guardtime ®

INTEGRITY AND PROVENANCE OF EO DATA AND AI TOOLS FOR COPERNICUS-BASED APPLICATIONS

/LIVING PLANET SYMPOSIUM 2022

THE COPERNICUS PROGRAMME – LOOKING BACK, GOING FORWARD
DIGITAL COPERNICUS – CONVERGENCE OF EMERGING TECHNOLOGIES
SHAPING EUROPE'S DIGITAL FUTURE

MARIKA POPP

HEAD OF SPACE SOLUTIONS

GUARDTIME

25 MAY 2022

AGENDA

+ Why Guardtime?

+ Why do integrity and provenance matter for Copernicus and EO data?

+ Why do security issues matter for Copernicus and AI applications based on Copernicus data?

+ What can Guardtime EOGuard do for the provenance of the EO datasets and tracking of the AL/ML model training processes?

DESIGNED TO ENSURE TRUTH AND CERTAINTY IN THE DIGITAL WORLD

+ Guardtime invented KSI in 2007 to **replace trust with digital truth** – mathematical provable correctness of data, networks and systems

+ The goal was to secure at massive scale the identity, data, and processes at the center of Estonian digital society, under constant attack both outside and inside their networks by the most sophisticated nation-state level attackers

+ Close partnership with the European Space Agency since 2019, a joint whitepaper published in 2020 on **Earth Observation Data Provenance with KSI Blockchain**

+ BC4SA_validation of Guardtime KSI blockchain technology to verify the integrity and provenance of satellite data sets and support end-user adoption

ESTONIA

GUARDTIME'S KSI BLOCKCHAIN TECHNOLOGY APPLICABLE TO
ALL DIGITAL ASSETS AND TRANSACTIONS

+ a single technology stack to solve problems of **integrity, provenance, security, immutability, and audit** for any digital asset, event or transaction

+ for any industry and/or business that **relies on digital assets and systems for mission critical decisions and actions** - our technology is applicable to every vertical, from military to pharmaceuticals to the electric grid to insurance and everywhere else digital assets are deployed.

Front-end

proof of time

proof of integrity

proof of uniqueness

proof of machine identity

proof of provenance

proof of human identity

Kyiv

Bodies

MAXAR BUCHA MASSACRE SATELLITE PHOTOS:
CAN THEY BE TRUSTED?

Source: english.pravda.ru, 2022

'DEEPFAKE GEOGRAPHY' PRESENTS SIGNIFICANT RISKS?

Source: https://www.gislounge.com/deepfake-satellite-imagery/, 2022

WHY DO INTEGRITY AND PROVENANCE MATTER FOR COPERNICUS AND EO DATA?

+ EO data as an increasingly valuable and relevant **digital asset** - representing one of the largest stores of latent value in human history

+ New EO data architectures – distributed systems vs monolithic infrastructures

+ New stakeholders and end-users – without EO specialised skillset

+ New areas of application for critical/high security decision making -transportation/logistics, environmental monitoring and protection, energy/risk management, security and defense

+ Assured AI – growing need for "clean data", i.e., verifiable, untampered and authentic satellite images for AI/ML algorithm

EOGUARD:
A SECURITY AND TRUST SERVICE, PROVIDING A FULL END TO END CHAIN OF CUSTODY FOR EO DATA

THE PROBLEM WE ARE SOLVING

EO DATA SECURITY

+ Provision of a secure, reliable archive of EO data

+ Automated Data integrity for each link in the data supply chain

+ Recording and trace provenance: archiving, dissemination, end-user

+ Alerting to unauthorised changes, specific alerts to dashboard

EO DATA DISTRIBUTION

+ Evidence and validation to users (L1 and L2 products)

+ Full chain of custody for downstream services (parametric insurance)

See more: **guardtime.com/eoguard**

WHY DO SECURITY ISSUES MATTER FOR COPERNICUS AND AI APPLICATIONS BASED ON COPERNICUS DATA?

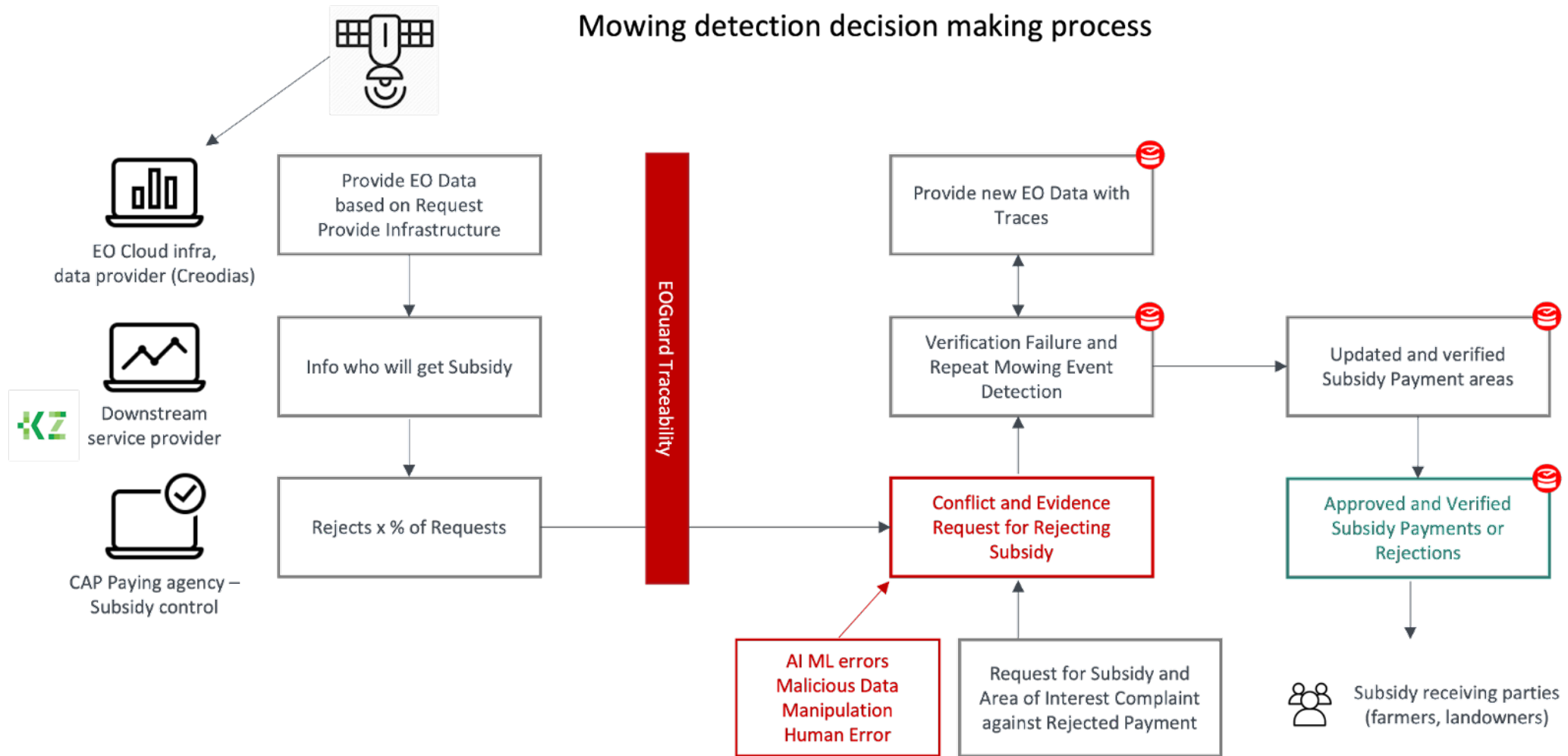ENISA's Main Recommendations on Artificial Intelligence Threat:

+ Promote a robust, safe, secure and inclusive Artificial Intelligence where humans can **understand** the rationale and **trust** the results

+ Foster verification, validation, security, control of the machine learning algorithms and input data **have not been manipulated**

Source: Analysis of the European R&D priorities in cybersecurity. Strategic priorities in cybersecurity for a safer Europe. ENISA, 2018

EOGUARD FOR COMMON AGRICULTURAL POLICY:
KAPPAZETA FULLY AUTOMATED MOWING DETECTION SYSTEM

Mowing detection decision making process

EO Cloud infra, data provider (Creodias)

Downstream service provider

CAP Paying agency – Subsidy control

Provide EO Data based on Request Provide Infrastructure

Info who will get Subsidy

Rejects x % of Requests

EOGuard Traceability

Provide new EO Data with Traces

Verification Failure and Repeat Mowing Event Detection

Conflict and Evidence Request for Rejecting Subsidy

AI ML errors Malicious Data Manipulation Human Error

Request for Subsidy and Area of Interest Complaint against Rejected Payment

Updated and verified Subsidy Payment areas

Approved and Verified Subsidy Payments or Rejections

Subsidy receiving parties (farmers, landowners)

THANK YOU

guardtime.com

guardtime