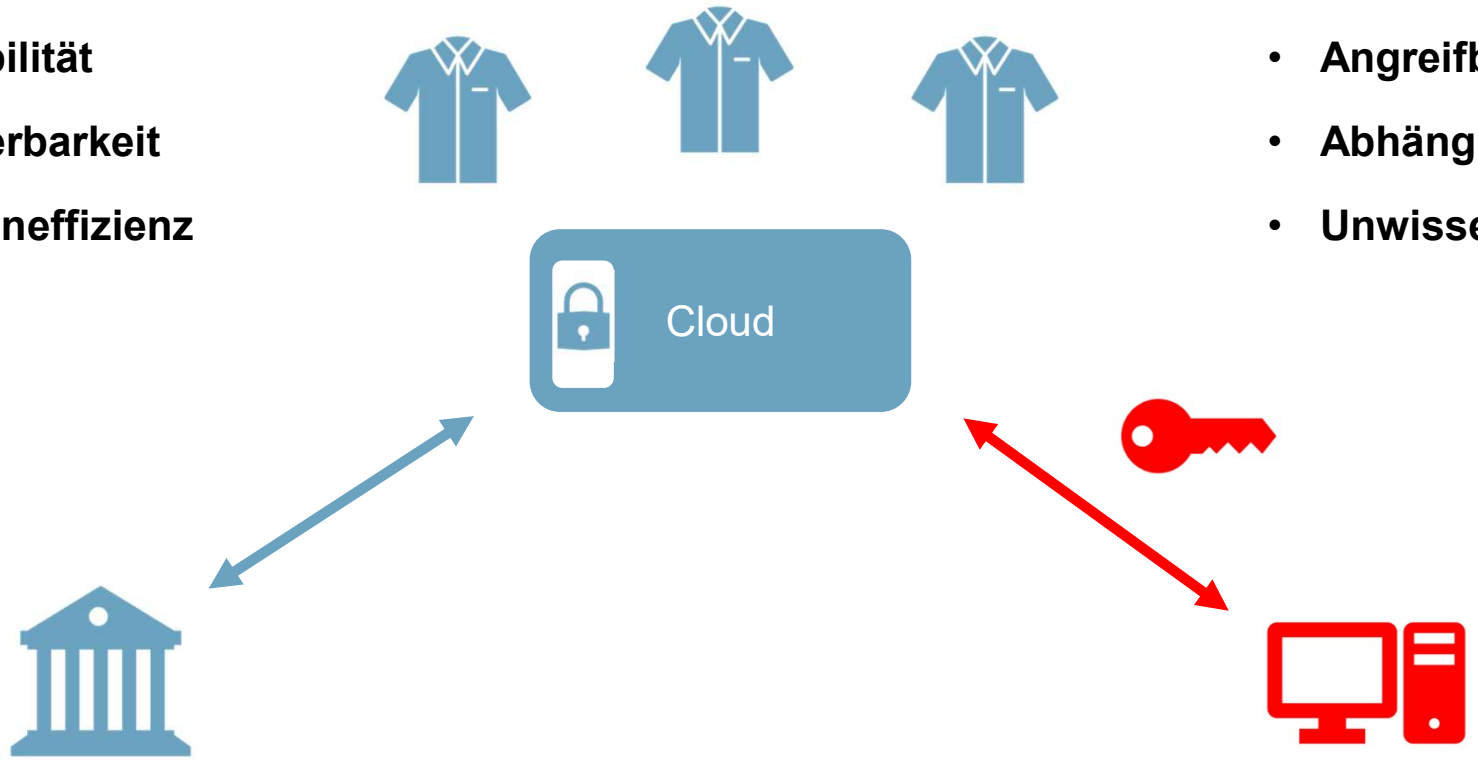
Friedrich-Alexander-Universität
Technische Fakultät

FAU

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

Die Cloud ist gut, aber …

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



- **Angreifbar**
- **Abhängigkeit**
- **Unwissend (?)**

Übersicht

01 Grundlagen

Trusted Execution Environment

Kompartimentierung

02 Angriffe

Datenkorruption

Datenlecks

03 Fazit

Trusted Execution Environment (TEE)

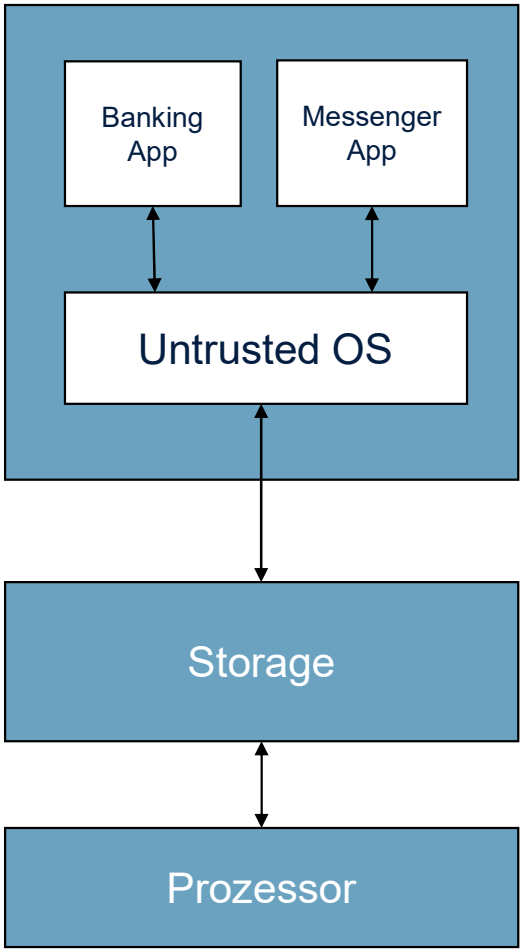
3 Eigenschaften:

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

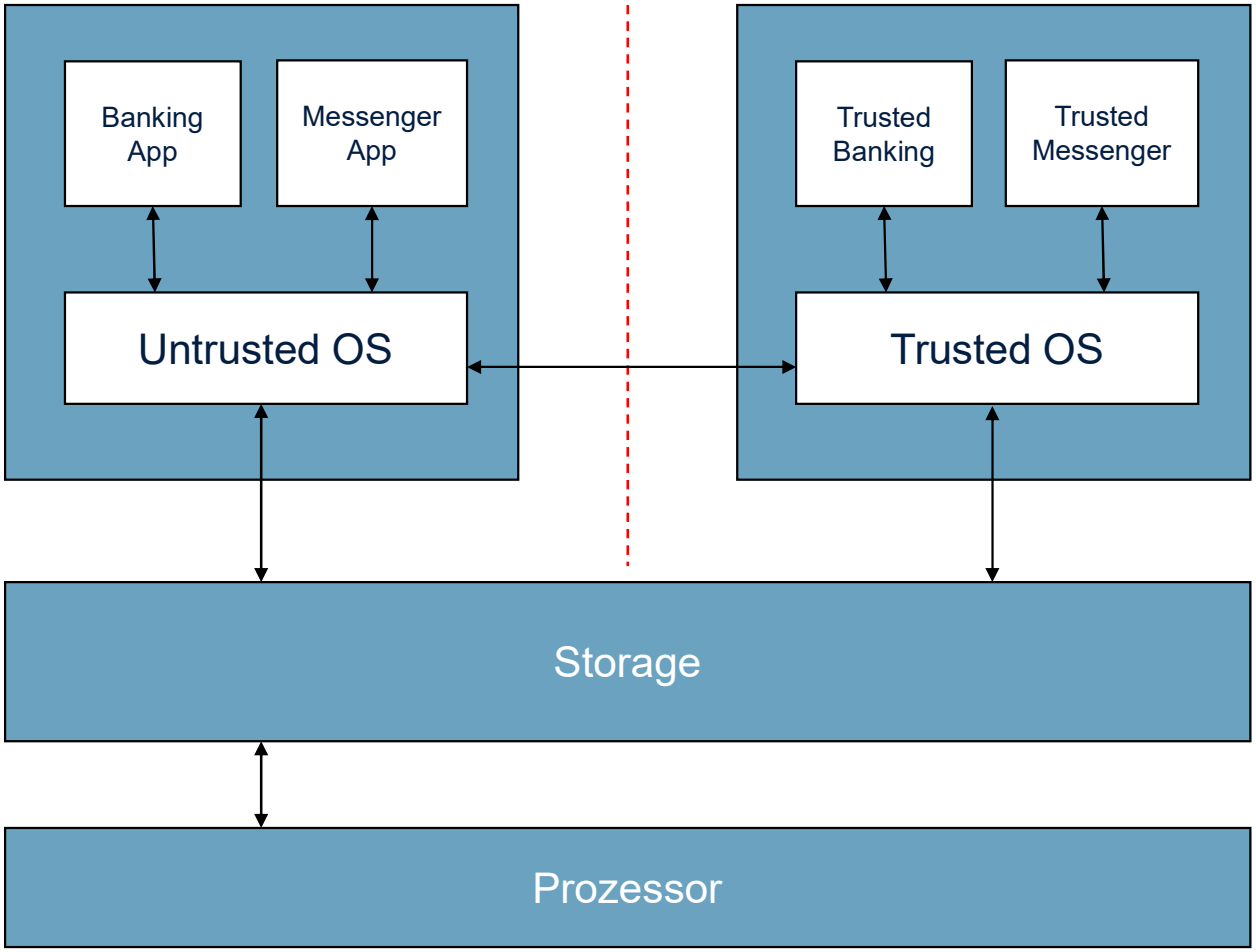
Feingranulare TEE:

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

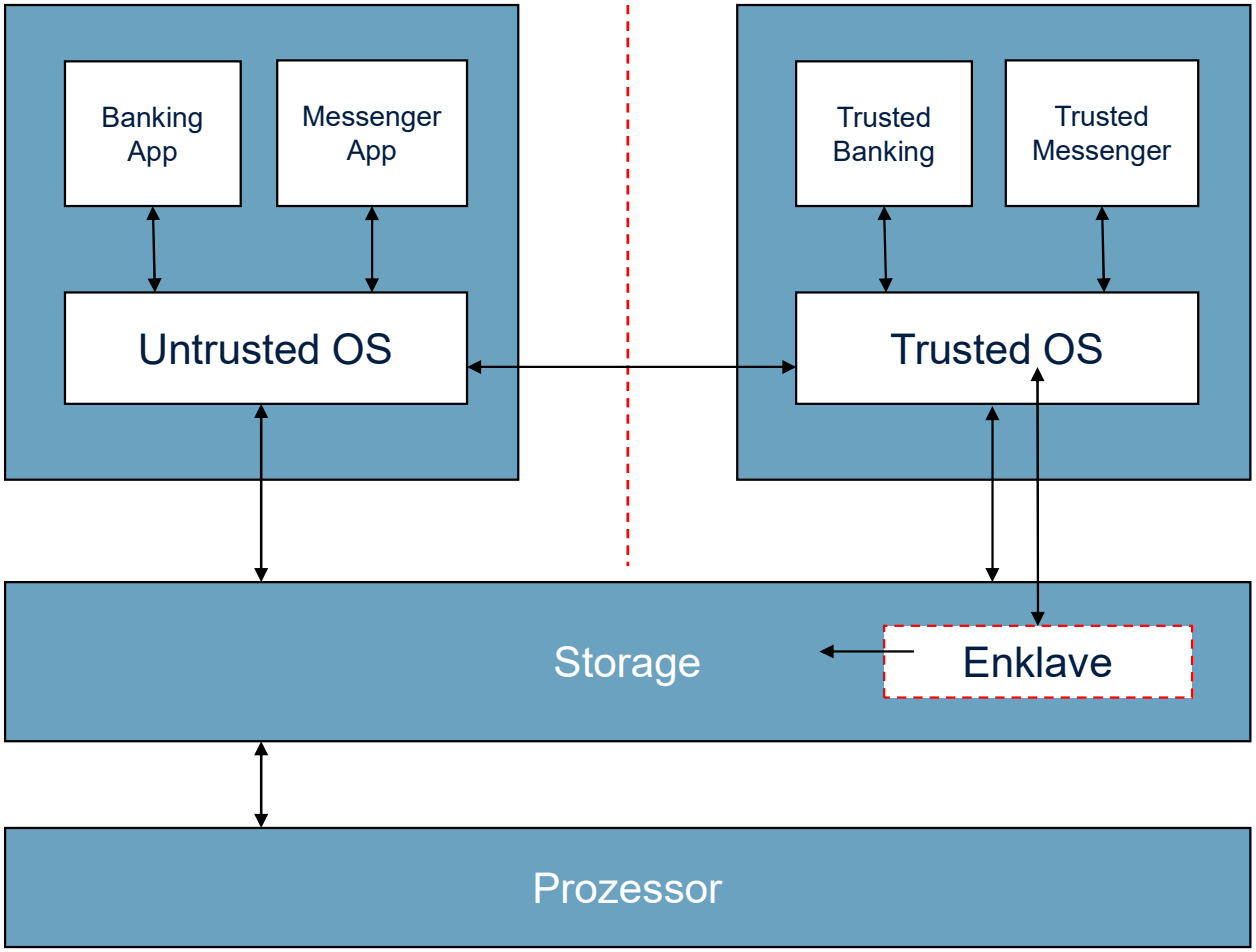
Trusted Execution Environment (TEE)



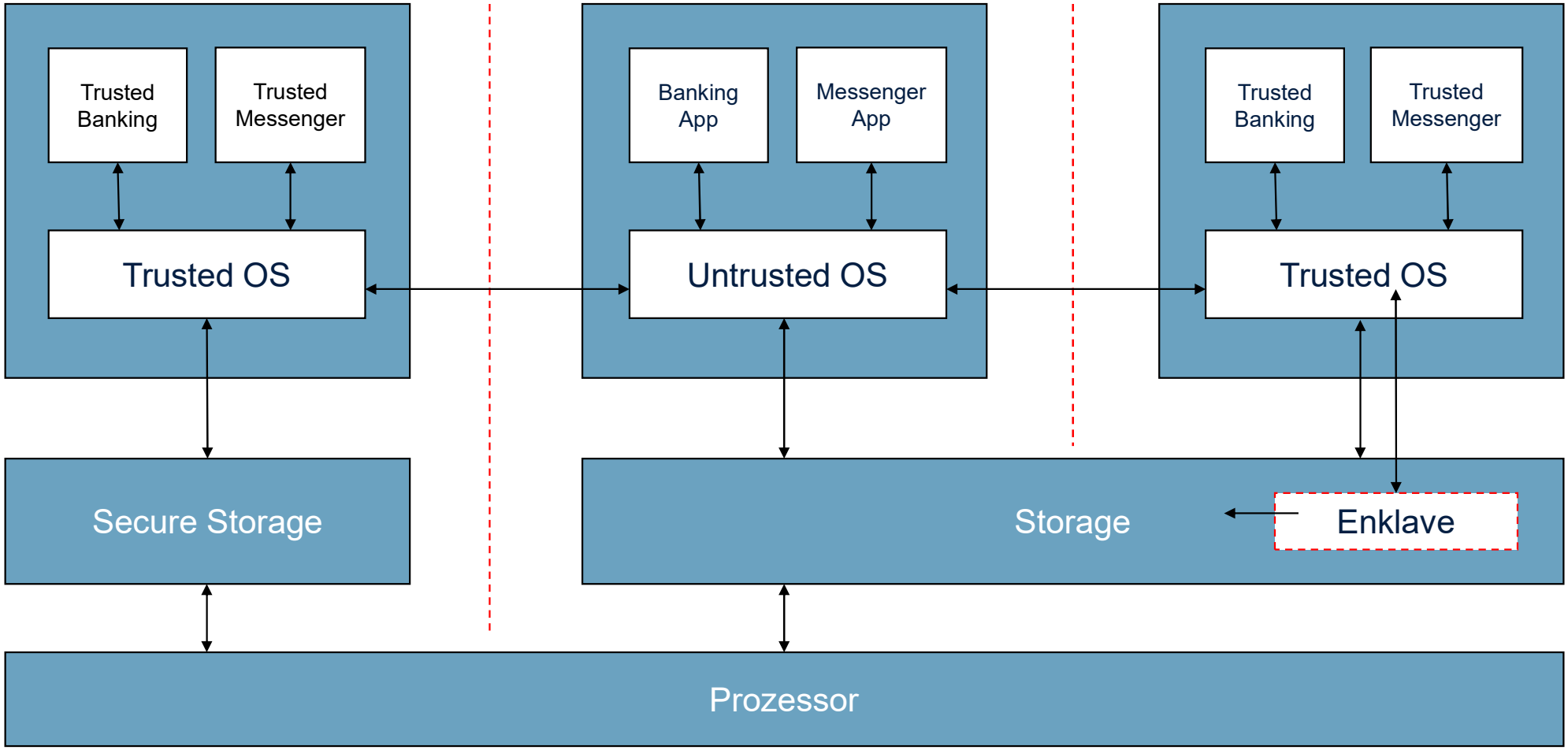
Trusted Execution Environment (TEE)



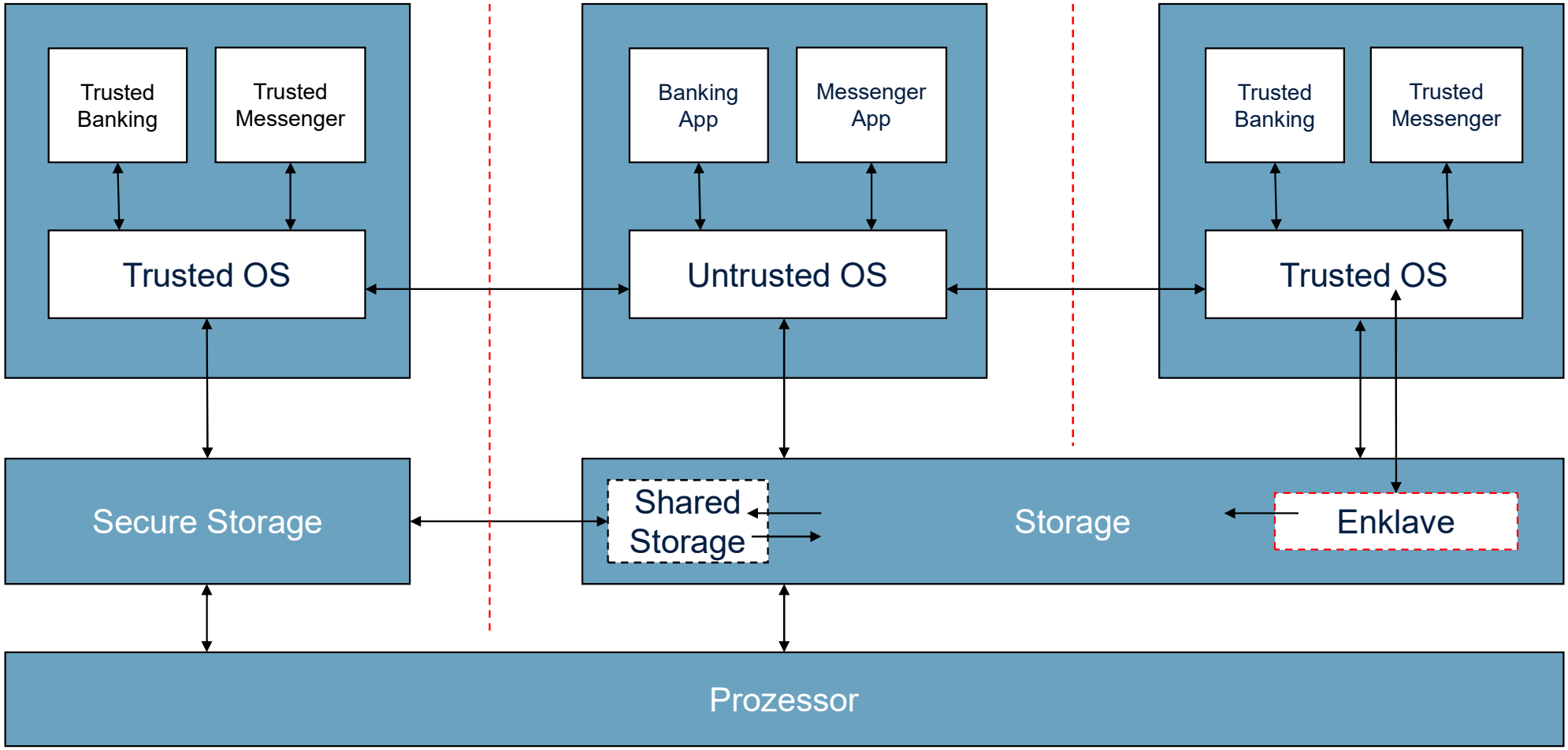
Trusted Execution Environment (TEE)



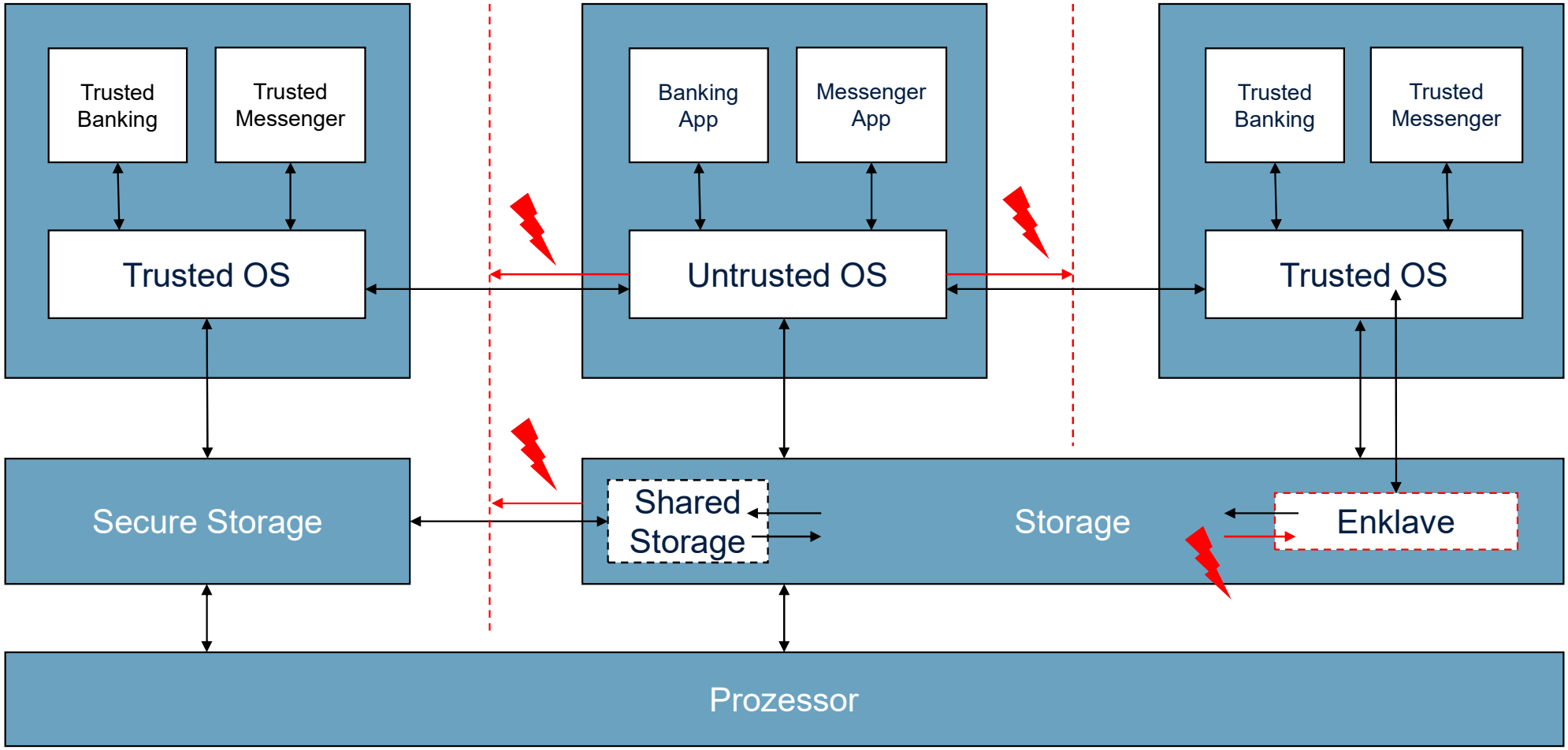
Trusted Execution Environment (TEE)



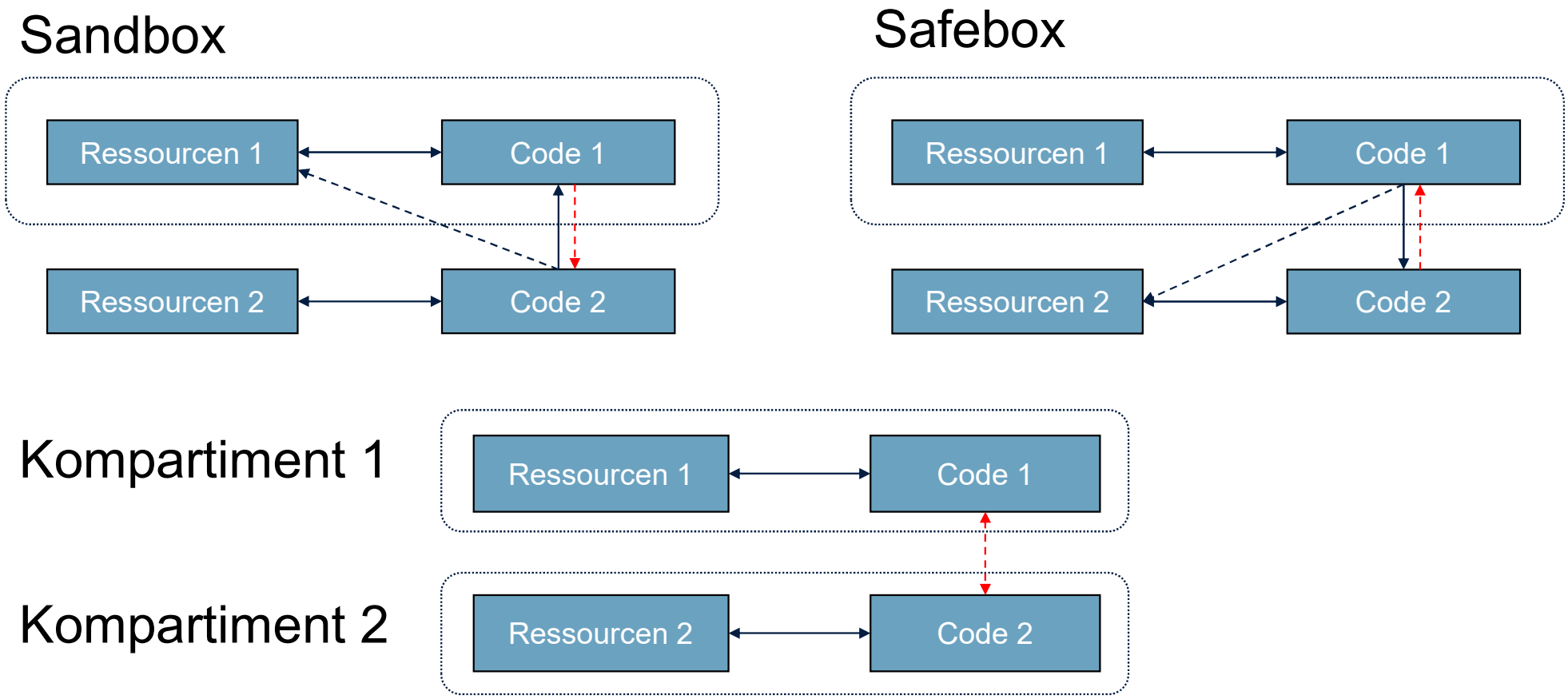
Trusted Execution Environment (TEE)



Trusted Execution Environment (TEE)



Kompartiment



Angriffe

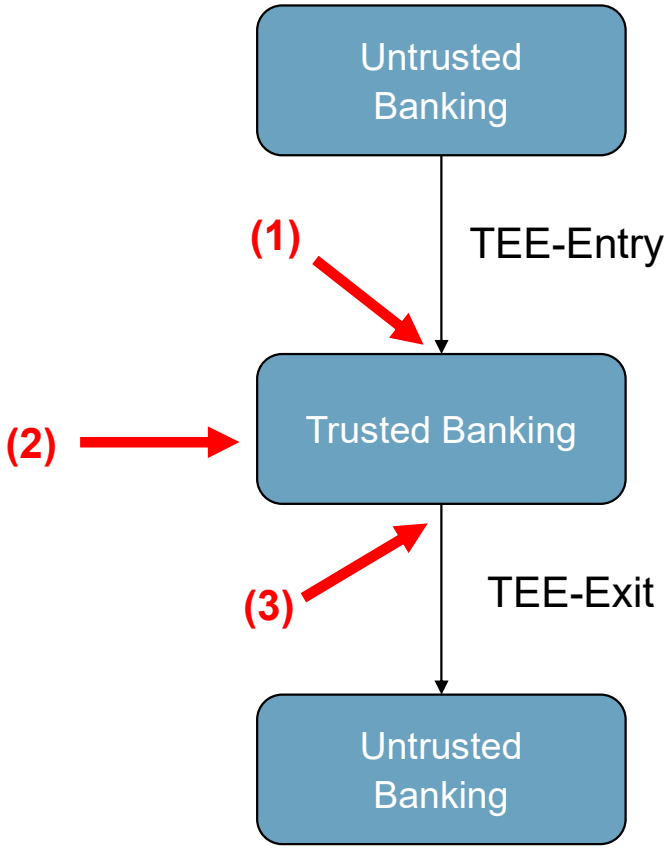
Reihenfolge ändern

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

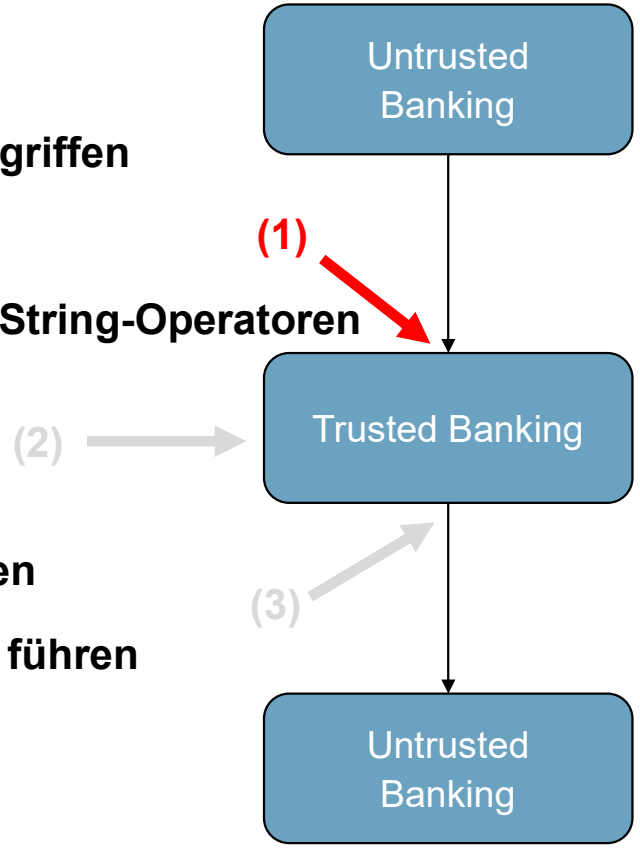
Alignment Check Flag

- **Ausrichtung von Datenzugriffen**

Direction Flag

- **Steuert die Richtung von String-Operatoren**

- **Beeinflussen das Verhalten**
- **Kann auch zu Datenlecks führen**



Datenkurroption – Pointer

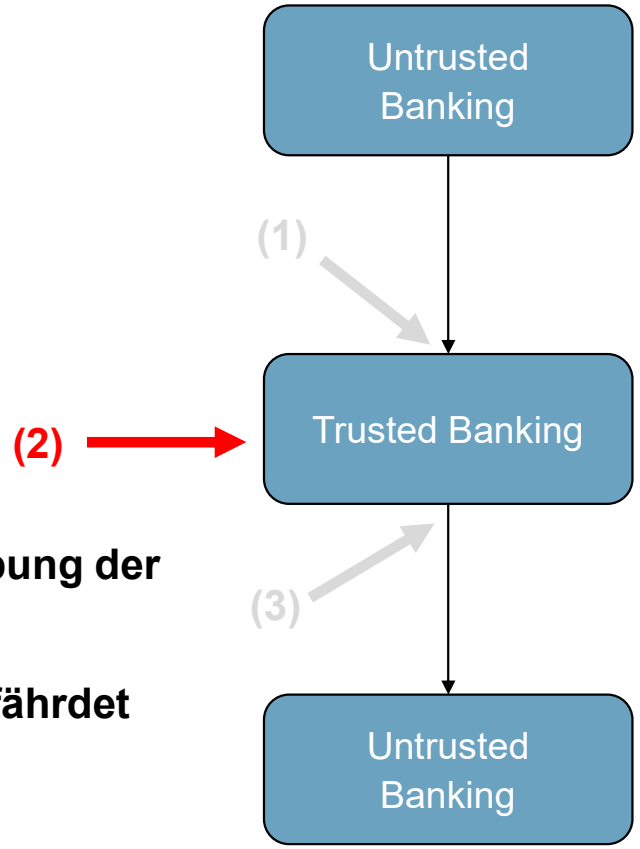
0x0	20	ef	13	10	20	ef	13	10
0x8	12	5c	e1	18	12	5c	e1	18
0x16	X	X	X	X	X	X	X	X
0x24	X	X	X	X	X	X	X	X
0x32	X	X	X	X	X	X	X	X
0x40	14	18	09	3e	14	18	09	3e
0x48	44	17	e1	5c	44	17	e1	5c

int ptr1 **//0x6**

int ptr2 **//0x31**

int ptr3 **//0x15**

Double ptr4 **//0x15**



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

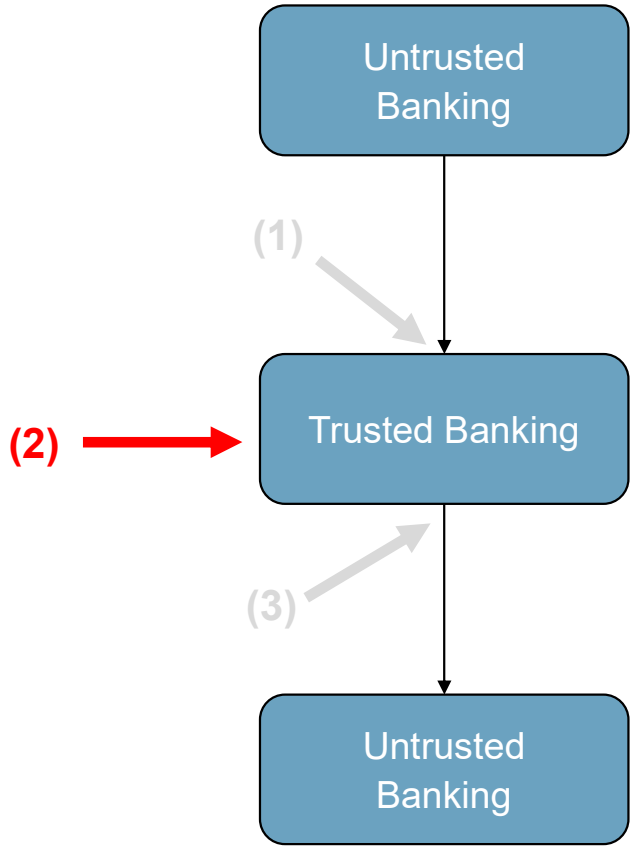
Datenkurroption – Double-Fetch

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**

ptr3 **//0x30**



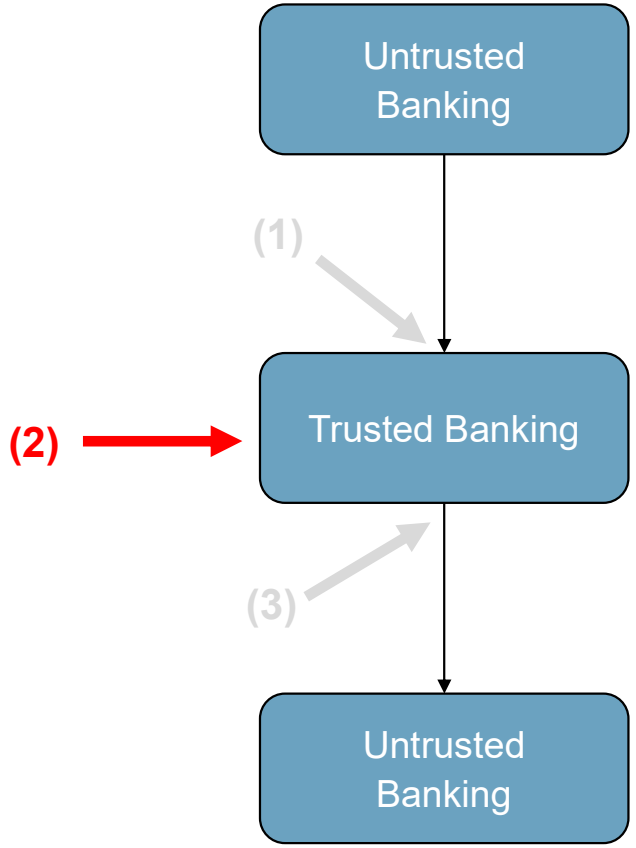
Datenleck – Pointer

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**

- **???**

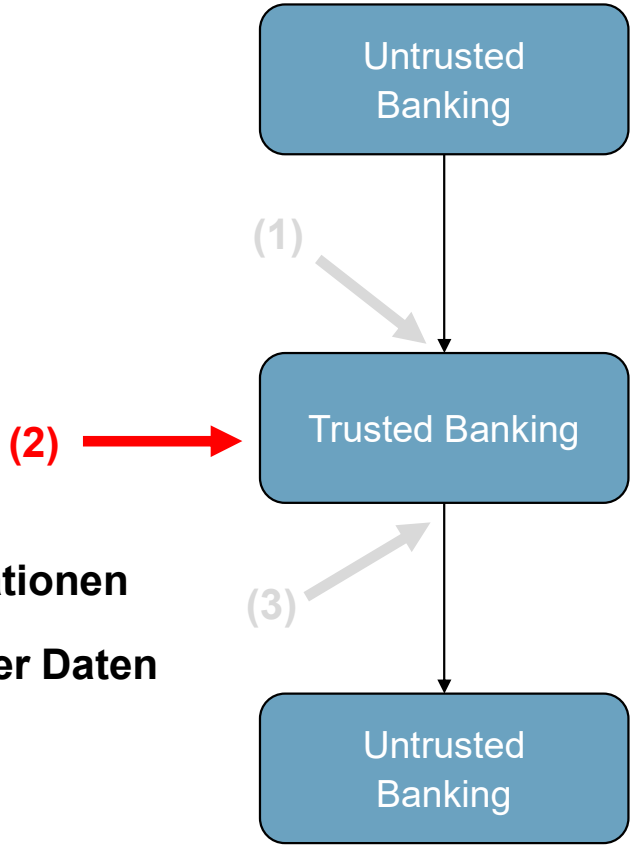


Datenleck – Strings

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

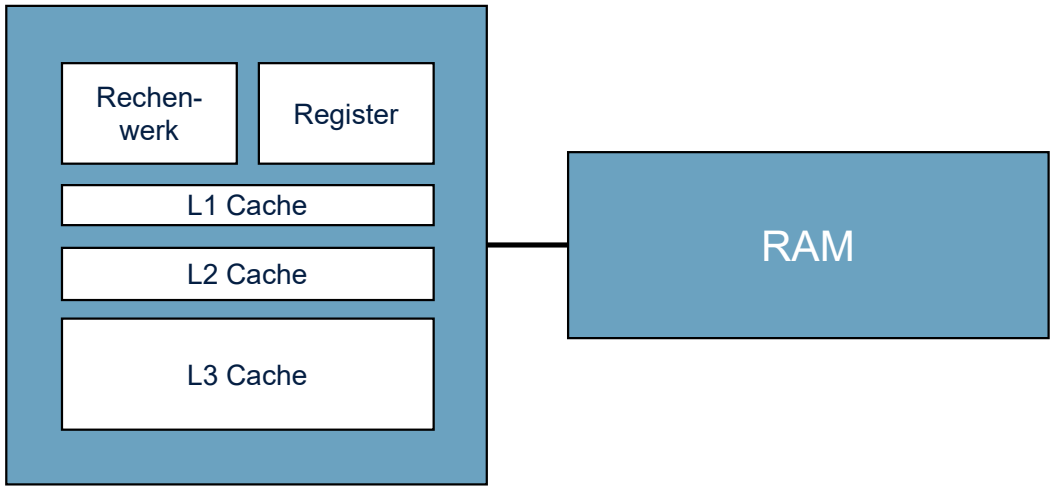


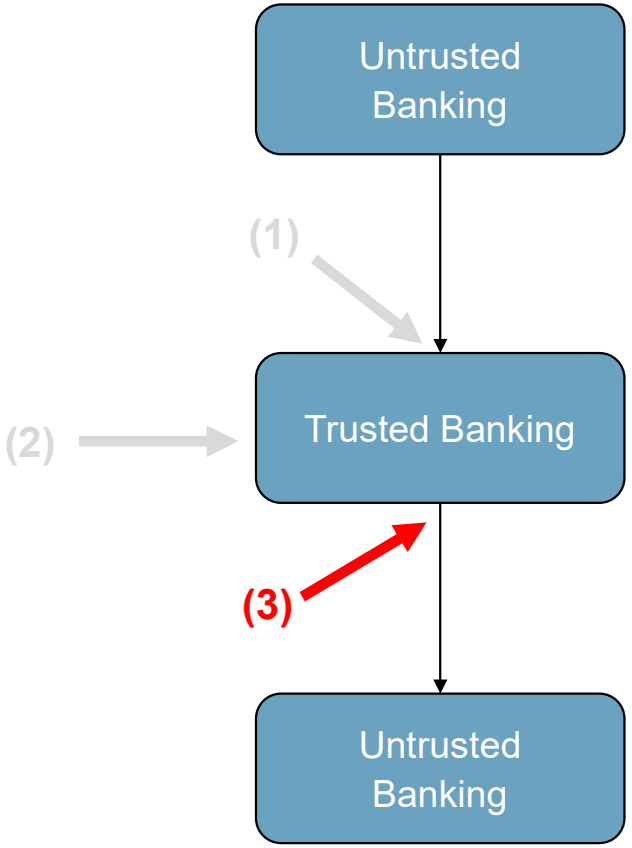
Seitenkanalangriff

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

Datenleck – Exit

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

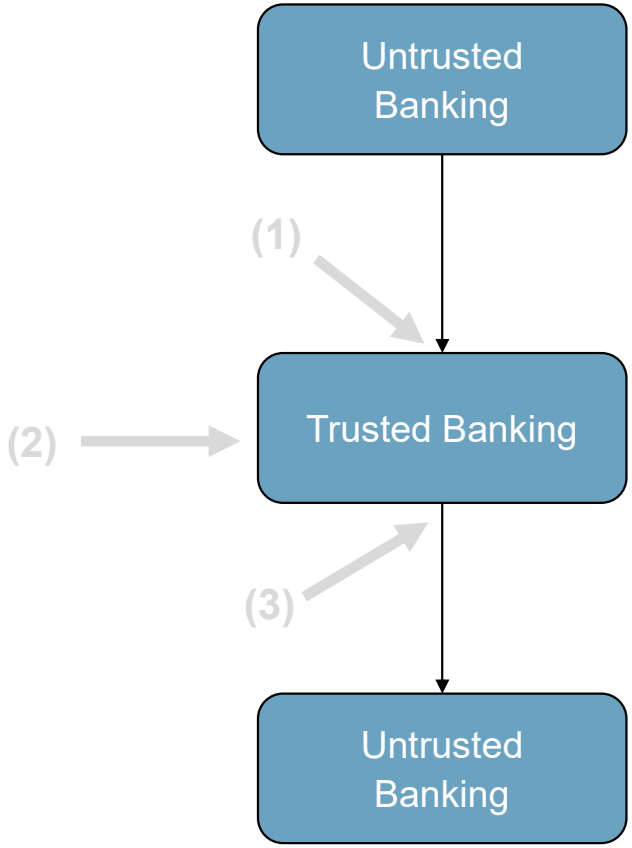




Fazit

- **TEEs bieten mehr Sicherheit**
- **Nicht zu 100% sicher**
- **Eine Sicherheitslücke reicht, um die TEE zu umgehen**

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



Friedrich-Alexander-Universität
Technische Fakultät

FAU

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

Backup Folien

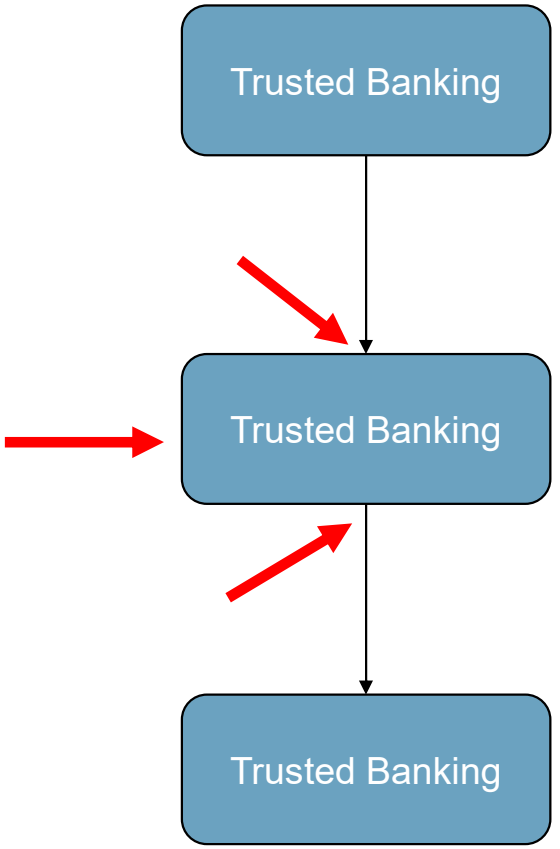
Angriffe

Datenlecks

- Enter oder Exit
- Pointer
- Strings

Datenkorruption

- Flags
- Pointer
- Double fetch



Datenleck – Pointer

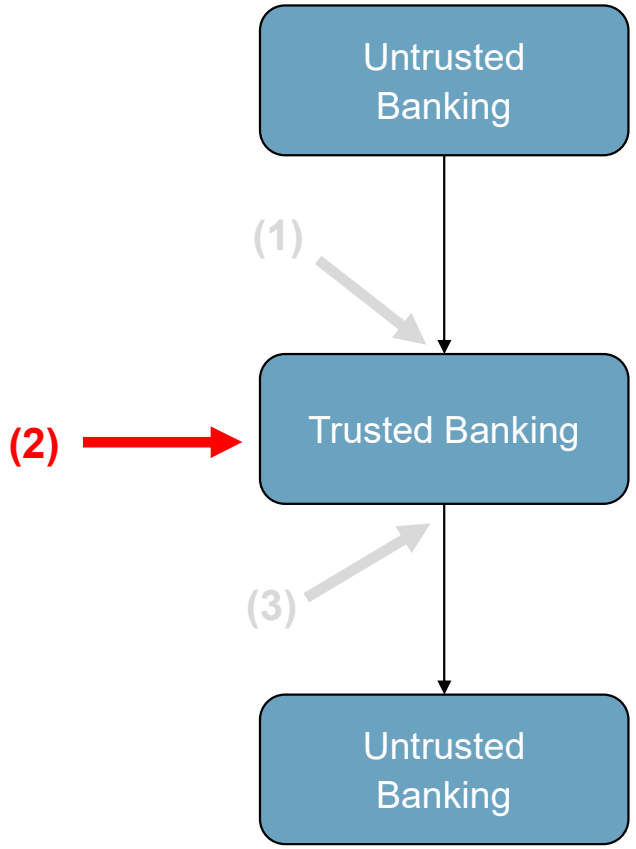
0x0	20	ef	13	10	20	ef	13	10
0x8	12	5c	e1	18	12	5c	e1	18
0x16	X	X	X	X	X	X	X	X
0x24	X	X	X	X	X	X	X	X
0x32	X	X	X	X	X	X	X	X
0x40	14	18	09	3e	14	18	09	3e
0x48	44	17	e1	5c	44	17	e1	5c

int ptr1 **//0x6**

int ptr2 **//0x31**

int ptr3 **//0x15**

Double ptr4 **//0x15**



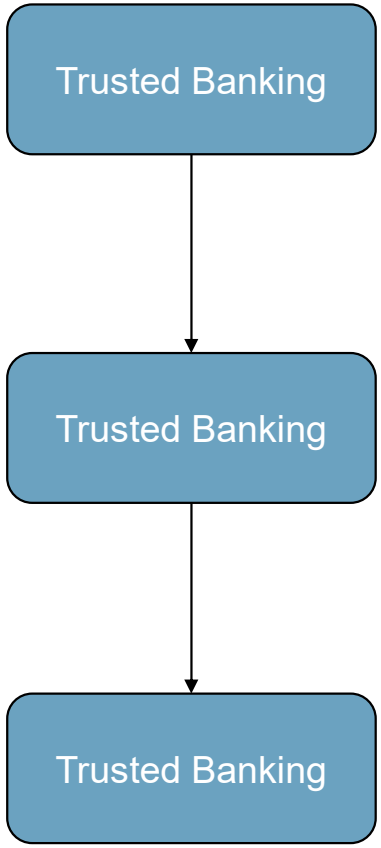
Angriffe

Datenlecks

- Enter oder Exit
- Pointer
- Strings

Datenkorruption

- Flags
- Pointer
- Double fetch



Datenlecks – Enter oder Exit

Beispielfolien

Agenda | mit Bild

Subheadline möglich. Gegebenenfalls löschen.

01 Agendapunkt / Kapitelthema

02 Agendapunkt / Kapitelthema

03 Agendapunkt / Kapitelthema

04 Agendapunkt / Kapitelthema

05 Agendapunkt / Kapitelthema

06 Agendapunkt / Kapitelthema

Bildunterschrift oder Beschreibung möglich.
Gegebenenfalls löschen.

Kapiteltrenner
Mehrzeilig möglich

Textfolie

Subheadline möglich. Gegebenenfalls löschen.

Lorem ipsum dolor sit amet,

consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

- Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi.

Textfolie | zweispaltig

Subheadline möglich. Gegebenenfalls löschen.

Lorem ipsum dolor sit amet,

consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

- Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam.

Lorem ipsum dolor sit amet,

consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

- Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam.

Textfolie | dreispaltig

Subheadline möglich. Gegebenenfalls löschen.

Lorem ipsum dolor sit amet,

consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

- At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus.

Lorem ipsum dolor sit amet,

consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

- At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus.

Lorem ipsum dolor sit amet,

consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

- At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus.

Text- Bildfolie

Subheadline möglich. Gegebenenfalls löschen.

Lorem ipsum dolor sit amet,

consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

- Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam.

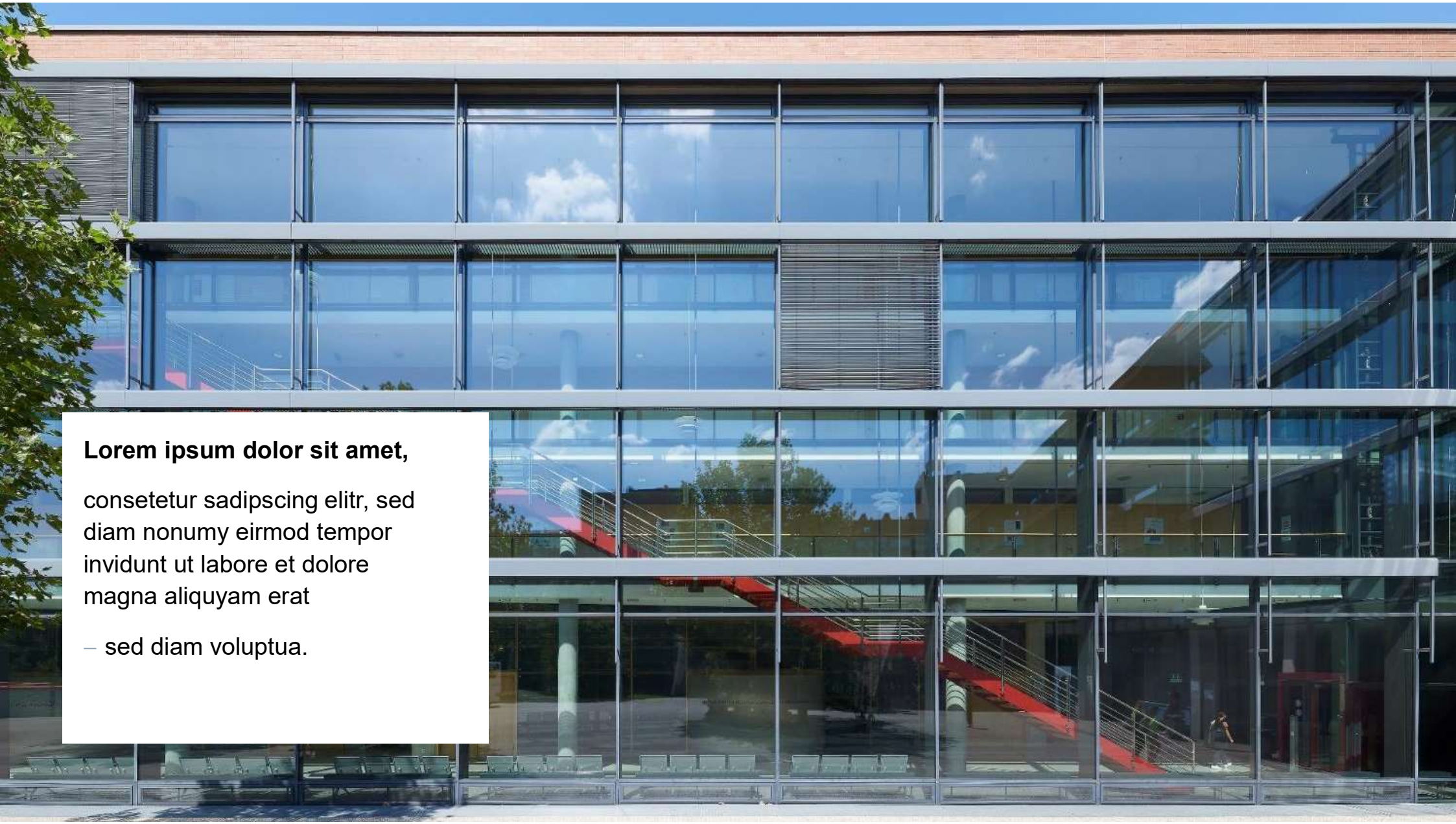
Bild- Textfolie

Subheadline möglich. Gegebenenfalls löschen.

Lorem ipsum dolor sit amet,

consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

- Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam.



Lorem ipsum dolor sit amet,

consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat

– sed diam voluptua.

Bildfolie

Subheadline möglich. Gegebenenfalls löschen.

Bildunterschrift oder Beschreibung möglich. Gegebenenfalls löschen.

Bildfolie | zweispaltig

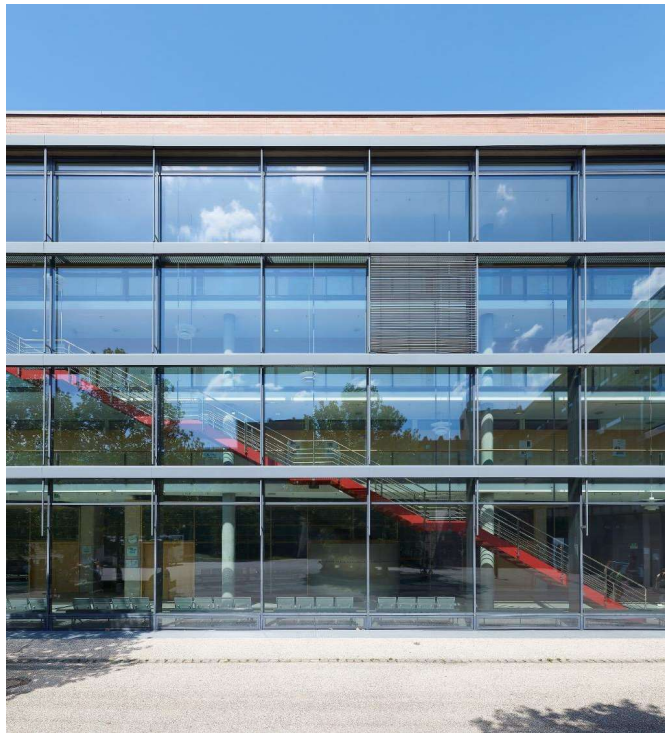
Subheadline möglich. Gegebenenfalls löschen.

Bildunterschrift oder Beschreibung möglich.
Gegebenenfalls löschen.

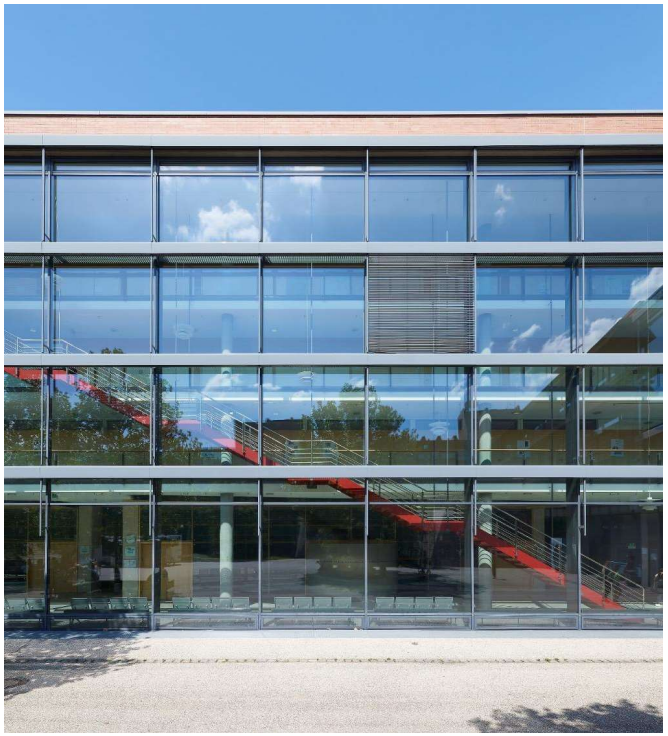
Bildunterschrift oder Beschreibung möglich.
Gegebenenfalls löschen.

Bildfolie | dreispaltig

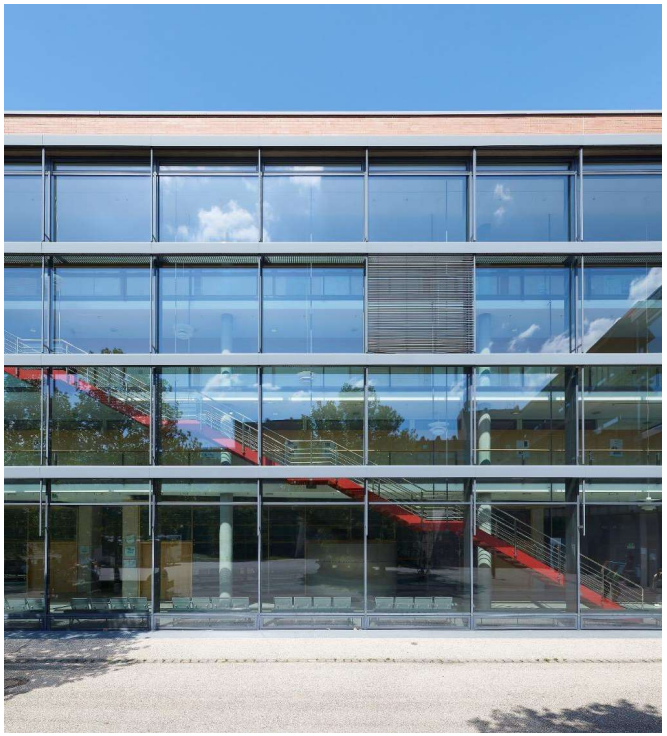
Subheadline möglich. Gegebenenfalls löschen.



Bildunterschrift oder Beschreibung möglich. Gegebenenfalls löschen.



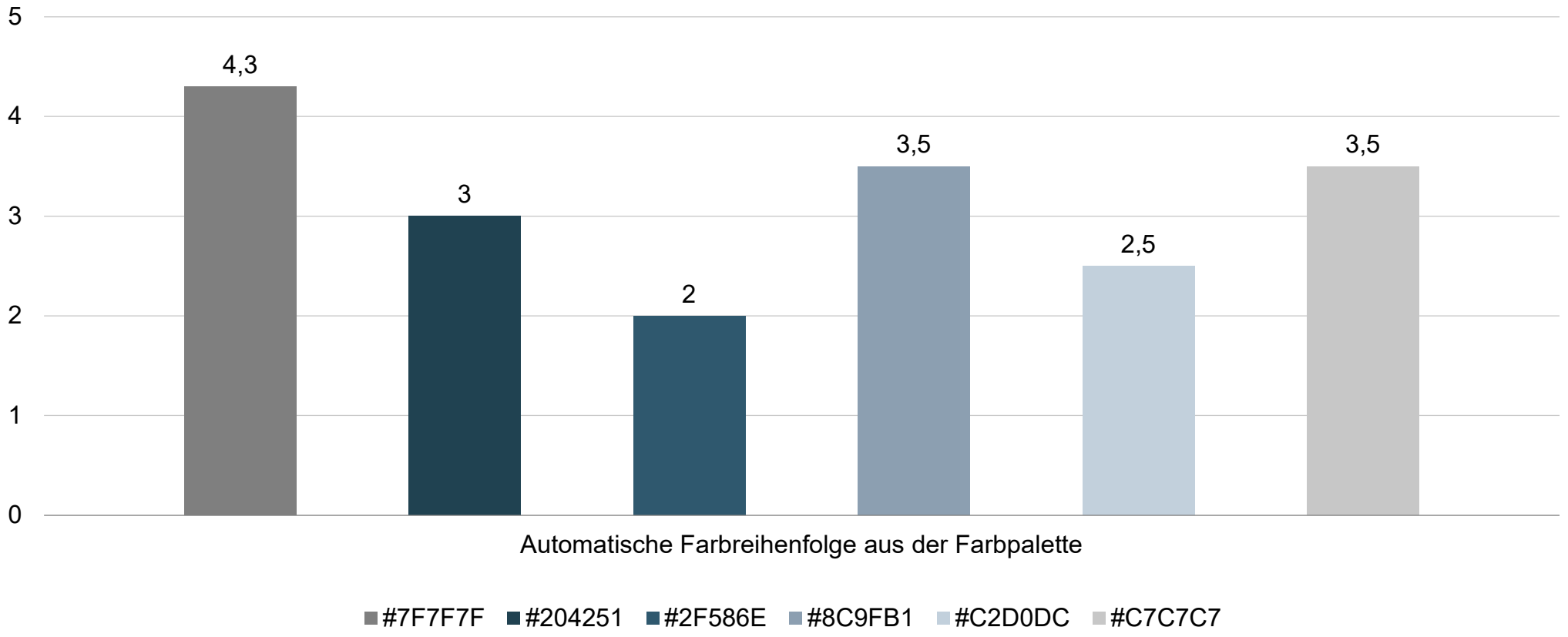
Bildunterschrift oder Beschreibung möglich. Gegebenenfalls löschen.



Bildunterschrift oder Beschreibung möglich. Gegebenenfalls löschen.

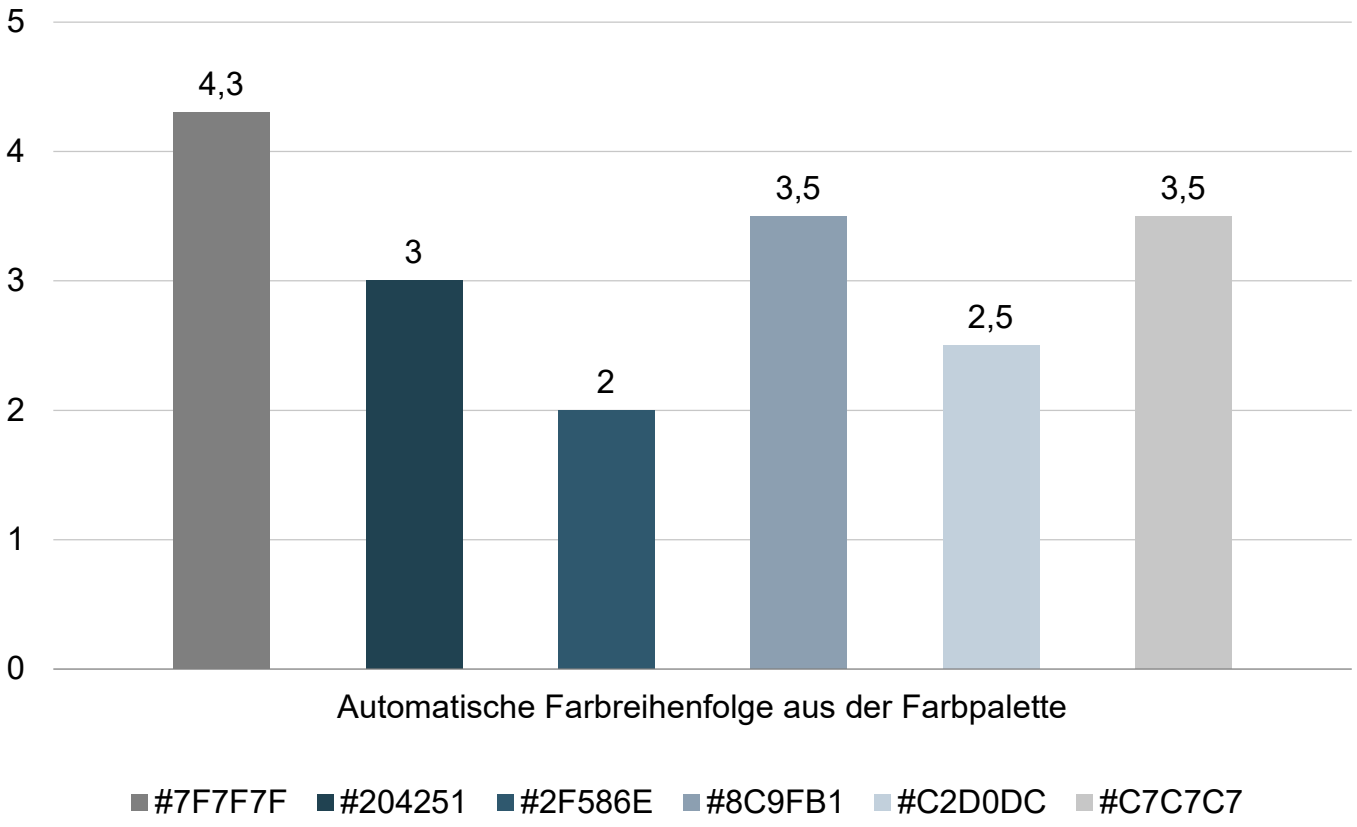
Inhaltsfolie | Säulendiagramm

Subheadline möglich. Gegebenenfalls löschen.



Inhaltsfolie mit Text | Säulendiagramm

Subheadline möglich. Gegebenenfalls löschen.



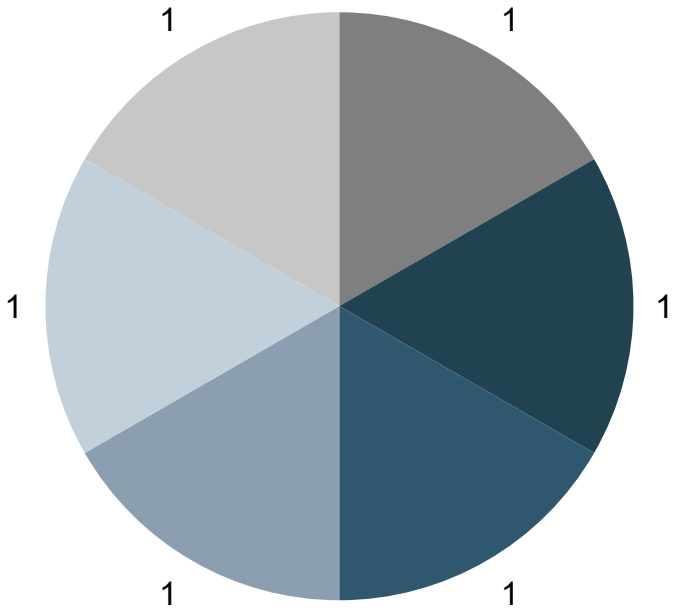
Lorem ipsum dolor sit amet,

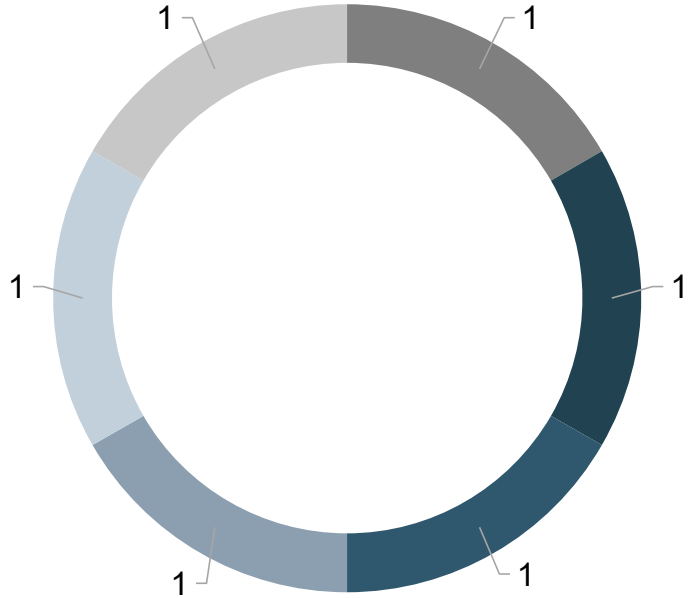
consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

- At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus.

Inhaltsfolie | Torten- & Ringdiagramm

Subheadline möglich. Gegebenenfalls löschen.



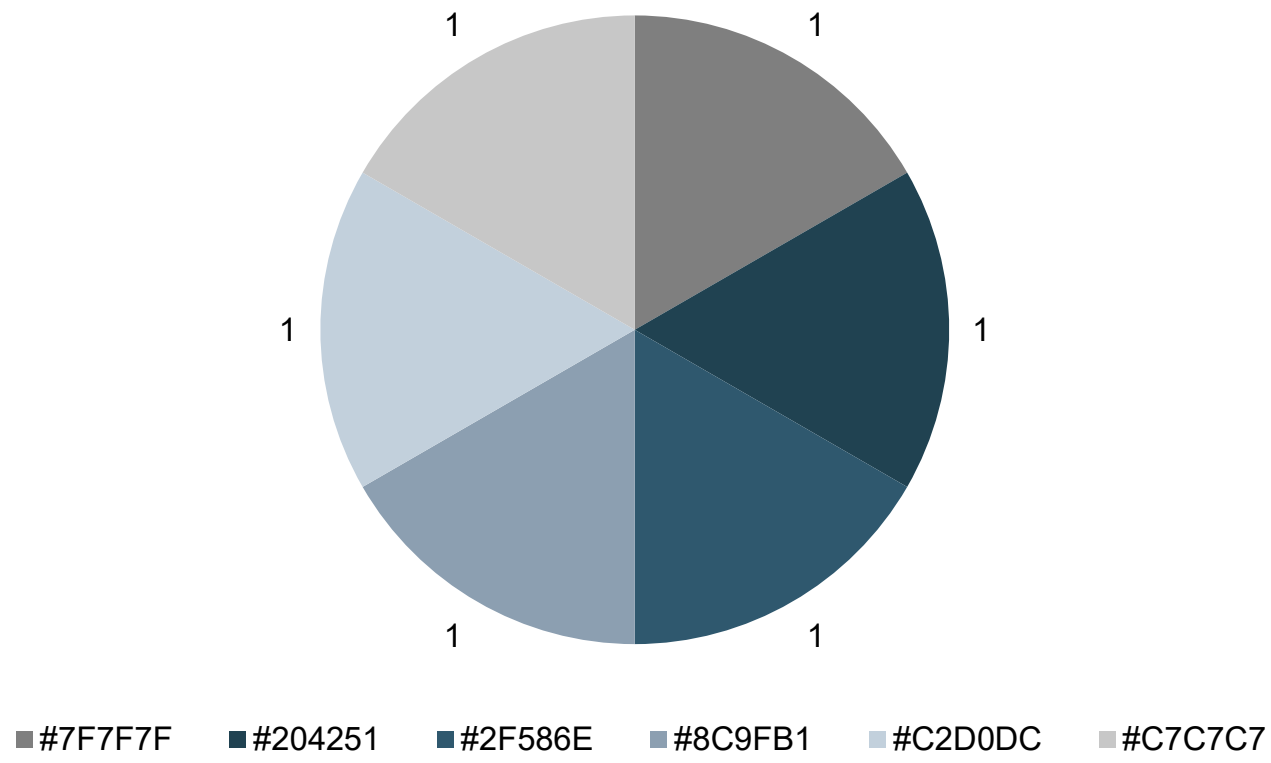


#7F7F7F #204251 #2F586E #8C9FB1 #C2D0DC #C7C7C7

#7F7F7F #204251 #2F586E #8C9FB1 #C2D0DC #C7C7C7

Inhaltsfolie mit Text | Torten- & Ringdiagramm

Subheadline möglich. Gegebenenfalls löschen.



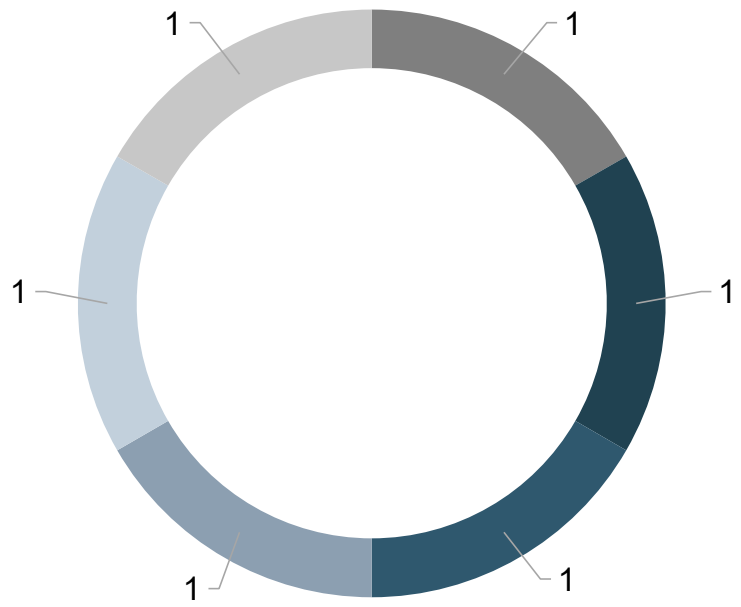
Lorem ipsum dolor sit amet,

consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

- At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus.

Inhaltsfolie mit Text | Torten- & Ringdiagramm

Subheadline möglich. Gegebenenfalls löschen.



#7F7F7F #204251 #2F586E #8C9FB1 #C2D0DC #C7C7C7

Lorem ipsum dolor sit amet,

consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

- At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus.

Inhaltsfolie | Tabellenbeispiel

Subheadline möglich. Gegebenenfalls löschen.

Lorem ipsum dolor sit amet	Lorem ipsum	Lorem ipsum	Lorem ipsum	Lorem ipsum	Lorem ipsum
Lorem ipsum dolor sit amet	xxxx	xxxx	xxxx	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx	xxxx	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx	xxxx	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx	xxxx	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx	xxxx	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx	xxxx	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx	xxxx	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx	xxxx	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx	xxxx	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx	xxxx	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx	xxxx	xxxx	xxxx

Inhaltsfolie mit Text | Tabellenbeispiel

Subheadline möglich. Gegebenenfalls löschen.

Lorem ipsum dolor sit amet	Lorem ipsum	Lorem ipsum
Lorem ipsum dolor sit amet	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx
Lorem ipsum dolor sit amet	xxxx	xxxx

Lorem ipsum dolor sit amet,

consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

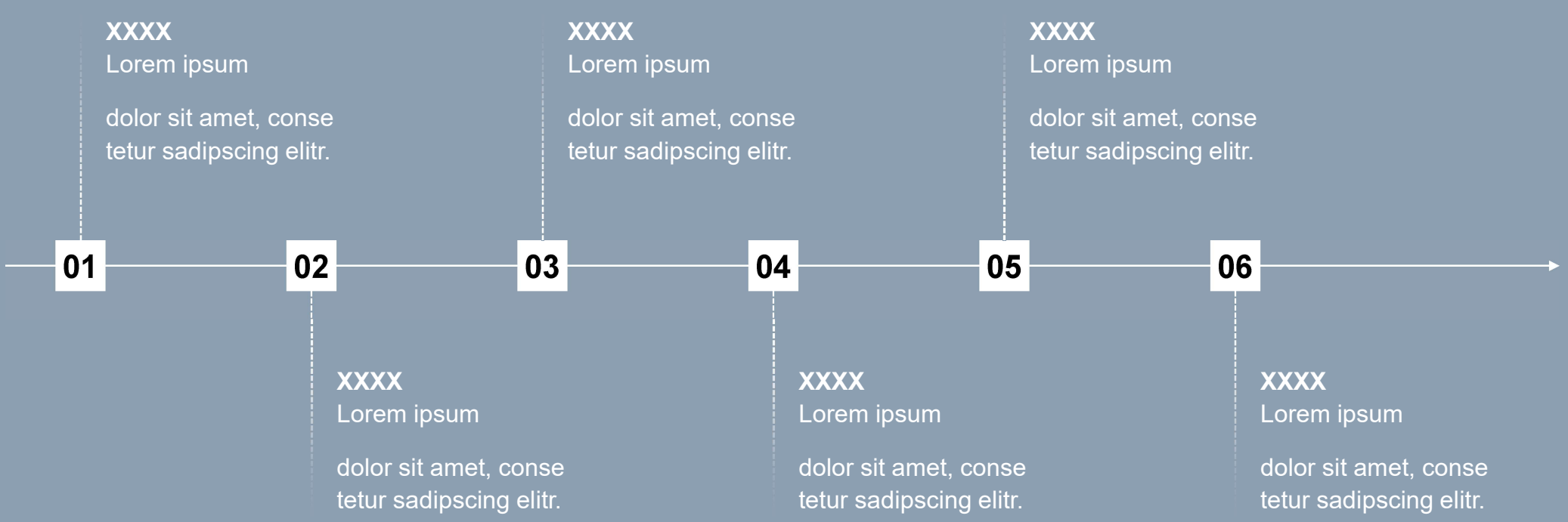
- At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus.

Folie zur freien Gestaltung | Grau

Subheadline möglich. Gegebenenfalls löschen.

Folie zur freien Gestaltung | Beispiel: Zeitstrahl

Subheadline möglich. Gegebenenfalls löschen.

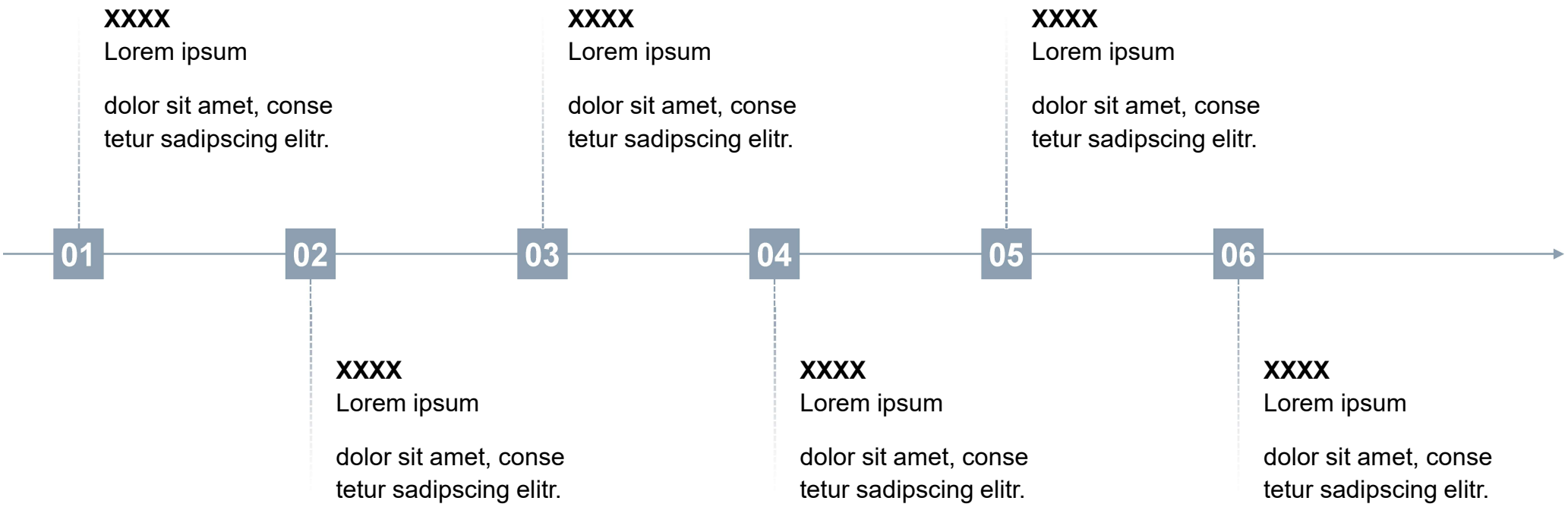


Folie zur freien Gestaltung | weiß

Subheadline möglich. Gegebenenfalls löschen.

Folie zur freien Gestaltung | Beispiel: Zeitstrahl

Subheadline möglich. Gegebenenfalls löschen.



Zitatfolie

Subheadline möglich. Gegebenenfalls löschen.

„Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.“

Vielen Dank
für Ihre Aufmerksamkeit!