoods for independent living

Mydex is working in a three-year £ 12.5 million project led by Blackwood housing funded by UK Government to design age-friendly homes and communities where the elderly can sustain physical activity, manage common complaints relating to ageing and be nourished by supportive social connections.

All these activities and related services require the sharing of personal data. All such data will flow through the individual's personal data store provided by Mydex, making it easier for individuals to access services, cheaper for service providers to provide them, while creating rich new person-centric data assets to aid further insights into healthy ageing.

Macmillan My Data Store

Working with Macmillan Cancer Support in Glasgow and West Dunbartonshire, Mydex CIC is developing the data sharing infrastructure that enables all the many different parties (organisations, friends and family, carers) assisting cancer patients through their cancer journeys to share the data they need, via the individual's personal data store.

This helps ensure that available services are as integrated and 'joined up' as possible and minimises the friction, stress and the duplication of effort that patients currently incur when services are not 'joined up'.

Inclued citizen engagement platform

Working with Glasgow City Council, Mydex CIC has developed a new citizen engagement platform *'Inclued'* that helps the Council deliver personalised notifications and service offers via an easy-to-use web-based app. The platform is designed to work for any city/town/village/community.

Because the data used for, and generated by, every interaction is automatically stored in the individual's Personal Data Store, it is always available for reuse. Service providers can constantly refine their insights and improve the targeting of their messages while citizens experience increasing convenience.

Streamlining and improving debt advice

Working with Advice Direct Scotland, Mydex CIC is developing mechanisms by which individuals can collect and aggregate facts from multiple different service providers to create a single, rounded, comprehensive view of their financial situation. Debt advisors can access this data, with the individual's permission, in order to provide advice. Individuals can then re-use this data when acting on this advice e.g. when applying for consolidated loans.

This approach significantly reduces the cost and hassle of accessing the data needed to make debt advice (and acting on this advice) better, cheaper *and* easier.

Reimagining health and social care

Mydex CIC is working with the Digital Health and Care Institute in a multi-year collaboration to improve the delivery of health and social care services in Scotland. Its citizen centred approach is based on an untethered personal health record (e.g. a personal data store) to drive apps and services that provide real time support and guidance for citizens, creating a sense of coherence and easier access to the support they need.

One aspect of this work is enabling citizens to hold Covid vaccination and test certificates (examples of ‘Verified Attributes’) in their personal data stores and to present these certificates to other parties as and when needed.

Involving citizens in designing their services

Working with the Office of the Chief Designer and the Connecting Scotland programme Mydex CIC is building a Digital Public Design Service - an adaptable, easy-to-use platform for citizens to co-design services with service designers and service providers.

The main purpose of the platform is to improve citizens' experiences of accessing and using public services, but it also helps citizens learn from one another in the process.

Scottish Attribute Provider Service

Working with Scottish Government Mydex CIC has built and tested systems for the safe, efficient sharing of verified attributes to improve public service provision and enable citizens to access and use services easier and quicker.

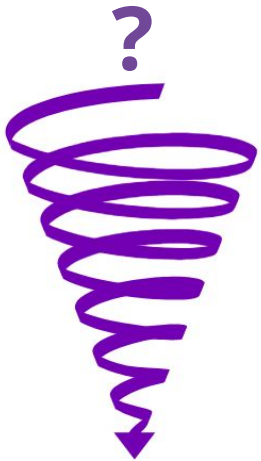
Mydex CIC also developed a practical implementation and roll-out strategy in its Smart Entitlements strategy report.

These recommendations have been largely accepted by Scottish Government and embedded into a procurement that is currently under way.

What's next? Tackling poverty

In today's digital society, data exclusion has become a major driver of social exclusion. Even though they can least afford it, it is the poor who have to invest the most effort, money and time handling data: filling out application forms, provide information to different people time and time again, proving identity, status or entitlement when they are vulnerable or distressed.

By helping individuals store and share their data, Mydex wants to promote people's access to available services and provide them with a tool kit for the future - while also helping service providers improve the efficiency and quality of their services.



Mydex is enabling systemic change

Achieving our mission

Mydex aims to achieve its mission (of empowering every individual with their own data) via new enabling infrastructure which provides every individual with their own safe, secure, privacy-protecting personal data store.

This new infrastructure delivers both short and long term benefits, unleashing changes in how the system itself works.

What Mydex enables vs the status quo - 1

What Mydex personal data stores enable	The organisation-centric status quo
Individuals can accumulate their own data in their own personal data store independently of their relationship with any specific service provider.	Individuals' data is dispersed across many separate data organisational data silos. Individuals cannot accumulate their own data under their own control.
Individuals can build a single data view of their lives.	A single view can never be obtained without major invasions of privacy.
Individuals can bring this rich data to their dealings with service providers.	Each service provider starts from scratch, collecting or creating its own data each time it starts dealing with a new individual.
'Make once use many times' data enables both individuals and service providers to cut friction, effort, risk and cost.	'Make afresh every time' creates built-in duplication of cost and effort for both individuals and service providers

What Mydex enables vs the status quo - 2

What Mydex personal data stores enable	The organisation-centric status quo
Data sharing is made safe, simple and often automatic.	Data sharing is legally and technically difficult if not impossible.
Data can be used by many users for many different uses thereby unleashing its full personal, social and economic potential.	Data uses are restricted to the purposes of the organisations collecting the data.
Individuals enabled to use their own data to make better decisions and manage their lives better. This drives innovation.	Only organisations can use data to make better decisions and improve their operations. This stifles innovation.
System is designed to protect Individuals' privacy and data, leading to enhanced trust.	Organisations are incentivised to conduct data landgrabs thereby undermining trust.

alex@mydex.org

Anexo 8

True aerial autonomy for any aircraft and any flight

FLAREBRIGHT

Cluster 3 Partner or Collaborator

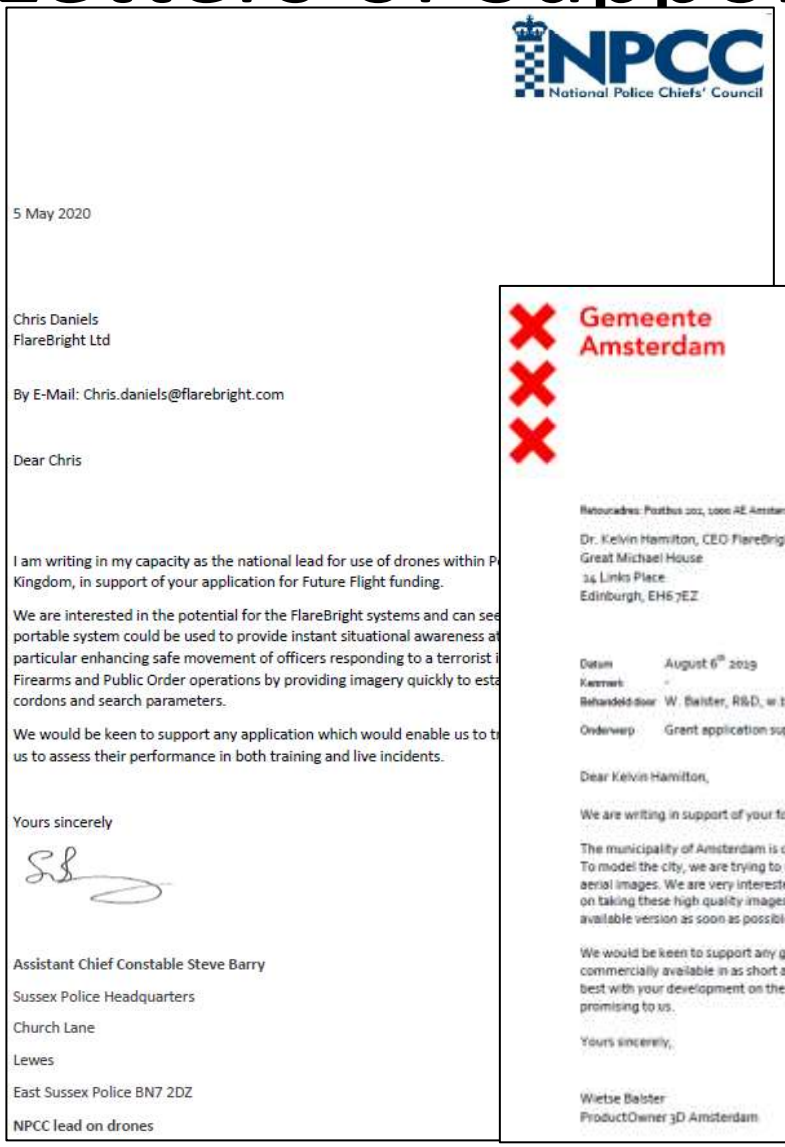
Flare Bright are leaders in autonomous drone solutions for the security sector and believe we are key partners in a number of Cluster 3 challenges, notably:

> ***HORIZON-CL3-2021-BM-01-01: Enhanced security and management of borders, maritime environment, activities and transport, by increased surveillance capability, including high altitude, long endurance aerial support***

Flare Bright is actively seeking European partners for a consortium, who have complementary innovation skills in border security and maritime patrol, or can enhance our drone's sensing or image output with analysis.

We have received Letters of Support from the Head of Drones of the UK's National Police Chief Council and the Head of Innovation at the UK Govt's Maritime and Coastguard Agency.

Letters of Support



NPCC
National Police Chiefs' Council

5 May 2020

Chris Daniels
FlareBright Ltd

By E-Mail: Chris.daniels@flarebright.com

Dear Chris

I am writing in my capacity as the national lead for use of drones within P
Kingdom, in support of your application for Future Flight funding.

We are interested in the potential for the FlareBright systems and can see
portable system could be used to provide instant situational awareness at
particular enhancing safe movement of officers responding to a terrorist i
Firearms and Public Order operations by providing imagery quickly to esta
cordons and search parameters.

We would be keen to support any application which would enable us to t
us to assess their performance in both training and live incidents.

Yours sincerely

Assistant Chief Constable Steve Barry

Sussex Police Headquarters

Church Lane

Lewes

East Sussex Police BN7 2DZ

NPCC lead on drones

Gemeente Amsterdam

Bezoekadres
Stadhuis, Amstel 1
1011 PN Amsterdam

Postbus 202
1000 AE Amsterdam
Telefoon 14020
www.amsterdam.nl

Retouradres: Postbus 202, 1000 AE Amsterdam

Dr. Kelvin Hamilton, CEO FlareBright Ltd.
Great Michael House
14 Links Place
Edinburgh, EH6 7EZ

Datum August 6th 2019
Kenmerk -
Behandeld door W. Balster, R&D, w.balster@amsterdam.nl
Onderwerp Grant application support

Dear Kelvin Hamilton,

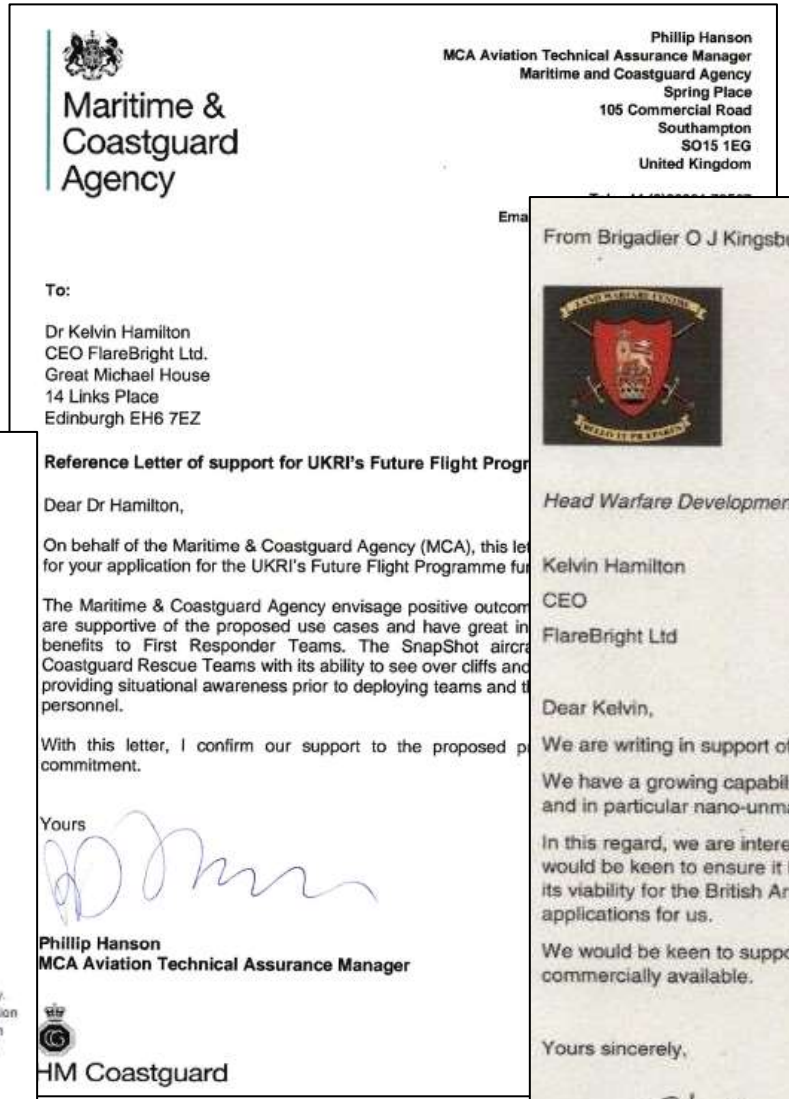
We are writing in support of your forthcoming grant application.

The municipality of Amsterdam is currently working on a Digital Twin, a digital model of the city. To model the city, we are trying to use photogrammetry techniques which requires high resolution aerial images. We are very interested to see the possibilities of the FlareBright SnapShot system on taking these high quality images. Therefore, we would like to be able to trial a commercially available version as soon as possible.

We would be keen to support any grant application that enables this technology to become commercially available in as short a period as possible. Furthermore, we would wish you all the best with your development on the FlareBright SnapShot system which so far look really promising to us.

Yours sincerely,

Wietse Balster
ProductOwner 3D Amsterdam



Maritime & Coastguard Agency

Phillip Hanson
MCA Aviation Technical Assurance Manager
Maritime and Coastguard Agency
Spring Place
105 Commercial Road
Southampton
SO15 1EG
United Kingdom

To:

Dr Kelvin Hamilton
CEO FlareBright Ltd.
Great Michael House
14 Links Place
Edinburgh EH6 7EZ

Reference Letter of support for UKRI's Future Flight Progr

Dear Dr Hamilton,

On behalf of the Maritime & Coastguard Agency (MCA), this le
for your application for the UKRI's Future Flight Programme fu

The Maritime & Coastguard Agency envisage positive outcom
are supportive of the proposed use cases and have great in
benefits to First Responder Teams. The SnapShot aircra
Coastguard Rescue Teams with its ability to see over cliffs and
providing situational awareness prior to deploying teams and t
personnel.

With this letter, I confirm our support to the proposed p
commitment.

Yours

Phillip Hanson
MCA Aviation Technical Assurance Manager

HM Coastguard

From Brigadier O J Kingsbury OBE

Headquarters Land Warfare Centre
Waterloo Lines
Warminster
Wiltshire BA12 0DJ

Telephone: 01985 22 2537
Military: 94381 2537
Fax: 01985 210204
MODnet: Kingsbury, Oliver Brig (LWC-WARDEV-H
Email: Oliver.Kingsbury247@mod.gov.uk

Head Warfare Development

15th October 2019

Kelvin Hamilton
CEO
FlareBright Ltd

Dear Kelvin,

We are writing in support of your forthcoming grant application.

We have a growing capability need and a keen interest in unmanned systems for ISTAR, and in particular nano-unmanned systems with ideally low to zero emissions.

In this regard, we are interested in the potential of the FlareBright SnapShot system and would be keen to ensure it has support for its development so we could trial it to ascertain its viability for the British Army. We think it could potentially have a wide range of applications for us.

We would be keen to support any grant application that enables this technology to become commercially available.

Yours sincerely,

Innovative Aerial Autonomy experts

Flare Bright are specialists in autonomous nanodrones, which can capture aerial imagery or sense gases and particles. We use machine learning digital twin to tune all aspects of our flight control and development which saves huge amounts of time and cost.

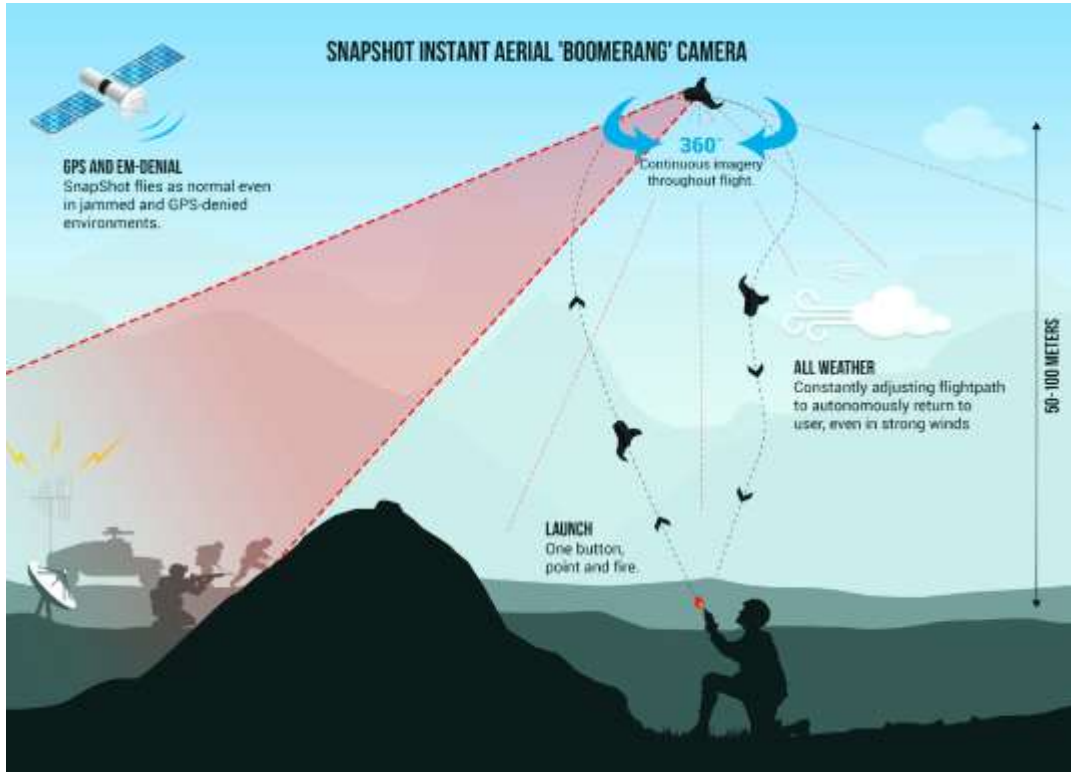
Flare Bright has miniaturised autonomy in drones. Using inertial navigation, this has resulted in creating a nanodrone that can fly without any need for GPS, remote control or visual cues. It is currently used to fly up to 100m and return directly to the user filming as it flies.

Working inertial navigation systems are large and weigh many kilograms, we have created one without significant navigation drift that weighs around 20 grams in a drone that is just 85 grams. This miniaturisation puts military jet level navigation in the hands of any drone user and will have a significant impact on drone safety in the future.

We are a 14 person SME, with a mix of high quality software engineers, aerodynamicists and mechanical and electrical engineers.

We have developed the simplest method of obtaining aerial imagery, that works in GPS-denied, jammed and spoofed environments, as well as strong winds and other challenging weather. Our solution is a lightweight (<100gm) but robust autonomous drone, that requires no training (it works off a single press of a button) and can be easily adapted to launch automatically based on a ground sensor or any other signal thus giving immediate situational awareness instantaneously for any border or maritime scenario.

By the time of the competition, we will have nearly completed a funded project to develop (to TRL 6) a powered aircraft giving longer, precision endurance autonomously.



Grant-funding expertise and collaborations

Currently delivering 2 UKRI Future Flight grant-funded programmes:

- Safezone, where we are equal partners in a £500k project with another SME: https://zenotech.com/winning-partnership-to-improve-urban-drone-safety-in-a-world-first-project/

- SATE, a £3.7m project where we are part of a 12-organisation consortium: https://www.hial.co.uk/news/article/11/hial-leads-37-million-sustainable-aviation-project-at-kirkwall-airport

Flare Bright completed a UK MOD Defence and Security Accelerator grant (which was written up by the UK Govt as a Case Study): https://www.gov.uk/government/case-studies/autonomous-nanodrone-captures-aerial-intelligence-in-a-snap

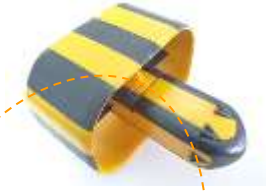
Commenced a follow-up £425k DASA grant on 1 June

We have an extensive network across the aerospace, defence and security sectors in the UK and elsewhere (notably have been selected to participate in the US Army's Expeditionary Warrior Experiment), and were part of the British Army's Warfare Experiment 2020.

We have been shortlisted / won a number of Awards: CogX Best Innovation in Autonomous Vehicles; LA New Mobility Challenge; ADS Security Innovation Award; and Octopus Investments Entrepreneur Award.

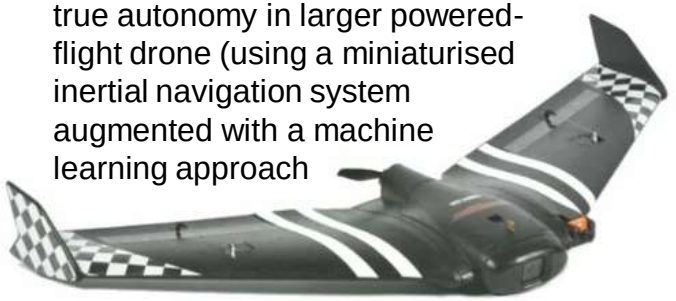
Flare Bright projects currently (completion mid-2022)

- Autonomous image-capture 85 gram nanodrone (Snapshot through DASA contract) up to 100m
- Autonomous wind measurement nanodrone (Safezone Future Flight grant) up to 100m



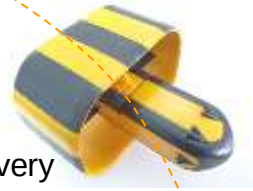
Digital Twin teaming (as a projectile) through MOD contract

DASA contract for embedding true autonomy in larger powered-flight drone (using a miniaturised inertial navigation system augmented with a machine learning approach



Ground to Air missions

Air-launched effects



Precision aerial nanodrone delivery (SATE Future Flight project)

Experienced tech-entrepreneur team

Dr. Kelvin Hamilton CEO & Co-Founder
PhD in Autonomous Systems. Co-founded autonomous systems company SeeByte with successful exit in 2014. Granted several patents, 33 years experience in autonomous systems.

Dr. Conrad Rider CTO & Co-Founder
PhD in Artificial Intelligence. Autonomy and simulation expert. Founded software company StarSoftQA in 2015. 10 years scale-up experience.

Chris Daniels, CCO
Commercialised several high-profile aerospace start-ups. Created and grew the Airlander brand at Hybrid Air Vehicles and raised £20m in funding (including 2 high-profile Crowdcube campaigns of £2m each). £100m of value created from scratch at Lloyds Bank running its London 2012 Olympic sponsorship. Former Investment Banker & British Army Officer.

Carl Sequiera, Head of Engineering
Carl was a Research Associate at the Whittle Lab, having completed his PhD on the ‘Hydrodynamics of Tidal Stream Turbines’. Prior to his PhD, he was an undergraduate of the Cambridge University Engineering Department, where he specialised in Aerospace and Aerothermal Engineering. He has worked on a range of aerospace related subjects in the past with Rolls-Royce in Derby-UK, ONERA in Meudon-France and the VKI in Rhode.St.Genese-Belgium.

Contact Details

We have the capability to be either a Coordinator or a Partner

Chris Daniels, Chief Commercial Officer

Chris.Daniels@flarebright.com

+447517940575

https://www.linkedin.com/in/chrisjwdaniels/

Chris Daniels has been commercialising aerospace start-ups for a decade and has extensive experience in bidding and managing grant-funded programmes, including a €2.5m Horizon 2020 project and a £2m Regional Growth Fund grant. He chairs the ADS Group's (the UK's main aerospace, defence and security trade body) Security Export Focus Group and is on the Management Team of the Drone Platform and Counter-drone group; and is also a member of the UKRI EPSRC's Mathematical Sciences Strategic Advisory Team.

Chris worked in Investment Banking and was a British Army Officer. He has a maths degree from Oxford University and an MBA from IESE Business School in Barcelona. His lifelong interest in aerospace started after gaining a Private Pilot's Licence aged 17 through a Royal Air Force Flying Scholarship.

FLAREBRIGHT

June 2021

www.flarebright.com