29 January
2026

{code &
compliance}

FOSDEM EDITION

From Regulation to Reality: CRA compliance journey for default products with OSS Review Toolkit (ORT)

Martin von Willebrand

29.1.2026

Table of Contents

doubleOpen()

Introduction

Double Open Oy
- Automated software supply chain governance
- Services based on open source OSS Review Toolkit (ORT) and Eclipse Apoapsis
    - SaaS, Hybrid, Managed Support offerings
- OCCTET.EU project
- 7 person team, ORT ecosystem quite a bit larger than Double Open

Martin von Willebrand
- CEO at Double Open
- Lawyer for 25+ years, formerly practicing attorney
- Board member at Open Source Finland (former chair), open source advocate, FSFE Fellow
- Engaged in CRA standards review and drafting at the Finnish SSO

doubleOpen()

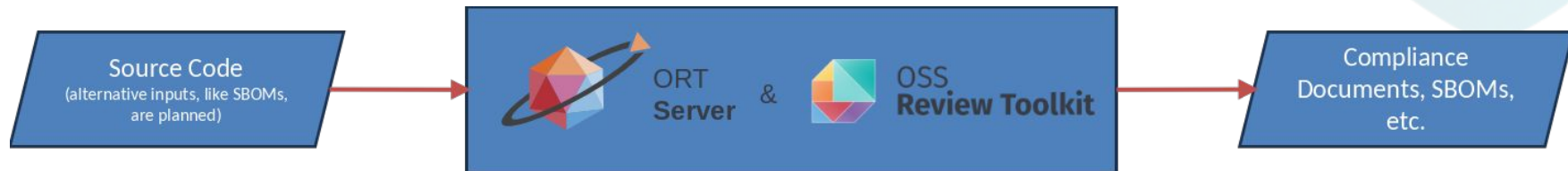# OCCTET.EU

Open CyberSecurity Compliance Toolkit

EU funded project to help SMEs comply with the requirements of the Cyber Resilience Act (CRA). Seven partners, timeline 11/2024 - 10/2026, total budget 2,2M euro.

The toolkit is intended to provide a comprehensive suite of tools and resources tailored to the needs of SMEs:

- Compliance Checklist
- Conformity Assessment Specifications
- Automated Evaluation Method and Tool
- Federated Database platform for publishing the results of OSS component assessments allowing contributions from various stakeholders
- Inventory of Automatic Dependency Analysis Tools
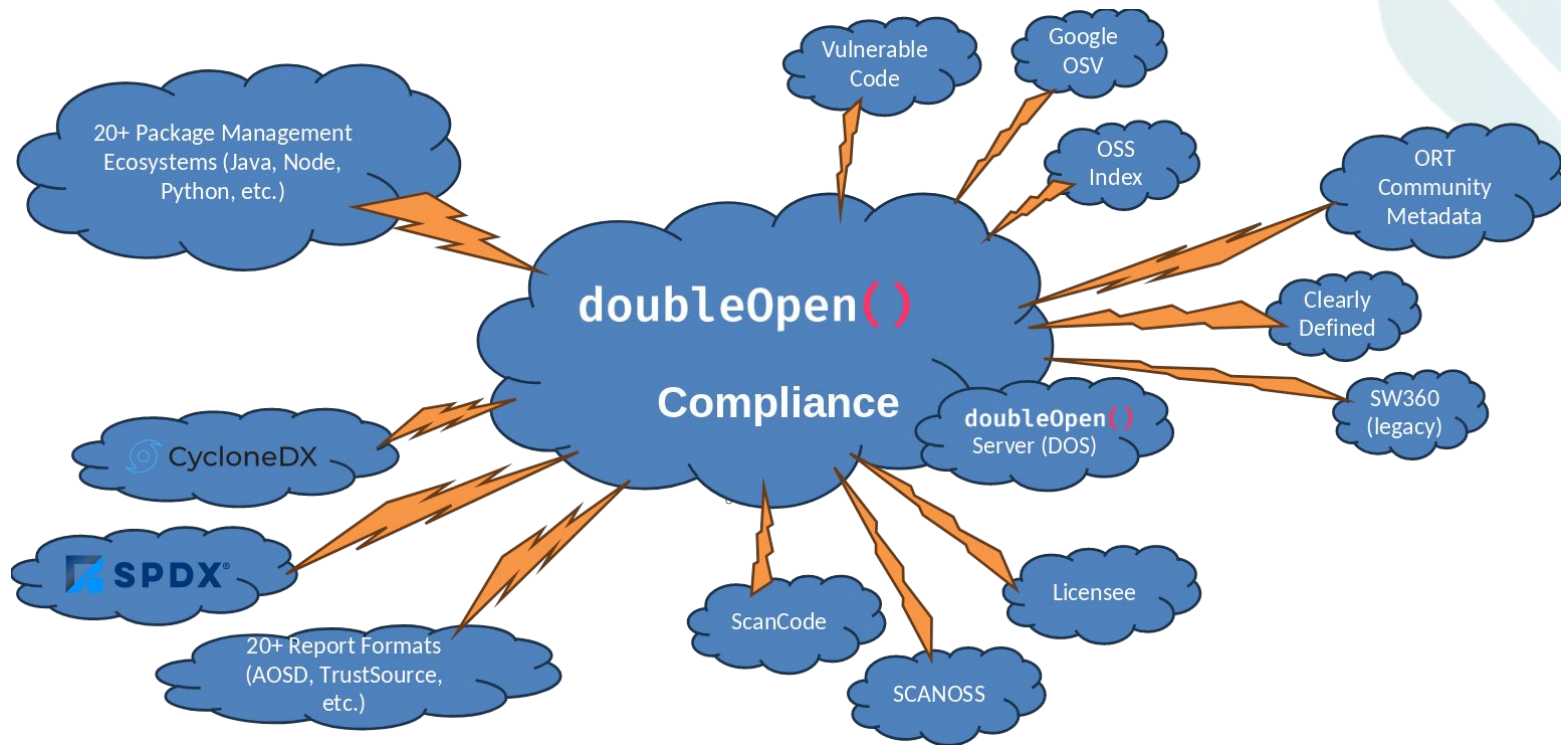- Reporting tool

OSS Review Toolkit (ORT) ecosystem

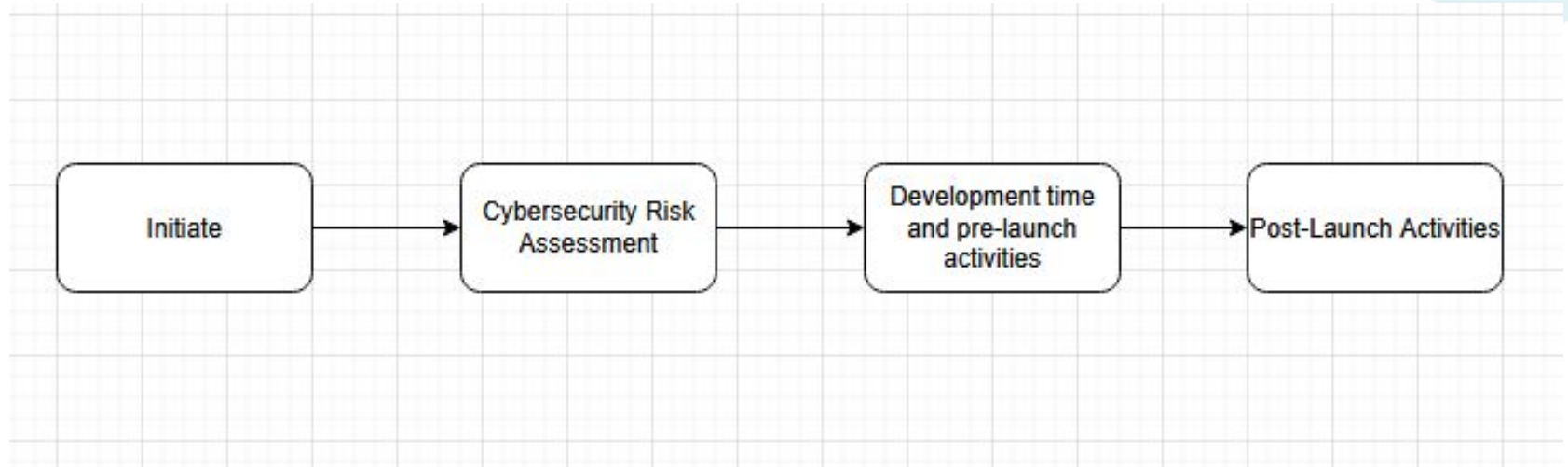Open source projects under Apache 2.0 ⁵
- ORT cli: https://github.com/oss-review-toolkit/ort and https://oss-review-toolkit.org/ort/
- ORT Server: https://eclipse-apoapsis.github.io/ort-server/

doubleOpen()

ORT ecosystem integrations

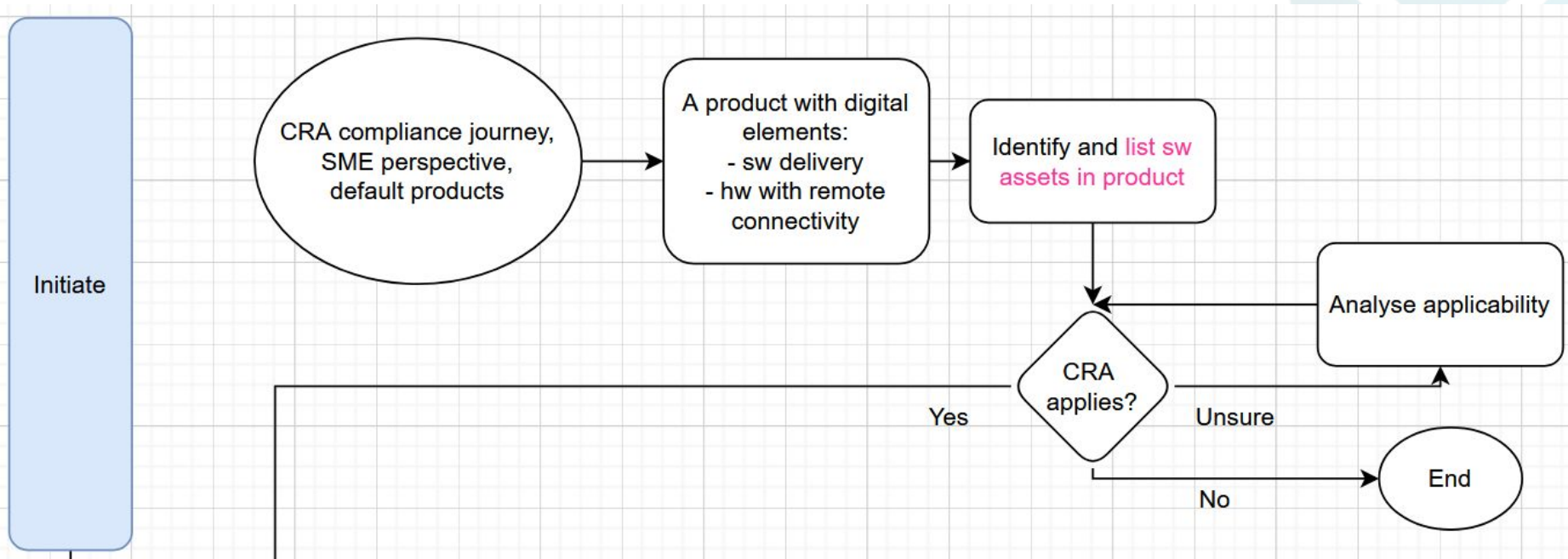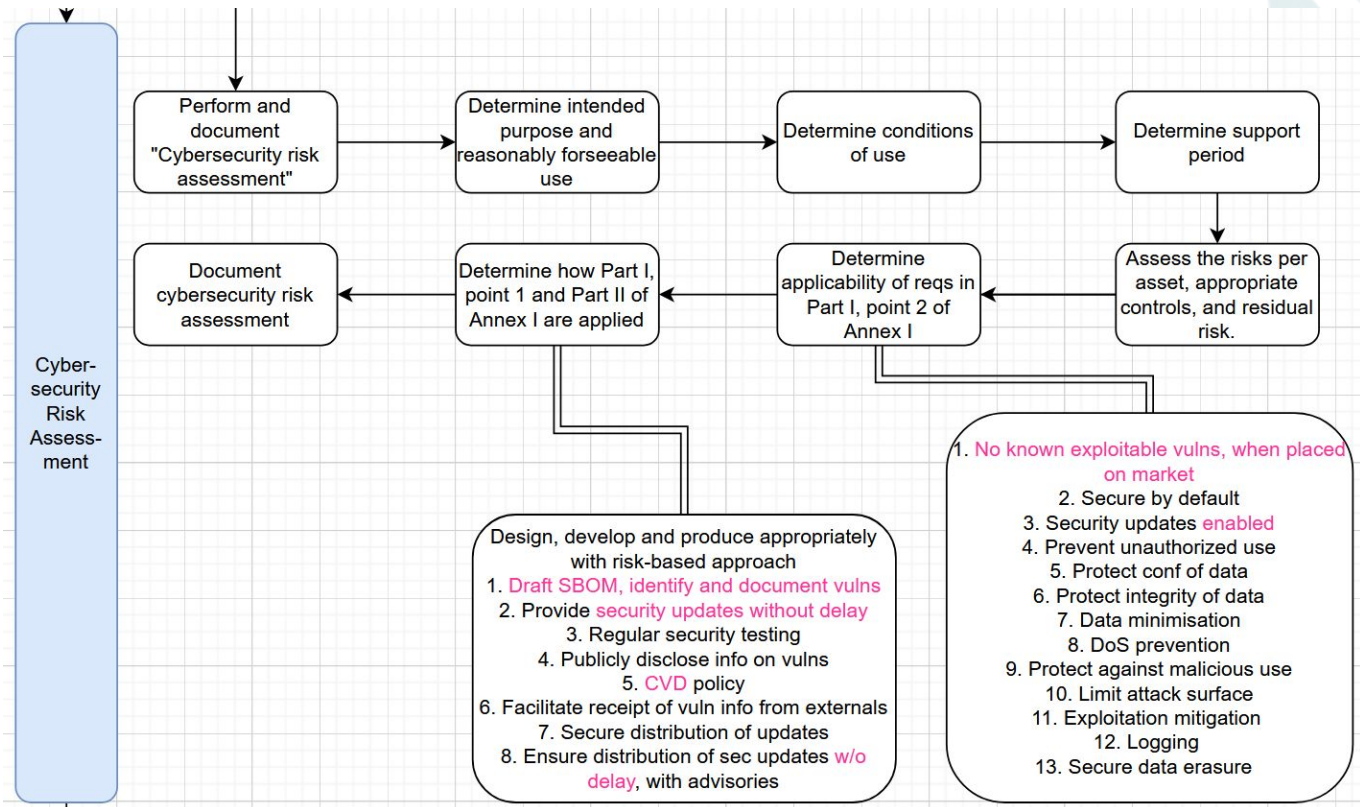# CRA Journey, very high-level

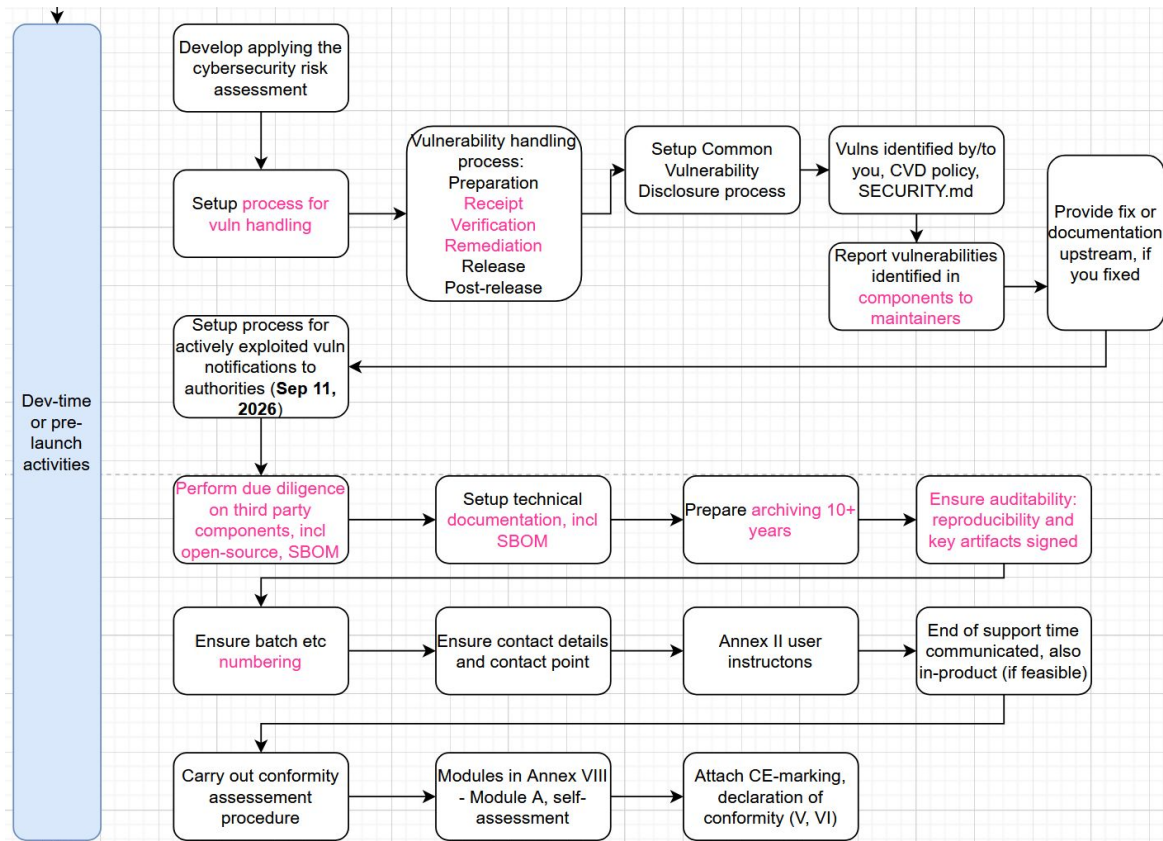

doubleOpen()

CRA-compliance, initiate

doubleOpen()

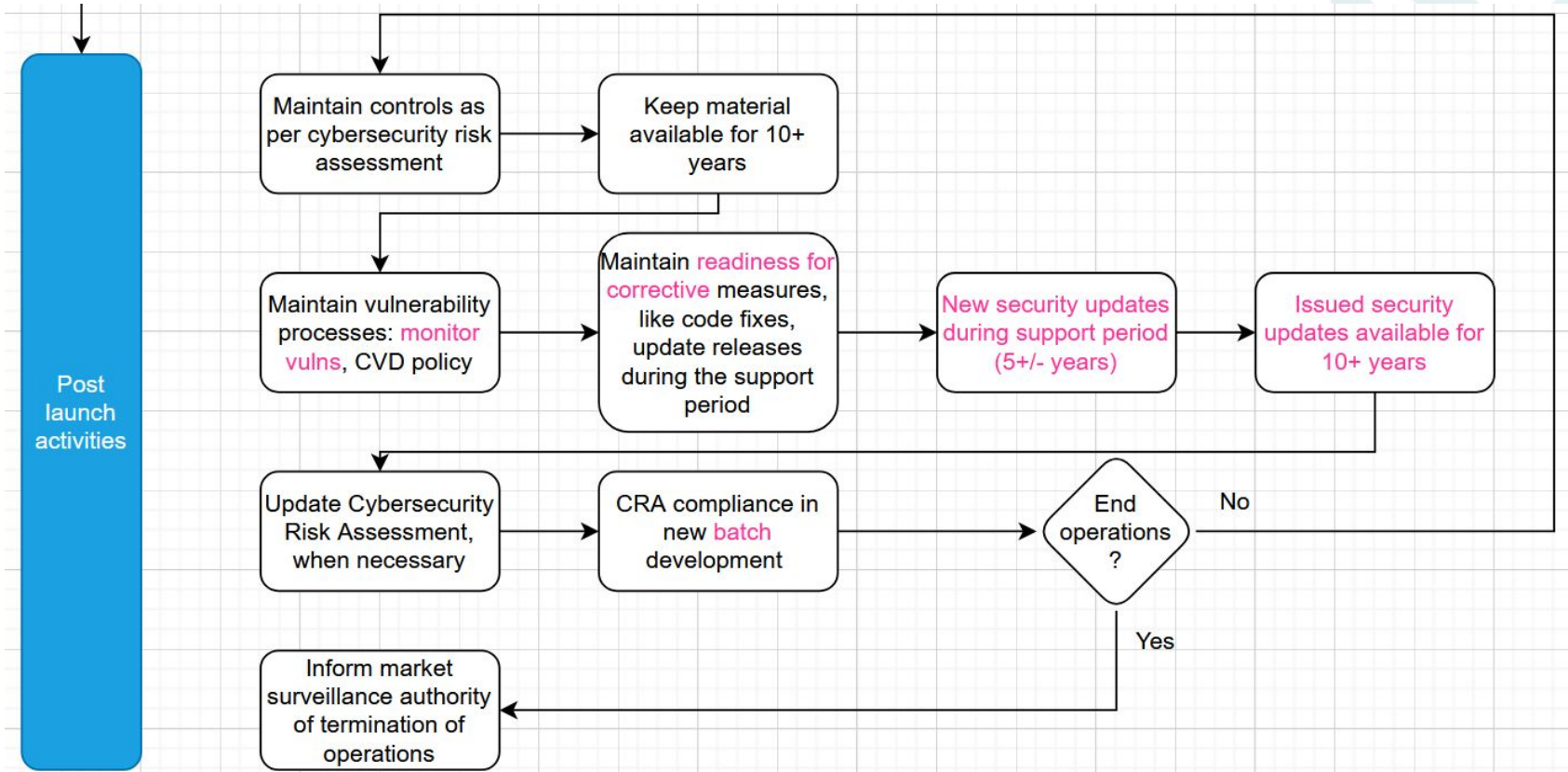# CRA-compliance, Cybersecurity Risk Assessment

doubleOpen()

CRA-compliance, Dev-Time and Pre-Launch Activities

doubleOpen()

CRA-compliance, Post-Launch Activities

doubleOpen()

Tooling support in CRA compliance

✓ Create and maintain a list of sw assets in product
✓ Ensure no known exploitable vulnerabilities when entering the market
✓ Create SBOMs
✓ Perform third party sw due diligence - dependency graph + analysis
✓ Handle receipt, verification and remediation of vulnerabilities, including monitoring, identifying and documenting, ensure that your own CVD policy exists
✓ Minimise delays in providing security updates
  ○ Automatic dependency management, dependency paths, recommended updates for fixing issues
✓ Ensuring auditable signed documentation, batch numbering, archiving 10+ years

doubleOpen()

Thank You

Martin von Willebrand
CEO
Double Open Oy

martin.vonwillebrand@doubleopen.org
doubleopen.io

doubleOpen()