Dokumentationswerkzeuge für Sicherheitszertifizierungen

Alexander Krumeich

Die Kompetenz in eHealth

KoCoBox MED+

eHealth Konnektor für die Telematikinfrastruktur

Entwicklung und Test der Anwendungssoftware

Zertifizierung nach Common Criteria EAL 3+

Fachliche Herausforderungen

Hohe Sicherheitsanforderungen
ca. 130 Sicherheitsfunktionale Requirements (SFR)

Komplexer Evaluierungsgegenstand (EVG)
160 Module, 23 Subsysteme,
66 Außenschnittstellen (TSFI)

Umfangreiche Dokumentation
15 Dokumente, ca. 3.000 Seiten

Herausforderungen an Technik und Organisation

Koordination der gemeinsamen Arbeit

Versionierung sichert Nachvollziehbarkeit

Konsistenz in Inhalt und Form

Navigation durch generierte Hyperlinks

Akzeptanz bei Autorinnen und Autoren

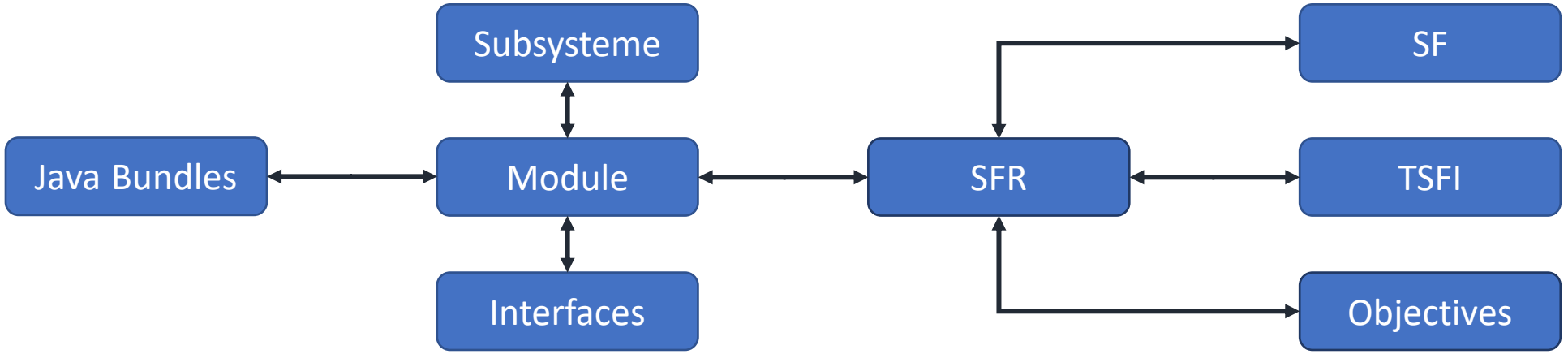
Entwicklung einer eigenen Plattform **n-doc**

Datenbankbasiertes Modell des EVG

LaTeX als Dokumentationswerkzeug

Best Practices des Software-Engineering

Modell des Evaluierungsgegenstandes in einer relationen Datenbank



Wir gewinnen Sicherheit über Zuschnitt und Relationen.

„Unentdeckte“ Relationen erkennen und nutzen

Verwendung der Datenbank

Innerhalb der Dokumente

Konsistenz der Terminologie sichern

Generieren von Tabellen und Querverweisen

Als eigenständiges Dokument

Auslieferung der Datenbank an den Evaluator

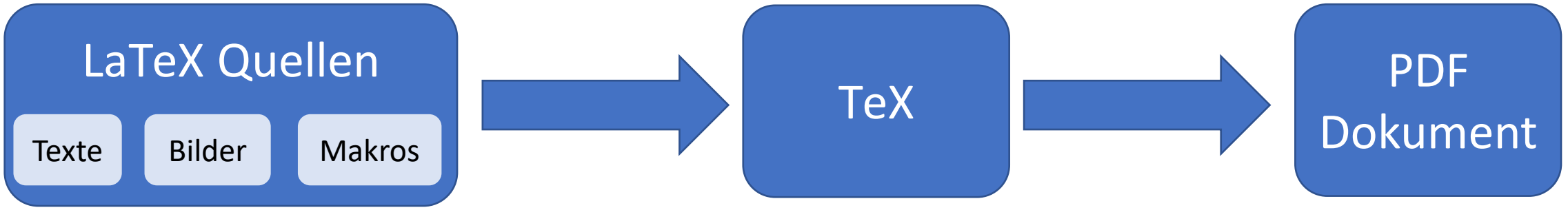
LaTeX

Textsatzsystem im akademischen Umfeld

40 Jahre alt – aber kein bisschen müde

Arbeitsablauf bekannt aus Softwareentwicklung

Allgemeiner LaTeX Workflow



LaTeX liest Textdateien und produziert PDF

Formatierung und Struktur durch Makros

```
\textit{Dieser Text wird kursiv}
\section{Überschrift}
```

Domänenspezifische Makros

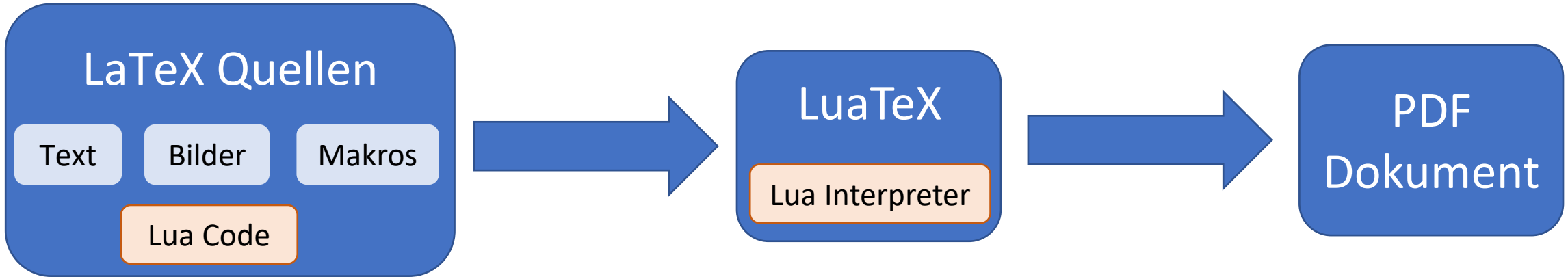
`\keyword{}` für Schlüsselwörter

`\kocobox{}` Name des Produkts

`\tds{}` Subsystem, Modul oder Interface

Semantisches Markup

LuaTeX Workflow

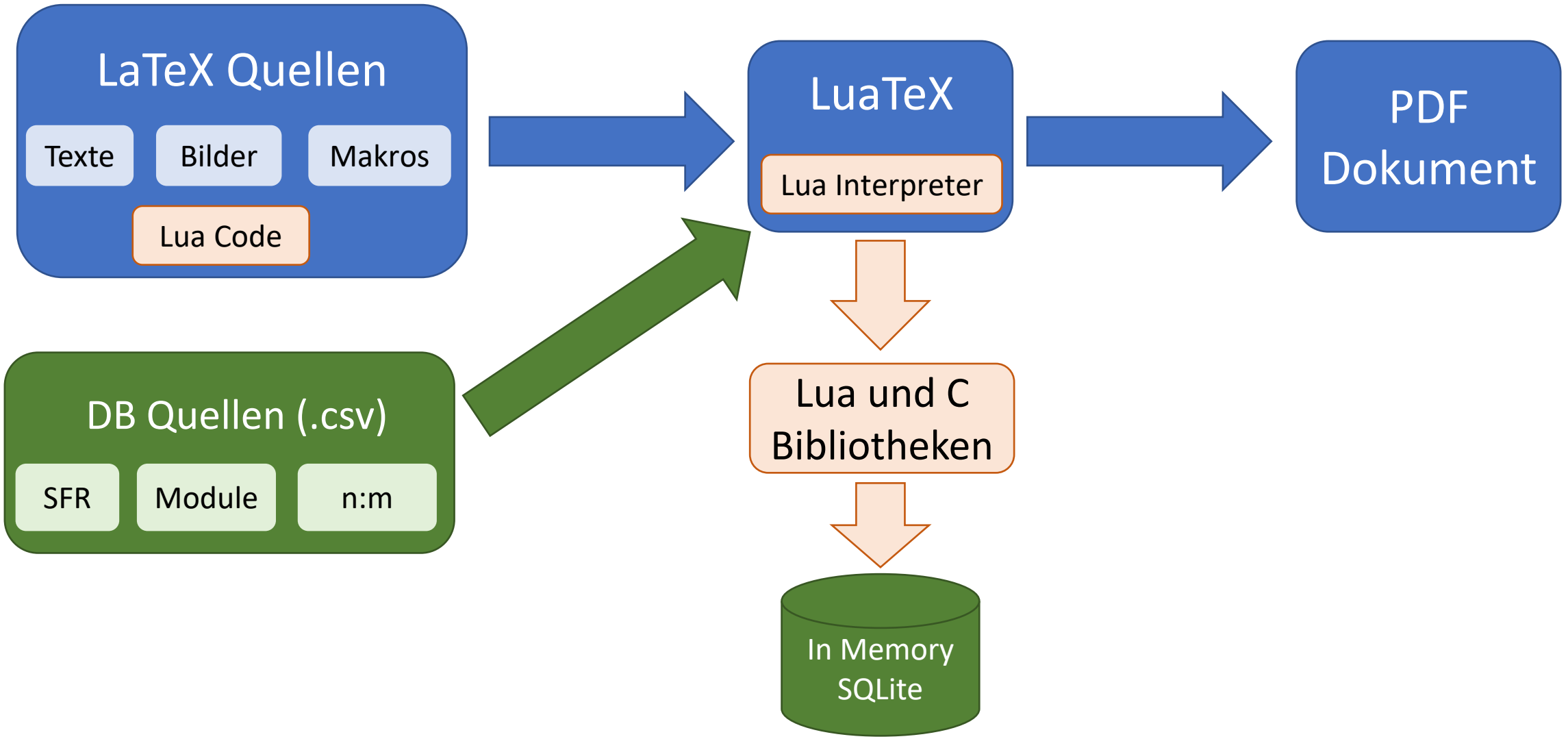


Der Lua Interpreter führt Programme aus

Text kann programmatisch erstellt werden

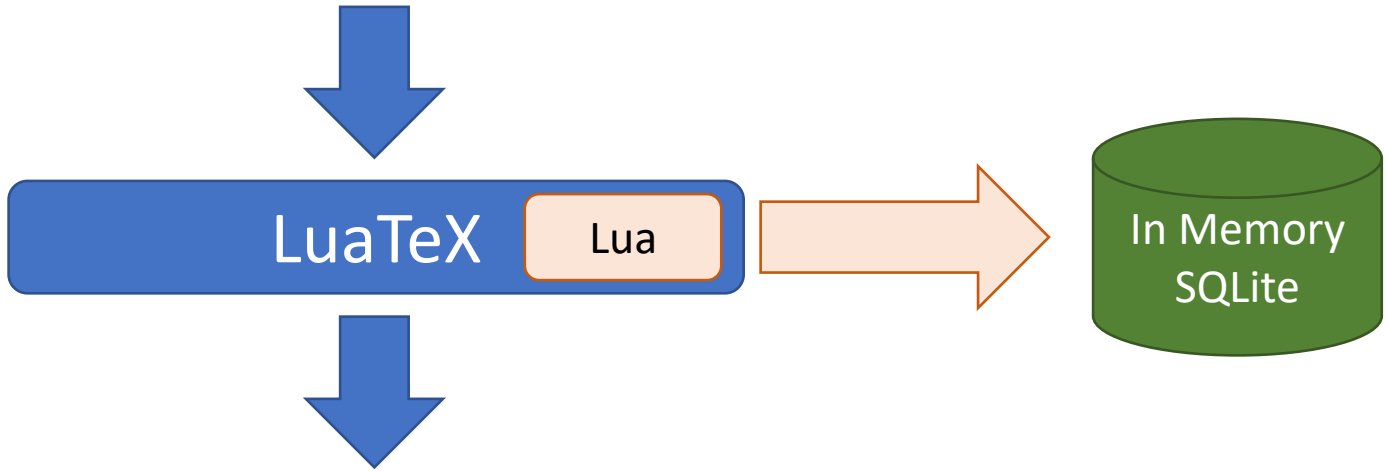
Zugriff auf Bibliotheken und Systeme

n-doc Workflow



Konsistenz in der Terminologie sichern

```
\tds{mod.aas.core}
```




```
AccessAuthorizationService::Core
```

Generieren von Text und Tabellen

Programmatisch generierter Text

Automatisch generierte Hyperlinks

3.14.1. Modul AccessAuthorizationService::Core

Für den Gesamtkonnektor: SFR-enforcing
Für den Netzkonnektor: non-TSF

Das Modul erfüllt die Anforderungen, die durch die SFR in Tabelle 3.348 an den EVG gestellt werden.

Enforcing SFR		
FDP_ACC.1/AK.Infomod	FDP_ACF.1/AK.KD	FMT_MTD.1/AK.eHKT_Abf
FDP_ACC.1/AK.KD	FMT_MSA.1/AK.Infomod	FMT_SMF.1/AK
FDP_ACF.1/AK.Infomod	FMT_MSA.3/AK.Infomod	FPT_FLS.1/AK
Supporting SFR		
FDP_ACC.1/AK.Sgen	FDP_ACF.1/AK.Sgen	
FDP_ACC.1/AK.SigPr	FDP_ACF.1/AK.SigPr	

Tabelle 3.348.: SFR des Moduls AccessAuthorizationService::Core

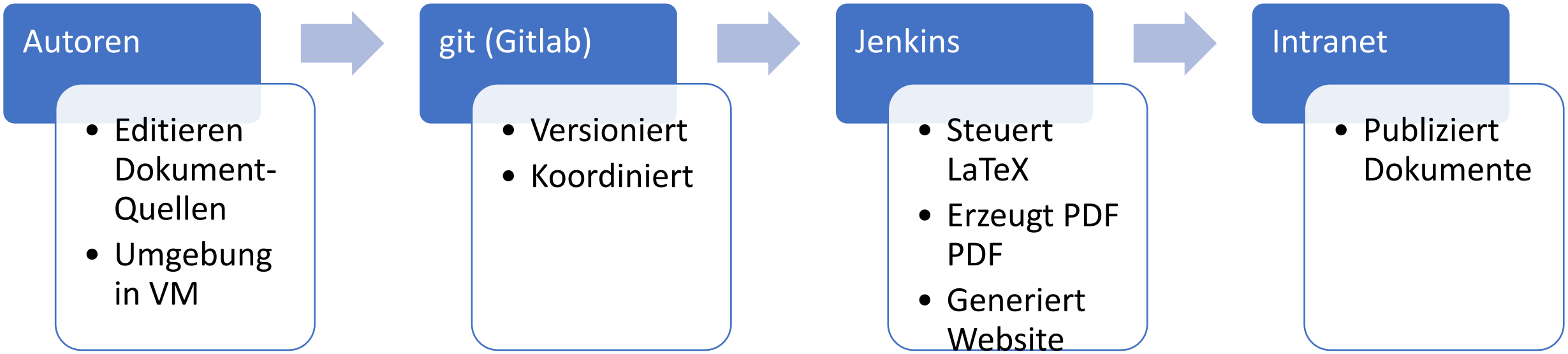
Generieren von Text und Tabellen

Programmatisch generierter Text

Automatisch generierte Hyperlinks

SFR	Relation	Subsystem::Modul
FDP_ACC.1/AK.eHKT	Enforcing	CardService::de.ndesign.koco.ifd.sicct
		Systembibliotheken und Werkzeuge::JRE
	Supporting	CardService::CardTerminalService
		SystemInformationService::Core
FDP_ACC.1/AK.Enc	Enforcing	CertificateService::Core
		EncryptionService::Core
	Supporting	(Keine)
FDP_ACC.1/AK.Infomod	Enforcing	AccessAuthorizationService::Core
	Supporting	(Keine)
FDP_ACC.1/AK.KD	Enforcing	AccessAuthorizationService::Core
	Supporting	CardService::Core

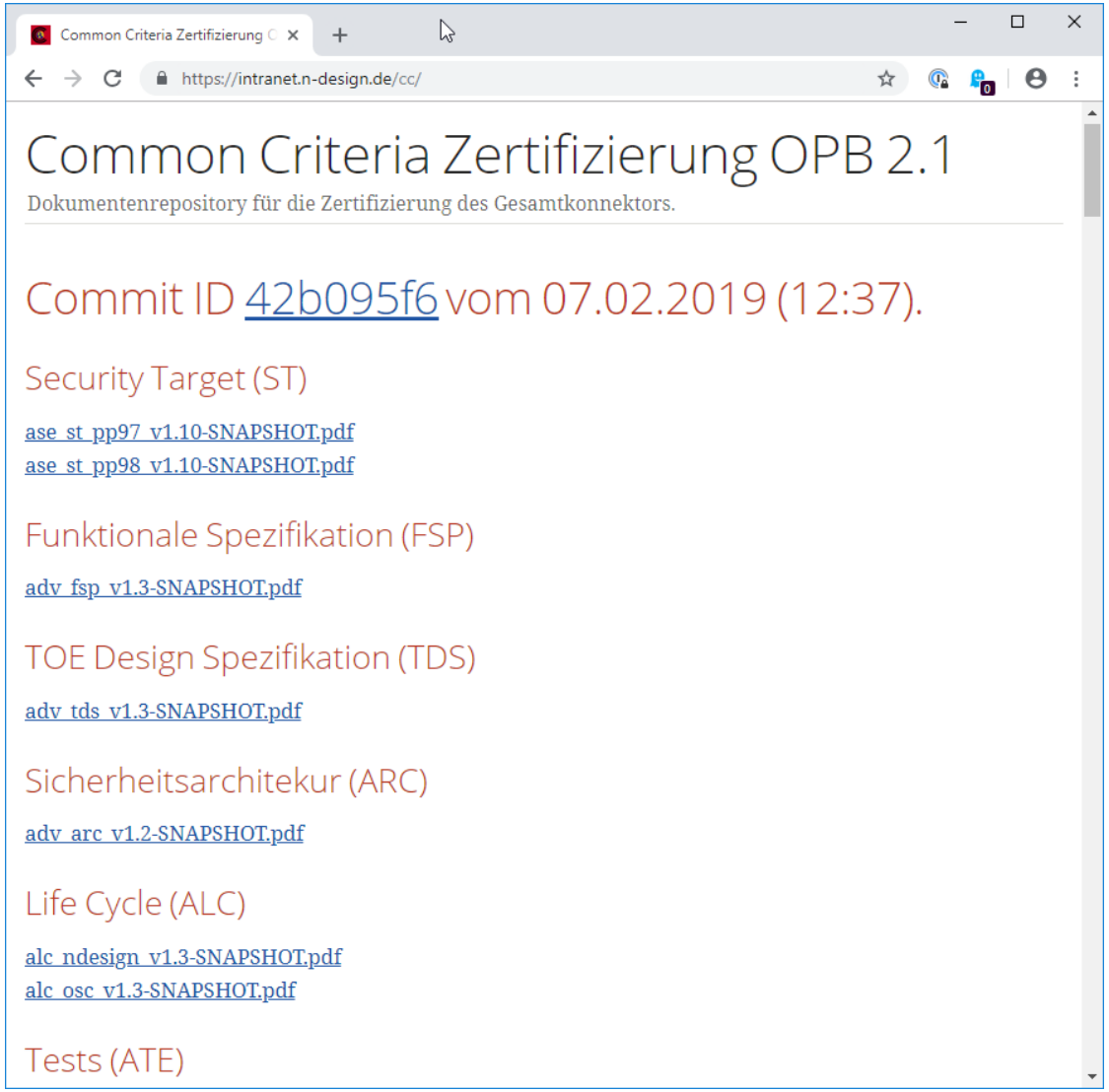
Continuous Delivery der Dokumente

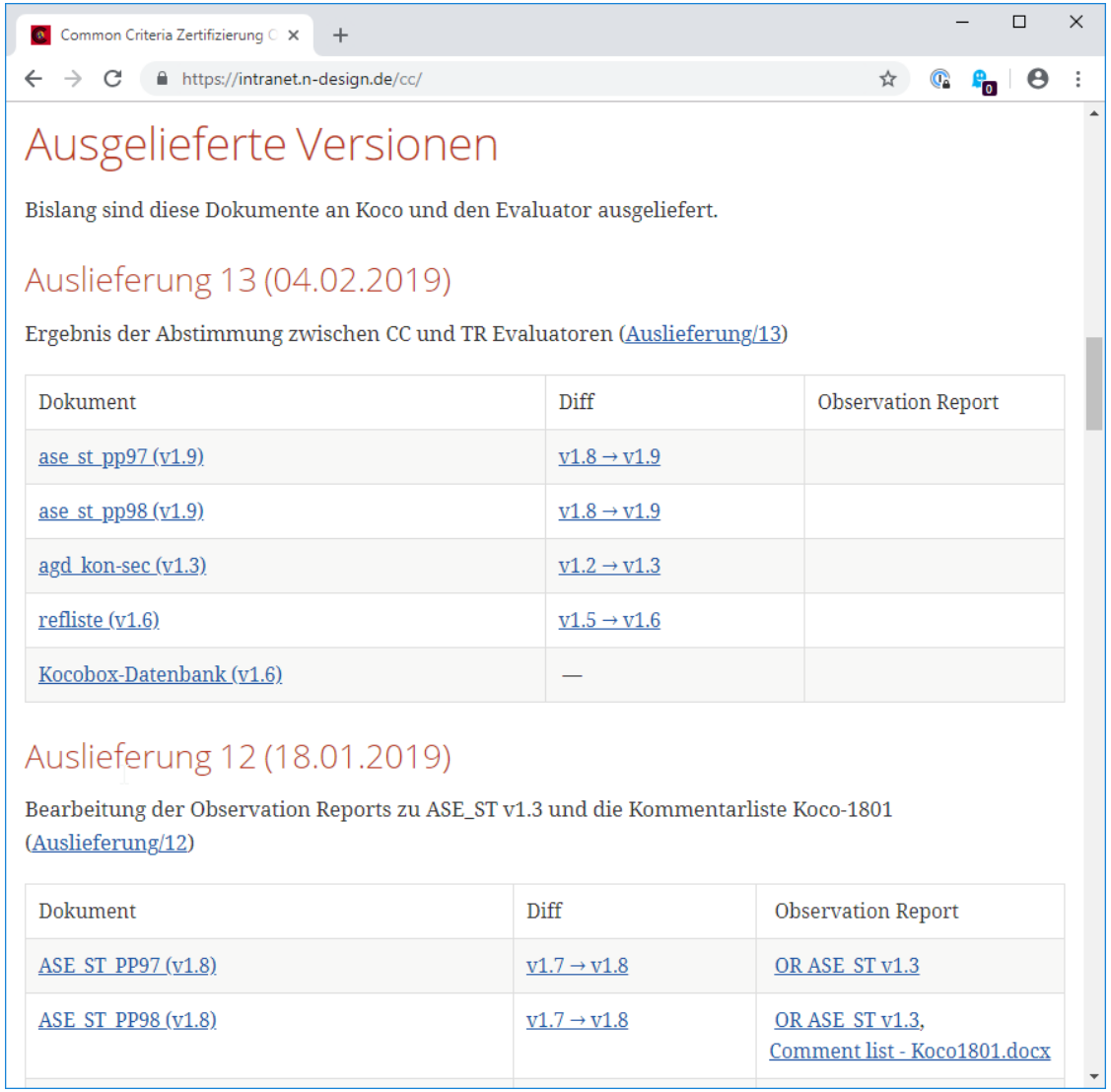


„Wo liegt die aktuelle Version?“

„Was haben wir bisher ausgeliefert?“

Intranet Website





Schlussbetrachtung

Skalierbarkeit

Effizienz / Wirtschaftlichkeit

Akzeptanz

Kundenzufriedenheit

Vielen Dank!

Fragen?

alexander.krumeich@n-design.de
+49 221 222896-16