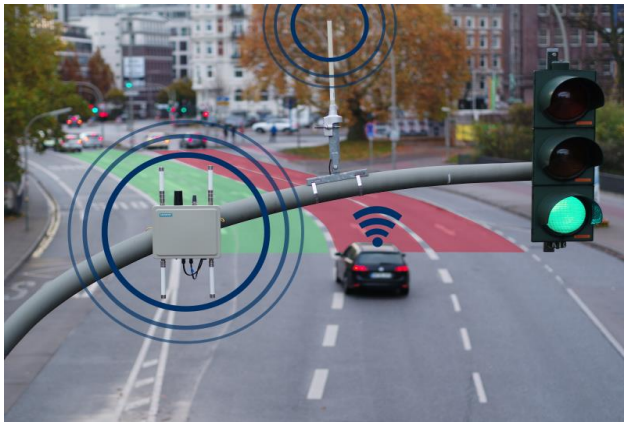
C-ITS: SAFETY UND SECURITY

GRUNDSÄTZE DER IT-SICHERHEIT

30. November 2023 | Hamburg | Dr. Per-Arno Plötz

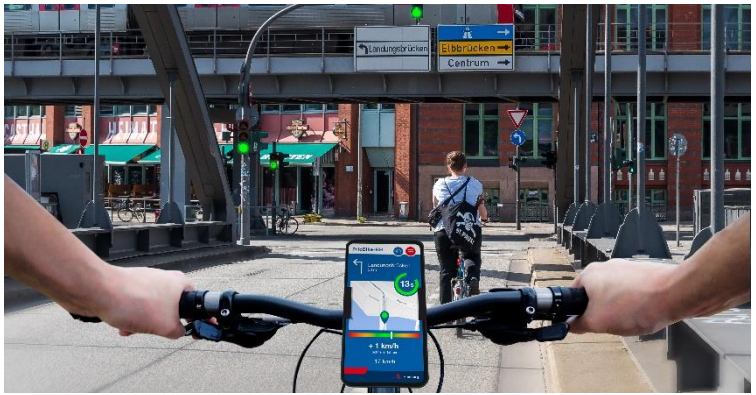
Hamburg

RUND UM TAVF

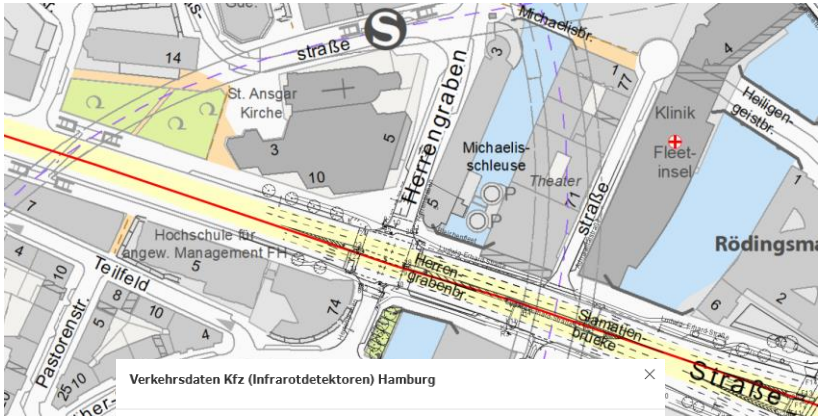


- GLOSA an mehr als 100 Knoten verfügbar
- PVD mit Testfeldnutzenden realisiert
- CPM Dienst in Vorbereitung
- Fokus auf Dienste die Mobilitätswende vorran bringen

- Safety und Security in Vielzahl von Projekten behandelt
- PKI projektübergreifend in Betrieb
- Beteiligung an Kooperationen und Planungen



TAVF: IN DIREKTER NACHBARSCHAFT



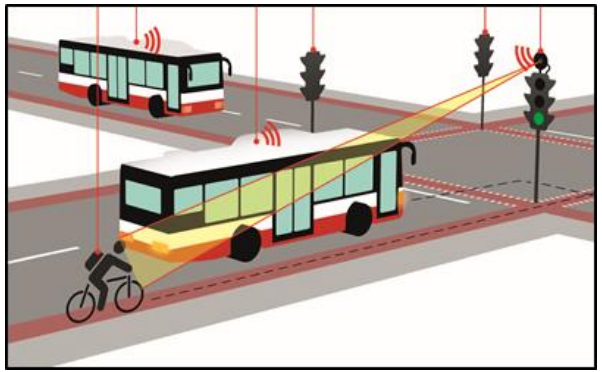
- GLOSA
- Feuerwehrpriorisierung
- Infrarotzählung
- Prognose für PrioBike-App
- PVD-Zählung
- HD-Karte vorhanden

Hamburg

LEVEL DER C-ITS DIENSTE

CAR 2 CAR Communication Consortium

Emergency Vehicle Warning



Vulnerable Road User Protection

CAR 2 CAR Communication Consortium

Cooperative Merging

Gewahrsein → Erfassung → Kooperation

WAS MUSS FÜR DAS DEPLOYMENT ERFÜLLT SEIN?

- **Effizienz**

Betriebskosten im Vergleich zur Erreichung von Zielen, pers. Aufwand, Opportunitätskosten

- **Akzeptanz bzw. Rechtssicherheit**

Hier auch Datenschutz und Level of Service

- **Verständnis der Inhalte**

Harmonisierung und Verfügbarkeit

- **Funktionssicherheit**

Keine unzulässigen Zustände, Betriebssicherheit → Safety

- **Resistenz**

Sicherheit vor Angriffen → Security

Viele der Anforderungen sind eng verknüpft zu IT-Sicherheit

Anforderungen steigen mit zunehmendem Level

vs.

Anforderungen müssen in Gänze von (produktivem) Beginn an erfüllt sein

ÜBERBLICK SCHUTZZIELE

- **Klassische Schutzziele (CIA)**
  - Vertraulichkeit
  - Integrität (Unverfälschtheit)
  - Authentizität (Echtheit)
- **Weitere Schutzziele**
  - Zurechenbarkeit
  - Verfügbarkeit
  - (Pseudo-)Anonymität

AUTHENTIZITÄT

Huhu Uet / CC BY-SA 3.0 DEED

Definition:
Unter Authentisierung wird der Nachweis der behaupteten Identität durch ein Subjekt verstanden. Authentifikation oder auch Authentifizierung bedeutet dann die Prüfung des Nachweises.

Baier et. al., Vorlesungsskript IT-Sicherheit Hochschule Darmstadt

Signatur einer Malerin, chinesisch

- Beispiel TSP: Bus oder Hacker?
- Zielkonflikt zu Anonymität
- Abschwächung: Gruppenzugehörig und abschnittsweise Traceability
- Umsetzung PKI: Öffentliche Schlüssel und SSP

TSP in Hamburg

INTEGRITÄT

DE68 2105 ~~0170 0012~~ 3456 78

1675 4531

Definition:
Unter Integrität versteht man die Vollständigkeit und Unverfälschtheit der Daten für den Zeitraum, in dem sie von einer autorisierten Person erstellt, übertragen oder gespeichert wurden. (…)

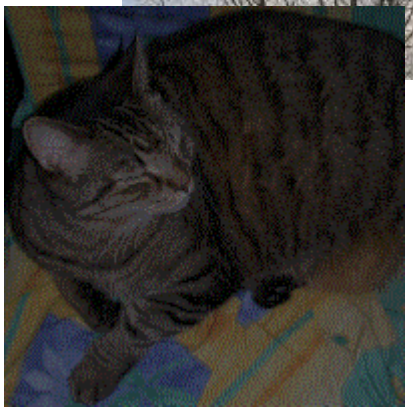
Baier et. al., Vorlesungsskript IT-Sicherheit Hochschule Darmstadt

Quentin Massys: Notar

- Beispiel VRU: Hinzufügen von Personen in CPM
- Umsetzung PKI: Signierung

VRU Schutz in Hamburg

VERTRAULICHKEIT

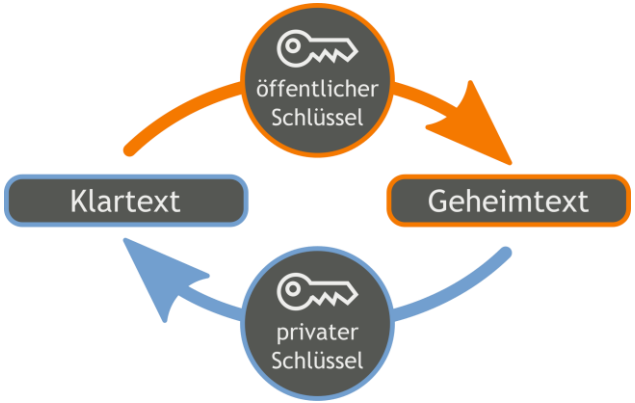


Steganographie / Cyp / CC BY-SA 3.0

Definition:
Confidentiality means ensuring that information is accessible only to those authorised to have access.

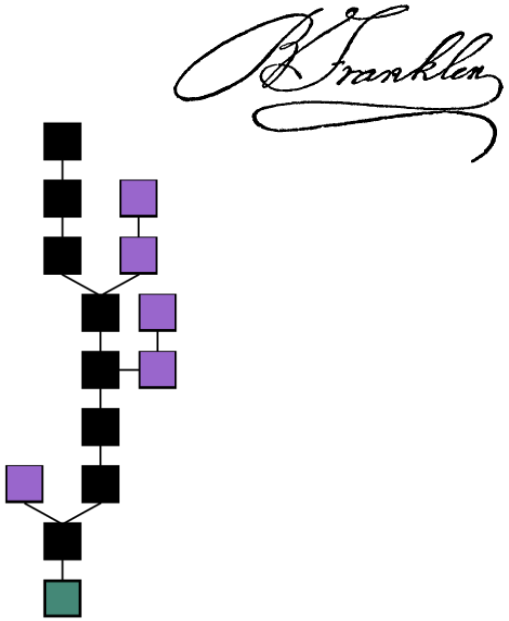
ISO 17799

- Zu unterscheiden: Verschlüsselung und Verbergung
- Bei C-ITS nur sekundär: Austausch der privaten Schlüssel, Nachrichten prinzipiell für alle lesbar
- Umsetzung PKI: HSM



Prinzip asymmetrische Verschlüsselung

ZURECHENBARKEIT
VERBINDLICHKEIT / NICHTABSTREITBARKEIT / NACHWEISBARKEIT



Blockchain Schema / Razorbliss / CC BY-SA 3.0

Definition:
Die Zurechenbarkeit von Daten ist gewährleistet, wenn der Ersteller der Daten die Erzeugung im Nachhinein nicht abstreiten kann (gerade auch gegenüber Dritten).

Baier et. al., Vorlesungsskript IT-Sicherheit Hochschule Darmstadt

- Forderung ggü. Dritten grenzt von Authentizität und Integrität ab
- Eintritt von Festlegungen abhängig: Fristen, Abrufgenehmigung, Verantwortlichkeiten
- Umsetzung offen aber Vorraussetzung einer Rechtsgültigkeit und Enforcement

VERFÜGBARKEIT

404

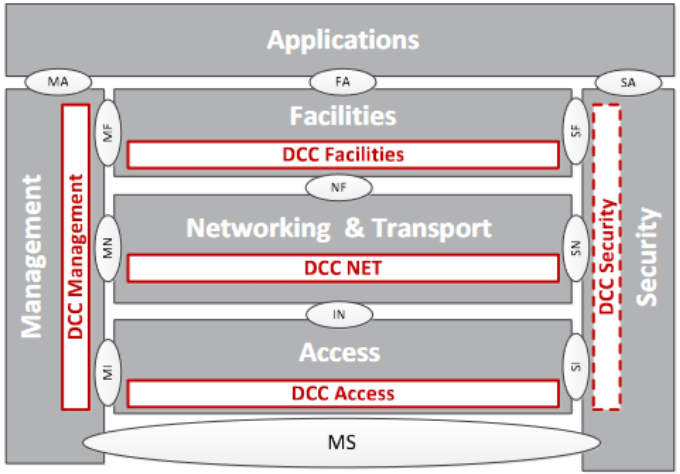
page not found!

old link

Definition:
Unter Verfügbarkeit einer Ressource (…) wird die Eigenschaft verstanden, dass einem autorisierten Subjekt oder Objekt ermöglicht wird, die Funktionalität der Ressource zu nutzen, wenn diese benötigt wird.

Baier et. al., Vorlesungsskript IT-Sicherheit Hochschule Darmstadt

- U.a. durch Redundanz zu erreichen
- Maß: Anteil der Ausfallzeit an Gesamtlaufzeit
- Fragestellungen im C-ITS Kontext: maschinenlesbare Verortung von Serviceangeobten, Backups für Protokolle (siehe Zurechenbarkeit), Ressource Funkkanal
- Einschränkung der These, dass IT-Sicherheit von Anfang an gewährleistet sein muss
- Wichtig für ITS-G5 vs. 5G Diskussion



DCC in der Layerstruktur der ITS-G5 Nachrichten | ETSI 102 724

ANONYMITÄT

OFTMALS EIGENTLICH PSEUDONYMITÄT

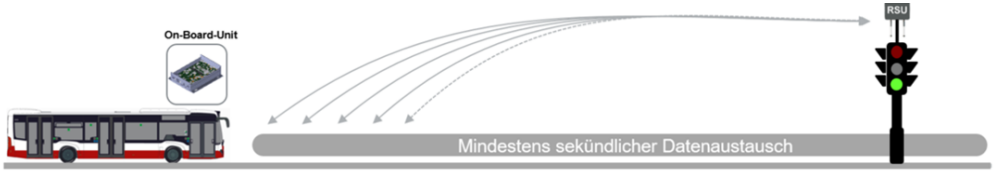
- Vorgaben der DGSVO
- Zielkonflikt mit Zurechenbarkeit und Vertraulichkeit
- Zuordnung von Nachrichten des gleichen Sender währen Knotenüberfahrt notwendig
- Realisierung von AA und EA in PKI, Zertifkatsrotation

Definition:
Das Schutzziel Anonymität bezeichnet die Veränderung personenbezogener Daten in einer Weise, dass diese nicht oder nur mit unverhältnismäßigem Aufwand einer Person zugeordnet werden können.

Baier et. al., Vorlesungsskript IT-Sicherheit Hochschule Darmstadt

Definition:
Unter Pseudonymität versteht man die Veränderung personenbezogener Daten, so dass diese nur unter Kenntnis der Zuordnungsvorschrift einer Person zugeordnet werden können.

Baier et. al., Vorlesungsskript IT-Sicherheit Hochschule Darmstadt

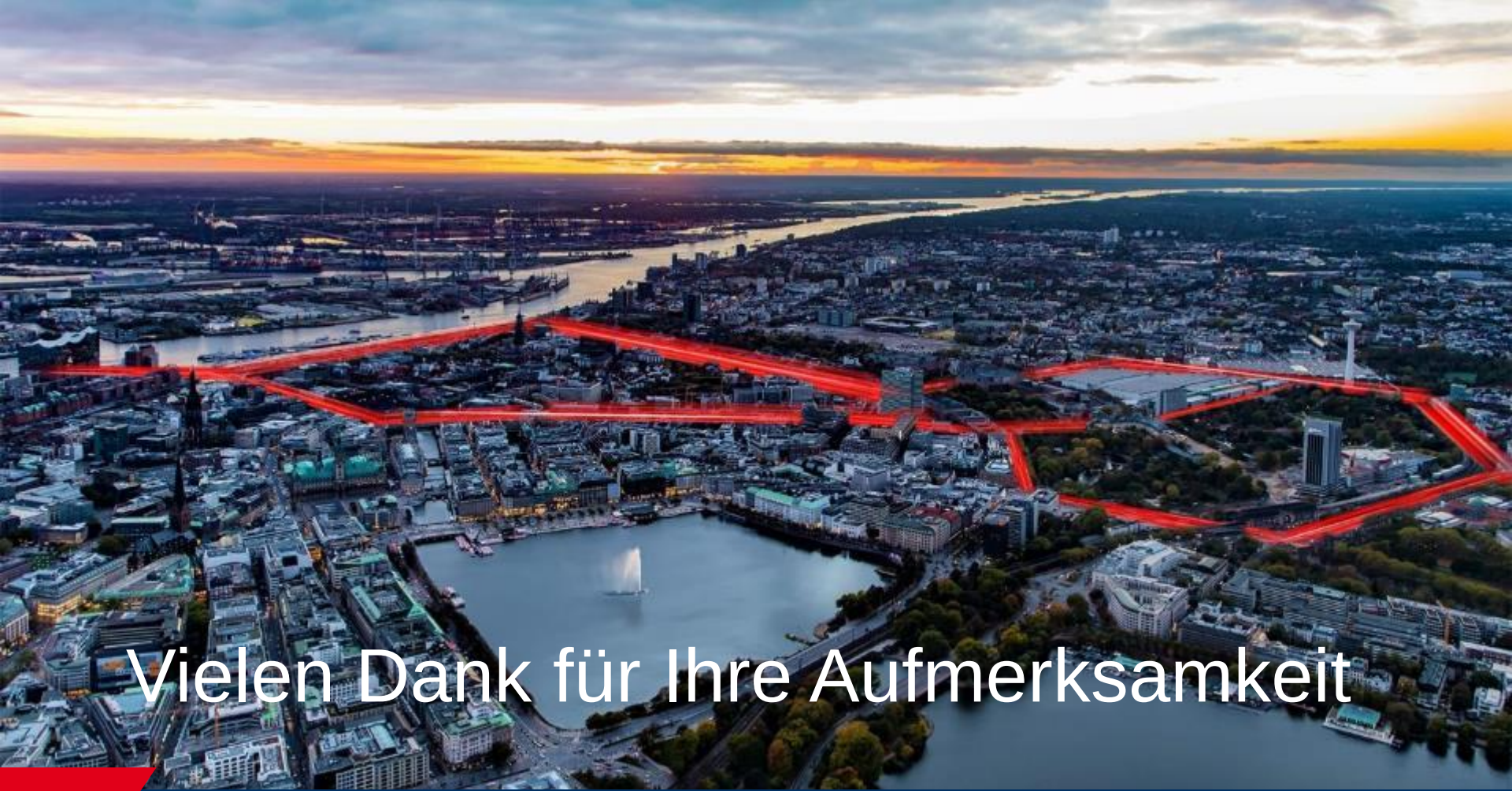


ZUSAMMENFASSUNG

- **CIA-Schutzziele (Verraulichkeit, Integrität, Authentizität) eindeutig**
- **Weitere Schutzziele (Zurechenbarkeit, Verfügbarkeit, (Pseudo-)Anonymität mit zu definierenden Kriterien**
- **Erreichung Vorraussetzung für produktive C-ITS-Dienste (gilt auch für frühe Level)**

UNSERE ERWARTUNGEN

- **Kritische Diskussion unserer Ansätze**
- **Austausch mit anderen Testfelder zum Thema IT-Sicherheit verstetigen**
- **Harmonisierung vorrantreiben (Z.B. gemeinsame Service- und Sicherheitskriterien, Rollendefinition im föderalen System)**
- **Best Practise und Worst Practise kommunizieren**



Vielen Dank für Ihre Aufmerksamkeit