Panel M31b: Is Automation Necessary for the CC Survival?

MODERATOR

- **José Ruiz**
- Co-Director at jtsec Beyond IT Security

PANELISTS

- **Kevin Gallicchio**

Technical Leader, NIAP

- **Pascal Van Gimst**

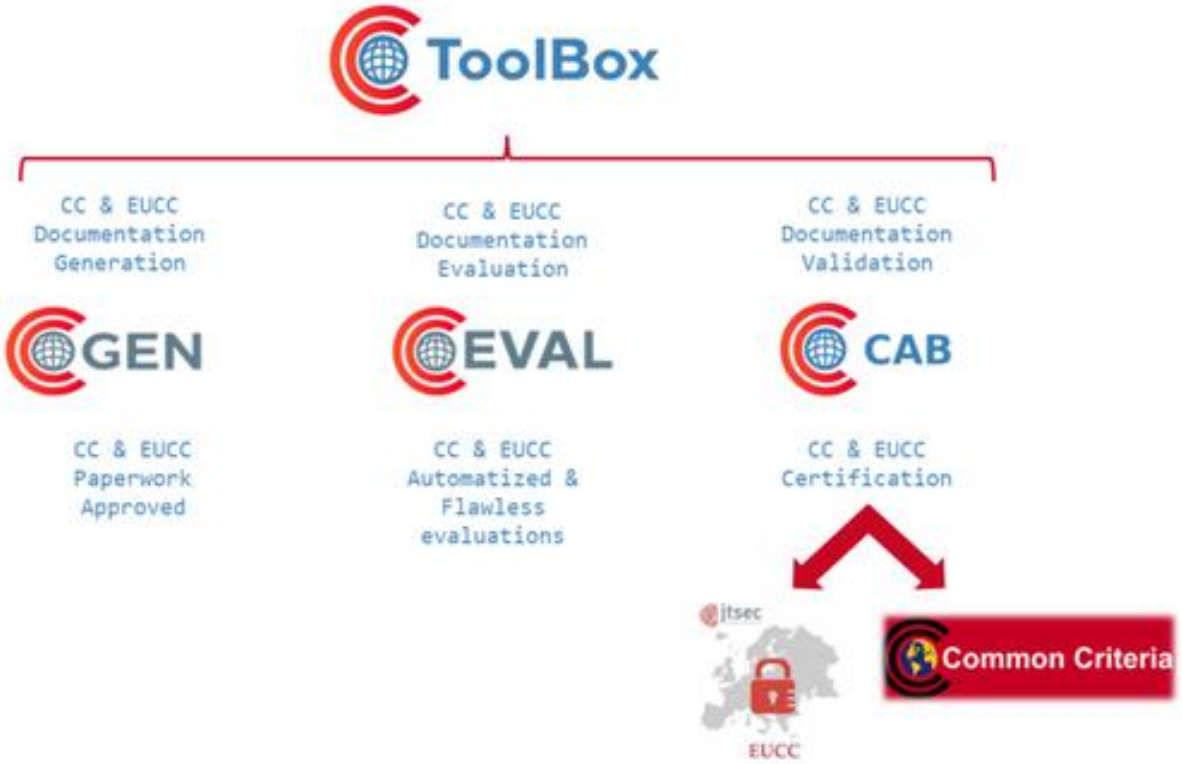
Vice President Global Services Sales and Business Development, Riscure

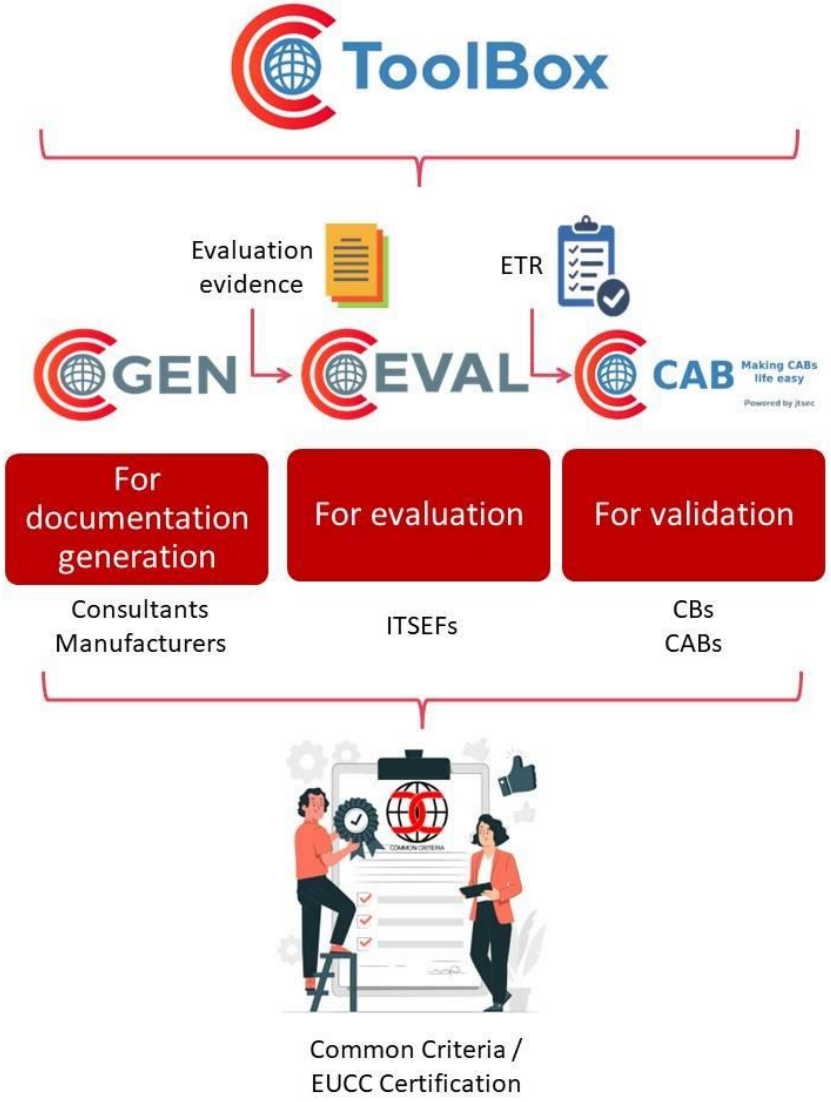
- **Alexander Krumeich**

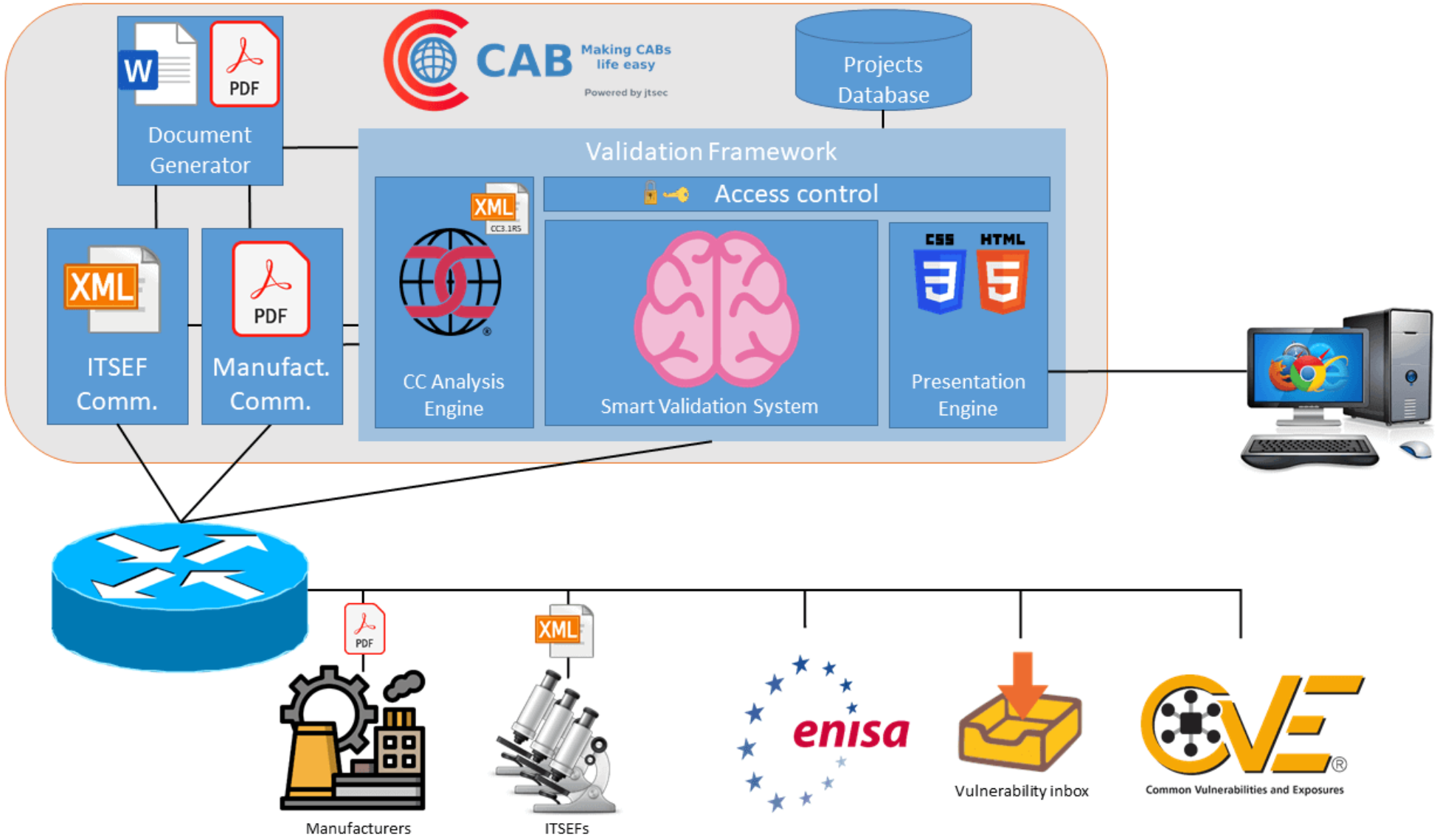
Head of Certification/Senior Software Developer, CGM

- **Lachlan Turner**

Director Consulting, Lightship Security


ToolBox
CC & EUCC Documentation Generation
CC & EUCC Documentation Evaluation
CC & EUCC Documentation Validation
GEN
EVAL
CAB
CC & EUCC Paperwork Approved
CC & EUCC Automatized & Flawless evaluations
CC & EUCC Certification
jtsec
EUCC
Common Criteria


ToolBox
Evaluation evidence
ETR
GEN
EVAL
CAB
Making CABs life easy
Powered by jtsec
For documentation generation
For evaluation
For validation
Consultants
Manufacturers
ITSEFs
CBs
CABs
Common Criteria / EUCC Certification


W
PDF
Document Generator
CAB
Making CABs life easy
Powered by jtsec
Projects Database
Validation Framework
Access control
XML
CC3.1R5
CC Analysis Engine
Smart Validation System
CSS
HTML
Presentation Engine
XML
ITSEF Comm.
PDF
Manufact. Comm.
PDF
Manufacturers
XML
ITSEFs
enisa
Vulnerability inbox
CVE
Common Vulnerabilities and Exposures

- **Alexander Krumeich**
  - Job Software Developer, Certification Specialist
  - Company CompuGroup Medical Deutschland
  - CC EAL 3+ for KoCoBox MED+ since 2015
  - Background Java, Unix, LaTeX, DevOps
  - Automation Project Developing n-doc

CGM CompuGroup Medical

CGM Deutschland AG, Cologne, Germany

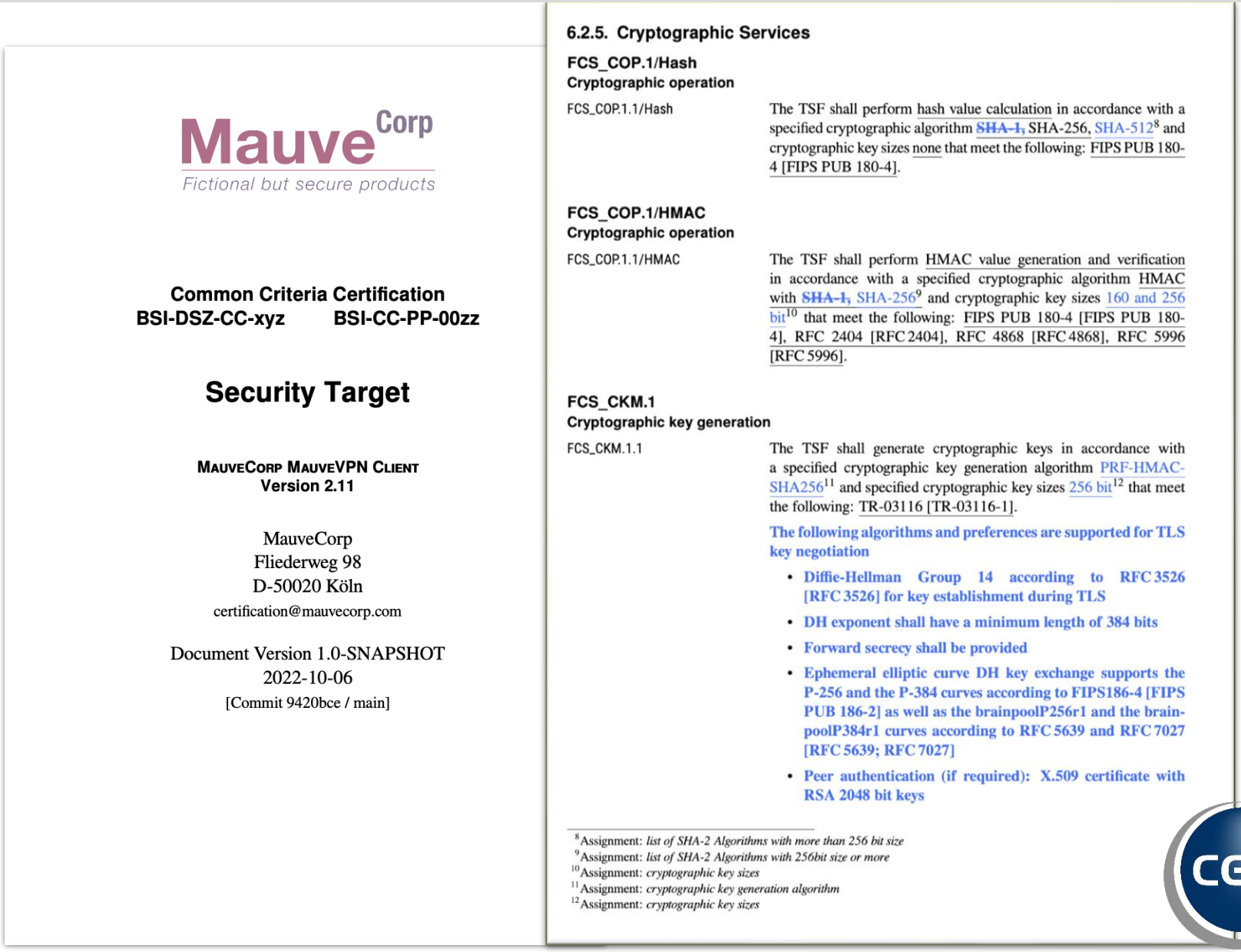
High-Quality, hyperlinked PDF Documents

In development since 2017

Deployed in customer and in-house projects

Adaptable to different certification schemes

Published in 2020 as Open Source Software under MIT license.



Mauve Corp

Fictional but secure products

Common Criteria Certification
BSI-DSZ-CC-xyz BSI-CC-PP-00zz

Security Target

MAUVECORP MAUVEVPN CLIENT
Version 2.11

MauveCorp
Fliederweg 98
D-50020 Köln
certification@mauvecorp.com

Document Version 1.0-SNAPSHOT
2022-10-06
[Commit 9420bce / main]

6.2.5. Cryptographic Services

FCS_COP.1/Hash
Cryptographic operation

FCS_COP.1.1/Hash	The TSF shall perform hash value calculation in accordance with a specified cryptographic algorithm ~~SHA-1,~~ SHA-256, SHA-512[8] and cryptographic key sizes none that meet the following: FIPS PUB 180-4 [FIPS PUB 180-4].

FCS_COP.1/HMAC
Cryptographic operation

FCS_COP.1.1/HMAC	The TSF shall perform HMAC value generation and verification in accordance with a specified cryptographic algorithm HMAC with ~~SHA-1,~~ SHA-256[9] and cryptographic key sizes 160 and 256 bit[10] that meet the following: FIPS PUB 180-4 [FIPS PUB 180-4], RFC 2404 [RFC 2404], RFC 4868 [RFC 4868], RFC 5996 [RFC 5996].

FCS_CKM.1
Cryptographic key generation

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm PRF-HMAC-SHA256[11] and specified cryptographic key sizes 256 bit[12] that meet the following: TR-03116 [TR-03116-1].

The following algorithms and preferences are supported for TLS key negotiation

- **Diffie-Hellman Group 14 according to RFC 3526 [RFC 3526] for key establishment during TLS**
- **DH exponent shall have a minimum length of 384 bits**
- **Forward secrecy shall be provided**
- **Ephemeral elliptic curve DH key exchange supports the P-256 and the P-384 curves according to FIPS186-4 [FIPS PUB 186-2] as well as the brainpoolP256r1 and the brainpoolP384r1 curves according to RFC 5639 and RFC 7027 [RFC 5639; RFC 7027]**
- **Peer authentication (if required): X.509 certificate with RSA 2048 bit keys**

[8] Assignment: *list of SHA-2 Algorithms with more than 256 bit size*
[9] Assignment: *list of SHA-2 Algorithms with 256bit size or more*
[10] Assignment: *cryptographic key sizes*
[11] Assignment: *cryptographic key generation algorithm*
[12] Assignment: *cryptographic key sizes*

n-doc Key features

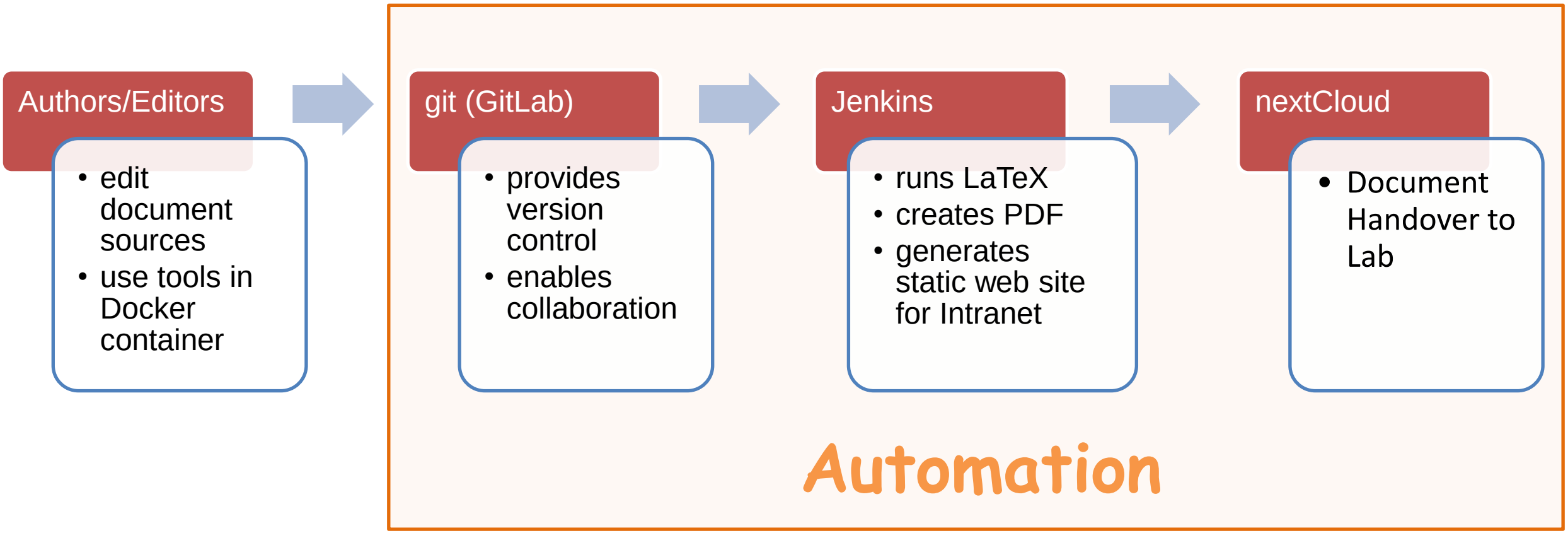
TOE model in a relational database

LaTeX as typesetting tool

Best practices of software engineering

Automation

Continuous Delivery of Documents



Pain Points (developer Perspective)

Insufficient/Incompatible tooling mandated by enterprise policies and ALC

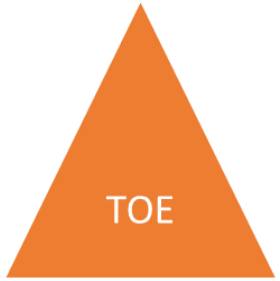
- ALC restrictions prevent using cloud-based tools such as bug trackers
- Office documents are sent by email, all processing is manual
- Developers/Labs/CABs rely on decades-old, outdated Office templates
- Software Developers are not necessarily familiar with Office tools

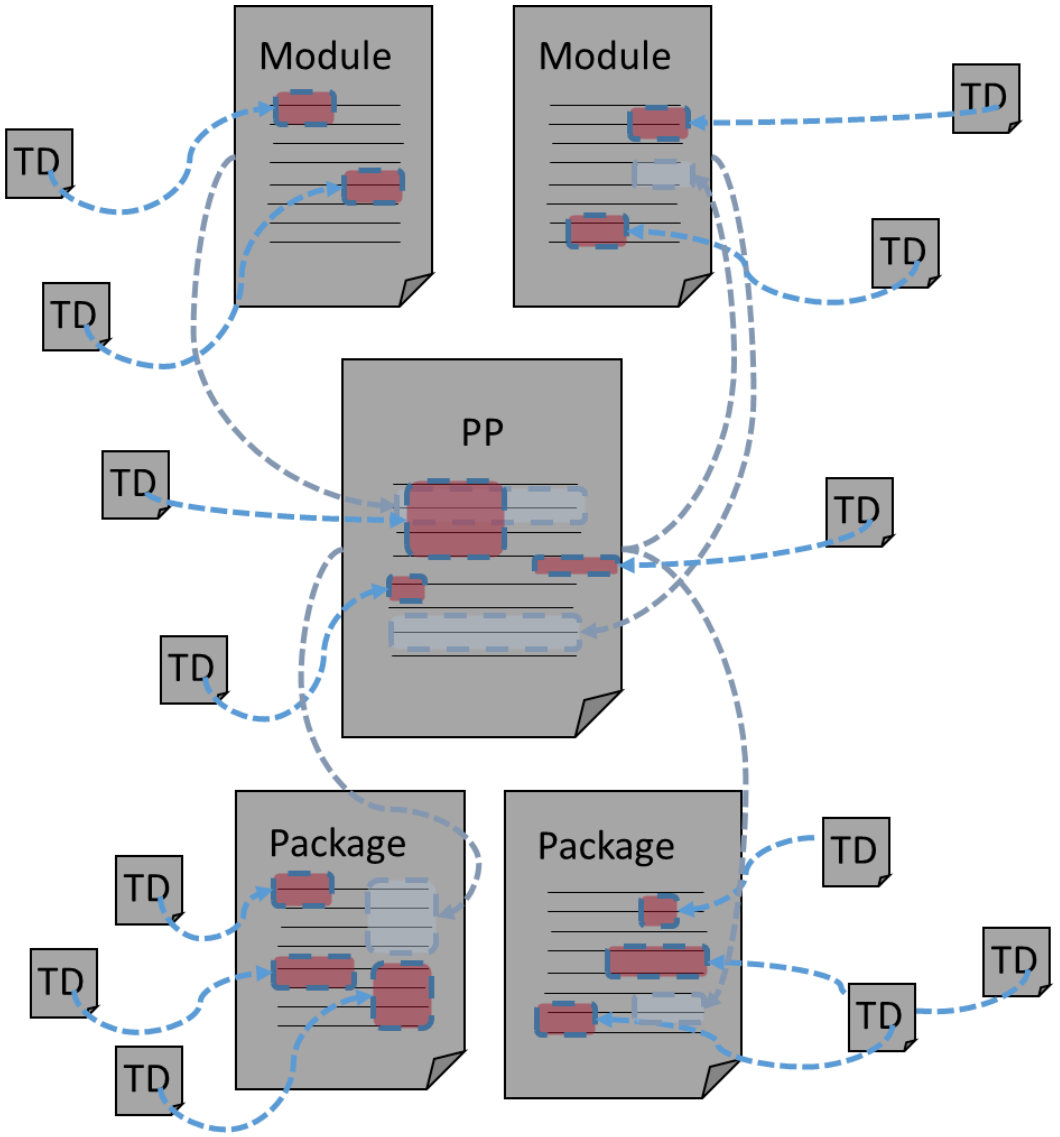
=> Automation not only saves time but ensures reliability: fewer manual, error-prone tasks

=> CC can learn a lot from software engineering: Automation comes natural to software engineers

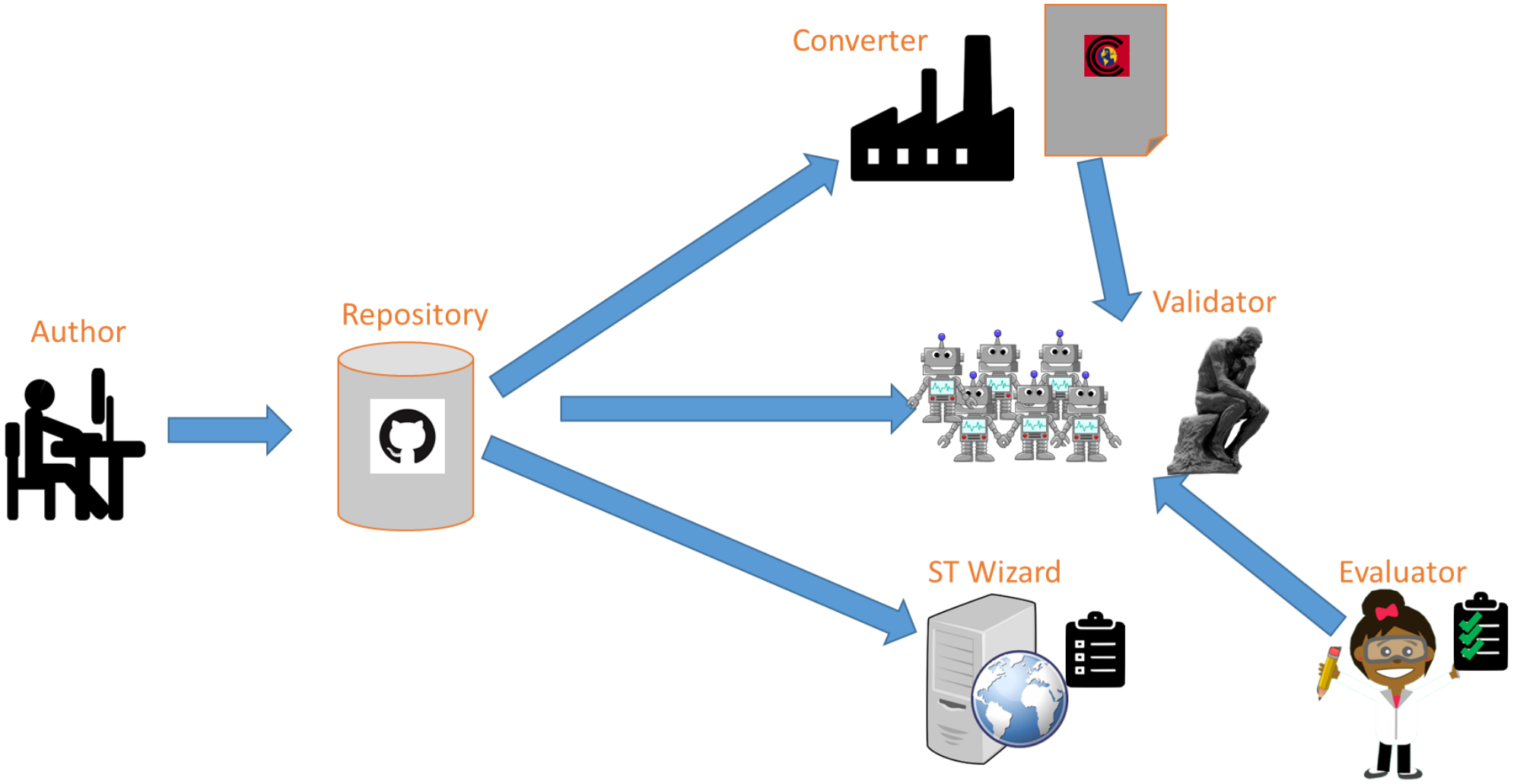
CGM CompuGroup Medical

The Challenge – Part 1





The Challenge – Part 1



Panel M31b: Is Automation Necessary for the CC Survival?

QUESTIONS?

jtsec BEYOND IT SECURITY
riscure
NIAP
CGM CompuGroup Medical
Lightship Security