



Ik geef meer duiding rond:

- de beweegredenen van Smals om te werken met open source
- de grootte orde van open source die we gebruiken (eigenlijk is de betalende open source maar een klein %)
- de uitdagingen rond open source (oa beveiliging en zoals gebleken door de log4J vulnerability gebruiken grote vendors zoals vmware, oracle, ... ook open source in hun systemen)
- de nood om goed na te denken over verschillende aspecten van open source (oa de demographics van de contributoren, men spreekt vaak over “community”, maar veel zaken worden onderhouden door 1 individu)
- hoe wij open source een plaats willen geven in public cloud om “portability” te garanderen overheen hyperscalers (azure, aws, google, ...)
- hoe de verschillende initiatieven (g-cloud, reuse, EA, ...) eigenlijk geïnspireerd zijn op het concept open source & community
- hoe deze initiatieven een logische opbouw vormen om binnen onze micro-community verder te springen

Open source, a driving force in our digital society, must step into the limelight once more. It's not just about promoting its adoption or principles; understanding its inner workings and the community dynamics is crucial. By harnessing the power of micro-communities,

we can fully leverage open source to enhance public sector services. However, open source is currently under continuous threat, requiring a renewed commitment to its protection and advancement.

As a tight-knit public sector family, we must elevate our efforts by reimagining how we engage with open source in a systematic manner. Now is the time to step up our game by forging bonds and building bridges to uphold the principles of openness and community-driven development that lie at the heart of open source.

Let's work together to reimagine and shape a sustainable digital future for the public sector.

Smals



- Belgian **In-house** ICT Service Provider/Integrator
- For and by the **Public Sector**
- **Nonprofit** organization
- **2,122** collaborators
- Operates as a **shared service center** for **319** government organizations
 - Infrastructure management
 - Software development
 - Data management
 - Security services
 - ...
- Main role: **enabler** for government ICT
- Established in **1939**





<https://www.smals.be/nl/content/activiteitenverslag-2022>





Supporting cross-institution ICT Initiatives

-  **G-Cloud Programme (2015-...)** – gcloud.belgium.be
 - For and by public institutions
 - Focus on infrastructure services & platforms, shared procurement, ...
-  **Software ReUse Programme (2019-...)** – ict-reuse.be
 - For and by public institutions
 - Focus on components, authentic data sources, API's, ...
- **Full Stack Approach (2021-...)**
 - Enterprise Architecture across public institutions
 - Focus on architectural principles, processes, building blocks, ...
- **Public Cloud Computing & AI (2023- ... Accelerated)**
 - Emphasis on security, business continuity, cloud portability, data sovereignty
 - Strong governance

Slide 6

OPEN ('24)
ENTERPRISE OPEN SOURCE 10th EDITION

Smals & Open Source Challenges

Progress 50%

Dirk Deridder

Smals
ICT for society

Slide 7



Why is Smals interested in open source?

- **Alignment with our Vision, Culture, and Mindset**
 - Principal values & drivers resonate with how we look at the ICT world
- **Quality-driven Community**
 - Fostering a quality-driven mindset to ensure operational stability and robustness
- **Open standards**
 - Adoption of open standards to facilitate longevity and to mitigate vendor lock-in
- **Business Continuity Assurance by Embracing 'Free(dom)' technology**
 - Utilizing free technology & the freedom to operate
 - Counter 'Machiavellian Licensing Plots' and balance the power of proprietary vendors
- **Creative Nexus**
 - It is where innovation magic happens

Quick & easy 15 seconds braindump:

Committed to high quality standards

→ Hence, we require enterprise versions/support



Red Hat

Linux, Openshift, JBoss, AMQ,...



EDBTM
POWER TO POSTGRES

...

5-10 technologies



Bit more comprehensive & less easy 5 minute braindump...

Committed to high quality standards

7-zip	Argocd	Docker	Git	InfluxDB	Kibana
Acm	AsciiDoc	Dokuwiki	Gitea	Inspec	Linux
ActiveMQ	AWX	Eclipse	GitLab	Java	Log4J
Alerta	Camel	EclipseLink	Gpg4win	Java Spring Boot	Mattermost
Angular	CEPH	ElasticSearch	Grafana	Jenkins	Maven
Ansible	Checkmk	Emacs	Grafana Loki	JFrog Artifactory	Minio
Apache	Chef Inspec	Firefox	gVim	JMeter	MySQL
Apache JMeter	Cloudform	Fluentd	HAProxy	JPA	NEO4J
Apache Nifi	Curl	Foreman	Hashicorp Consul	Kafka	Netbeans
Apache Zookeeper	DBeaver	Gatling	Hashicorp Vault	Keepass	NGINX
Notepad++	OpenFT	OpenSearch	Open Text	Percona	Postgress EDB
OBS Studio	OpenJDK	OpenStack	Oracle Linux	PHP	Prometheus
PlantUML	Podman	PostgreSQL (non-EDB)	Python	Red Hat JBoss	Redis
Rundeck	Sonarqube	Testlink	WSL	Red Hat Linux	Renovate
Satellite	Stolostron	Vaultwarden	Zabbix	Red Hat Openshift	Restic
SecureID	Symfony	PuTTY	ZAPProxy	Red Hat Openstack	Ruby
Selenium	Telegraf	WinSCP	Zend	Red Hat Satellite	React
Signal	Testkube	Wordpress	Red Hat AMQ	Prometheus Node Exporter	Prometheus AlertManager
					...

100-120 technologies


→ Apparently, we don't always require enterprise versions/support

... adding Community-Driven Open Source Technology


Open source is more often than not invisible

Open Source is everywhere @Smals

- It depends on what you include:
 - Products, Platforms, Tools, Libraries, Drivers, Code snippets, ...
- [OSSRA report](#) finding (2024)
 - Open source components and libraries are the backbone of nearly every application across all industries
 - 96% of total codebases contain open source



96%
of the total codebases
contained open source



➔ **Proprietary vendors would not exist without open source !**

Even if you only believe half of it... this is still an impressive number !

The screenshot shows the top navigation bar of the National Cyber Security Centre website with links for 'ABOUT NCSC', 'CISP', 'REPORT AN INCIDENT', and 'CONTACT US'. The main heading is 'Log4j vulnerability - what everyone needs to know'. Below the heading is a sub-heading: 'Information about the critical vulnerability in the logging tool, who it could affect and what steps you can take to reduce your risk.' A text box contains the following information: 'Log4shell is a critical vulnerability in the widely-used logging tool Log4j, which is used by millions of computers worldwide running online services. A wide range of people, including organisations, governments and individuals are likely to be affected by it. Although fixes have been issued, they will still need to be implemented.' The article is dated 'PUBLISHED 14 December 2021'. The background image shows computer monitors displaying code.

Thanks vulnerability, for the insight 😊😞

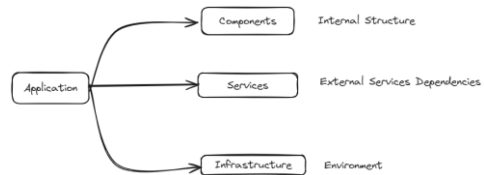
- It is highly unlikely that your system doesn't contain open source elements
- Your code contains more than you know
 - Their code also contains more than they know
 - Since they are suppliers, they should know !
- [OSSRA report](#) finding (2024)
 - 84% of codebases contained at least 1 open source vulnerability
 - 91% of codebases were found to contain components 10 versions or more behind
- It is highly certain that your code contains (un)discovered vulnerabilities
 - Regardless of whether it is open source or not...

➔ **Visibility is thus a top priority**

The infographic features two circular icons: a teal one with code symbols and a yellow one with a warning triangle and code symbols. A vertical orange bar on the right is labeled 'Almost all codebases'. The statistics are: 96% of the total codebases contained open source, and 84% of codebases contained at least one open source vulnerability.

xBOM to the rescue?

- Bill of Materials for
 - Software (SBOM), SaaS (SaaS-BOM), Hardware (HBOM), Machine Learning (ML-BOM), ...
 - Include all direct and transitive components
 - Include the dependency relations between them
- [OWASP CycloneDX Software Bill of Materials \(SBOM\) Standard](#)
 - Open source Component Analysis platform
 - Identifies risks in the software supply chain
- Primary use cases
 - Vulnerability identification, license compliance, outdated component analysis
- Main drivers @ Smals?
 - Cybersecurity, ISO/IEC27001, NIS2
 - Lifecycle management
 - Log4J reality check



xBOM to the rescue?

- **Component Identification:** Lists all components, including libraries, modules, etc.
- **Version Information:** Specifies versions or commit hashes of each component.
- **Metadata:** Provides details like description, author, and release date for each component.
- **Licensing Information:** Indicates the licenses under which components are distributed.
- **Dependencies:** Documents both direct and transitive dependencies.
- **Vulnerability Information:** Includes known vulnerabilities with severity ratings and remediation guidance.
- **Provenance Information:** Identifies the source from which each component was obtained.
- **Checksums or Hashes:** Offers cryptographic hashes for verifying component integrity and authenticity

Can we treat the OS community as “yet another supplier”?

```

{
  "creationInfo": {
    "created": "2024-02-07T08:09:00Z",
    "creators": [
      {
        "Organization": "Red Hat Product Security (secalert@redhat.com)"
      }
    ],
    "licenseListVersion": "3.8"
  },
  "dataLicense": "CC0-1.0",
  "documentDescribes": [
    {
      "SPDXRef-227f7b84-025c-45ae-bb43-bf5ec09cc13b"
    }
  ],
  "documentNamespace": "https://access.redhat.com/security/data/sbom/beta/spdx/RHOSE-4.9.2",
  "name": "RHOSE-4.9.2",
  "packages": [
    {
      "copyrightText": "NOASSERTION",
      "downloadLocation": "registry.redhat.io/openshift/ose\u002Dcluster\u002Dnode\u002Dtuning\u002Doperator:v4.9.0\u002D202203081819.p0.gce0b3ae.assembly.stream",
      "externalRefs": [
        {
          "referenceCategory": "SECURITY",
          "referenceLocator": "cpe:/a:redhat:openshift:4.9::el8",
          "referenceType": "cpe22Type"
        },
        {
          "referenceCategory": "PACKAGE_MANAGER",
          "referenceLocator": "pkg:oci/ose-cluster-node-tuning-operator@sha256:c05025965a23568d177f84e30adda1f2b4677a54baf1a0f1a67005a2cfd7cb52?repository_url=registry.redhat.io/openshift/ose-cluster-node-tuning-operator&tag=v4.9.0-202203081819.p0.gce0b3ae.assembly.stream",
          "referenceType": "purl"
        }
      ],
      "filesAnalyzed": false,
      "homepage": "registry.redhat.io/openshift/ose\u002Dcluster\u002Dnode\u002Dtuning\u002Doperator",
      "licenseComments": "Licensing information is automatically generated and may be incomplete or incorrect.",
      "licenseConcluded": "NOASSERTION"
    }
  ]
}
    
```

<https://access.redhat.com/security/data/sbom/beta/spdx/>

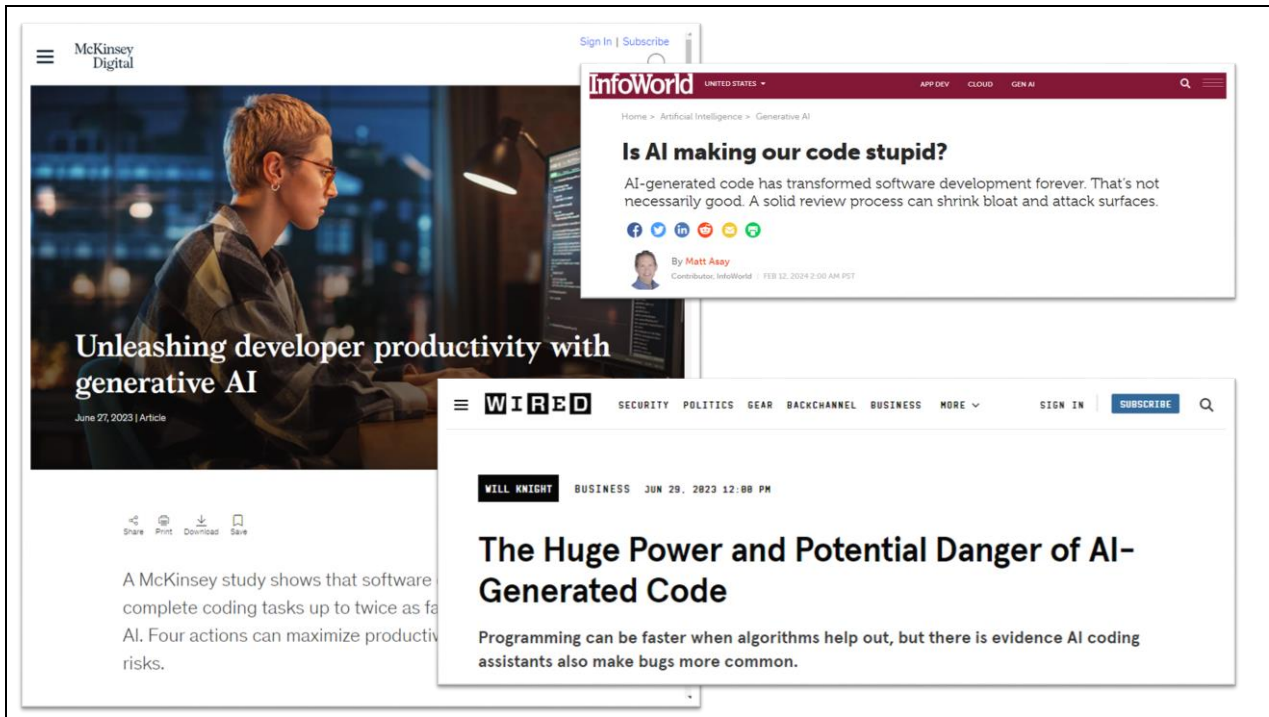
xBOM doesn't solve everything !

- **Position in Technology Landscape?**
 - Understanding its role and relevance within our technology ecosystem, what value does it bring
- **Criticality and Reliability?**
 - Assessing the potential impact if it malfunctions or if it requires replacement
- **Characteristics and Attributes?**
 - Evaluating various aspects such as its complexity, size, maturity, and other –ities
- **Contributors and Community?**
 - Determining the number of active contributors and their demographics
- **Availability of Support?**
 - Confirming the availability of support channels, either commercial or in-house
- **Release Cadence and Update Frequency?**
 - Analyzing the frequency of releases and updates is a quality indication, yet some components are simply “done”
- **Track Record?**
 - Reviewing the history of bugs, vulnerabilities, fixes, and overall performance/score in the community
- **Visibility and Recognition?**
 - Identifying if it's recognized or on the radar of major industry players ...

Software development/use practices require a security-by-design approach that goes beyond the old normal

The image shows two overlapping content elements. The top element is an Arstechnica article snippet with the title "GitHub besieged by millions of malicious repositories in ongoing attack" and a sub-headline "ATTACK OF THE CLONES —". Below the title, it says "GitHub keeps removing malware-laced repositories, but thousands remain." and "DAN GOODIN - 2/28/2024, 11:12 PM". The bottom element is a presentation slide from The Linux Foundation Europe, featuring a red binary background. The slide title is "The Rising Threat of Software Supply Chain Attacks: Managing Dependencies of Open Source projects" and the author is "PAOLO MAINARDI | 15 AUGUST 2023". A pink "JOIN" button is visible in the top right of the slide.

<https://arstechnica.com/security/2024/02/github-besieged-by-millions-of-malicious-repositories-in-ongoing-attack/>



<https://www.infoworld.com/article/3712685/is-ai-making-our-code-stupid.html>

<https://www.wired.com/story/fast-forward-power-danger-ai-generated-code/>

<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/unleashing-developer-productivity-with-generative-ai>

Questionable Open Source Practices... in the proprietary, commercial/hybrid community



RANT MODE: ON

- **Exploiting Open Source**
 - Opportunistic use of the term "open source" to mask profit-driven motives
- **Profit Over Principles**
 - Prioritizing profit margins over openness and community-driven innovation
- **Hollow Commitments**
 - Paying lip service to open source ideals while prioritizing profit over principles, community, and collaboration
- **Deceptive Marketing Tactics**
 - Manipulate the perception of openness to push proprietary models
- **Betrayal of Community**
 - Leech of the goodwill of the open source community without contributing back or upholding its values
- **Undermining Open Standards**
 - Interoperability standards are not the objective
- **Tech Oligarchy**
 - Large tech companies exerting undue influence over the direction and governance of open source projects, stifling innovation and diversity.

As a community we should condemn these practices, but also come up with ideas for sustainable business models

Yet still, we aren't against open source use?

- We follow at the same time a strategic and an opportunistic approach
- We continuously evaluate its use
- We continuously balance proprietary versus commercial/hybrid versus community-driven OS
- Drivers?
 - Financial & procurement considerations (cost, scale of deployment, tendering, ...)
 - Enterprise risk mitigation (vendor lockin, business continuity, ...)
 - No-brainer (linux, core tools, drivers, ...)
 - Didn't even know it was open source
- When we follow a dual vendor approach, open source is typically the alternative
 - This is a major challenge: Lack of enterprise (low & high level) "features" hamper wide-scale adoption
- We ~~think believe~~ hope open standards will bring us 99% of portability (on premise)
 - Or at least more than 0%
 - Proven in the past that proprietary → open source is a lot harder than the other way round
- We trust our people to make the right choices and to be smart





We definitely want to see an increase in its usage,
employing an embedded, disciplined, and methodological approach

The future looks bleak if we don't come up with a revived/revised/reimagined open source concept

Open source is and remains a Strategic Asset

Supporting cross-institution ICT Initiatives

-  **G-Cloud Programme (2015-...)** – gcloud.belgium.be
 - For and by public institutions
 - Focus on infrastructure services & platforms, shared procurement, ...
-  **Software ReUse Programme (2019-...)** – ict-reuse.be
 - For and by public institutions
 - Focus on components, authentic data sources, API's, ...
- **Full Stack Approach (2021-...)**
 - Enterprise Architecture across public institutions
 - Focus on architectural principles, processes, building blocks, ...
- **Public Cloud Computing & AI (2023- ... Accelerated)**
 - Emphasis on security, business continuity, cloud portability, data sovereignty
 - Strong governance

HET RESULTAAT VAN EEN GEZAMENLIJKE AANPAK

Het G-Cloudprogramma is het resultaat van een gezamenlijk initiatief door meerdere publieke instellingen: federale overheidsdiensten, instellingen van de sociale zekerheid en de zorgsector. De praktische realisatie wordt aangestuurd vanuit de « Cloud Governance Board ».

Een gemeenschappelijke roadmap wijst de weg naar de ontwikkeling van deze 'community Cloud' van de overheid. Tervijl de eerste generatie van G-Cloud-diensten al operationeel is sinds maart 2015, zijn er nog talrijke nieuwe evoluties op komst.

De G-Cloud is een hybride cloud, waarbij enerzijds gebruik wordt gemaakt van diensten aangeboden door private firma's in publieke cloud-omgevingen, en anderzijds van diensten gehost in datacenters van de overheid. Het beheer van de G-Cloud gebeurt door de overheid. Voor de uitbouw en de operationele werking wordt in ruime mate beroep gedaan op de privé-sector.

<https://gcloud.belgium.be/>

g-cloud

G-Cloud – Sharing ICT infrastructure

- Programme of synergy-driven initiatives
 - Services, Projects, Procurement, Knowledge Sharing
 - Active cross-institution ICT Community
- Hybrid community cloud model
 - Private Community Cloud running from government-operated datacenters
- Public cloud?
 - Already the case for special purpose needs
 - Moving forward as a community for general purpose needs
 - Joint taskforce defining vision, strategy, policies, guidelines, architecture, ...

Avoided spending (federal)

Year	Avoided spending (K€)
2015	3,691
2016	7,657
2017	18,578
2018	31,474
2019	40,872
2020	45,681
2021	41,912
2022	49,532
2023	49,987
2024	54,950

Even if you only believe half of it... this is still an impressive number !

Public Cloud & Open Source?

- How to maximize potential public cloud “value”
 - And minimize potential public cloud “disvalue” for your organization?
 - This (dis)value depends heavily on your specific situation
 - An important multi-dimensional exercise of ICT maturity
- We ~~think~~ believe hope open standards will bring us 99% of portability (off premise)
 - Or at least more than 0%
 - Cloud Portability comes with a cost however and it limits your options
 - Requires careful consideration
- We do believe it paves the way to step up the operational stability / quality
 - Going public cloud means you need to get your act together – are you ready?
 - It will be beneficial for the on premise maturity as well
- Hybrid Cloud increases complexity
 - Optimizing your on premise installation for efficiency and effectiveness is a different beast
 - Technology evolution/delivery models are often optimized for a public cloud model and a profit-driven industry
 - Example: Vertical scaling (in the datacenter) versus Horizontal scaling (of the software)
- Is open source still relevant / viable in an XaaS-only world?

Open source should cover a new strong concept of “open services” and “open cloud”

Ok, so then Smals is a top contributor?

- Our core business is not “technology product development”
 - We (ab)use technology to (retro)fit the needs of our context
 - Like most organisations we are mainly on the consumer side
 - Abstractions that are (re)usable for the rest of the world pop up occasionally but are not the norm
- Practical open source contribution in general is not for everyone
 - Less than 1% of the population is capable to directly contribute in a meaningful way
 - Coding competency, paying with your time, figuring your way around the code base and culture, ...
- We do pay others to contribute for us
 - e.g. RedHat, Postgres EDB, ...
- Contributions in any form remain a major challenge
 - In general, not limited to open source
 - Even for in-house contributions to our own transversal micro-cosmos of libraries, platforms, ...
 - It’s no free(dom) lunch

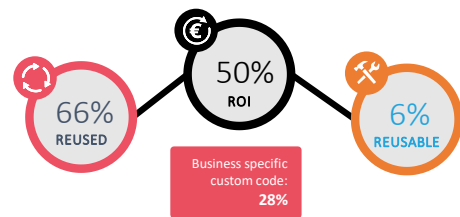


We do however contribute to a vibrant micro-community...

The screenshot shows the 'Verken de Software ReUse Catalogus' website. The header includes the 'ReUse' logo and navigation links for Home, Catalogus, Partners, and Contact. The main heading is 'Verken de Software ReUse Catalogus' with a sub-heading: 'Smals en haar leden streven naar hergebruik van software-onderdelen en het herbruikbaar maken van nieuwe ontwikkelingen. Deze catalogus bevat een overzicht van bestaande herbruikbare componenten.' Below this is a search bar with the text 'Zoek op trefwoord, of kijk in de categorieën hieronder.' and a 'Zoeken' button. The main content area lists several categories with icons and brief descriptions: 'Authentieke bron', 'Communicatie', 'Interfaces', 'Gebruikers- en toegangsbeheer', 'Veiligheid', and 'Dossierbeheer'. A grey box on the right contains the URL 'https://ict-reuse.be/'.

Reuse of software & business components

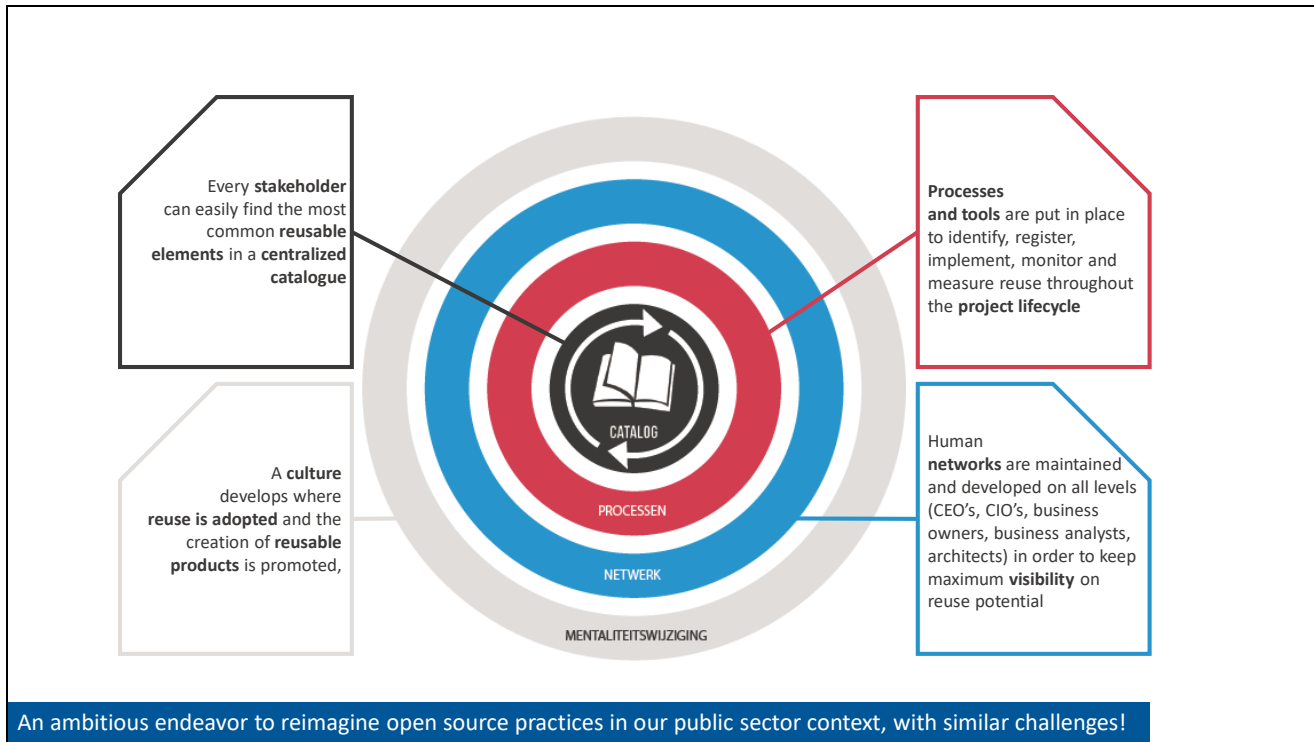
- Originated within Belgian public social security & Smals
 - Open to other federal public services
- Synergy around (technical) business components
 - Avoid multiple development of redundant components
 - Save costs & effort
- Catalogue of reusable components
- Active micro-community
- Regardless of whether development takes place by
 - The institution's own ICT department, Smals, subcontractors



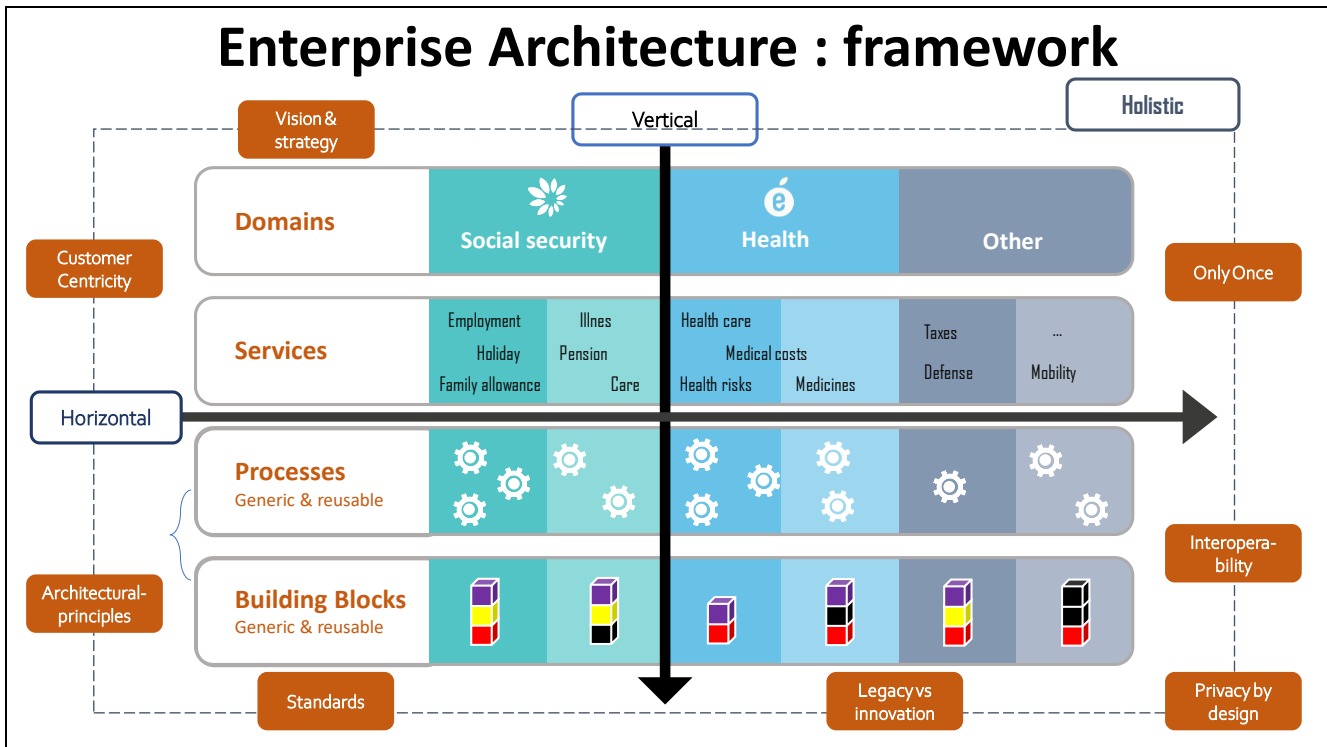
→ Total ROI 2022: € 32.000.000

Even if you only believe half of it... this is still an impressive number !

Slide 31



Slide 32



Open source is an inspiration for our own Community

Some Principal values & drivers of Smals

- Sustainable ICT solutions and services
- Community empowerment
- Collaborative innovation
- Overarching “enterprise” architecture vision for public sector ICT
- Quality driven with a particular focus on business continuity and security
- Data ethics and data protection as a fundamental cornerstone in our approach
- Digital inclusion and citizen-centricity as the default
- Cost-Conscious and lean mindset to maximize value for our community ...



- **Synergetic**, giving rise to a whole that is greater than the simple sum of its parts
- **Enabler**, ensuring indirect positive benefits for society
- **Invisible**, leaving the spotlight to our members

OPEN SOURCE MINDSET
APPROVED

Key takeaways...

- **Open source is the invisible engine of our digital society**
 - We must focus on making it visible again
 - Not only to promote it, but also to know what's inside our trusted engine
 - **Micro-communities can make a difference**
 - We must tap into the collective intelligence of the public sector community to deliver better services to citizens
 - It's about building bridges
 - We are all part of the public sector family: Together we stand strong(er)
 - **Open source is more than just software**
 - It's about building a culture of openness, collaboration, and trust
 - It's about building a methodological approach covering all aspects that keep us awake
 - With great freedom comes great responsibility
- **Join existing communities**, create new ones - every type of contribution matters
 - **Reimagine open source** in the broadest sense
 - Ensure that **trust in open source** and the public sector doesn't dwindle
 - Make a future of XaaS sustainable for the public sector by **pushing open services and open cloud**
 - Install a **structural, methodological approach** for public sector to embed open source in our digital landscape

Thank you !

If you have any questions, do not hesitate to contact me,
dirk.deridder@smals.be

gcloud.belgium.be

ict-reuse.be

www.smals.be

