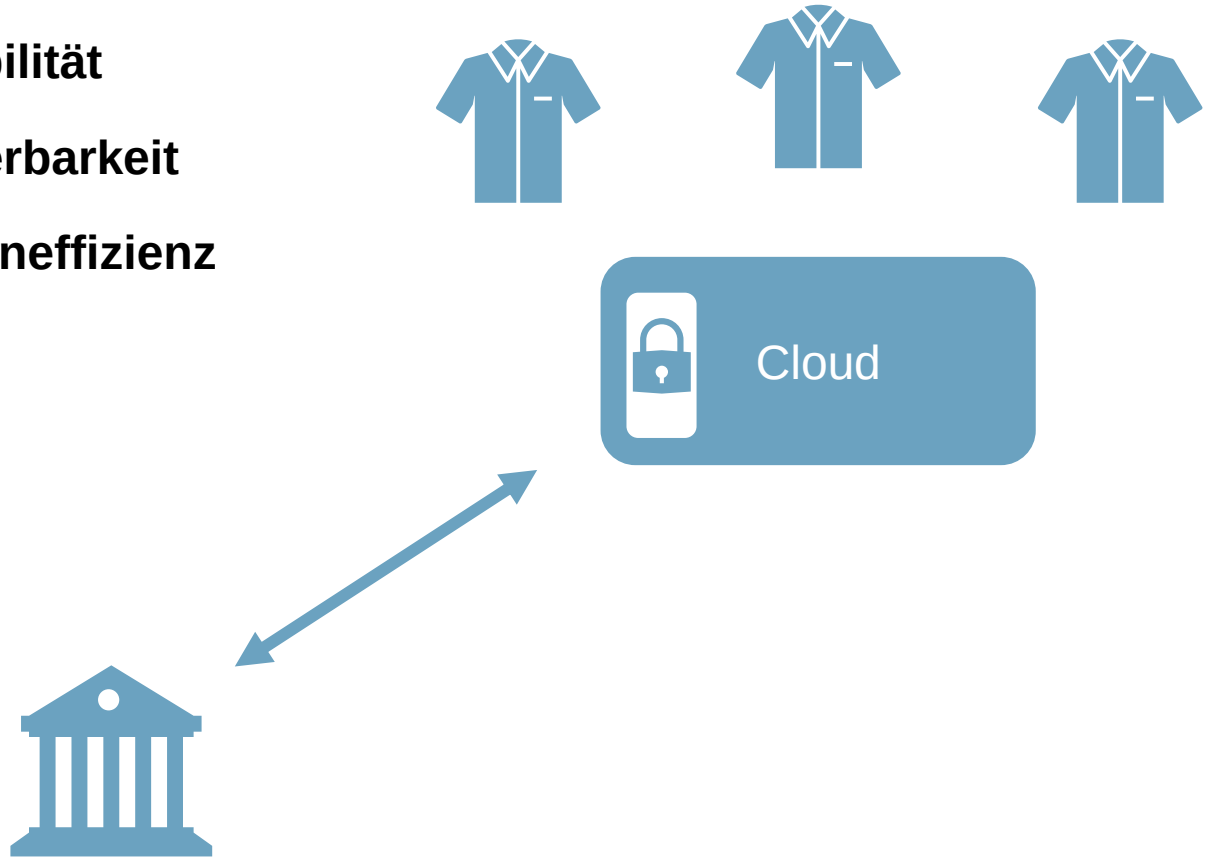
Friedrich-Alexander-Universität
Technische Fakultät

FAU

The Devil is in the Detail: Issues with Fine-Grained Trusted Execution Environments

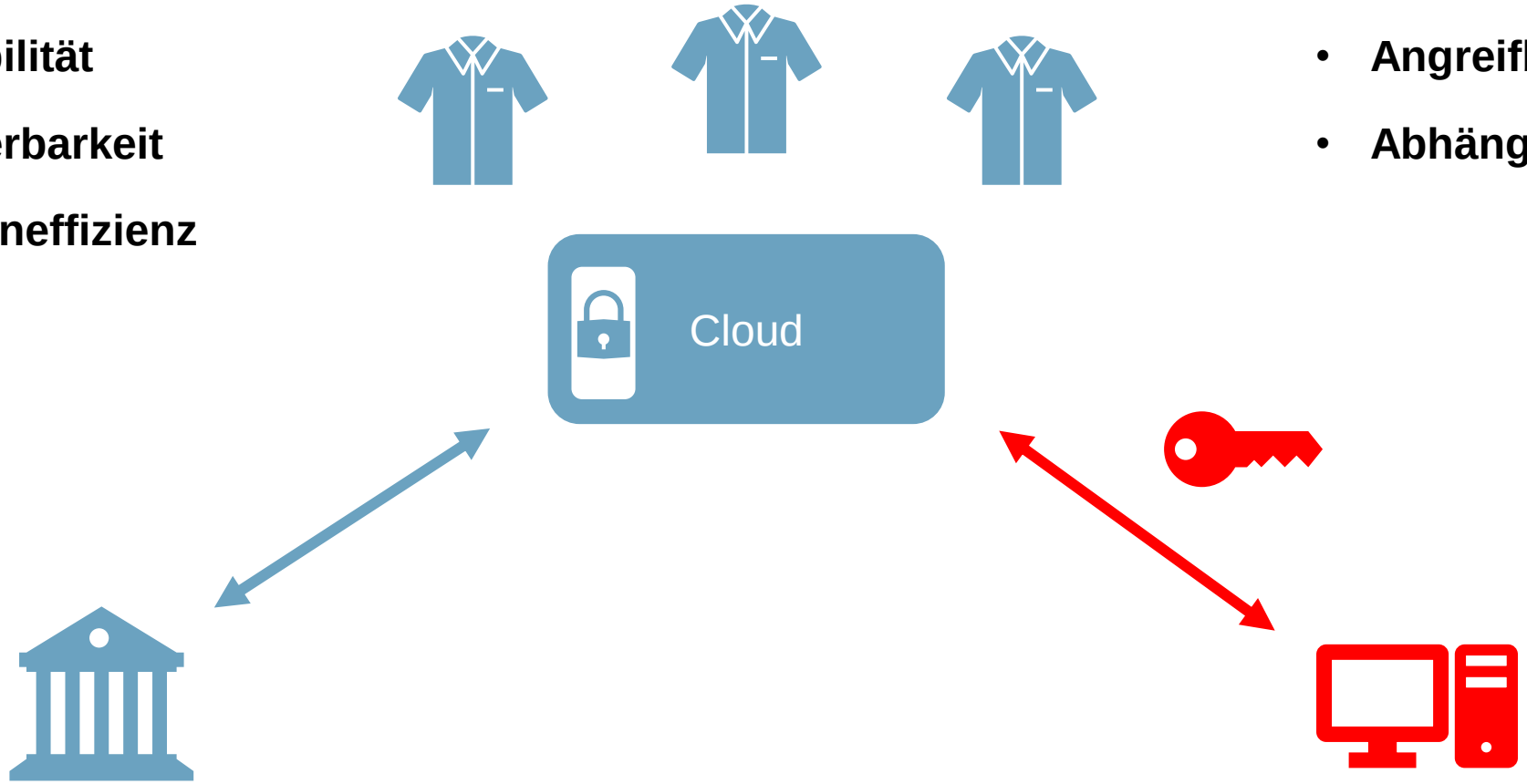
Die Cloud ist gut, aber …

- **Flexibilität**
- **Skalierbarkeit**
- **Kosteneffizienz**



Die Cloud ist gut, aber …

- **Flexibilität**
- **Skalierbarkeit**
- **Kosteneffizienz**



- **Angreifbar**
- **Abhängigkeit**

Übersicht

Trusted Execution Environment (TEE)

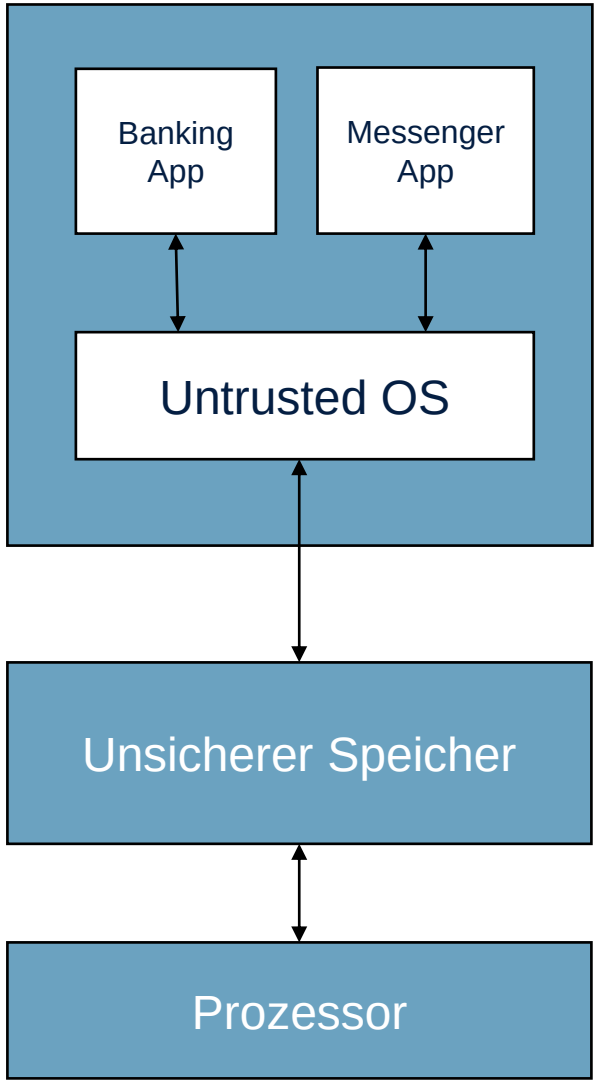
3 Eigenschaften:

- **Integrität**
- **Vertraulichkeit**
- **Authentizität (mit Remote Attestation)**

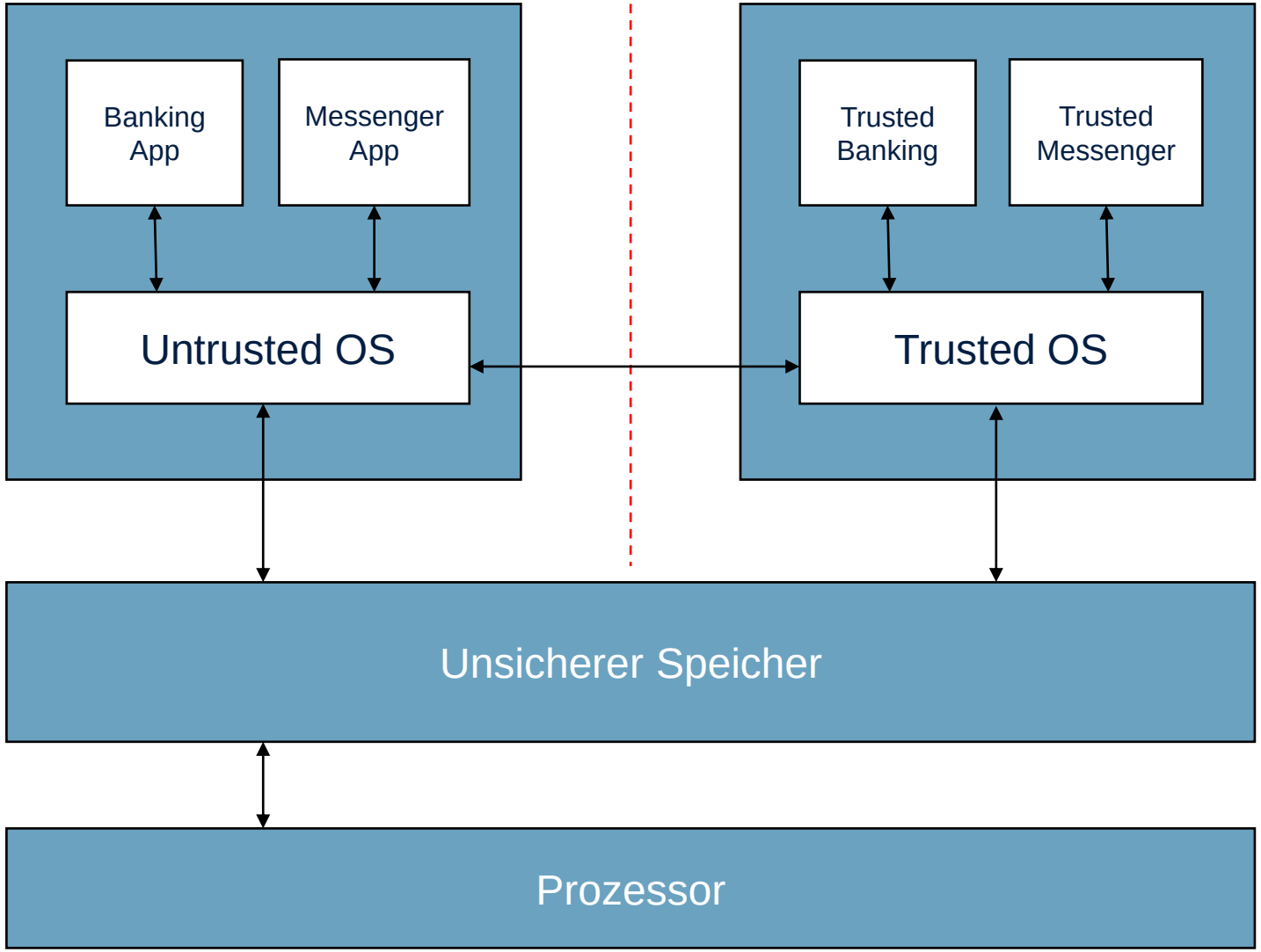
Feingranulare TEE:

- **Teil der Anwendung wird in einer TEE ausgeführt**

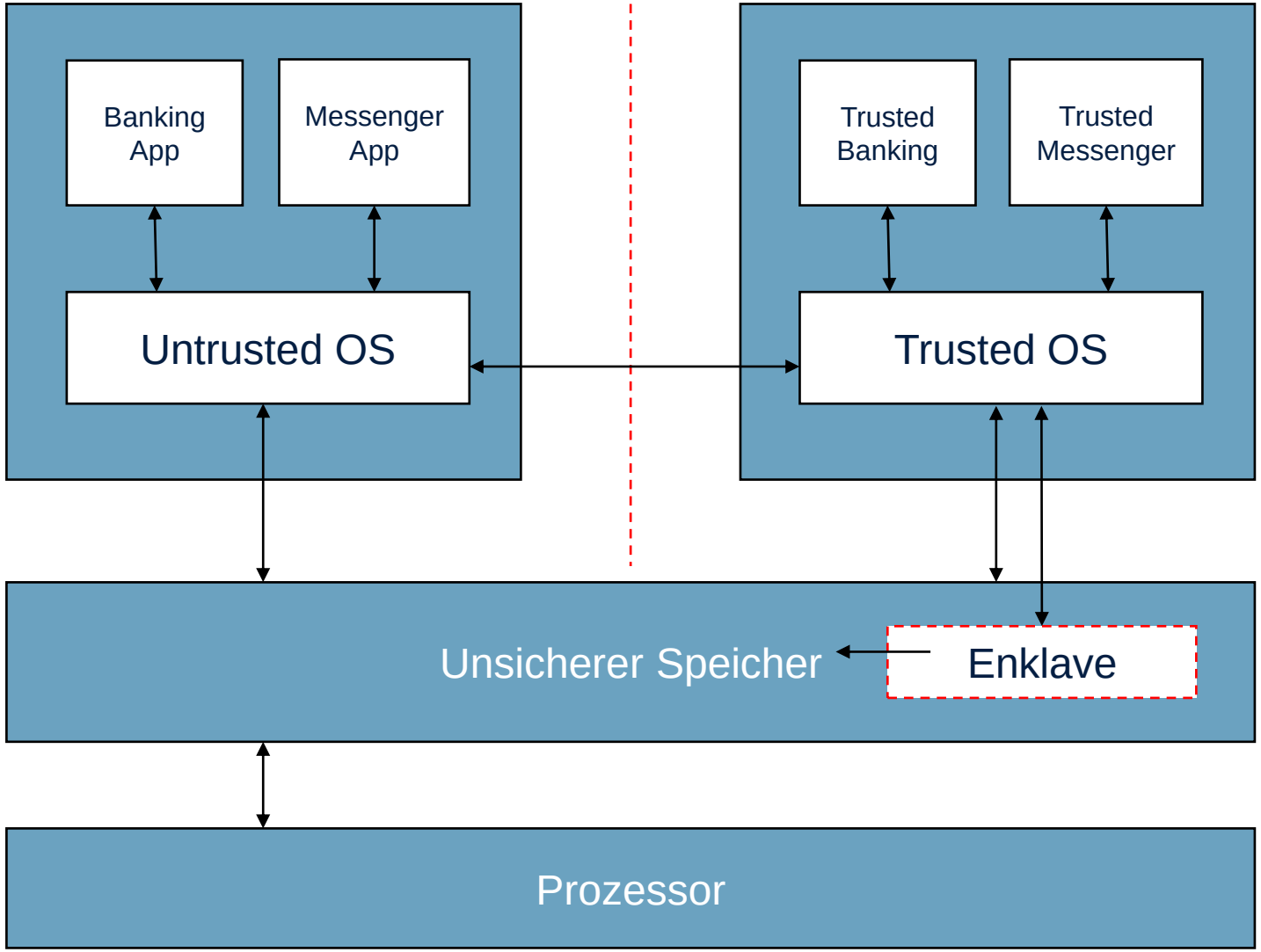
Trusted Execution Environment (TEE)



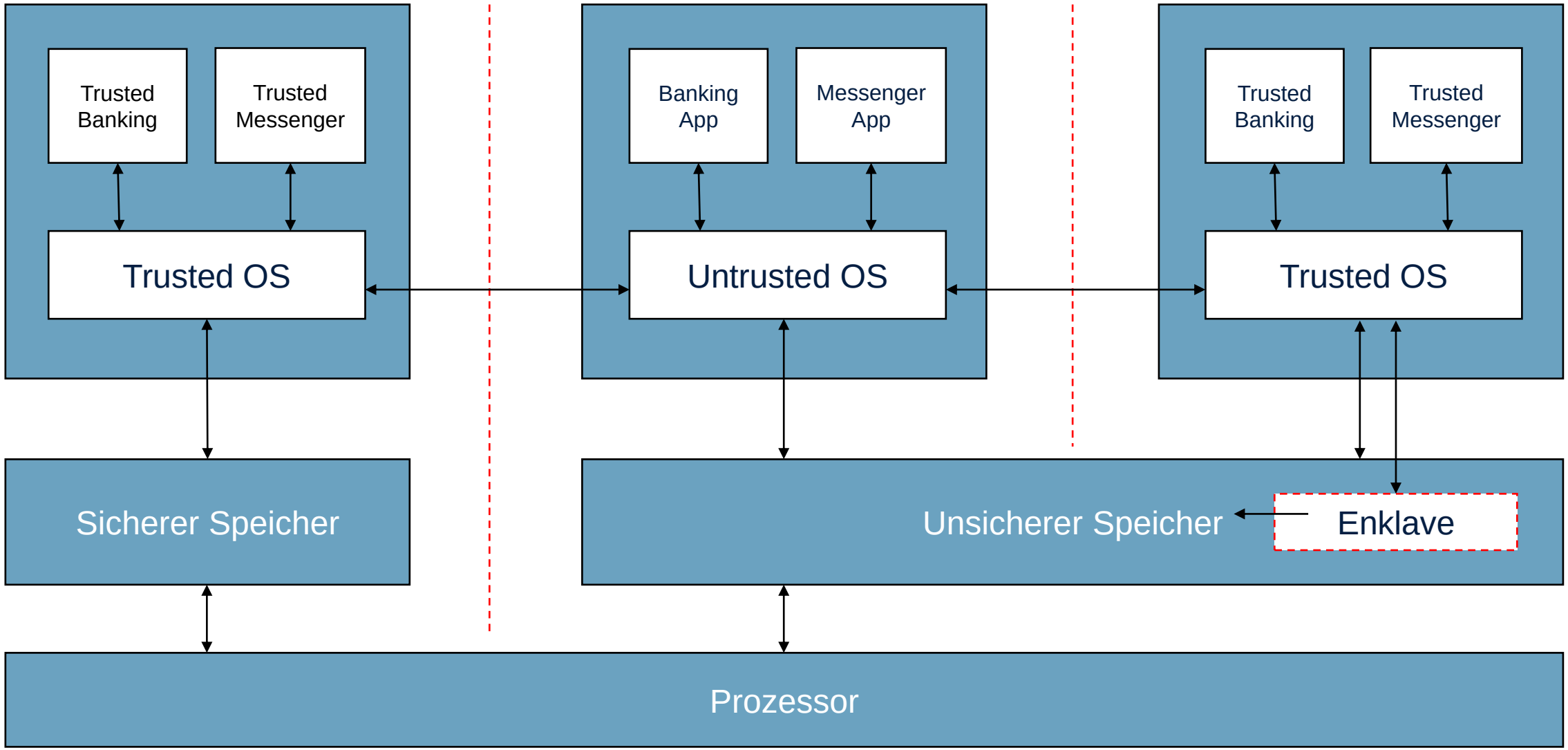
Trusted Execution Environment (TEE)



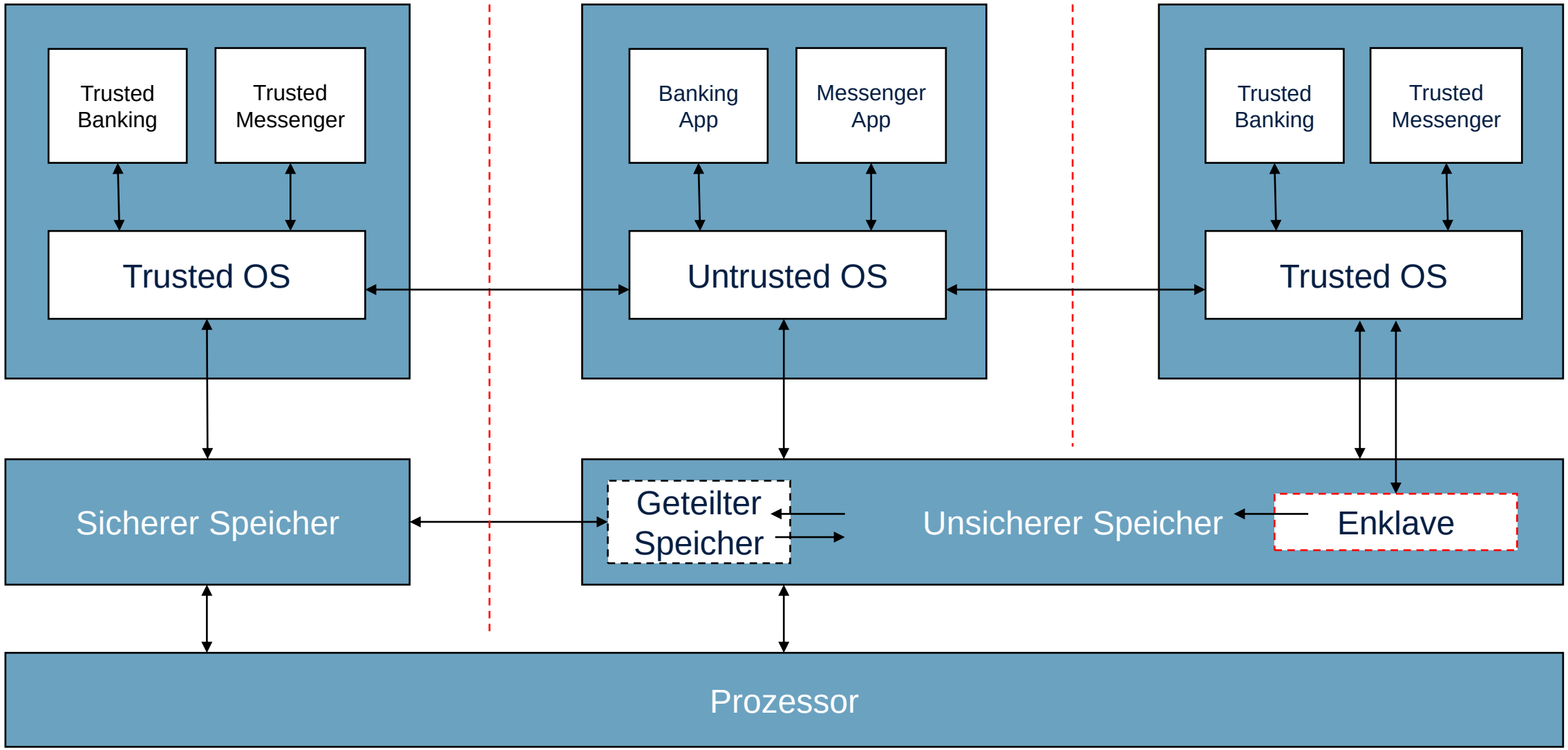
Trusted Execution Environment (TEE)



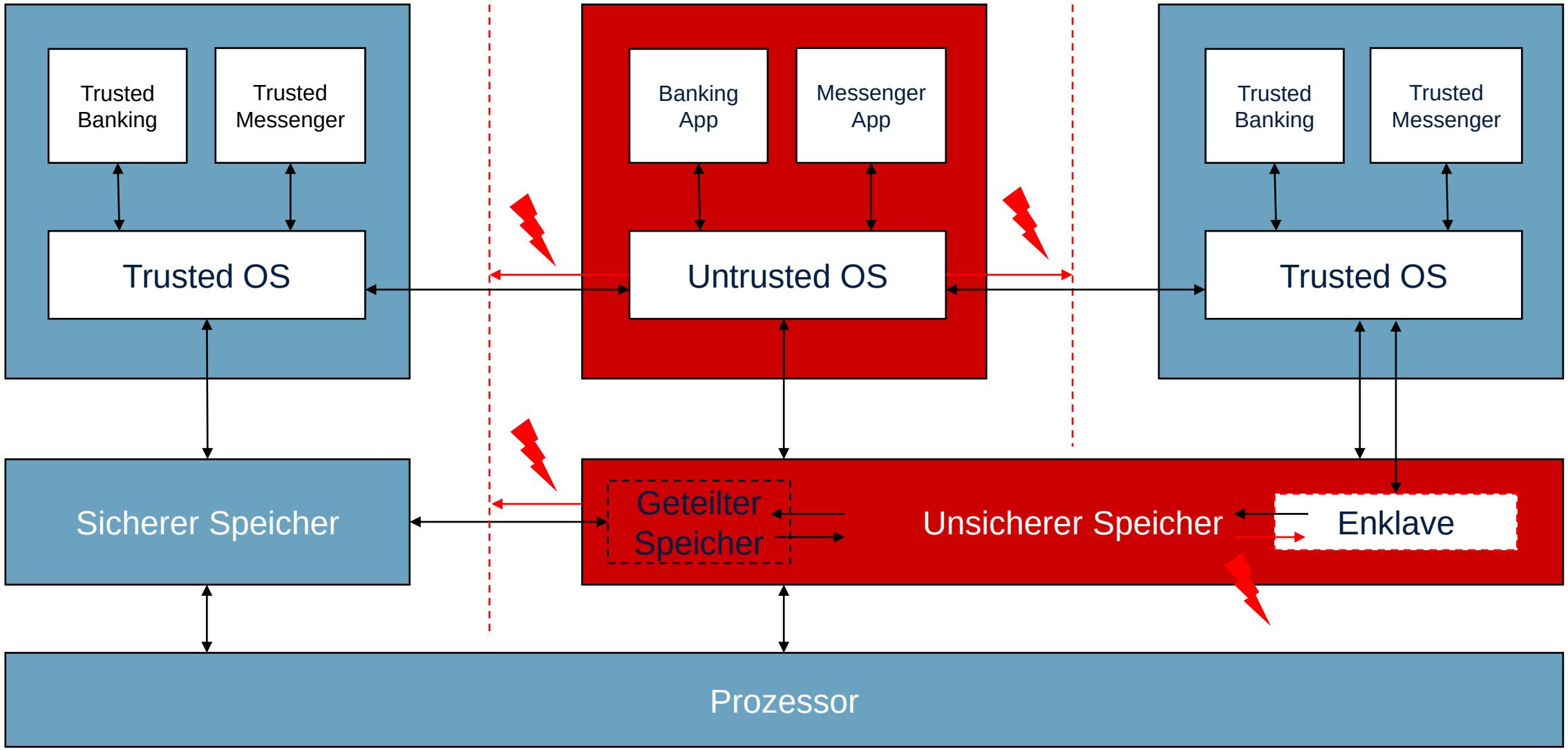
Trusted Execution Environment (TEE)



Trusted Execution Environment (TEE)

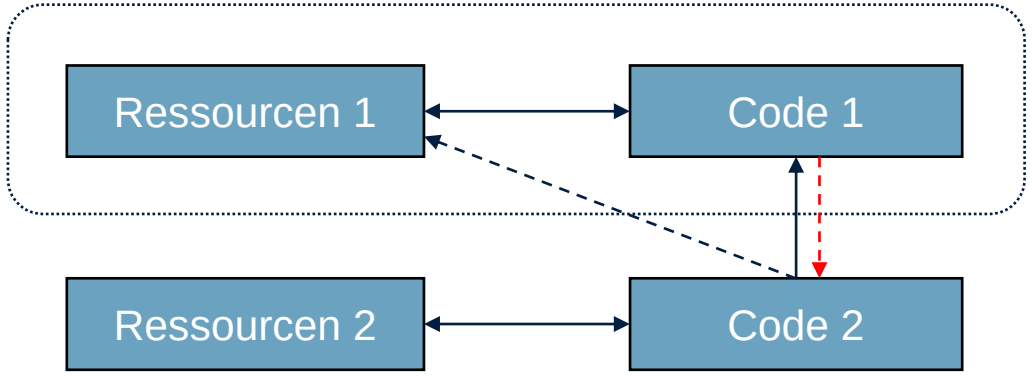


Trusted Execution Environment (TEE)

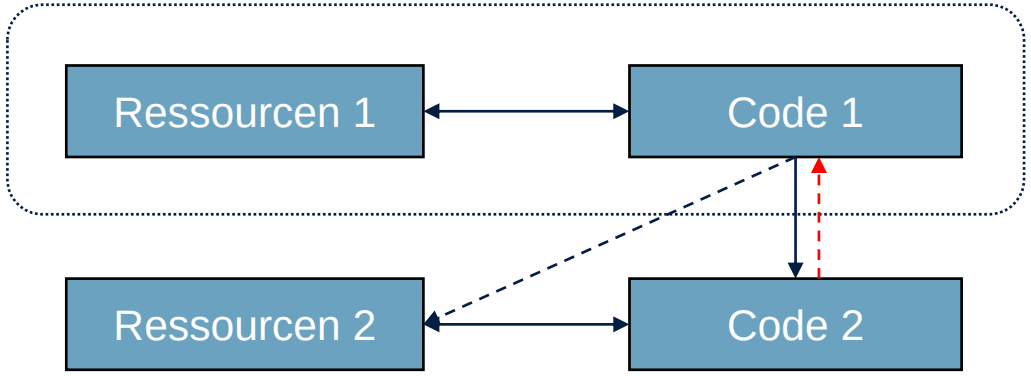


Kompartiment

Sandbox

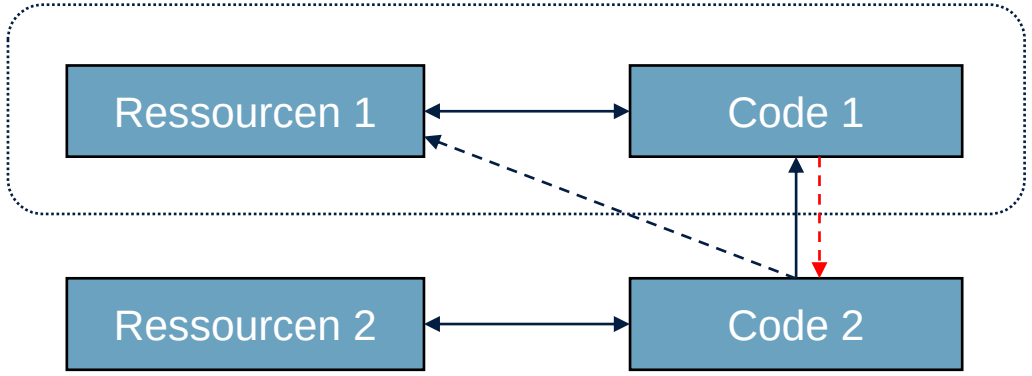


Safebox

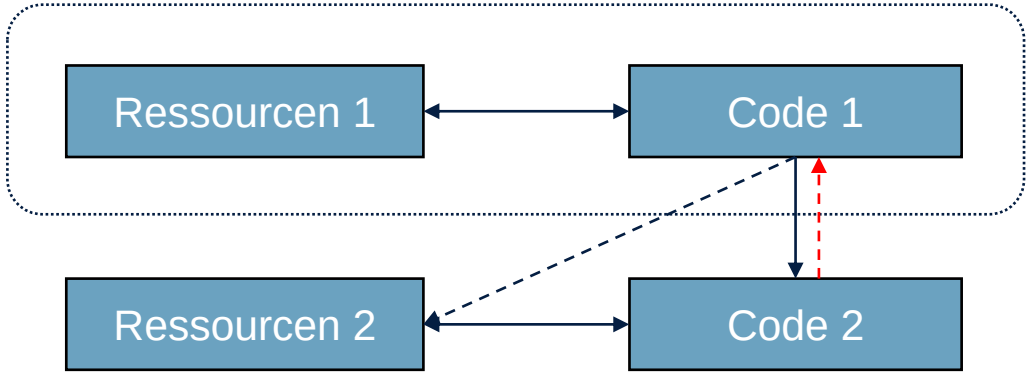


Kompartiment

Sandbox

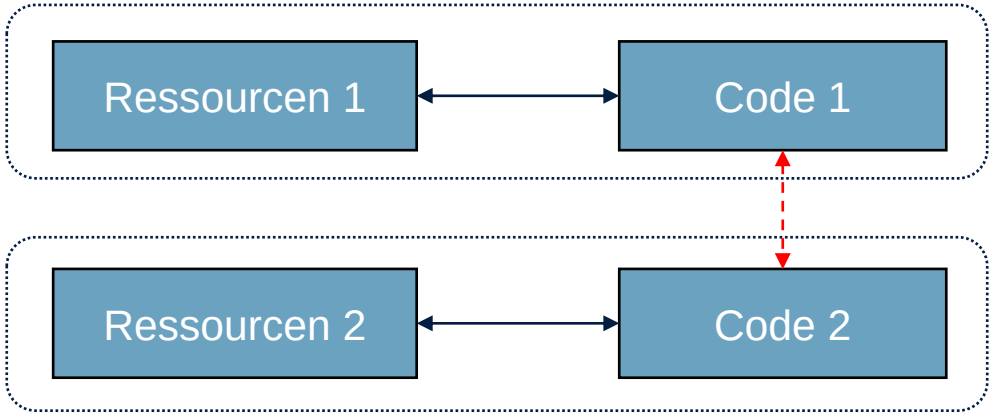


Safebox



Kompartiment 1

Kompartiment 2



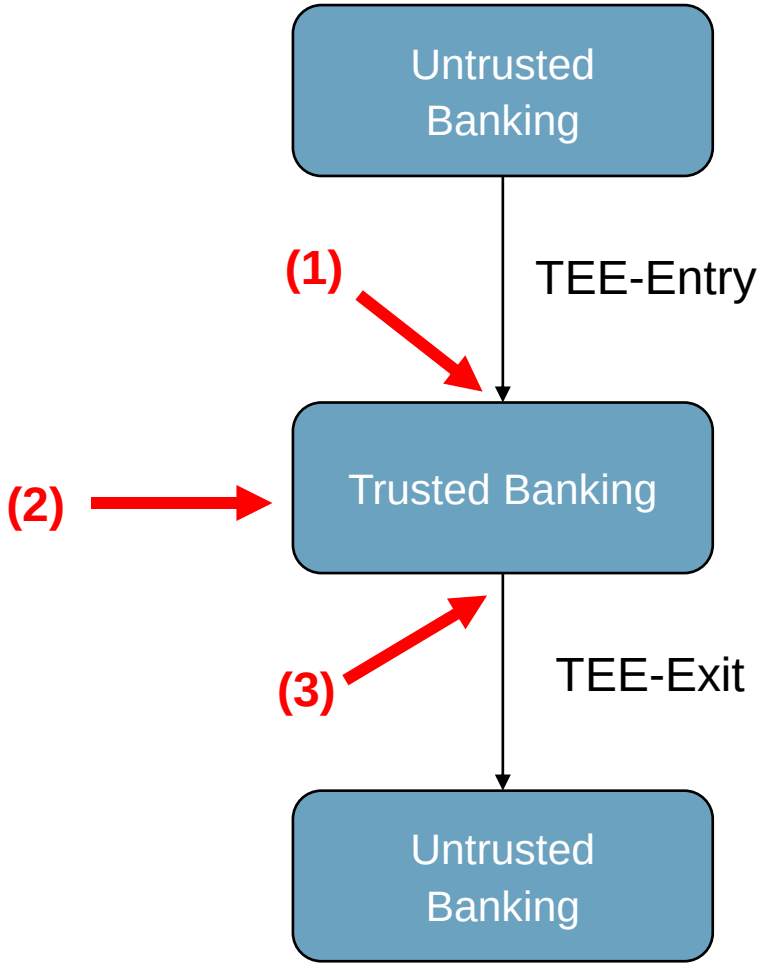
Angriffe

Datenkorruption

- (1) Flags
- (2) Pointer
- (2) Double fetch

Datenleck

- (2) Pointer
- (2) Strings
- (3) Exit



Datenkorruption - Flags

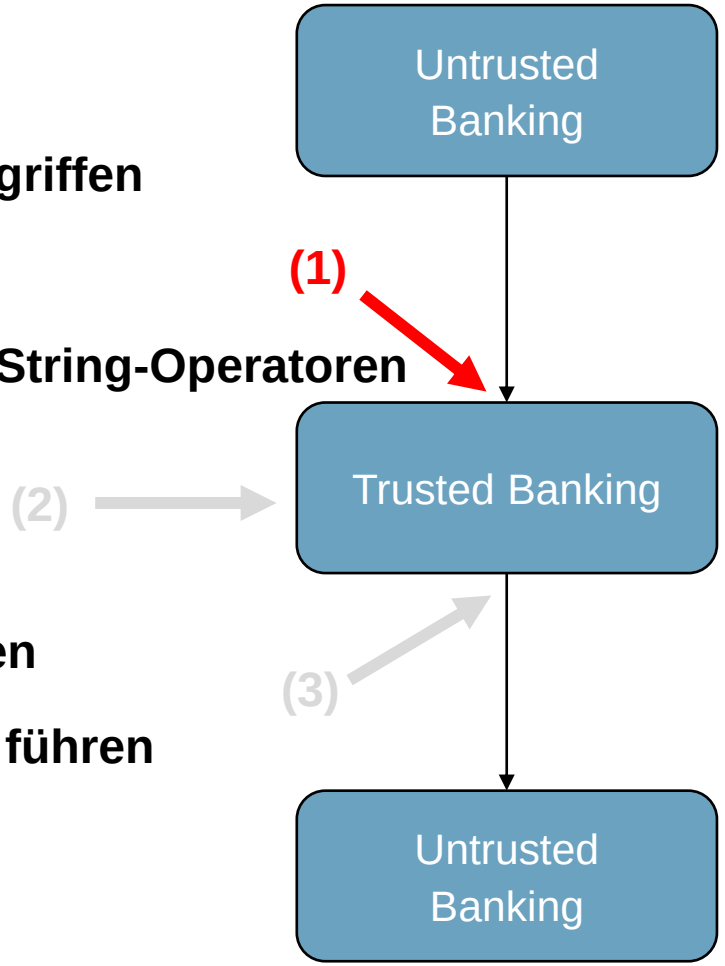
0x0	20	ef	13	10	20	ef	13	10
0x8	12	5c	e1	18	12	5c	e1	18
0x16	X	X	X	X	X	X	X	X
0x24	X	X	X	X	X	X	X	X
0x32	X	X	X	X	X	X	X	X
0x40	14	18	09	3e	14	18	09	3e
0x48	44	17	e1	5c	44	17	e1	5c

Alignment Check Flag

- **Ausrichtung von Datenzugriffen**

Direction Flag

- **Steuert die Richtung von String-Operatoren**
- **Beeinflussen das Verhalten**
- **Kann auch zu Datenlecks führen**



Datenkurroption – Pointer

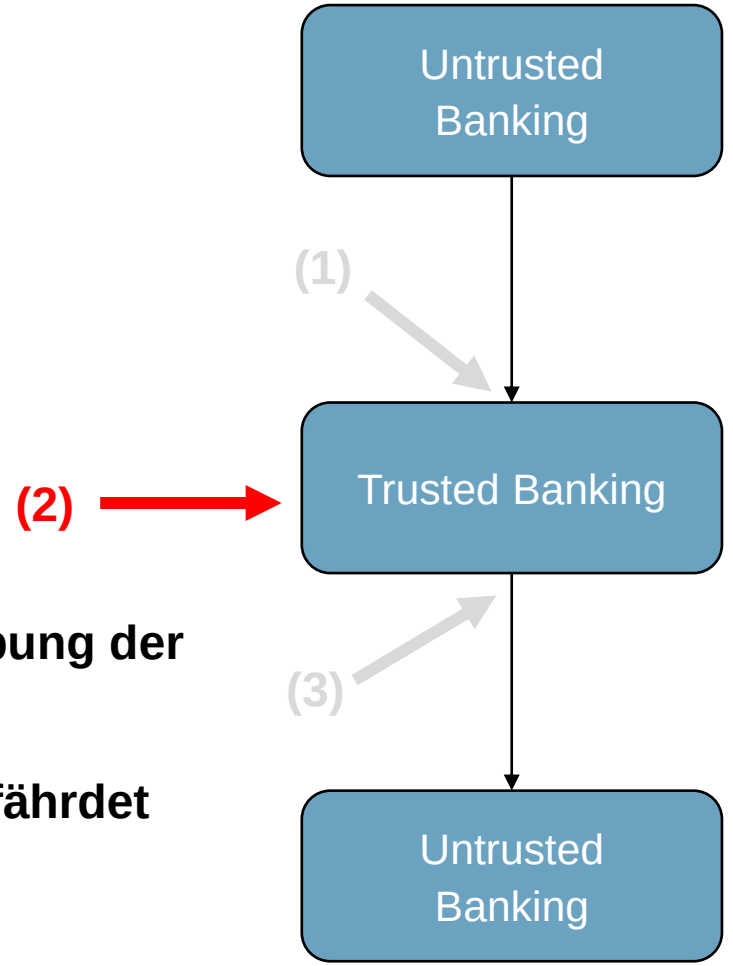
0x0	20	ef	13	10	20	ef	13	10
0x8	12	5c	e1	18	12	5c	e1	18
0x16	X	X	X	X	X	X	X	X
0x24	X	X	X	X	X	X	X	X
0x32	X	X	X	X	X	X	X	X
0x40	14	18	09	3e	14	18	09	3e
0x48	44	17	e1	5c	44	17	e1	5c

int ptr1 **//0x6**

int ptr2 **//0x31**

int ptr3 **//0x15**

Double ptr4 **//0x15**



- **Kann zur Überschreibung der eigenen Daten führen**
- **Datenintegrität ist gefährdet**

Datenkurroption – Pointer

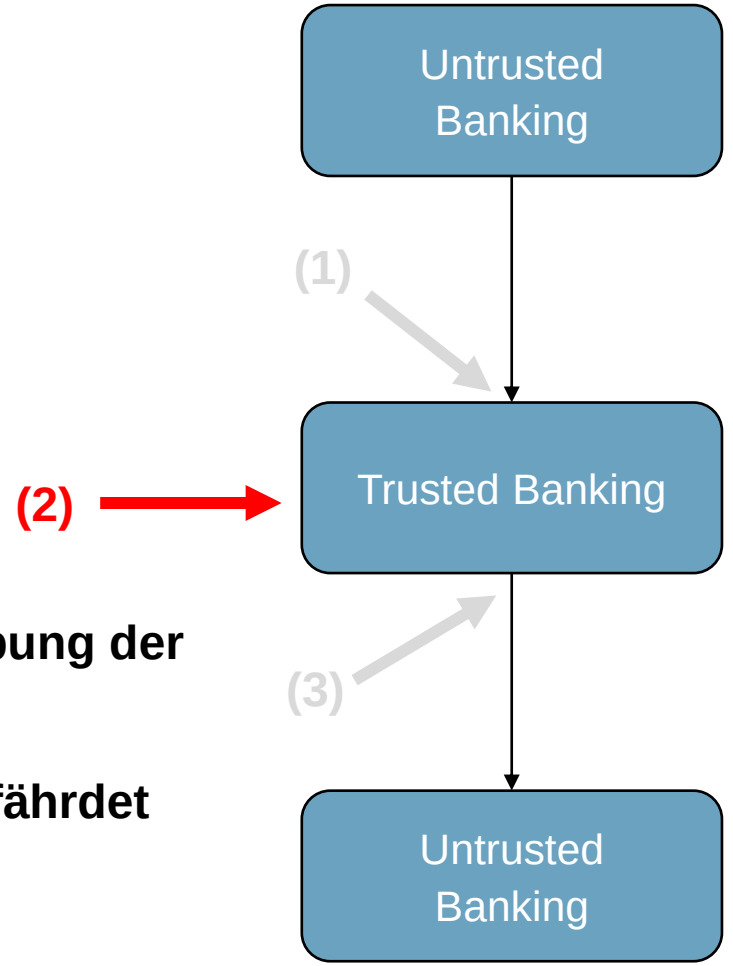
0x0	20	ef	13	10	20	ef	13	10
0x8	12	5c	e1	18	12	5c	e1	18
0x16	X	X	X	X	X	X	X	X
0x24	X	X	X	X	X	X	X	X
0x32	X	X	X	X	X	X	X	X
0x40	14	18	09	3e	14	18	09	3e
0x48	44	17	e1	5c	44	17	e1	5c

int ptr1 **//0x6**

int ptr2 **//0x31**

int ptr3 **//0x15**

Double ptr4 **//0x15**



- **Kann zur Überschreibung der eigenen Daten führen**
- **Datenintegrität ist gefährdet**

Datenkurroption – Pointer

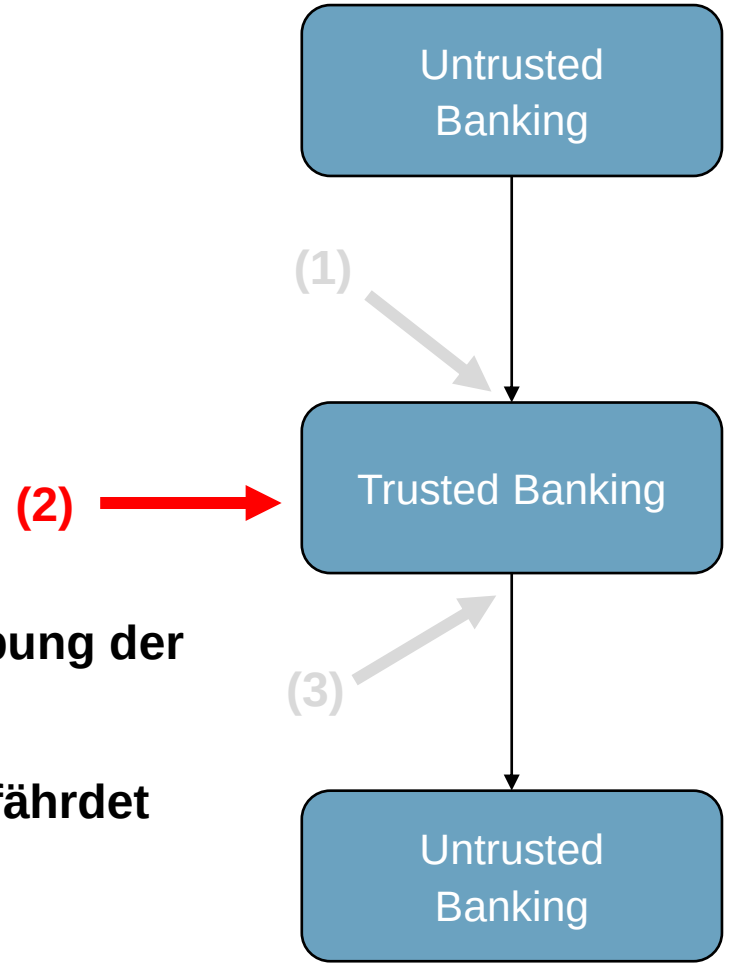
0x0	20	ef	13	10	20	ef	13	10
0x8	12	5c	e1	18	12	5c	e1	18
0x16	X	X	X	X	X	X	X	X
0x24	X	X	X	X	X	X	X	X
0x32	X	X	X	X	X	X	X	X
0x40	14	18	09	3e	14	18	09	3e
0x48	44	17	e1	5c	44	17	e1	5c

int ptr1 **//0x6**

int ptr2 **//0x31**

int ptr3 **//0x15**

Double ptr4 **//0x15**



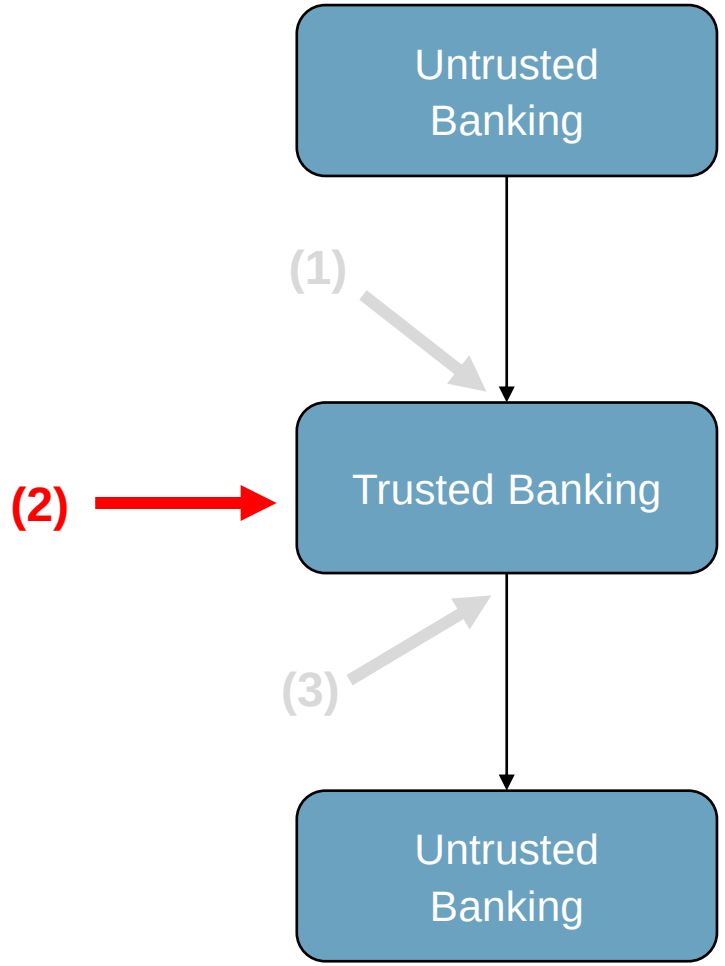
- **Kann zur Überschreibung der eigenen Daten führen**
- **Datenintegrität ist gefährdet**

Datenkurroption – Double-Fetch

0x0	20	ef	13	10	20	ef	13	10
0x8	12	5c	e1	18	12	ptr2	e1	18
0x16	X	X	X	X	X	X	X	X
0x24	X	X	X	X	X	X	X	X
0x32	X	X	X	X	X	X	X	X
0x40	14	18	09	3e	14	18	09	3e
0x48	44	17	e1	5c	44	17	e1	5c

ptr1 **//0x13**

ptr2 **//0x2**



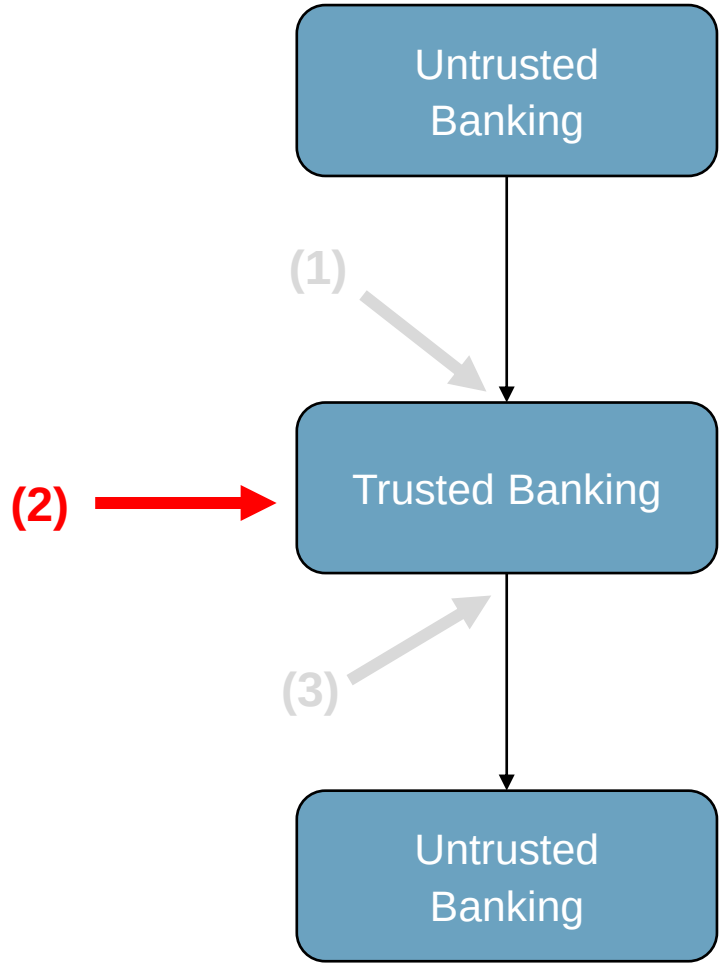
Datenkurroption – Double-Fetch

0x0	20	ef	13	10	20	ef	13	10
0x8	12	5c	e1	18	12	ptr3	e1	18
0x16	X	X	X	X	X	X	X	X
0x24	X	X	X	X	X	X	X	X
0x32	X	X	X	X	X	X	X	X
0x40	14	18	09	3e	14	18	09	3e
0x48	44	17	e1	5c	44	17	e1	5c

ptr1 **//0x13**

ptr2 **//0x2**

ptr3 **//0x30**

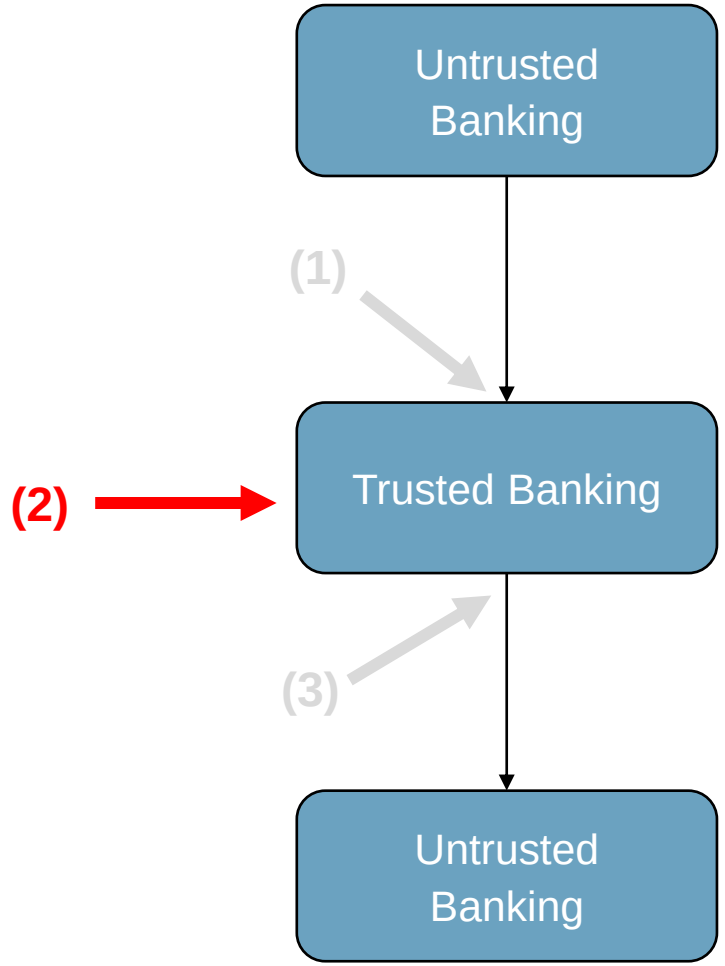


Datenleck – Pointer

0x0	20	ef	13	10	20	ef	13	10
0x8	12	5c	e1	18	12	5c	e1	18
0x16	X	X	X	X	X	X	X	X
0x24	X	X	X	X	X	X	X	X
0x32	X	X	X	X	X	X	X	X
0x40	14	18	09	3e	14	18	09	3e
0x48	44	17	e1	5c	44	17	e1	5c

ptr1 **//0x13**

ptr2 **//0x15**

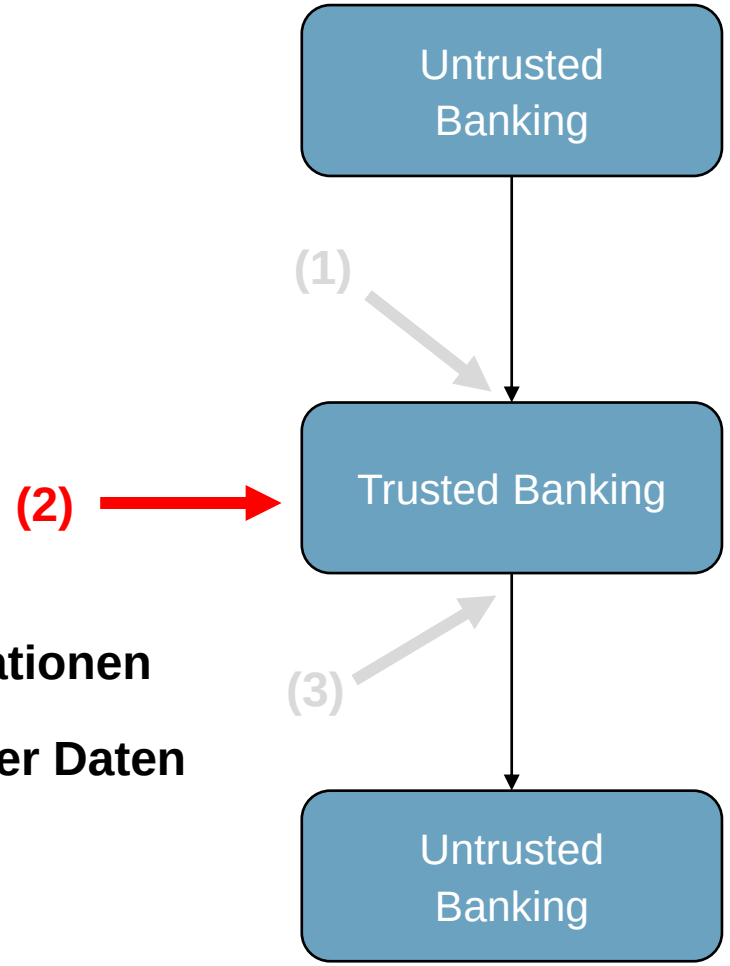


Datenleck – Strings

0x0	20	ef	13	10	20	ef	13	10
0x8	12	5c	e1	18	12	5c	e1	18
0x16	E3	03	54	13	00	18	12	44
0x24	d1	00	13	13	1a	00	5c	e1
0x32	a1	13	13	10	44	ef	20	12
0x40	14	18	09	3e	14	18	09	3e
0x48	44	17	e1	5c	44	17	e1	5c

char ptr1[3]; //0x13

char ptr2[3]; //0x27



Seitenkanalangriff

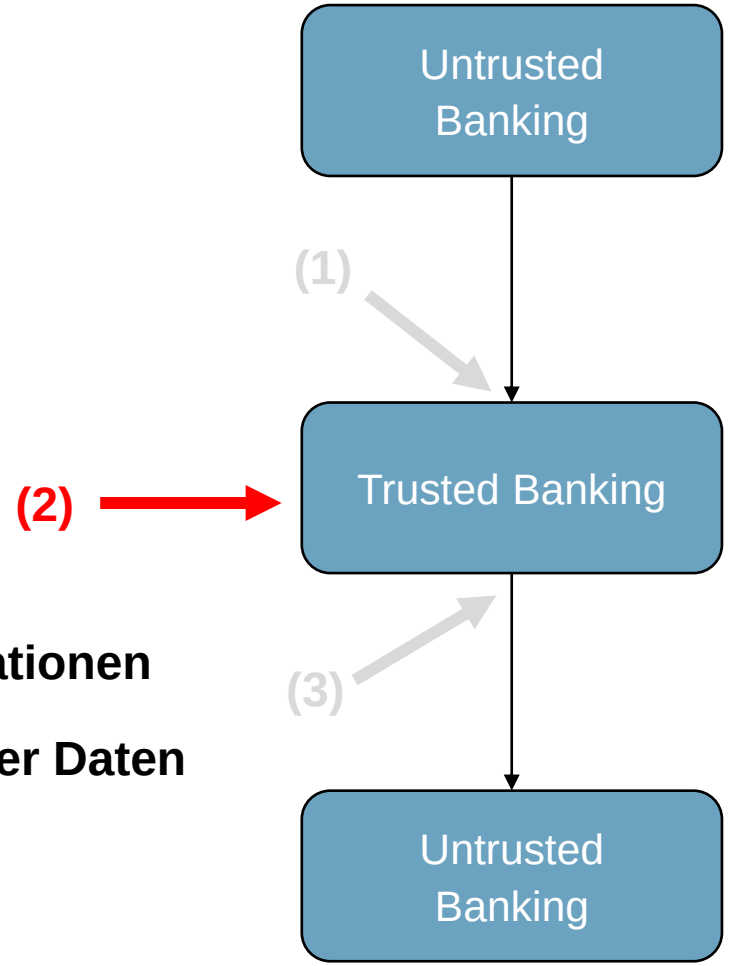
- **Nutzen von phys. Informationen**
- **Erlaubt Rückschlüsse über Daten**

Datenleck – Strings

0x0	20	ef	13	10	20	ef	13	10
0x8	12	5c	e1	18	12	5c	e1	18
0x16	E3	03	54	13	00	18	12	44
0x24	d1	00	13	13	1a	00	5c	e1
0x32	a1	13	13	10	44	ef	20	12
0x40	14	18	09	3e	14	18	09	3e
0x48	44	17	e1	5c	44	17	e1	5c

char ptr1[3]; //0x13

char ptr2[3]; //0x27

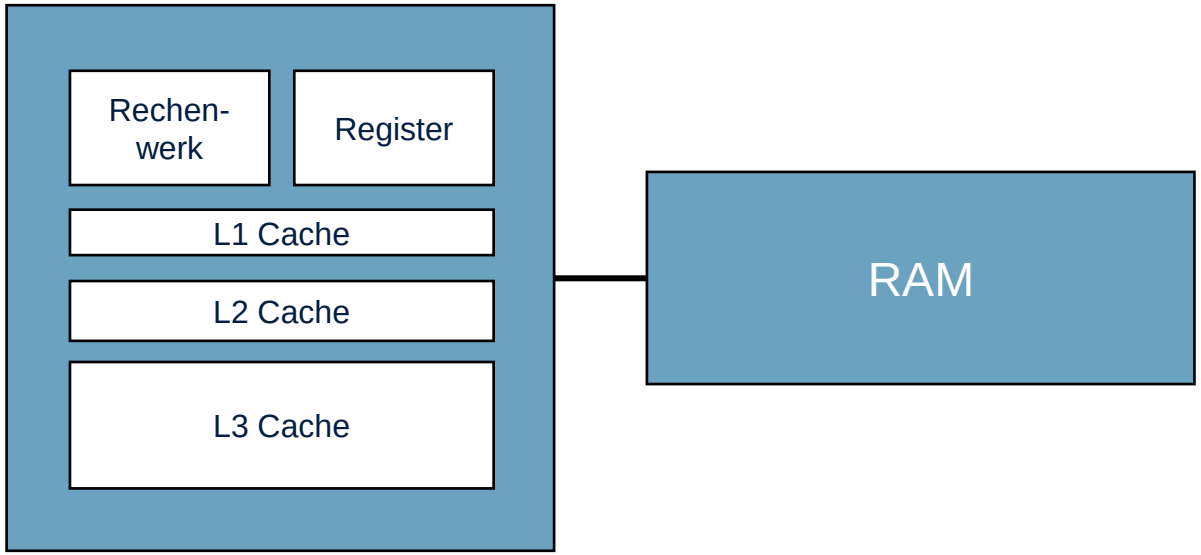


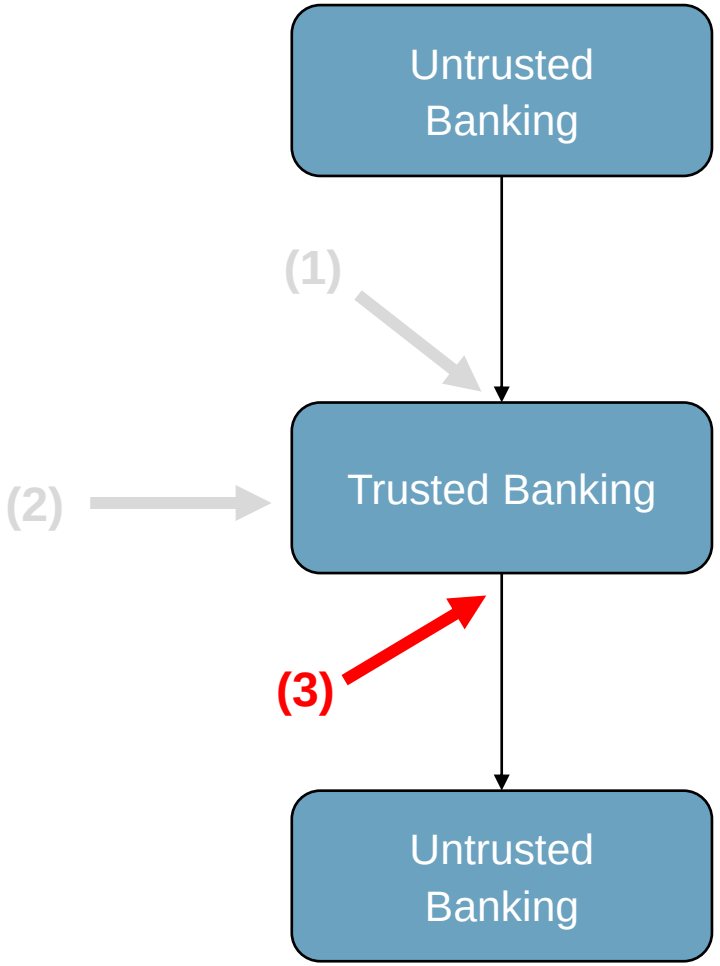
Seitenkanalangriff

- **Nutzen von phys. Informationen**
- **Erlaubt Rückschlüsse über Daten**

Datenleck – Exit

- **Daten im Speicher müssen gelöscht werden**
- **Speicher bereinigen ist Softwareaufgabe**





Fazit

- **TEEs bieten eine zusätzliche Sicherheitsebene**
- **Verhältnismäßig junges Angreifermodell**
- **Eine Sicherheitslücke reicht, um die TEE zu umgehen**

The Devil is in the Detail: Issues with Fine-Grained Trusted Execution Environments