

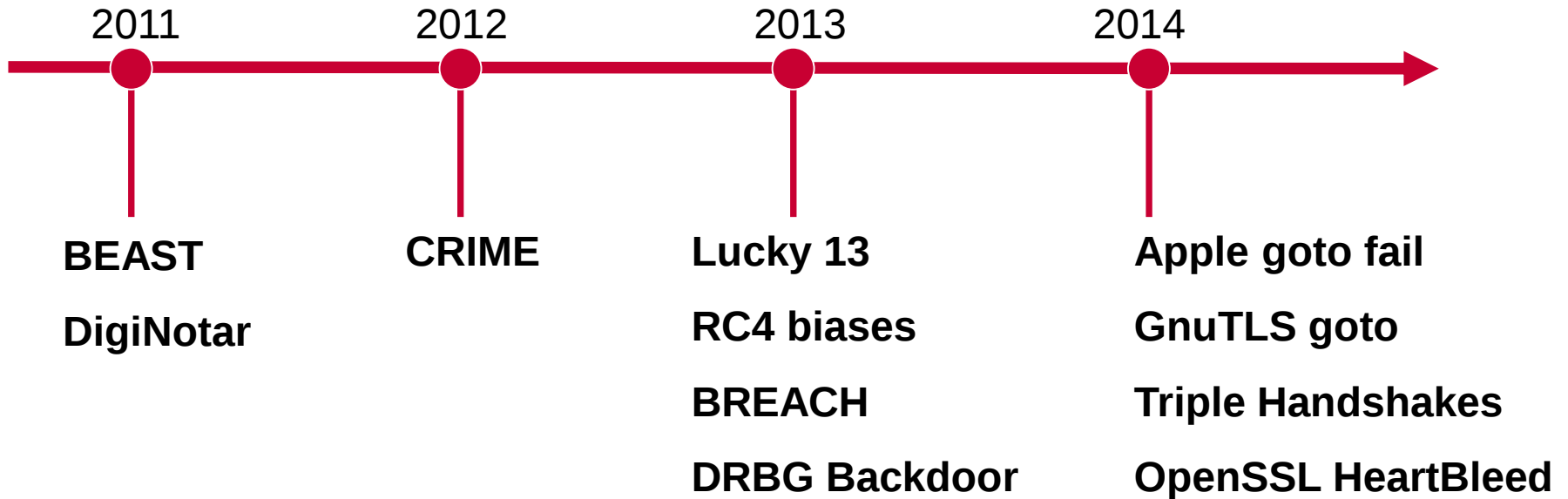
TeleTrust-interner Workshop

Berlin, 05.06.2014

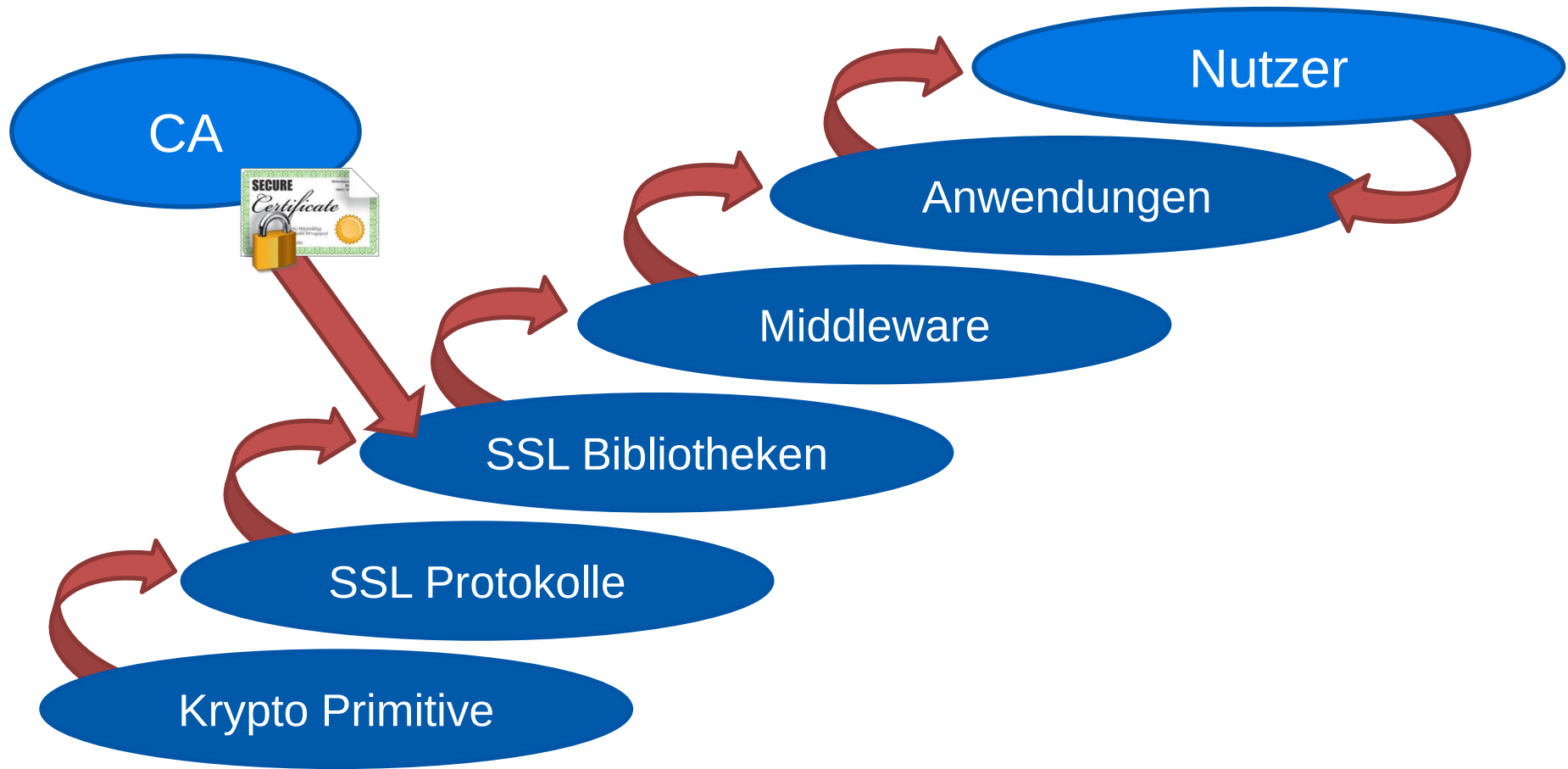
Wäre SSL mit System Security Engineering sicherer?

Christoph Weinmann
Secorvo Security Consulting GmbH

SSL kommt in Verruf



Komponenten der SSL-Implementierung



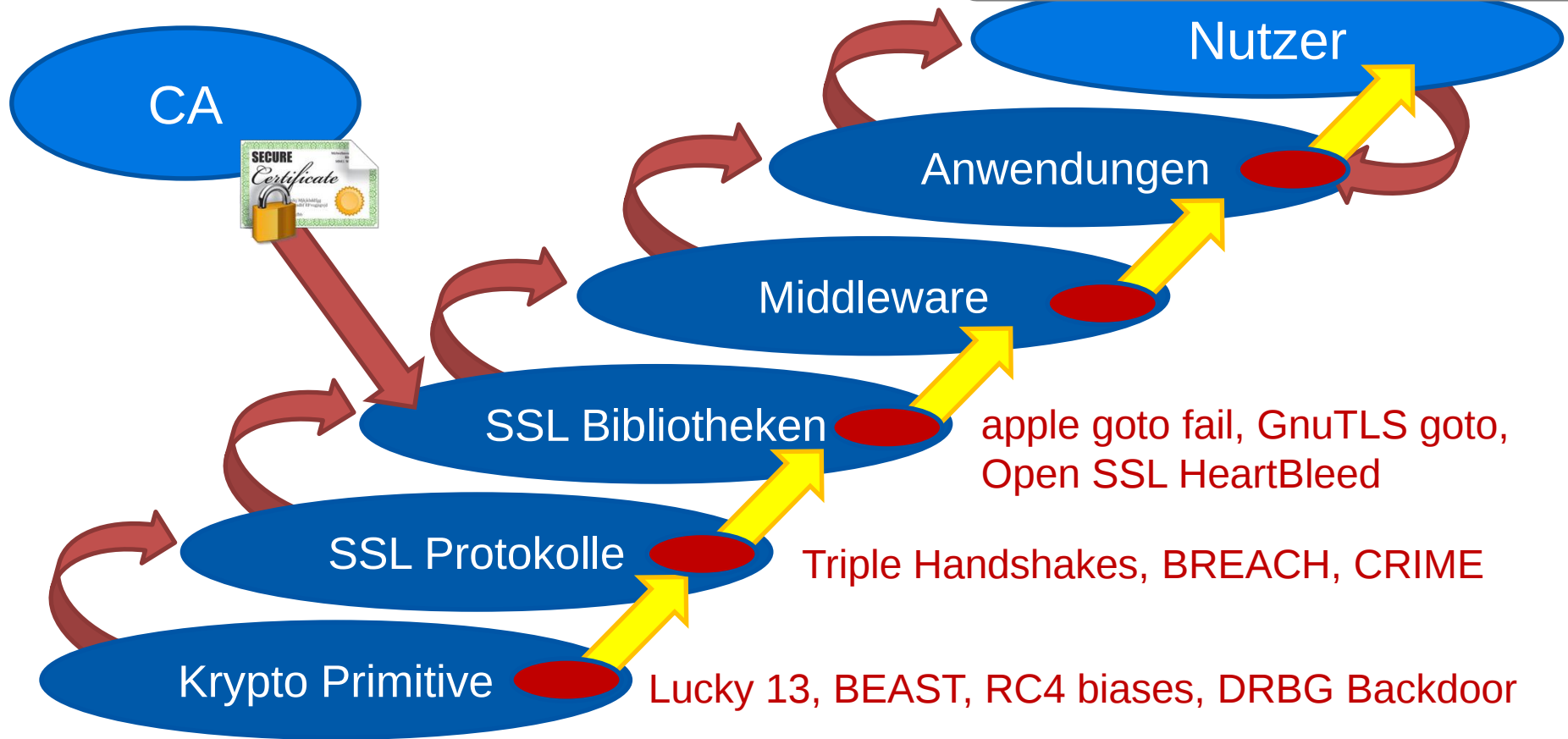
Auswirkungen der SSL-Schwachstellen



This Connection is Untrusted

You have asked Firefox to connect securely to _____, but we can't confirm your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove they are going to the right place. However, this site's identity can't be verified.





Wir sehen am Beispiel

■ Systeme ...

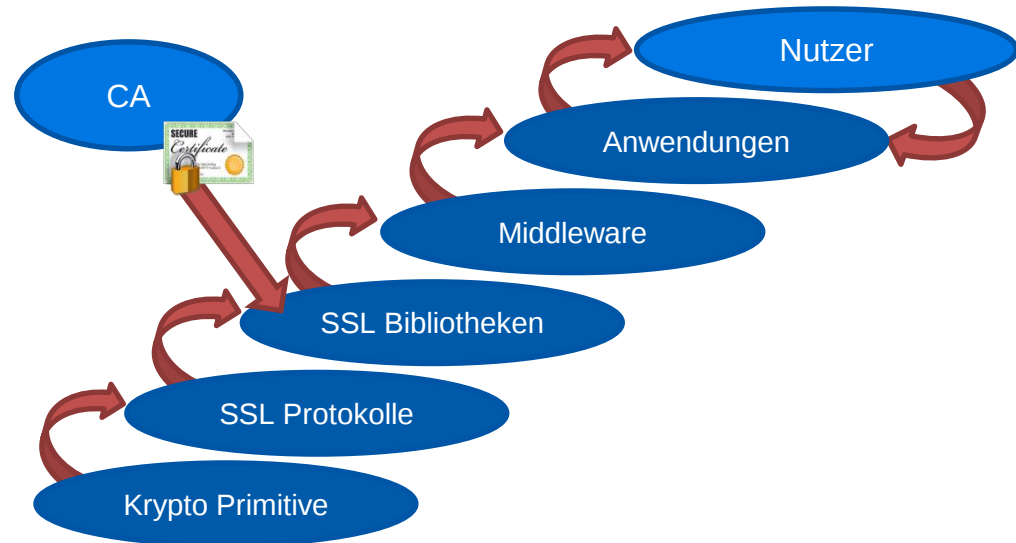


... bestehen aus vielen Komponenten

- Zusammenspiel der Komponenten ist in der Regel interdisziplinär

Wir sehen am Beispiel

■ Komponenten ...

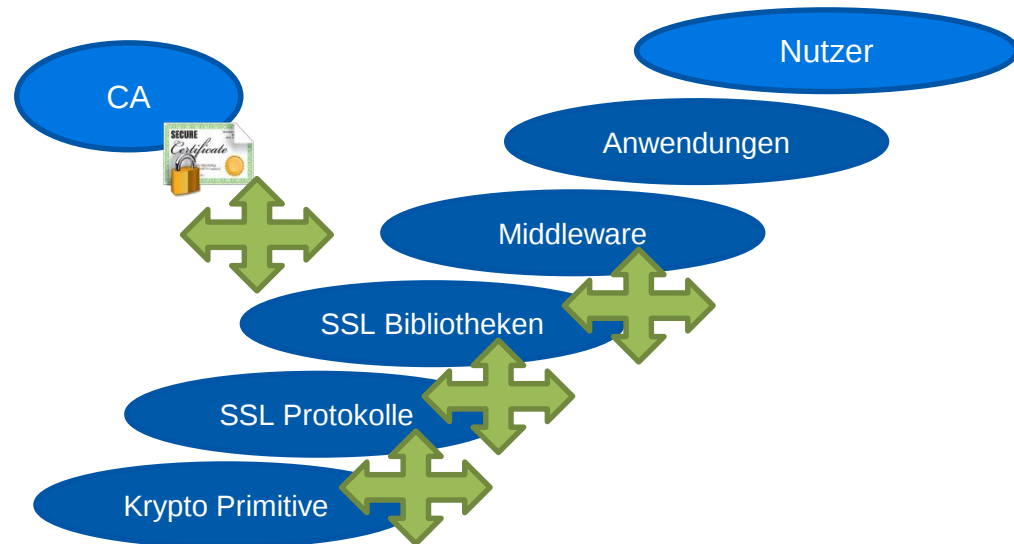


... interagieren

- Gegenseitige Beeinflussung
- Sichere Interaktion muss gewährleistet sein

Wir sehen am Beispiel

■ Komponenten ...

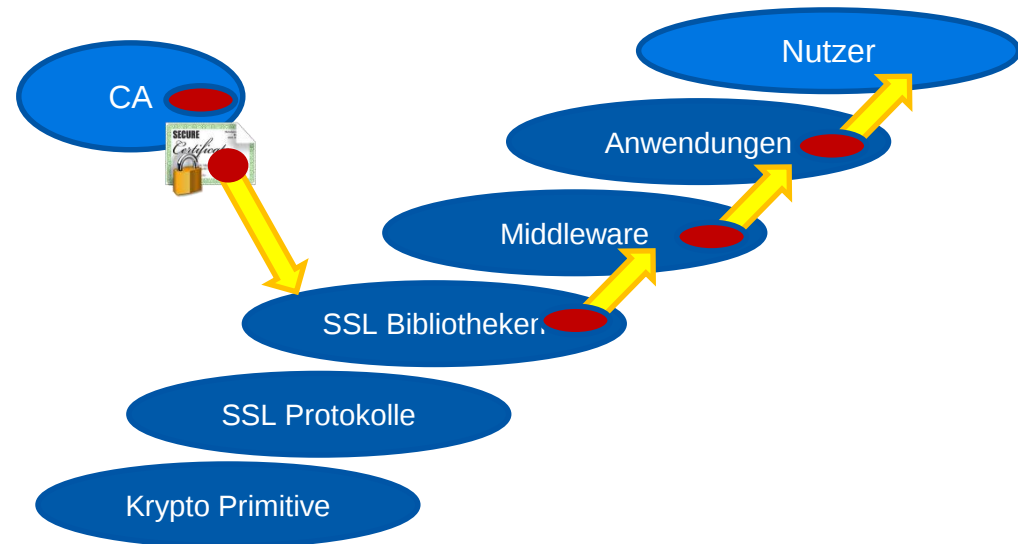


...arbeiten mit Annahmen über andere

- Sicherheit, Qualität, Leistung
- Annahmen sind notwendig

Wir sehen am Beispiel

■ Komponenten ...



- ... sind voneinander abhängig
- Fehler werden weitergegeben

System Security Engineering ...

... denkt immer an das gesamte System

- Überprüft die Relevanz von Sicherheit in jedem Entwicklungsschritt
- Identifiziert notwendige Sicherheitsmaßnahmen



Bildquelle: © Bigstock.com

System Security Engineering ...

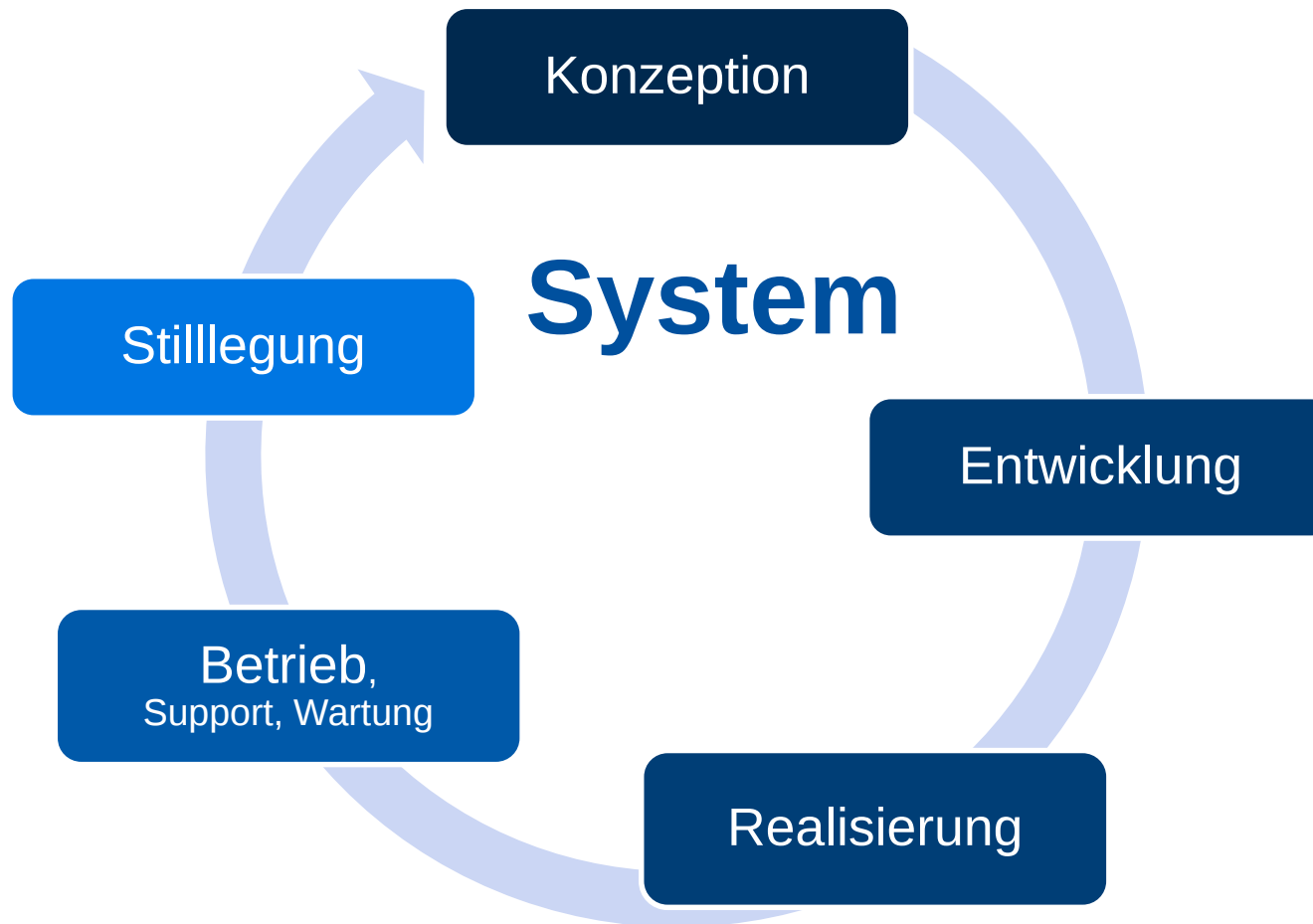
... denkt immer an das gesamte System

- Überprüft die Relevanz von Sicherheit in jedem Entwicklungsschritt
- Identifiziert notwendige Sicherheitsmaßnahmen
- Strebt Sicherheit in allen Komponenten an

➔ **Security built-in** anstatt ~~Security after thought~~

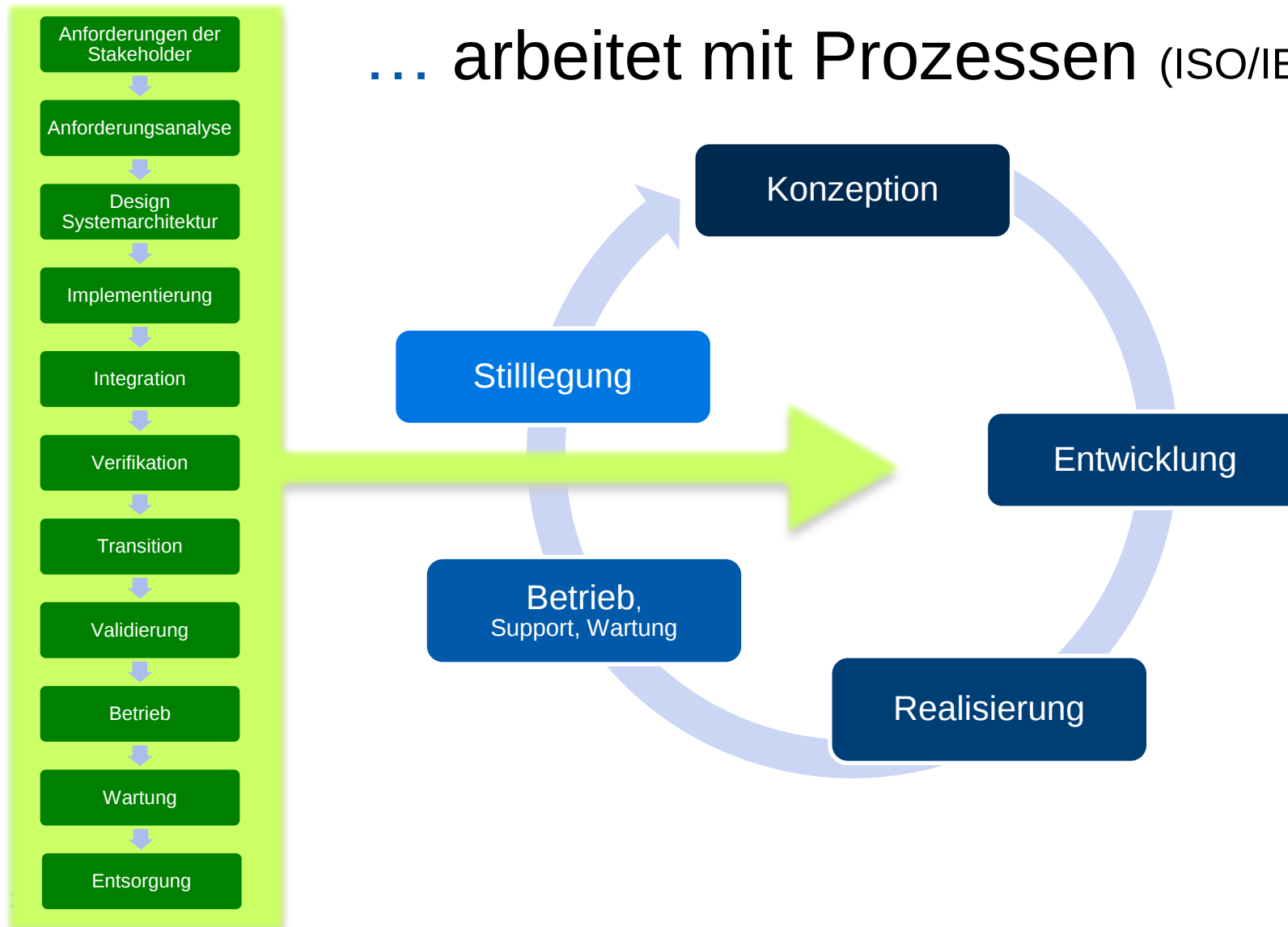
System Security Engineering ...

... stellt den Lebenszyklus ins Zentrum (NIST-SP800 160)



System Security Engineering ...

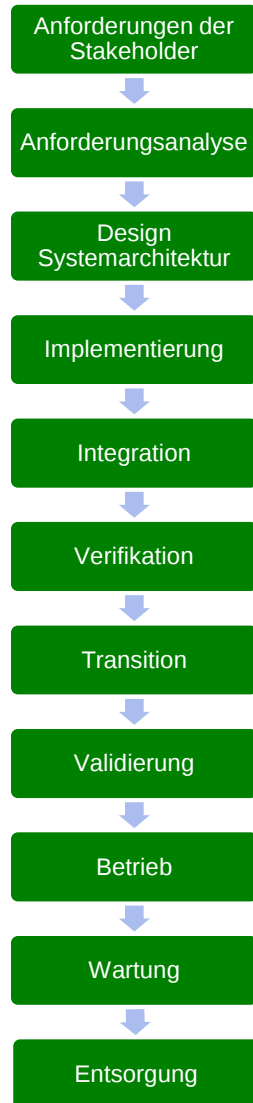
... arbeitet mit Prozessen (ISO/IEC 15288)



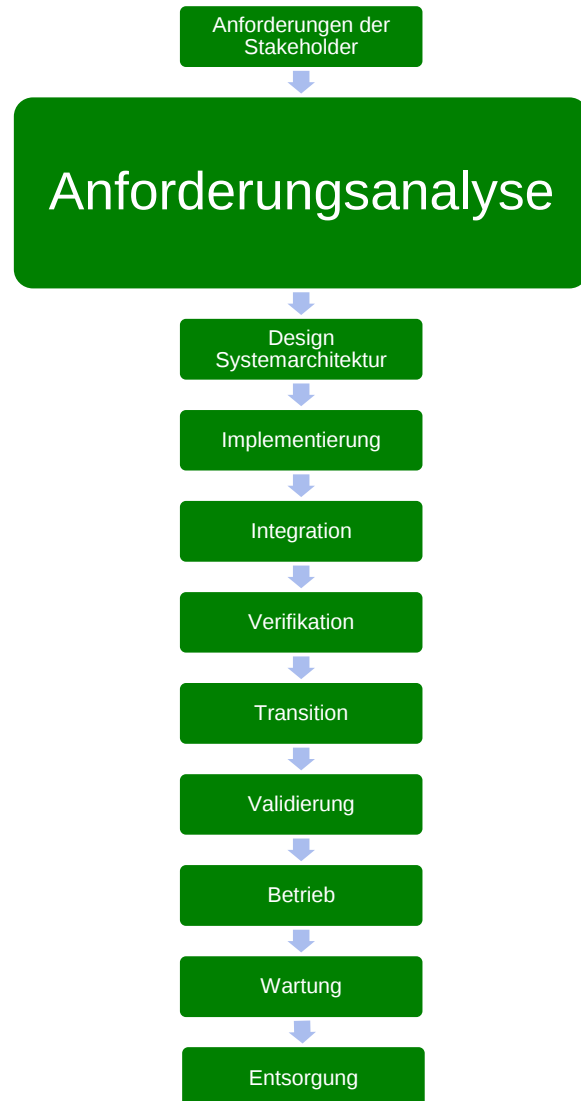
Was wäre bei SSL heute anders, ...

... hätte man System Security Engineering ...

Was wäre bei SSL heute anders, ...

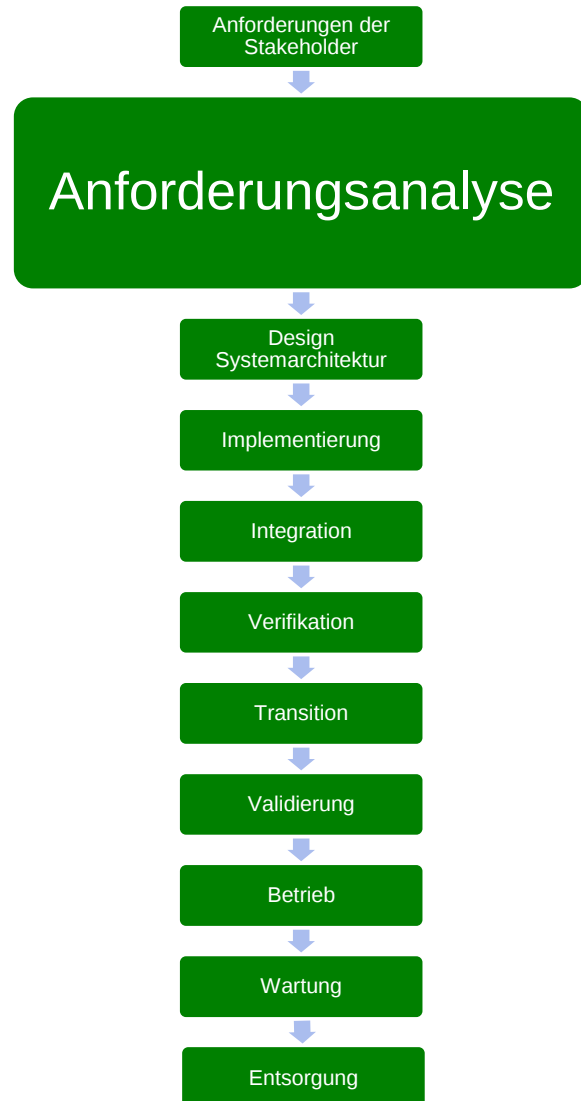


Was wäre bei SSL heute anders, ...



- Wenn die Anforderungen über das gesamte System sauber definiert werden, würde dies z. B. :
 - ermöglichen Sicherheitsziele über das gesamte System zu definieren
 - ermöglichen Annahmen zu verifizieren und konsolidieren
 - helfen die Qualität der Zertifikate zu verbessern

Was wäre bei SSL heute anders, ...



- Analysieren der Bedrohungen ermöglicht z. B. :
 - die Angriffsfläche systematisch zu analysieren, z. B. die Interaktion der Komponenten bei Triple Handshakes
 - die Angreifer zu analysieren, z. B. Motivation und Ressourcen der NSA

Was wäre bei SSL heute anders, ...



- Sichere Softwareentwicklungs-Prozesse sind etabliert und helfen z. B. :
 - Fehler bei der Implementierung zu vermeiden, siehe
 - Apple goto fail
 - GnuTLS goto
 - OpenSSL HeartBleed

System Security Engineering & TeleTrust?

■ Fragen

- Welche Schlussfolgerung ergeben sich daraus, dass aus Sicherheitssicht ein System immer mehr ist als die Summe seiner Komponenten?
- Welche Rolle kann System Security Engineering in der Arbeit der TeleTrust Mitglieder spielen?
- Ist ein Positionspapier sinnvoll?



TeleTrust Engineer System Security