

# Anwendungsfälle und Datenfluss

Welche Daten fließen bei welchen Anwendungsfällen wohin

# Anwendungsfälle – Gruppen

- Grundfunktionen
- Produkt- und Kontrollmodule (Umsetzung gegebenenfalls später als separates Projekt)
- Sperrwesen – Vorbereitung
- Sperrwesen – Durchführung
- Monitoring

# Grundfunktionen

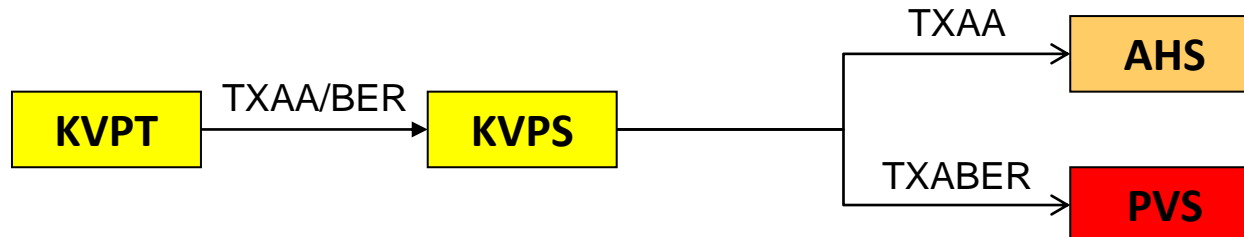
Ausgabe – Rücknahme Applikation/Berechtigung

# Vorbereitung – Ausgabe/Rücknahme

- Bevor Daten für eine Applikation oder Berechtigung geschrieben werden können, müssen sich Terminal und SAM sowie Chipkarte und SAM gegenseitig als authentisch erweisen
- Dies erfolgt über eine Prüfung von verschlüsselten Signaturen

# Applikation/Berechtigung – Ausgabe

- Die Ausgabe einer Berechtigung aber auch einer Applikation im KVPT besteht aus drei Teilen:
  1. Einbringen der Daten (Zeitliche Gültigkeit etc.)
  2. Einbringen von 6 Schlüsseln (Erfassungsschlüssel, KVP- und PV-Schlüssel in Regel- und Notfallversion)
  3. Durchführen der Ausgabetransaktion



## Berechtigung – Ausgabe

- Bei der Ausgabe einer Berechtigung muss vom KVP eine eindeutige berechtigungNummer vergeben werden (siehe auch SysLH\_KVPS)
- Diese berechtigungNummer muss über alle Systeme des KVP also auch über HandyTicket- und/oder Online-Ticket-Systeme eindeutig sein
- Nach Ablauf der Gültigkeit einer Berechtigung plus einer Karenzzeit kann die verwendete berechtigungNummer erneut vergeben werden

# Berechtigung - Rücknahme

- Die Rücknahme einer Berechtigung (aber auch einer Applikation) besteht aus zwei Teilen:
  1. Durchführen der Rücknahmetransaktion
  2. Löschen der Berechtigung (oder Applikation)



# Grundfunktionen

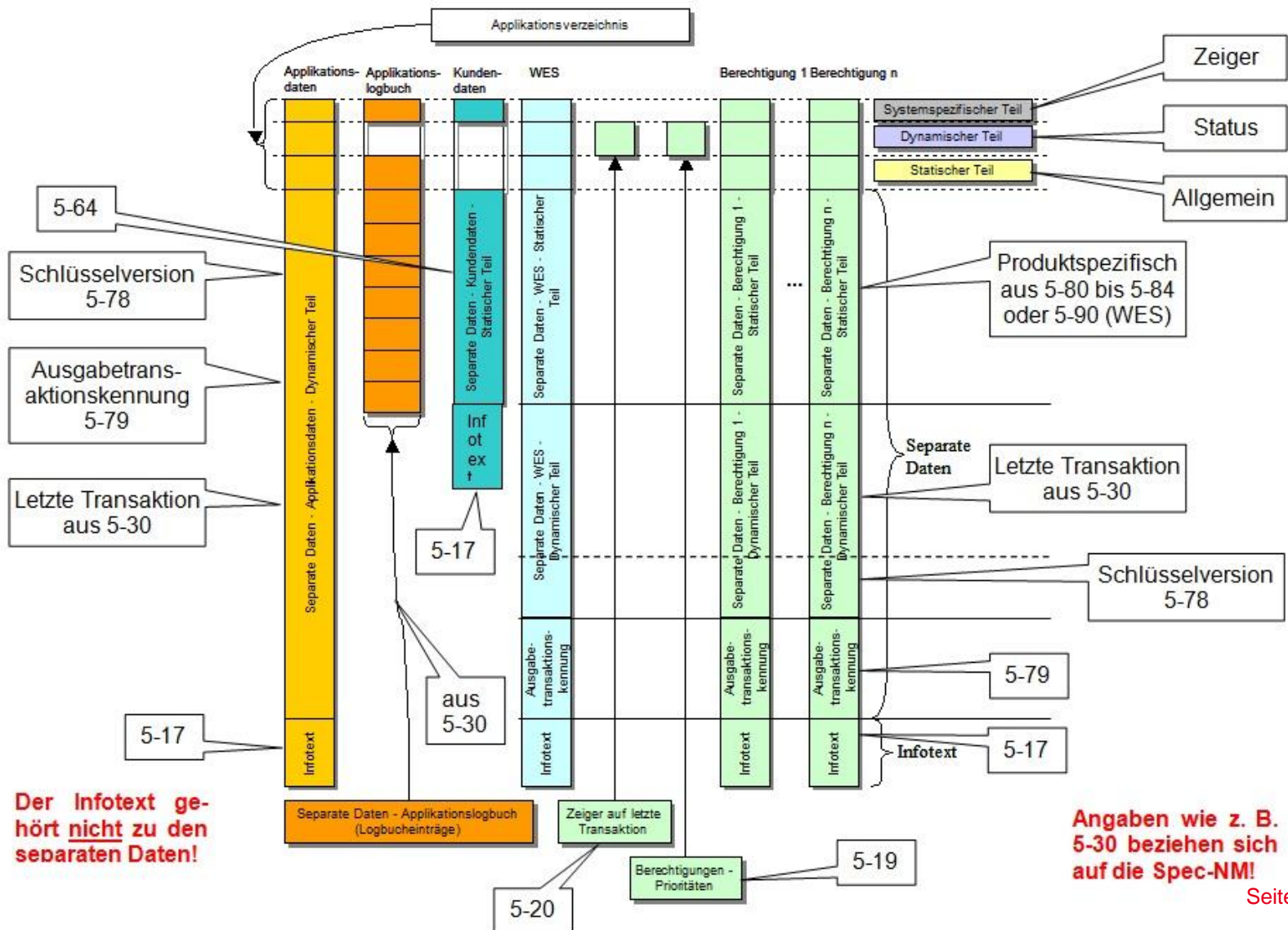
NM- und SAM-Inhalte anzeigen



# Anzeigen der Chipkarteninhalte (1)

- Beim KVP müssen die Daten der Applikation und der bekannten EFS angezeigt werden können. Auch die Kundendaten müssen zum Nachweis, dass sie nicht genutzt werden, angezeigt werden können.
- Tipp des KCEFM:
  - Der KVP sollte sich aus das Applikationslogbuch anzeigen (und ausdrucken) lassen können.

# Anzeigen der Chipkarteninhalte (2)



# Produktspezifische Teile (1)

- Die Produktspezifischen Teile dienen der Abbildung der unterschiedlichen Eigenschaften von Tarifprodukten
- Aufbau und Nutzung der Produktspezifischen Teile müssen vom PV beschrieben werden
- Zusätzlich muss die Nutzung des Infotextes beschrieben werden

## Produktspezifische Teile (2)

- Beispiele für die Beschreibung der Produktspezifischen Teile
  - NRW-KA-EFS (vom VRR und VRS definiert)
  - Referenz-EFS (für ((eTickets, in KA als Beispiel definiert)
  - Referenz-EFS (Statisch) (für Statische Berechtigungen als VDV-Barcode-Tickets, in KA als Beispiel definiert)
  - TLV-EFS (in KA als Beispiel definiert)

# Anzeigen der SAM-Daten

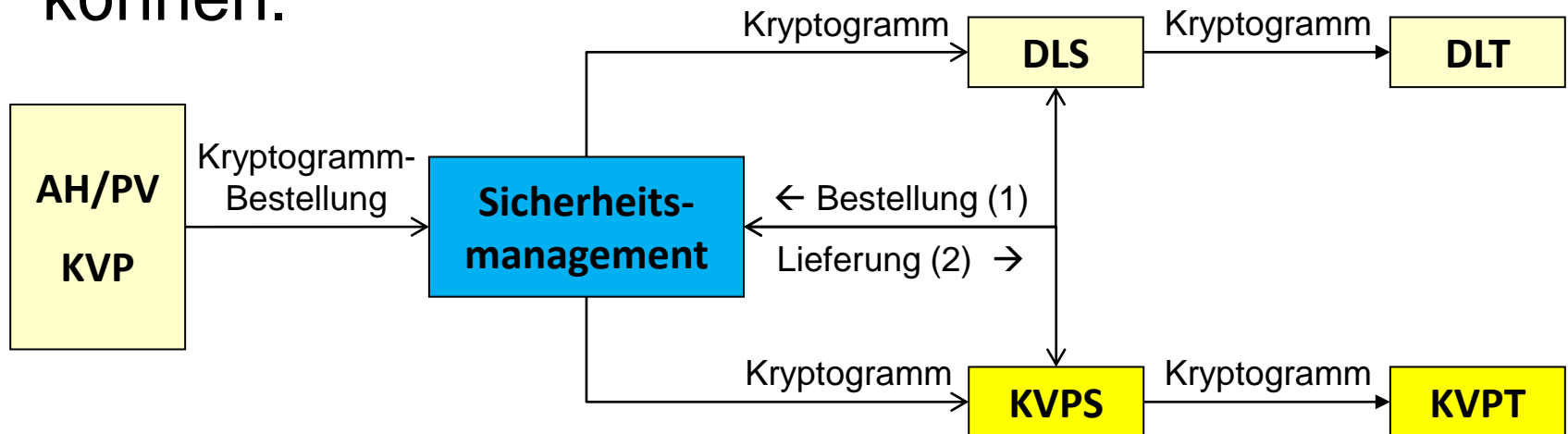
- Bei den DLT und KVPT müssen die SAM-Daten für die verschiedenen Prozesse beim Systemstart ausgelesen werden.
- Tipp des KCEFM:
  - Der DL und KVP sollte sich die SAM-Daten anzeigen (und ausdrucken) lassen können.
  - Vorschlag zum Umfang: Inhalt der Antwort auf die Anfrage TXLESKEY aus der Spec-PE

# Grundfunktionen

SAM- und Zertifikats-Verwaltung

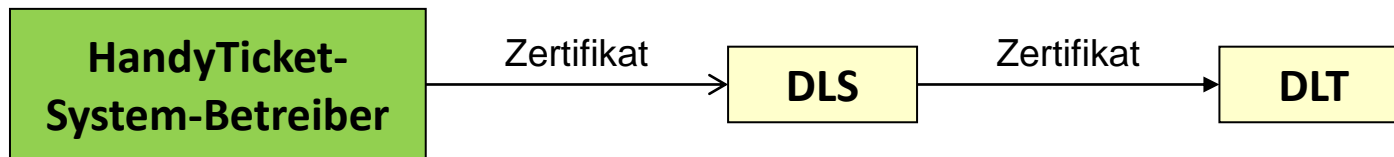
# SAM-Verwaltung

- SAMs müssen bestellt und verwaltet werden. Es muss auch ein Kryptogramm zum Laden, Ändern oder Löschen von Schlüsseln eingespielt werden können.



# Zertifikats-Verwaltung

- Bei einer Statischen Berechtigung als VDV-Barcode muss zur Prüfung von HandyTickets (noch) das Zertifikat des ausstellenden SAMs im DLT vorliegen.

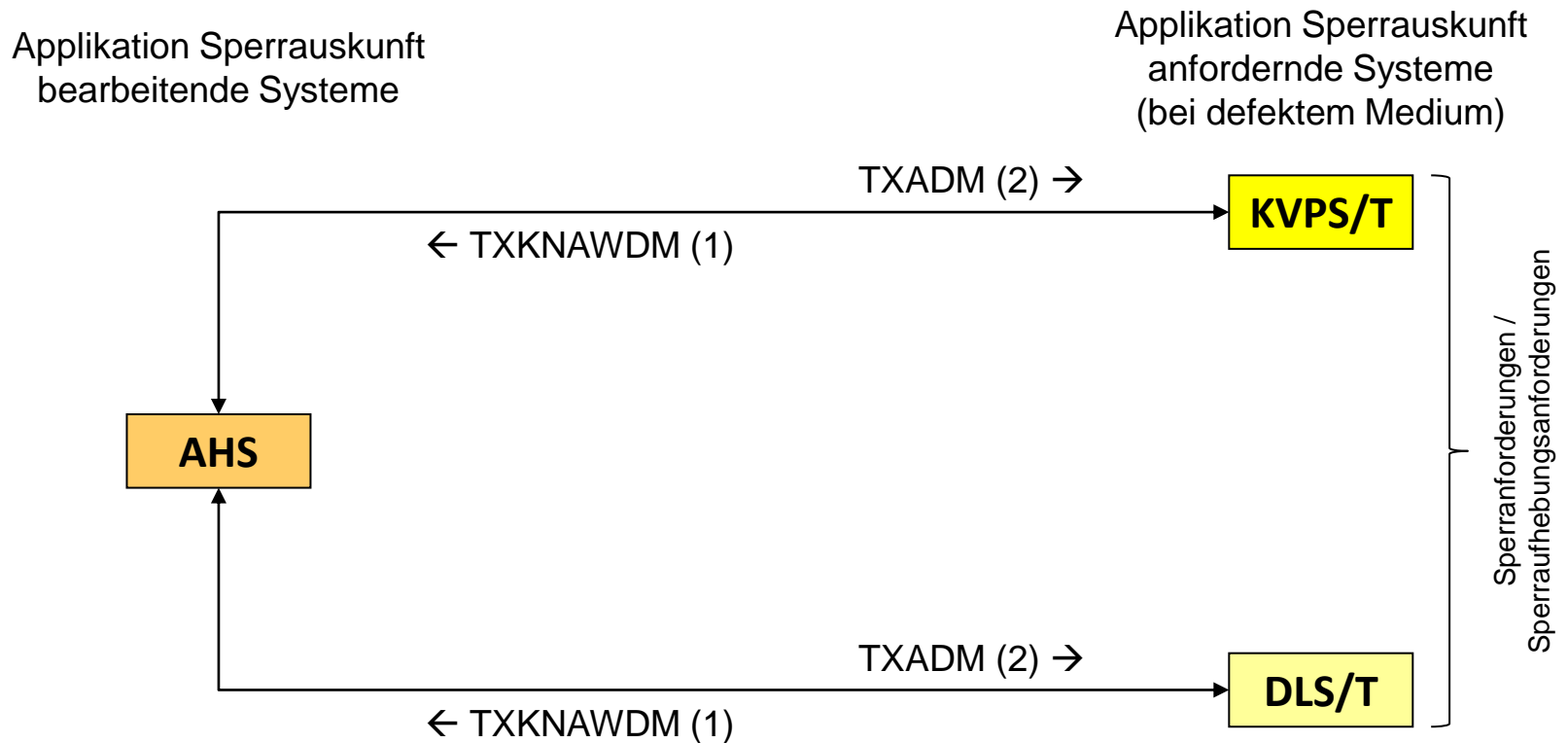




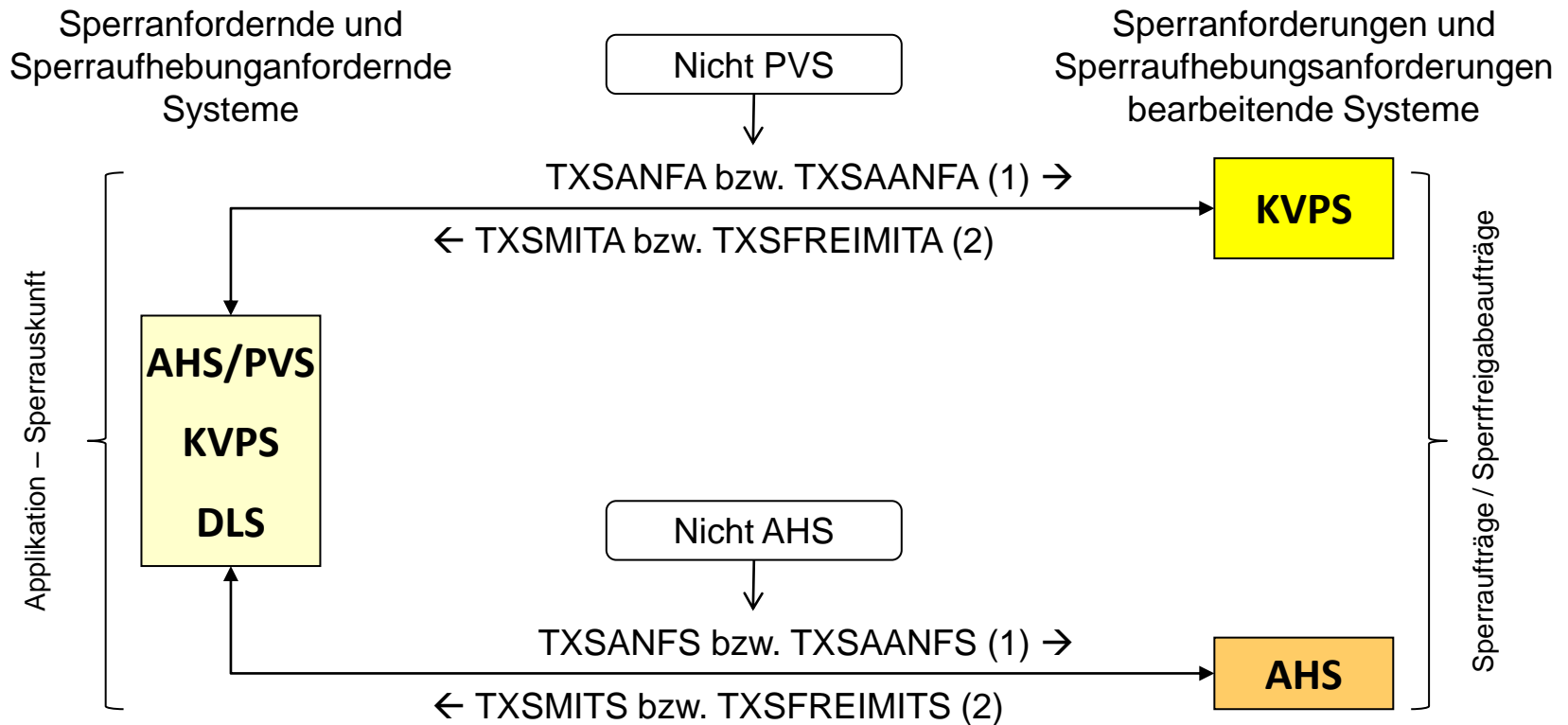
# Sperrwesen

Vorbereitung und Durchführung

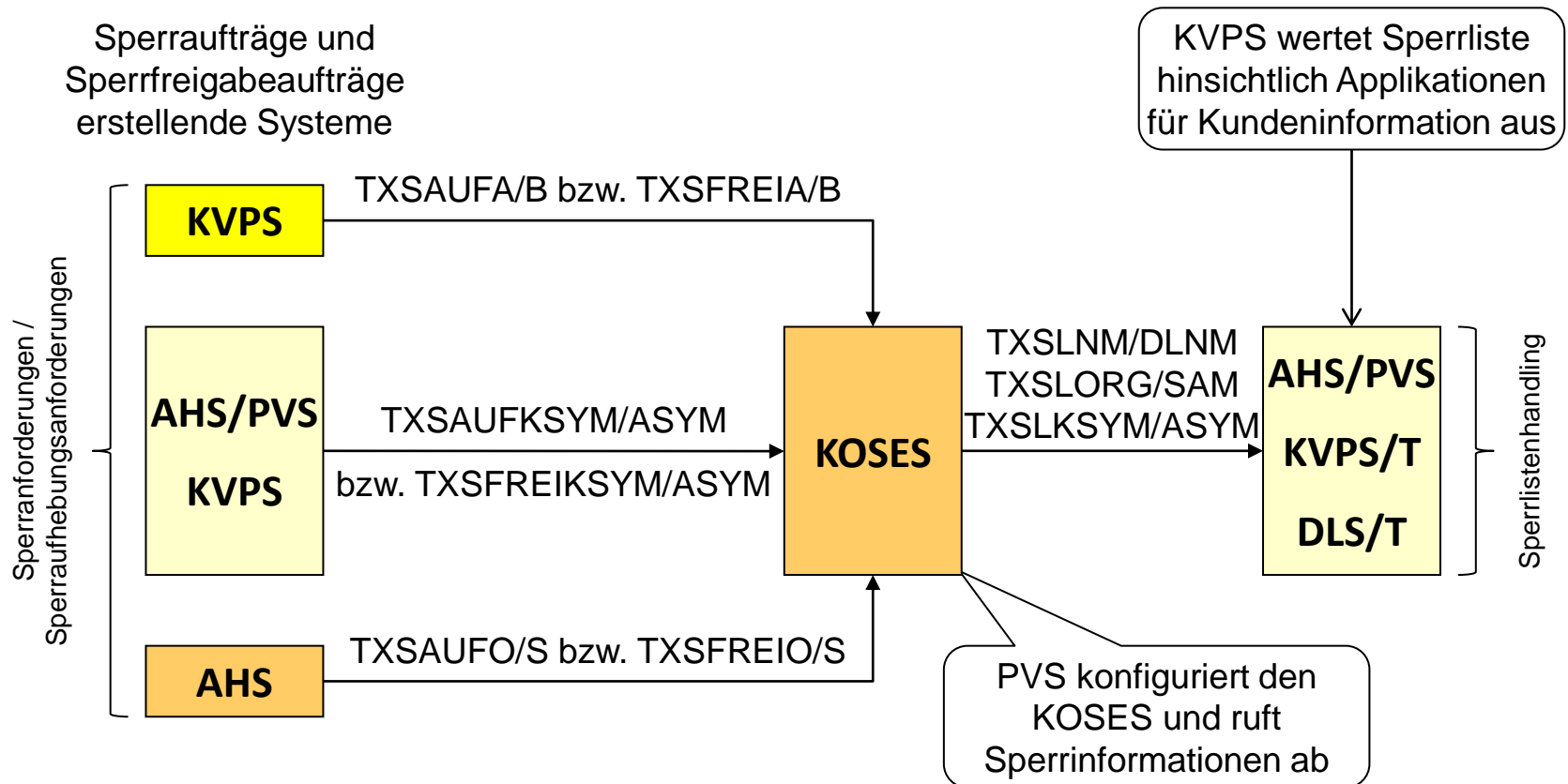
# Sperrwesen – Vorbereitung (1)



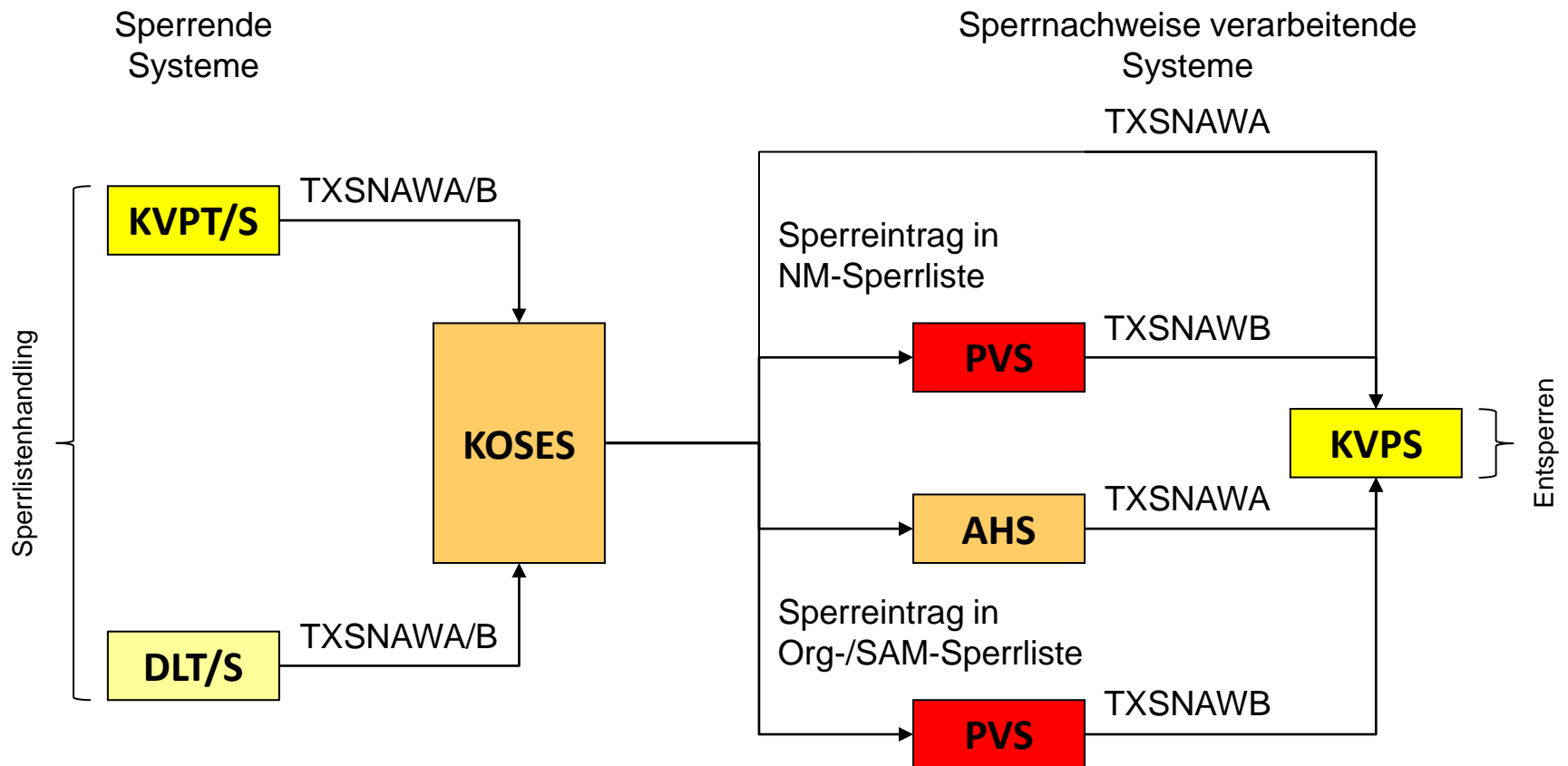
# Sperrwesen – Vorbereitung (2)



# Sperrwesen – Durchführung (1)



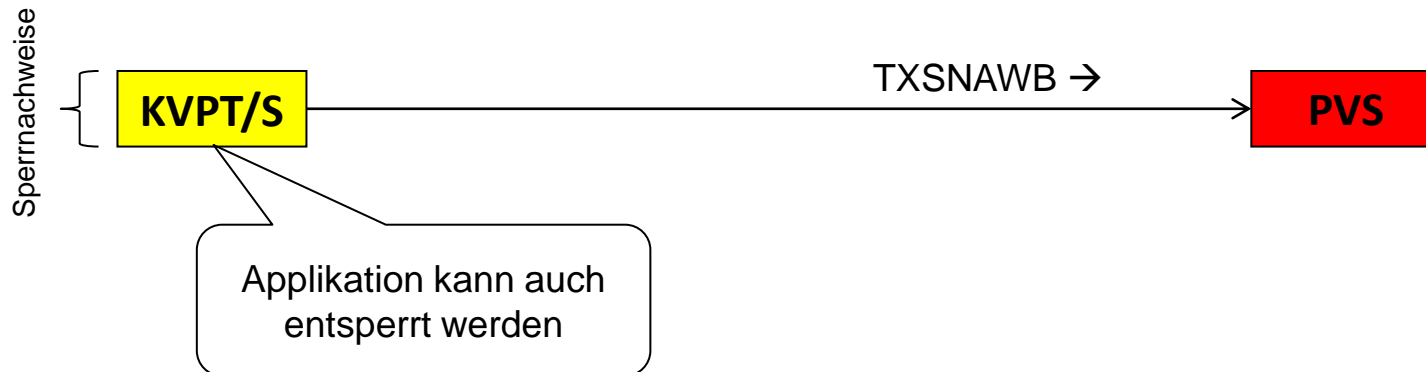
# Sperrwesen – Durchführung (2)



# Sperrwesen – Durchführung (3)

Entsperrende Systeme

Entsperrnachweise  
verarbeitende Systeme



# Sperrauftrag an den KOSE

- Wichtige Parameter für den Sperrauftrag
  - Sperrgrund
    - z. B. Abo gekündigt
    - Zertifikatssperre (irreversibel, nur bei Applikationssperre)
  - Sperrmodus
    - Einzug/Nichteinzug des Nutzermediums
    - Sperrung nicht durchführen, Berechtigung nur abweisen (temporäre Sperre)
  - Ablauf des Sperrauftrages
    - Ende der Gültigkeit von Applikation oder Berechtigung

# Monitoring

Überprüfung der korrekten Funktion des Gesamtsystems



# Monitoring (Kontrollprozess) (1)

- In der KA besteht der gesamte Kontrollprozess eines ((e)Tickets aus drei Teilen:
  1. Prüfung auf Authentizität vor Ort („Gesichertes Lesen“ durch MAC-Prüfung zum Erkennen der „Echtheit“)
  2. Tarifliche Prüfung vor Ort
  3. (MAC-)Prüfung beim DL, KVP und PV auf Basis des (pseudonymen) Kontrollnachweises



# Monitoring (Kontrollprozess) (2)

- In der KA besteht der gesamte Kontrollprozess einer Statischen Berechtigung als VDV-Barcode aus drei Teilen:
  1. Prüfung der Signatur (bei HandyTickets mit Hilfe des Zertifikats im Terminal) und des Kontrollmediums vor Ort
  2. Tarifliche Prüfung vor Ort
  3. Prüfung des (pseudonymen) Kontrollnachweises beim DL, KVP und PV

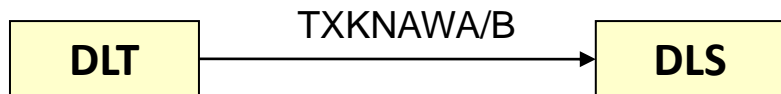


# Monitoring (Kontrollprozess) (3)

- Durch die Einstiegskontrollsysteme entstehen sehr viele Kontrollnachweise insbesondere für ((eTickets, die verarbeitet werden müssen
- Dadurch entstehen hohe Anforderungen an die DL- und KVP- und PV-Systeme hinsichtlich Datenübertragung und Speicherplatz
- Beispiel:
  - Das PV-System „light“ wird für 2 Millionen Kontrollnachweise pro Tag ausgelegt (basierend auf VRR-Zahlen)

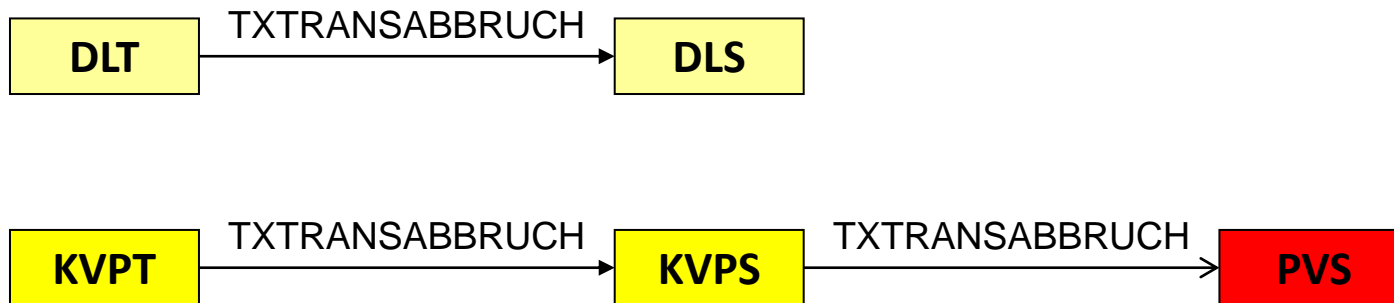
# Monitoring

- Erfassen von gesperrten und ungültigen Applikationen und Berechtigungen zum Erkennen von Angriffen



# Monitoring

- Erfassen von unvollständigen Transaktionen als Grundlage für die Überprüfung der Transaktionsvollständigkeit



# Monitoring

- Überprüfung der Transaktionsvollständigkeit

Zur Überprüfung der Transaktionsvollständigkeit sind verschiedenen Zähler auf Lückenlosigkeit hin zu überprüfen:

- logApplikationSeqNummer
- app/berProdLogSAMSeqNummer
- SAMSequenzNummer
- app/berSynchronNummer
- app/berLogSeqNummer

Näheres siehe „Verfahrensweisung zur Prüfung von Transaktionen in EFM-Referenzsystemen auf Anwendungsebene“

# Monitoring

- Überprüfung der MACs

Ob eine Transaktion wirklich mit einer vom KVP ausgegeben Applikation oder Berechtigung stattgefunden hat und die Applikation/das Produkt vom AH/angegebenen PV stammt, kann anhand des KVP- oder AH/PV-MACs überprüft werden. Ebenso kann ein DL anhand des MAC-Kontrolle überprüfen, ob er wirklich eine Berechtigung kontrolliert hat.

Näheres siehe „Verfahrensanweisung zur Prüfung von Transaktionen in EFM-Referenzsystemen auf Anwendungsebene“