Oka-Bi

Horizon 2020 Summary Proposal

Intelligent Security & Privacy Management (SU-DS02-2020)

Project SUISEKI (pronounce: “Sui-seki”)

Introduction

This document is to summarise a proposal for the development of the “SUISEKI” (“**S**mart **U**nified **I**nformation **S**ecurity with **E**ncoded, **K**ey abstracted **I**ntelligent automation”) enterprise data security and analytics platform.

Summary

The proposal is to design and develop an enterprise robotic data security platform framework incorporating “beyond state of the art” modern security tools and architectures. This is to facilitate the robust management of personal data and systems, which are exposed to risk of GDPR censure as a result of the emergence of Artificial Intelligence, Big Data and IoT technologies.

The platform integrates proactive and reactive technologies including a robotic cloud data analytics platform, that will enable subscriber customers to fast track the construction of a federated and/or centralised databases and data platforms. The platform will be constructed by intelligent bots. These bots will, during the build process, proactively secure corporate data assets which are subject to the provisions of the EU General Data Protection Regulation (GDPR), as well as automatically building data ingestion pipelines, master data management software and analytic models. The platform will monitor real time user access via audit trails.

GDPR specific features will be integrated into the platform to centrally manage the core GDPR tenets, such as “Right to Erasure” and “Right to Restriction of Processing”. To promote the sharing of encrypted data the platform will utilise blockchain and other advanced cryptographic technologies to protect data. As well as being proactive, the platform will have the ability to respond to logging data in order to identify and manage unusual or fraudulent access patterns in a customer network. The aim of this proposal is to enable organisations to quickly align their data to the tenets of the GDPR, and to enable business analytics to happen in a trusted, robust, scalable and ethical data platform, whilst employing a range of proactive and reactive mechanisms to safeguard data and in conjunction with the best practises of the “Privacy by Design” principle of the GDPR.

Consortium Partner Requirements

Types of Partner

- Innovative SME or Large enterprises, pushing boundaries of innovation in areas of data security, analytics, intelligent automation, machine learning, blockchain and penetration testing.
- Research/Public Organisations who are looking to become a testing partner in a consortium.
- Biotech firms who can provide specific medical domain expertise that the proposal technology can be aligned to (eg. Treatment of cancer, auto immune diseases, Covid-19 etc).
- Companies or Institutions who have experience of Smart City type projects.

Types of Expertise

- IoT as an enabling cloud technology for smart city projects.
- Blockchain related systems.
- AI and machine learning (at scale, in cloud platforms like Microsoft Azure).
- Penetration testing software and consultancy.
- Business analytics.
- Data Security / GDPR / Data Governance.