

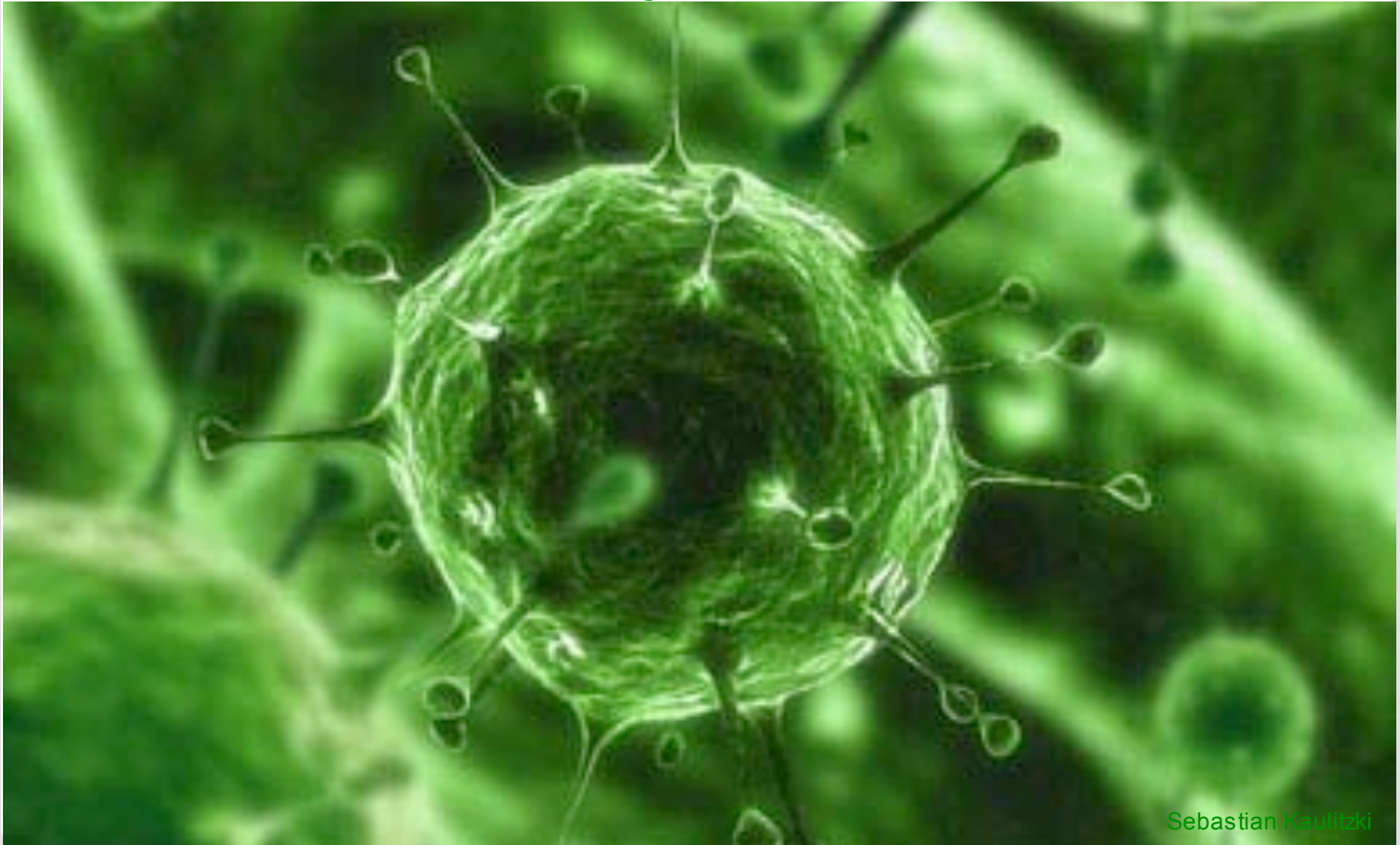
# KASTEL

## Kompetenzzentrum für Angewandte Sicherheits-TEchnoLogie

INSTITUT FÜR KRYPTOGRAPHIE UND SICHERHEIT  
FAKULTÄT FÜR INFORMATIK, KARLSRUHE INSTITUT FÜR TECHNOLOGIE



# Viren, Würmer und Trojaner



Sebastian Kaulitzki

# Industriespionage




# Industriespionage



Mit Malware kann man Ihre Produkte kopieren, bevor sie auf dem Markt sind:

IT-Sicherheit ist kritisch für das Geschäft

# Industriespionage



Mit M  
kopiere Ist schon passiert

IT-Sicherheit ist kritisch für das Geschäft

Groovevolt.com

## Sicherheitsvorfälle

- Datenklau bei RSA  
Security Tokens betroffen. Verbreitung: 40 Mio.
- Sicherheitsleck bei Bundesfinanzagentur  
Angebote von außen änderbar
- 20.000 Zugangsdaten zum Kauf angeboten  
Amazon, eBay, Packstation, PayPal, Mailkonten,...
- Virus sabotiert Krankenhaus IT  
geplante Operationen ausgesetzt
- 100.000 Namen, Adressen und  
Bankverbindungen unverschlüsselt bei einem  
Callcenter.

Quelle: Xamit

# Sicherheitsvorfälle

- Cyberkriminelle stehlen mehr als 70 Millionen US\$
- Google-Mitarbeiter hatte Zugang zu Nutzerdaten
- 800 geheime Kreditkartendaten abgefangen
- Versehentlich 380 Spione enttarnt
- Spanner beobachtet Schülerinnen per Webcam
- Google schneidet private E-Mails mit
- Unerlaubte Organentnahme wegen Datenpanne
- Sensible Daten von 40 Firmen öffentlich im Netz
- Gezielter Angriff mit PDF auf US-Unternehmen
- ...

Quelle: Xamit

# Sabotage: Stuxnet



# Sabotage: Stuxnet

## Besonderheiten

- Bisher unbekannt Sicherheitslücken (Zero Day Exploits)
- Tarnung mit gestohlenen digitalen Unterschriften
- Genaue Kenntnis des Ziels (gezielter Angriff)

# Sabotage: Stuxnet

## Möglicher Infektionsweg



# Sabotage: Stuxnet

Bekanntes Problem

Möglicher Infektionsweg



# Sabotage: Stuxnet

## Möglicher Infektionsweg

Bekanntes Problem



F  
I  
R  
E  
W  
A  
L  
L

Bekanntes Problem

Druckernetzwerk

Steuerung nicht direkt  
mit Internet verbunden

# Sabotage: Stuxnet

## Möglicher Infektionsweg

Bekanntes Problem



# Technische Lösungen?

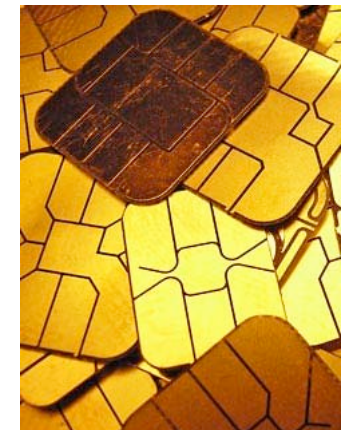
- Kryptographie ist erstaunlich, wie Magie.



- Public Key Kryptographie



- Digitale Signatur



# Technische Lösungen?

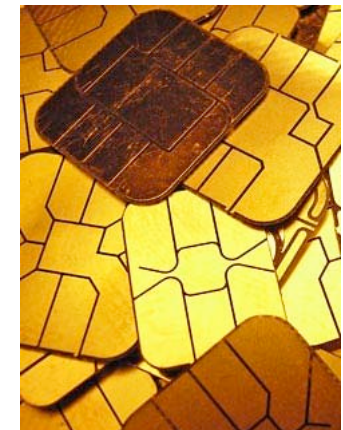
- Kryptographie ist erstaunlich, wie Magie.



- Public Key Kryptographie



- Digitale Signatur

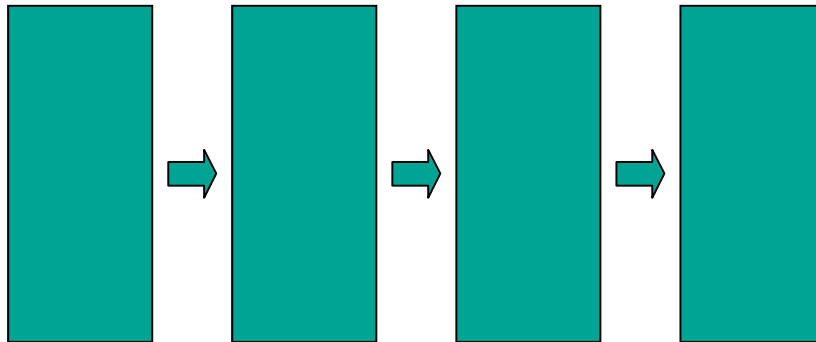


- Warum gehen trotzdem Dinge schief?

## Technische Lösungen?

- Systeme sind komplex und frei programmierbar
- Wirtschaftliche Gründe  
Sicherheit nicht spürbar, ständig neue Features,  
Unternehmen wollen Ihre Daten (Google, Samsung).
- Sicherheit ist unintuitiv (es existiert S: für alle A)
- Naive Lösungen
- Environment Creep (CAN Bus)
- Unvorhergesehene Nutzung (Handys/Gewaltvideos)
- Komposition (Chip & PIN)

# Technische Lösungen?



Bei der Entwicklung sicherer Systeme gibt es bisher keinen durchgängigen Prozess.



Fälschungssichere Medikamentenverpackungen  
und wie das Projekt gelaufen ist...

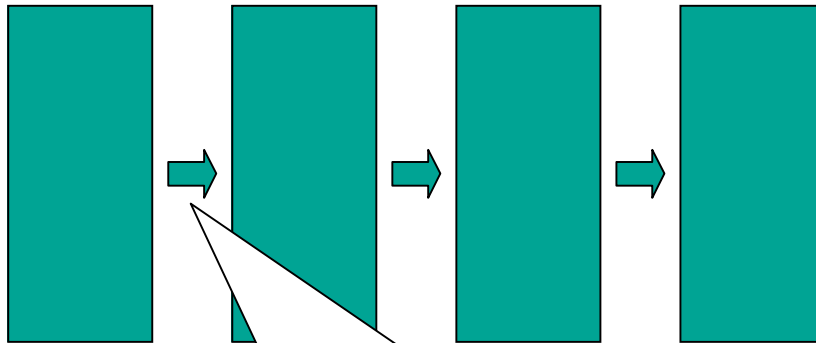
# IT-Sicherheit hilft

Ein Konzept für fälschungssichere  
Medikamentenverpackungen



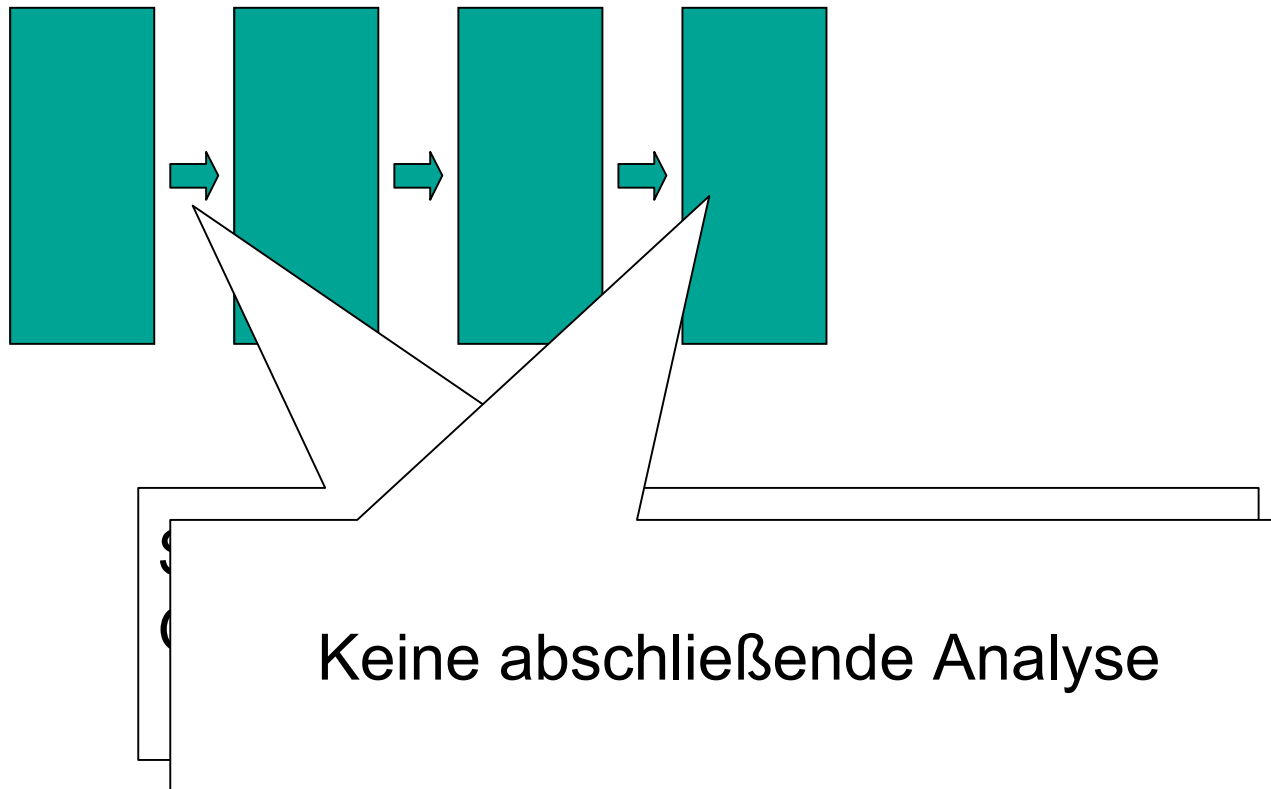
wdr

# Fälschungssichere Verpackungen

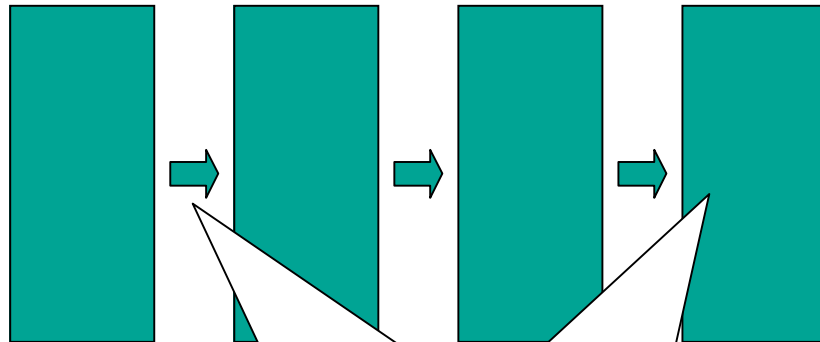


Sicherheitsberatung.  
Gemeinsame Sprache: Powerpoint

# Fälschungssichere Verpackungen



# Fälschungssichere Verpackungen



Keine abschließende Analyse

Keine gemeinsame Sprache  
keine durchgängige Entwicklung



Selbst Sicherheitsexperten verstehen einander manchmal nicht. Sicherheit kann so viel bedeuten...

# KASTEL

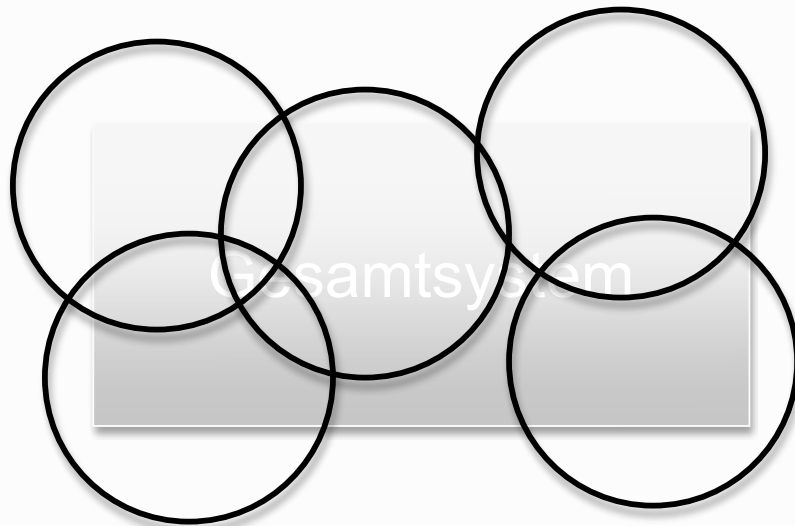


**KASTEL**



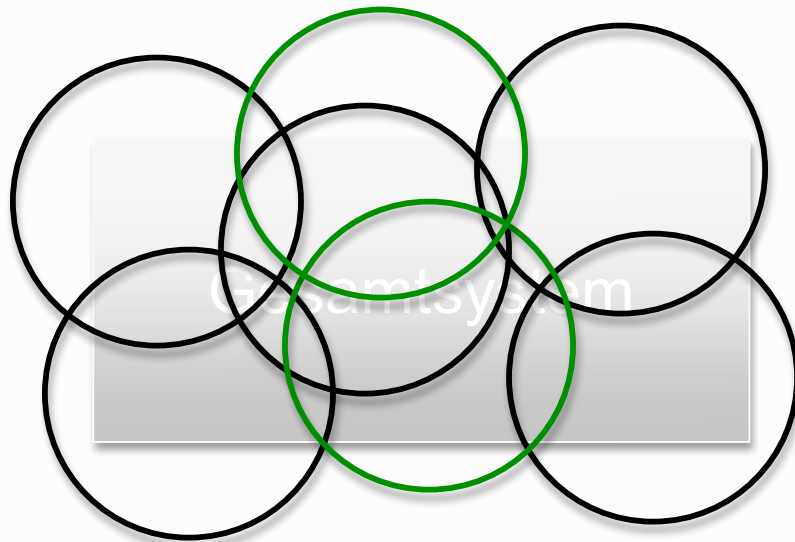
- Durchgängige Sicherheit
- Bei der Entwicklung, bei der Analyse.

- Durchgängige Sicherheit
- Bei der Entwicklung, bei der Analyse.



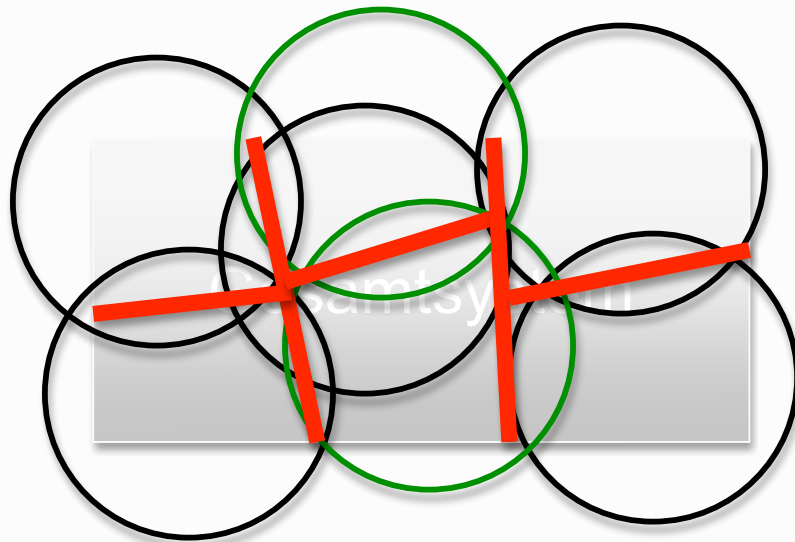
Abdeckung der  
Gesamtsicherheit  
bisher.

- Durchgängige Sicherheit
- Bei der Entwicklung, bei der Analyse.



Abdeckung der  
Gesamtsicherheit  
bisher.  
**Neue Methoden**

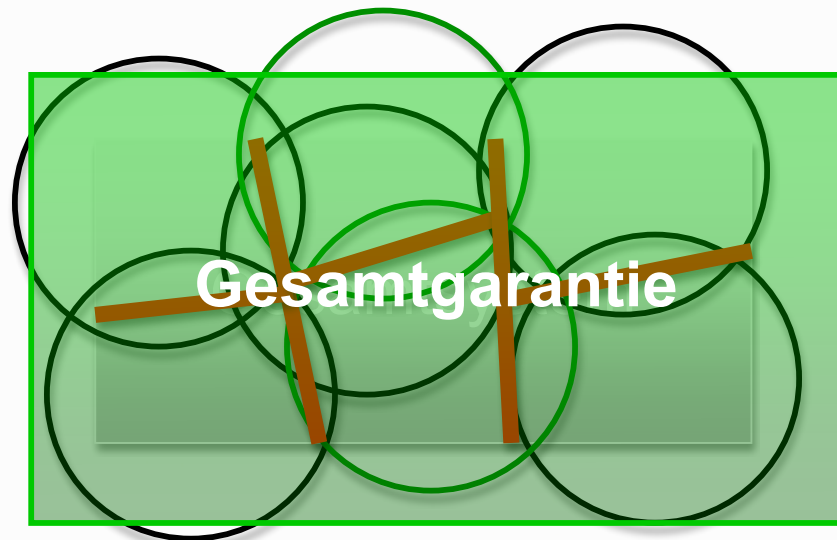
- Durchgängige Sicherheit
- Bei der Entwicklung, bei der Analyse.



Abdeckung der  
Gesamtsicherheit  
bisher.

Neue Methoden  
Neue Schnittstellen  
zwischen Gebieten

- Durchgängige Sicherheit
- Bei der Entwicklung, bei der Analyse.



Abdeckung der  
Gesamtsicherheit  
bisher.

Neue Methoden

Neue Schnittstellen  
zwischen Gebieten

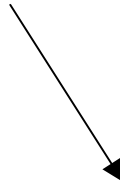
# Ein Beispiel für eine gemeinsame Sprache?

Karlsruher Institut für Technologie

Software-Engineering

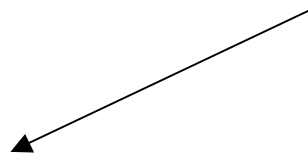
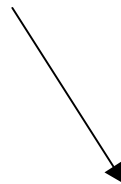
/

Kryptographie



Design by Contract

Dolev/Yao



Design by Contract  
mit idealisierter  
Kryptographie

# Ein Beispiel für eine gemeinsame Sprache?

Software-Engineering

/

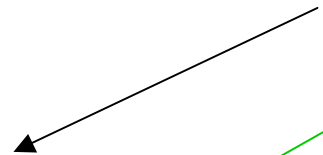
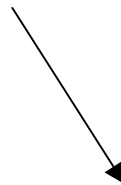
Kryptographie



Soundness

Design by Contract

Dolev/Yao

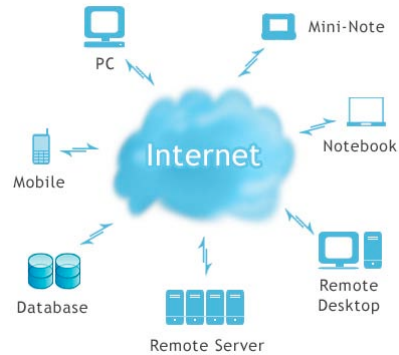


Sicherheitsbeweis

Design by Contract  
mit idealisierter  
Kryptographie

# Anwendungsgetrieben

Cloud



eEnergy



Sicherheit in öffentlichen Räumen

Ganzheitliche Sicherheit ist das Ziel:  
Drei Prototypen sollen entwickelt werden, um zu  
sehen welche Schnittstellen zwischen den  
Disziplinen fehlen.



# Die Grundfragen

Was bedeutet Sicherheit?

Wie entwirft man systematisch sichere Systeme?

Wie weist man ganzheitliche Sicherheit nach?

Wie archiviert und überträgt man Kompetenz?

# Die Grundfragen

Was bedeutet Sicherheit?

UC, Listeneigenschaften, rechtliche Aspekte

Wie entwirft man systematisch sichere Systeme?

Durchgängig von der Architektur zum Code

Wie weist man ganzheitliche Sicherheit nach?

Umgangssprache bis mathematische Beweise  
D/Y als Zwischensprache?

Wie archiviert und überträgt man Kompetenz?

Semantic Wiki, wächst mit der Organisation

# Semantic Wiki

Wissen soll nicht verloren gehen



# Der Helpdesk



businessweek.com

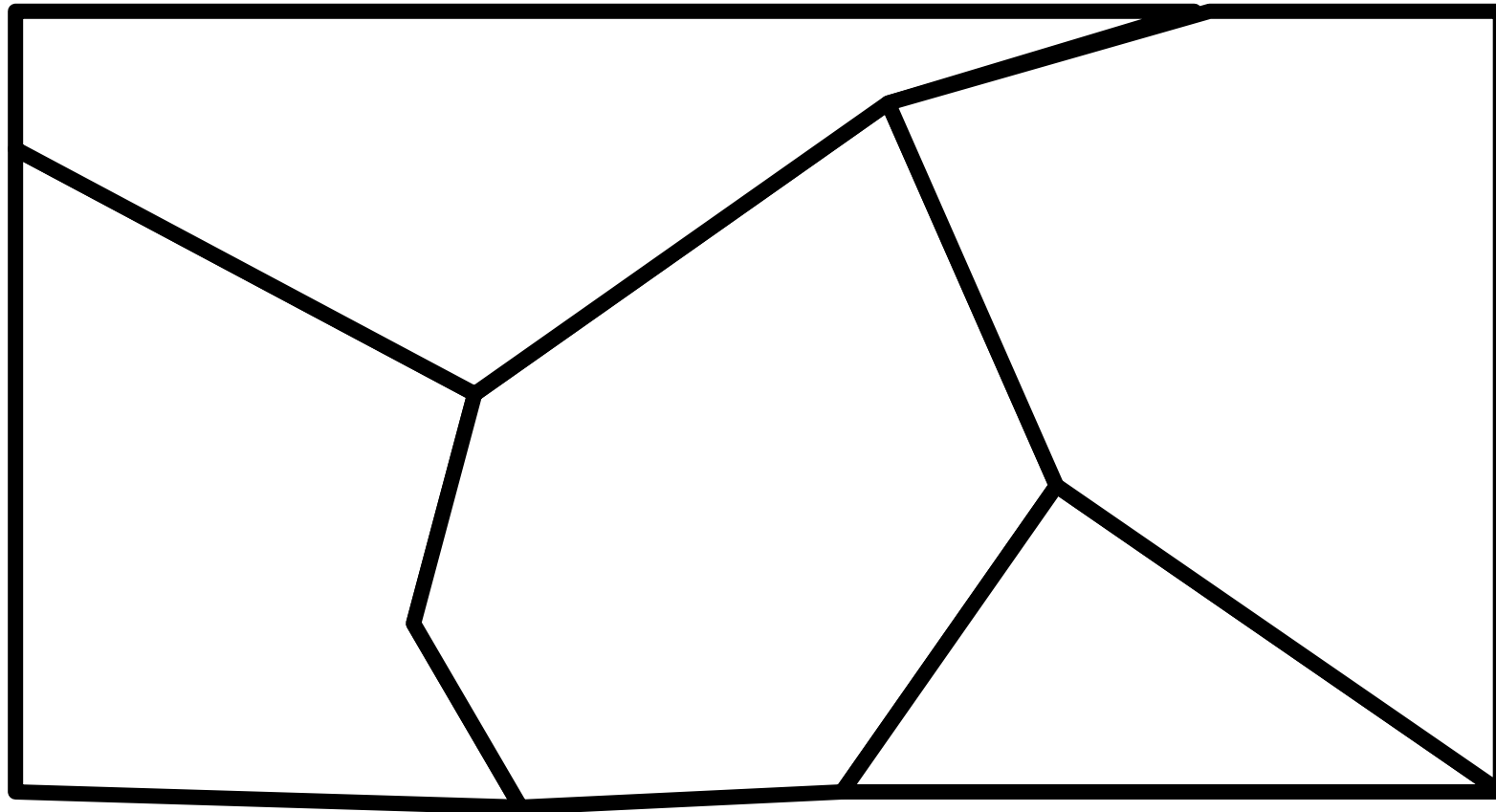
# Organisation

KASTEL ist in Projekte gegliedert.

- \* Realisierungsprojekte (die Prototypen)
- \* Kernprojekte (die vier Grundfragen)
- \* Unterstützende Projekte (fremdfinanziert aber passend)

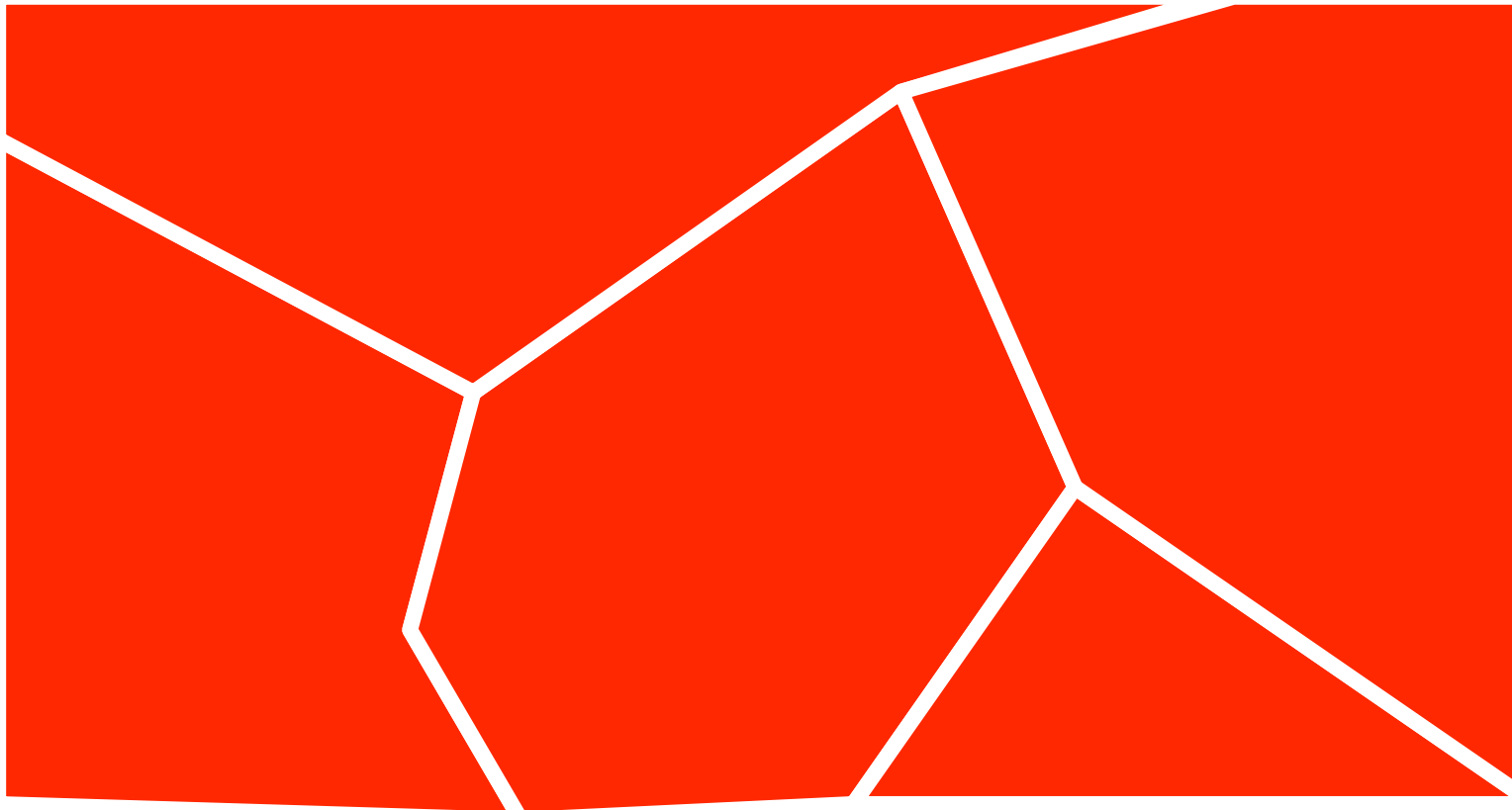
Subsidiaritätsprinzip und  
„Die Struktur kann atmen“

# Abgrenzung zu anderen Projekten



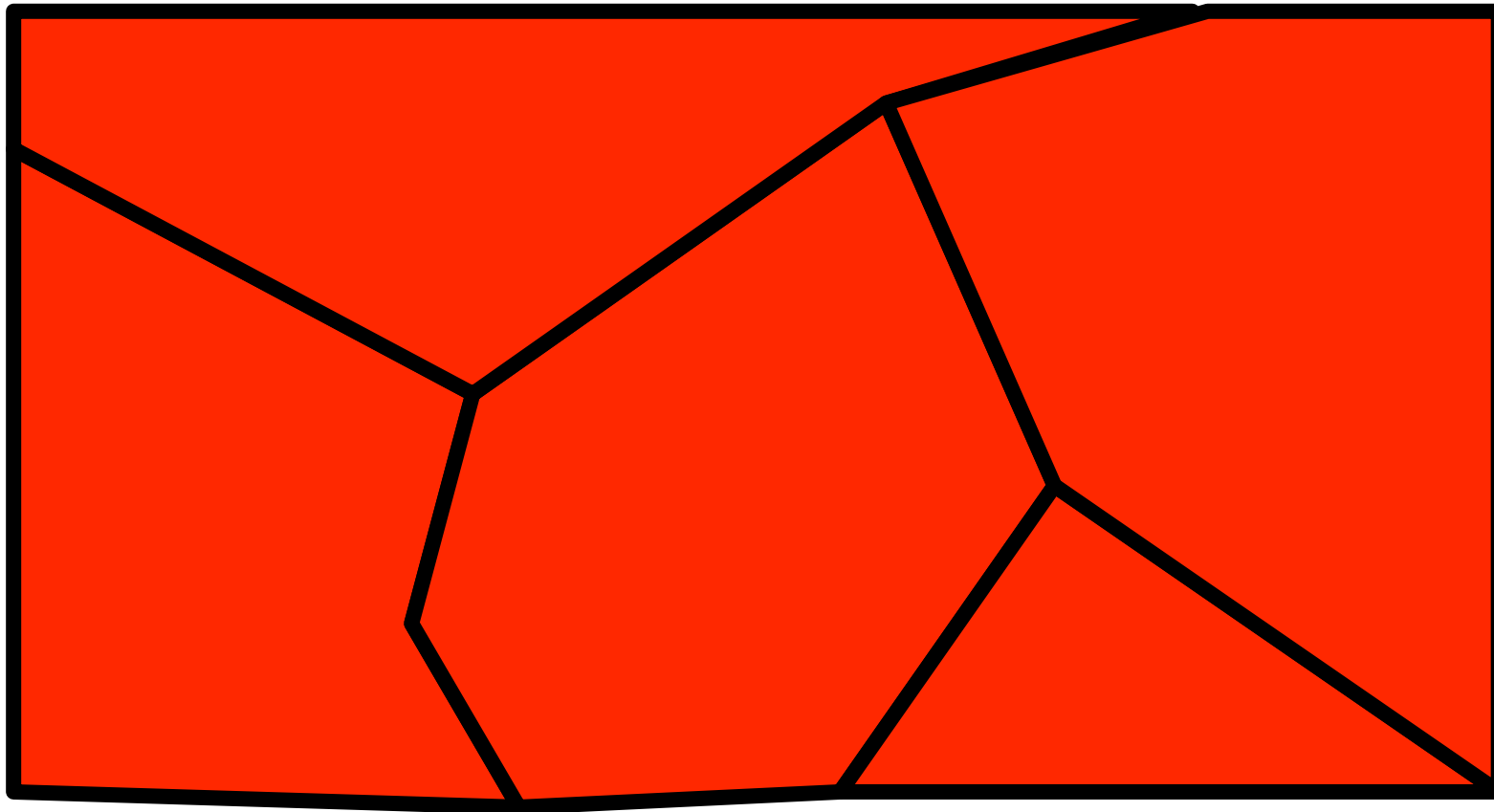
Fortschritt an den Schnittstellen

# Abgrenzung



Kaum Überlapp zu den Inhalten

# Abgrenzung



Zusammen ganzheitlich

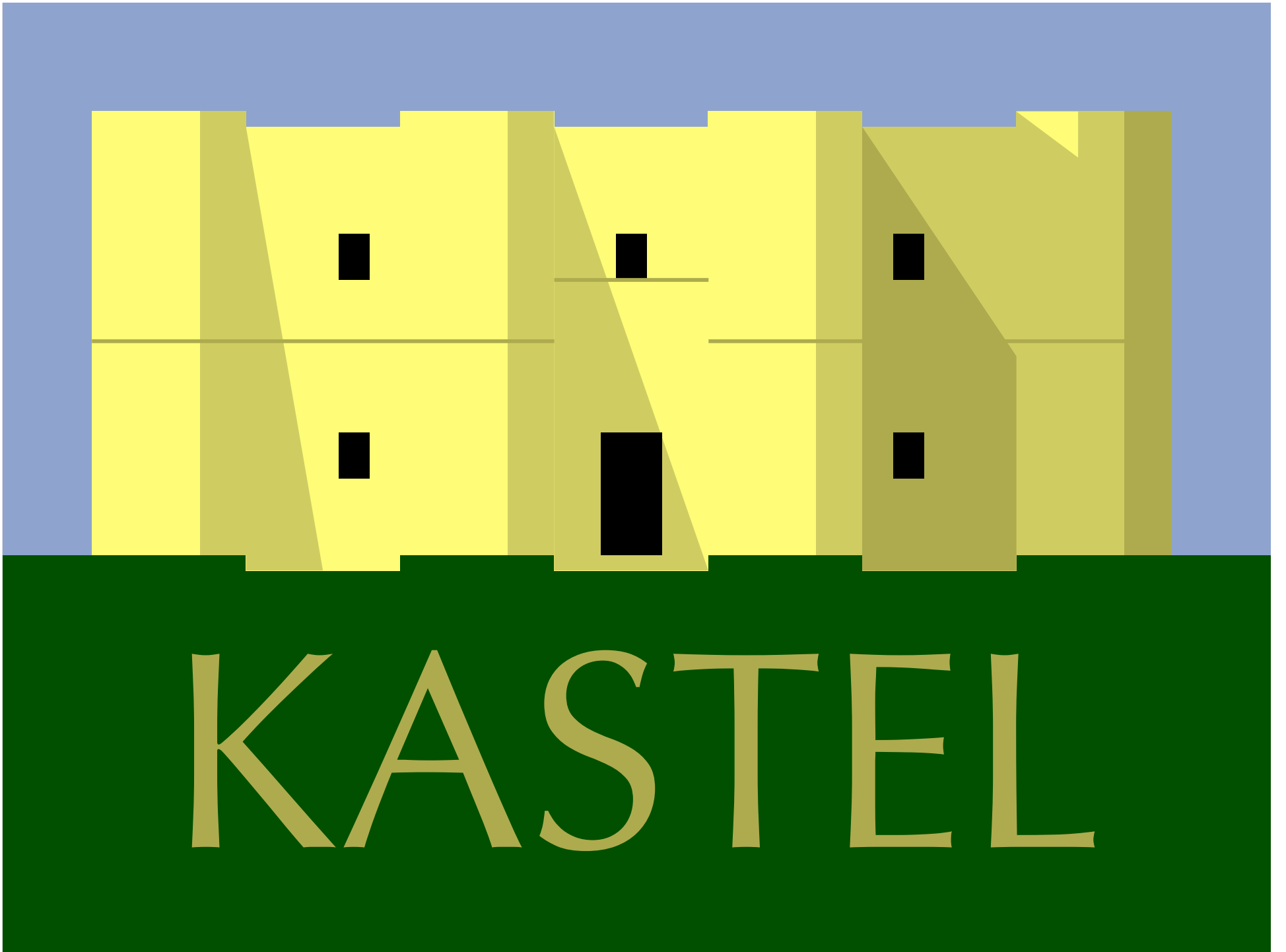
# Qualifikationskonzept

Bündelung von Lehrveranstaltungen mit Sicherheitsbezug

Abschlussarbeiten in KASTEL mit Blick auf Anwendung und Sicherheit

Studenten und Doktoranden in KASTEL erwerben ein Zusatzzertifikat

Absolventen erhalten Nachweis über die in KASTEL erworbenen Qualifikationen.



KASTEL