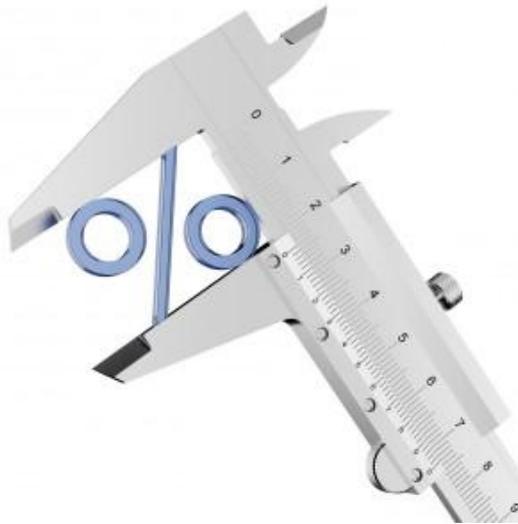


# OPTET



Operational Trustworthiness Enabling Technologies



## Vertrauenswürdigkeit von Software

Sandro Hartenstein  
FH Brandenburg





# Agenda

- Vorstellung OPTET
- Vertrauenswürdige Software
  - Ermittlung von Attributen
  - Messen der Vertrauenswürdigkeit
- Prototyp
- Ausblick



# OPTET

- FP7 EU-Projekt
- Projektdauer: 3 Jahre
- Start: 1. November 2012
- Fördersumme insgesamt 7,1 Millionen €
- Budget der FH Brandenburg: 321,779€
- 793,5 Personen Monate
- 15 Projektpartner
- 4 Universitäten





# OPTET

- Projektpartner



THALES



UNIVERSITY OF  
Southampton



MLstate



Weiterführende Informationen: [www.optet.eu](http://www.optet.eu)



# Zielsetzung

- Entwicklung von Strukturen für die Erstellung, Auswahl und den Betrieb von nachweislich vertrauenswürdigen Internet-basierten Anwendungen.

Entwicklungsphase

Zertifizierungsphase

Betriebsphase



# Schwerpunkte

- Wie kann im Entwicklungsprozess nachweislich vertrauenswürdige Software entstehen?
- Wie kann eine Zertifizierung diese Vertrauenswürdigkeit nachvollziehen?
- Wie ist in der Betriebsphase die Vertrauenswürdigkeit aufrechtzuerhalten?



# Aufgaben vom FHB-Team

- Die Fachhochschule Brandenburg bringt ihre Kompetenz im Bereich "Metriken" und "sichere Software-Entwicklung" in das Projekt ein.
- Die Messbarkeit von Softwarekomponenten stehen im Vordergrund



# Der OPTET Ansatz

## The OPTET Approach

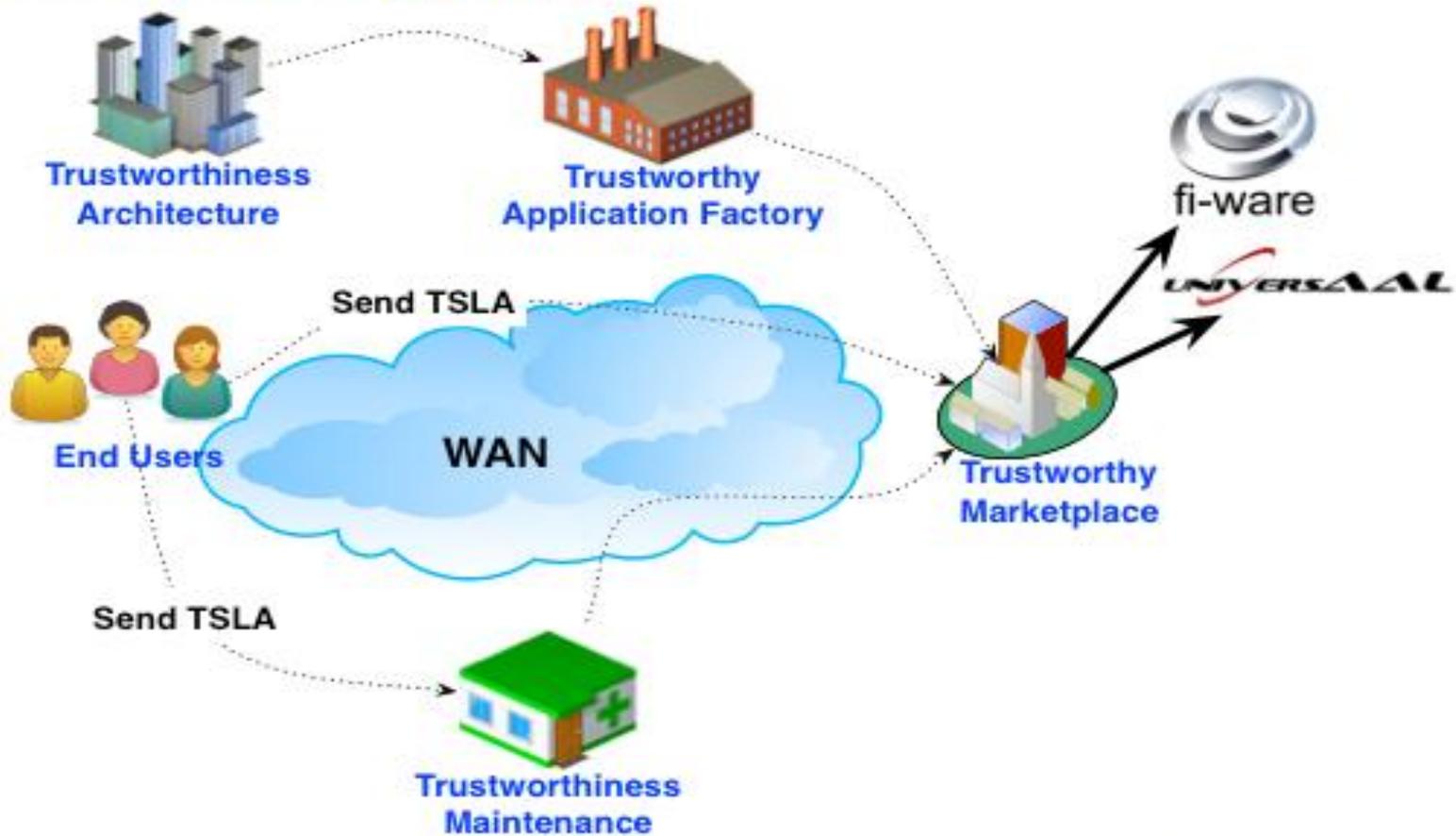


Figure 1 OPTET Lifecycle

# OPTET



Operational Trustworthiness Enabling Technologies

## VERTRAUENSWÜRDIGE SOFTWARE



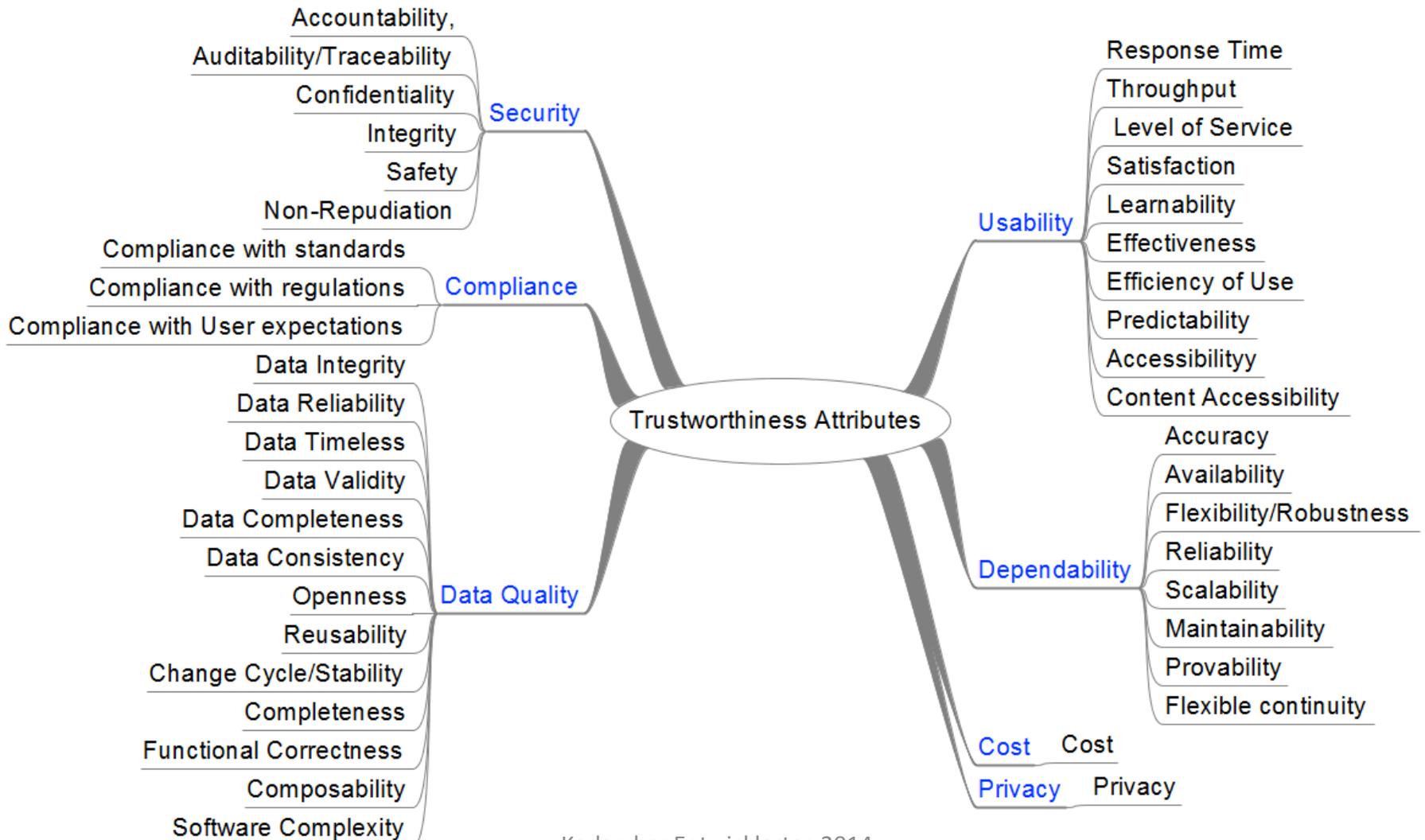


# Vertrauenswürdige Software

- Vertrauenswürdige Software
  - Vertrauenswürdigkeit der Software
  - Vertrauenswürdigkeit des Entwicklungsprozesses
  - Subjektiv
  - Ziel: Software in Bezug auf Vertrauenswürdigkeit vergleichbar zu bewerten.



# Attribute für Vertrauenswürdigkeit





# Messung der Vertrauenswürdigkeit

- Mit Metriken realisiert
  - derzeit 127 Metriken entwickelt
  - angestrebte Ergebnisse in Prozent
- Entwicklung der Metriken mit Goal Question Methode
- Einbeziehung gängiger Standards und Best Practice der Software Qualität
- Zusammenfassung der Metrikergebnisse auf Attributebene
- Zusammenfassung bis auf Einzelwert möglich (z.B Software A : 75% trustworthiness)



# Beispiel Produktmetrik

<b>Metric Info ID</b>	<b>154</b>
<b>Attribute</b>	<b>Confidentiality</b>
MetricID	APP-RUN-transitencr-01
Name	Confidentiality addressed transit
Description	It should be displayed as a percentage, how much data is encrypted transferred
Metric	% Of the data which is encrypted transferred
Metric_computation	$x = (\text{sum of encrypted transferred data} / \text{sum of transferred data}) * 100\%$
Formula	$X = A / B * 100$

# OPTET



Operational Trustworthiness Enabling Technologies

## PROTOTYP



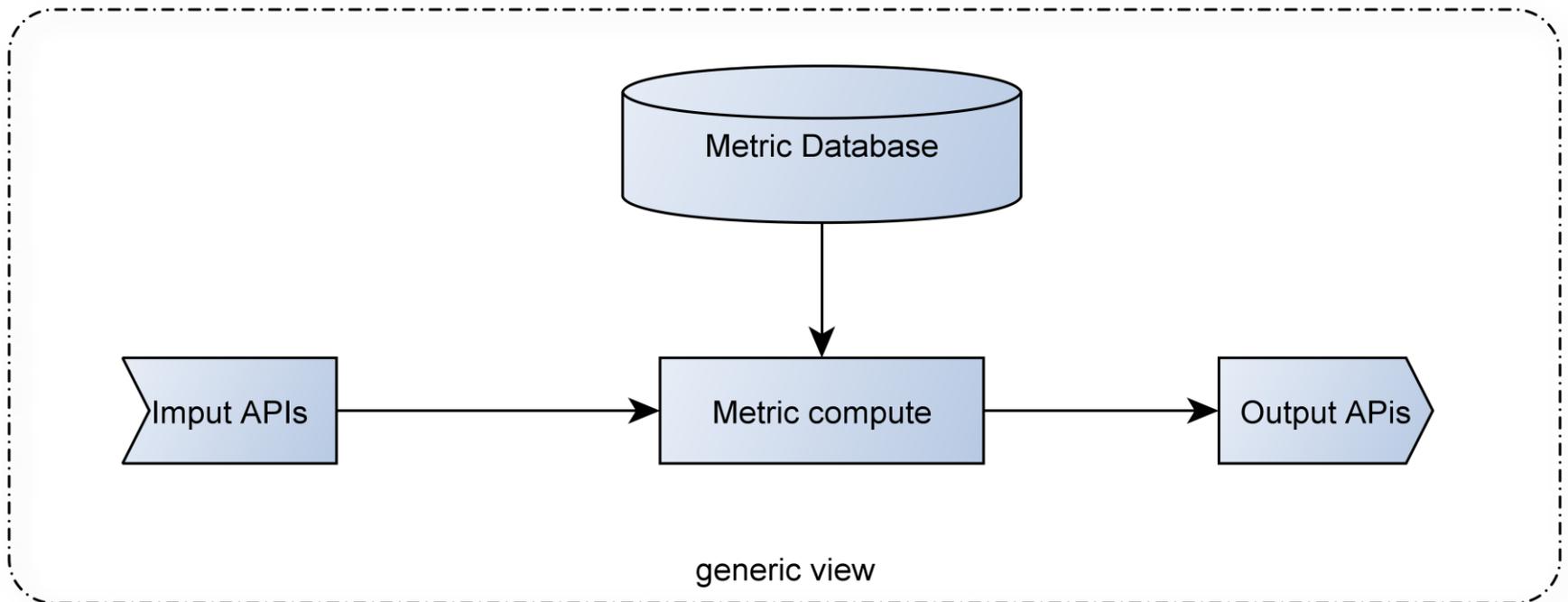


# Prototyp

- Berechnung
  - generisch
  - automatisch
  - der
    - Metriken
    - Attribute
    - Objectives
- Bereitstellung eines Repositories für Metriken
- Abbildung der Kategorisierung
  - Attributes
  - Objectives



# Prototyp





# Prototyp

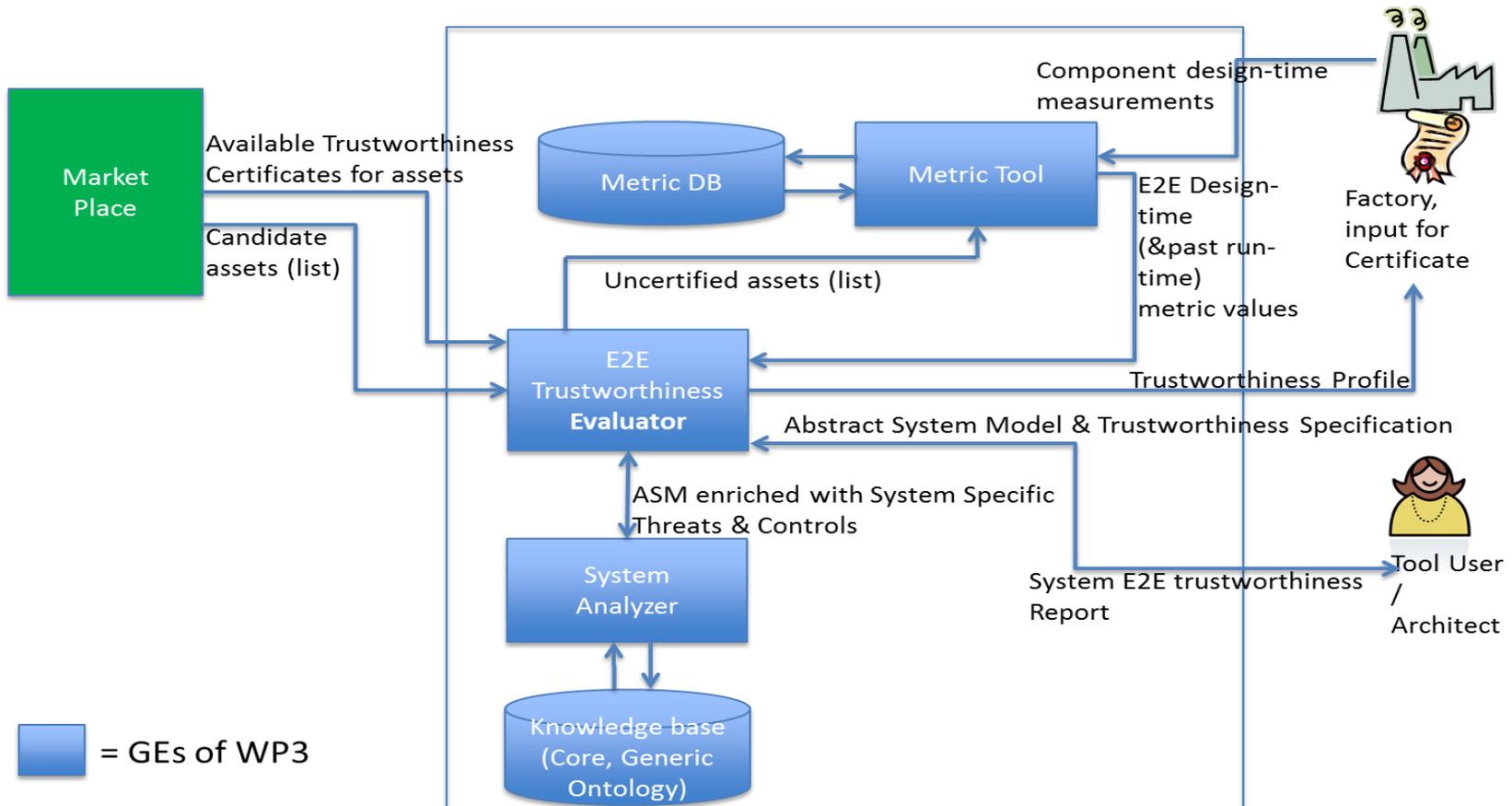
- Verwaltung des Repository durch Webfrontend
- Formeln sind zur Laufzeit erweiterbar
- Restful API zur Berechnung durch Komponenten des Projektes
  - Entwicklung (TW End To End Evaluator)
  - Marktplatz (Entscheidungssystem)
  - Runtime (Systemmonitor)





# Verwendung des Prototypen

- End 2 End TW Evaluator



# OPTET



Operational Trustworthiness Enabling Technologies

## AUSBLICK





# Ausblick: Vertrauenswürdigkeit des Entwicklungsprozesses

governance

requirements

design

coding

testing

deploy

support

- Ermittlung von Qualitätsfaktoren
  - Top Down
    - Common Criteria ISO 15408
    - SSE-CMM ISO 21827
    - BSIMM/ OpenSAMM
    - Microsoft SDL
    - OWASP CLASP
    - ...
  - Botton up
    - Verifizierung und Erweiterung
  - Umfrage
    - Verifizierung
- Messen von Qualitätsfaktoren
  - Via Metriken
  - Entwicklung mit GQM



# Ausblick: Vertrauenswürdigkeit des Entwicklungsprozesses

governance

requirements

design

coding

testing

deploy

support

- employees
- iterative
- policies and processes
- legal



# Ausblick: Vertrauenswürdigkeit des Entwicklungsprozesses

governance

requirements

design

coding

testing

deploy

support

- completeness
- consistent
- user oriented
- validated / traceable
- legal
- precise



# Ausblick: Vertrauenswürdigkeit des Entwicklungsprozesses



- simple
- traceable
- pattern based
- completeness



# Ausblick: Vertrauenswürdigkeit des Entwicklungsprozesses



- code generation
- documented
- error free
- verifiable



# Ausblick: Vertrauenswürdigkeit des Entwicklungsprozesses



- test coverage
- requirement coverage
- auditable
- fuzz coverage
- integration test coverage



# Ausblick: Vertrauenswürdigkeit des Entwicklungsprozesses



- documented
- Integrity
- customizable
- recorded



# Ausblick: Vertrauenswürdigkeit des Entwicklungsprozesses

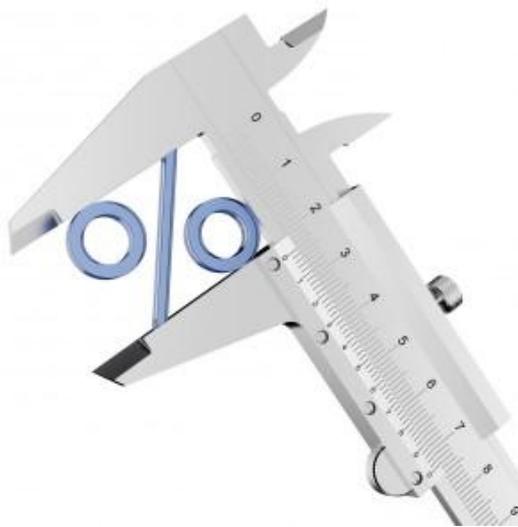


- user centricity
- competence
- effectiveness
- integrity
- reversible
- traceable

# OPTET



Operational Trustworthiness Enabling Technologies



**Vielen Dank für Ihre  
Aufmerksamkeit**

Sandro Hartenstein  
FH Brandenburg





**ET**  
ENTWICKLERTAG

**meet the SPEAKER  
@speakerlounge**



**1. OG DIREKT ÜBER DEM EMPFANG**