KCEFM Kompetenzcenter
Elektronisches Fahrgeldmanagement NRW

Die VDV-Kernapplikation

Eigenschaften

VRR

Was ist die VDV-Kernapplikation?

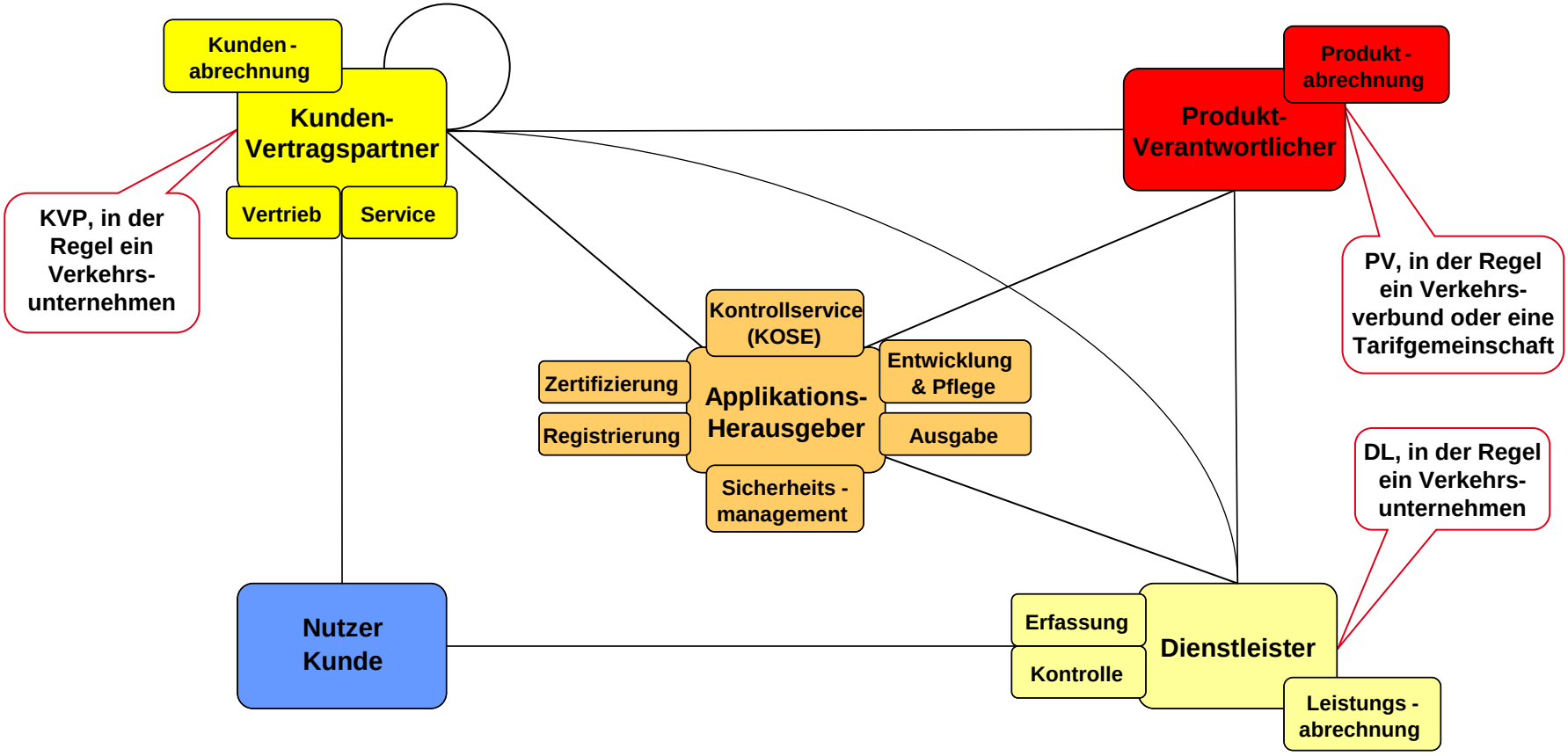
- Die VDV-Kernapplikation definiert einen interoperablen **Standard** für ein elektronisches Fahrgeldmanagement
- Dieser Standard definiert **Prozesse**, **Datenelemente** und **Schnittstellen** zwischen den **Rollen** der VDV-Kernapplikation
- Die VDV-Kernapplikation ist tarifunabhängig und definiert daher auch keinen Tarif

Wo ist dieser Standard beschrieben?

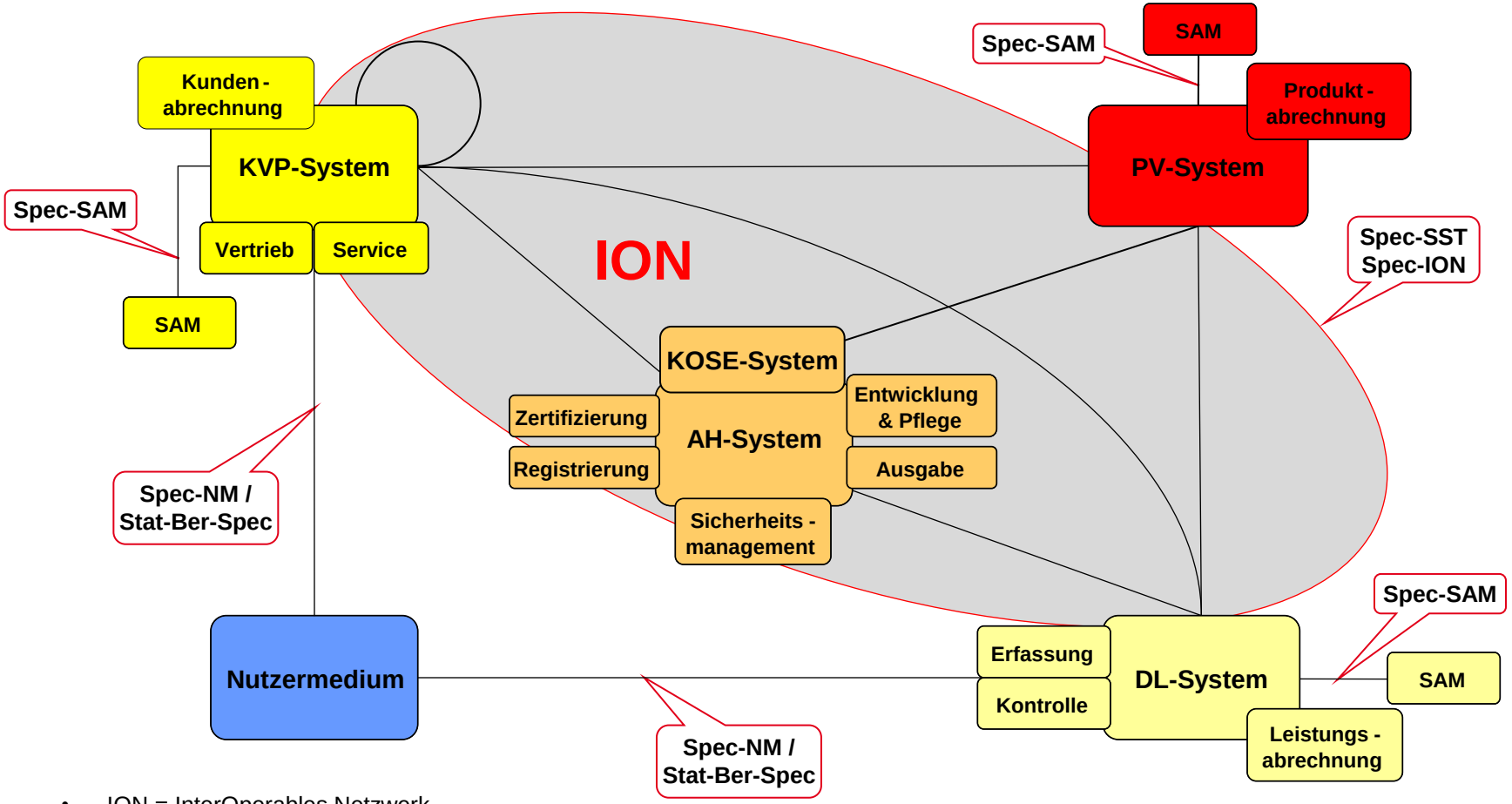
- Die Beschreibung der VDV-Kernapplikation besteht aus
  - Basisdokumenten (z. B. Glossar und HD_BOM)
  - Schnittstellenspezifikationen (Spec-…)
  - Systemlastenheften (SysLH…
  - Verfahrensanweisungen (z. B. Defekte Medien)

- www.eticket-deutschland.de

Rollenmodell der VDV-KA



Systemarchitektur der VDV-KA



- ION = InterOperables Netzwerk

Interoperabilität

- Technische Interoperabilität durch Schnittstellen
  - zum Nutzermedium (NM),
  - zum Sicherheitsmodul (SAM),
  - zum Interoperablen Netzwerk (ION) und
  - zum (gemeinsamen) Sicherheitsmanagement (manuell)
- Basis für Interoperabilität auf Produktebene
- Weitere Schnittstellen nur für Systemarchitektur von Bedeutung

Transaktionen (1)

- Eine Transaktion im Sinne der VDV-Kernapplikation bezeichnet
  - einerseits eine feste Folge von Operationen zur Veränderung eines Objektes auf dem Nutzermedium und
  - andererseits den Austausch von Nachrichten über das ION.

Transaktionen (2)

- Die VDV-Kernapplikation kennt beim Nutzermedium die folgenden Transaktionen:
  - Ausgabetransaktionen
  - Sperr-/Entsperrtransaktionen
  - Rücknahmetransaktionen
  - Fahrttransaktionen
  - Belastungstransaktionen (Kauf eines EFS)
  - Einzahlungsbelegtransaktionen (Einzahlung auf PEB-Konto)

Sicherheit der VDV-Kernapplikation (1)

- Die VDV-Kernapplikation muss zum Schutz der Interessen der Teilnehmer gewissen Sicherheitsaspekten genügen: **Integrität**, **Authentizität**, **Verbindlichkeit**, **Vertraulichkeit** und **Verfügbarkeit**
- Integrität, Authentizität, Verbindlichkeit und Vertraulichkeit können durch **kryptographische Verfahren** gewährleistet werden, Verfügbarkeit durch entsprechende Gestaltung der **Infrastruktur**

Sicherheit der VDV-Kernapplikation (2)

- **Integrität** ist gegeben, wenn Daten nicht unbemerkt verändert oder zerstört werden können
- **Authentizität** ist gegeben, wenn der Urheber der Daten nachweisbar ist

Sicherheit der VDV-Kernapplikation (3)

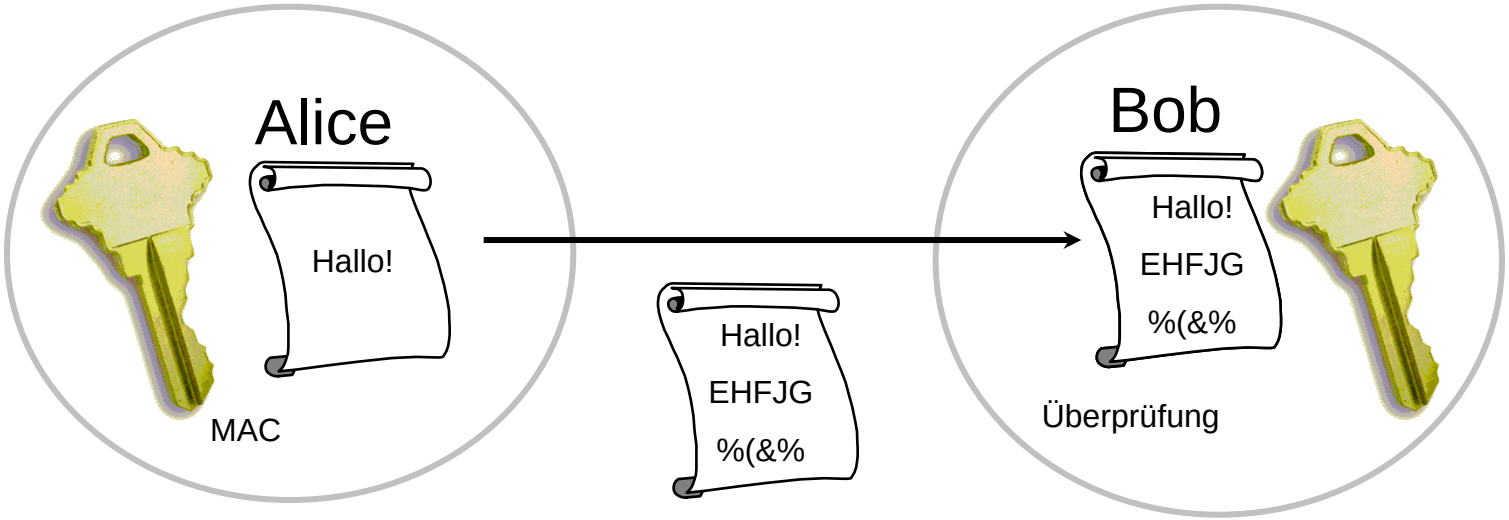
- **Verbindlichkeit** ist gegeben, wenn der Urheber der Daten nicht in der Lage ist, seine Urheberschaft zu bestreiten
- **Vertraulichkeit** ist gegeben, wenn Informationen nicht unautorisiert eingesehen werden können

Wie wird die Sicherheit gewährleistet?

- Die Sicherheit des Gesamtsystems wird durch die Verwendung von **asymmetrischen und symmetrischen Schlüsseln/Verfahren** gewährleistet
- Die Schlüssel dienen neben der Verschlüsselung von Daten dem Erzeugen und Prüfen von Signaturen bei asymmetrischen Schlüsseln bzw. MAC‘s (Message Authentication Code / Prüfzahl) bei symmetrischen Schlüsseln

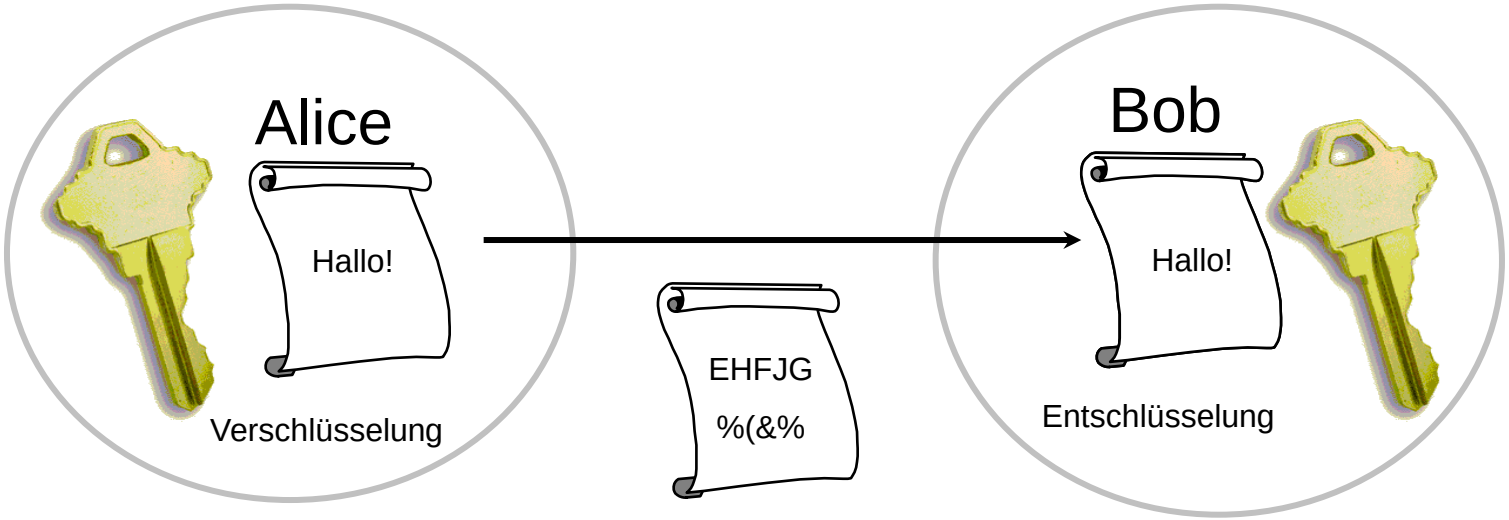
Symmetrische Schlüssel/Verfahren (1)

- Mit einem (vom Masterkey abgeleiteten) Schlüssel wird ein MAC erzeugt und (mit dem Masterkey) überprüft



Symmetrische Schlüssel/Verfahren (2)

- Mit einem (vom Masterkey abgeleiteten) Schlüssel wird eine Nachricht verschlüsselt und (mit dem Masterkey) entschlüsselt



Symmetrische Schlüssel/Verfahren (3)

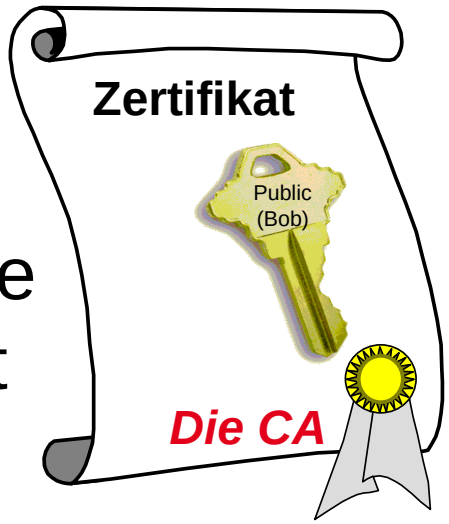
- Das Problem bei symmetrischen Verfahren ist die sichere Verteilung der Schlüssel
- Wenn man nur symmetrische Verfahren anwenden würde, wäre dies aus Sicht der VDV-Kernapplikation bundesweit ein großes organisatorisches Problem, da jeder den symmetrischen Schlüssel jeder teilnehmenden Organisation haben muss

Asymmetrische Schlüssel/Verfahren (1)

- Ein asymmetrisches Schlüsselpaar besteht aus einem geheimen privaten und einem öffentlichen Schlüssel
- Der öffentliche Schlüssel (Public Key) kann frei verteilt werden
- In einem offenen System wie bei der VDV-Kernapplikation muss er zertifiziert sein

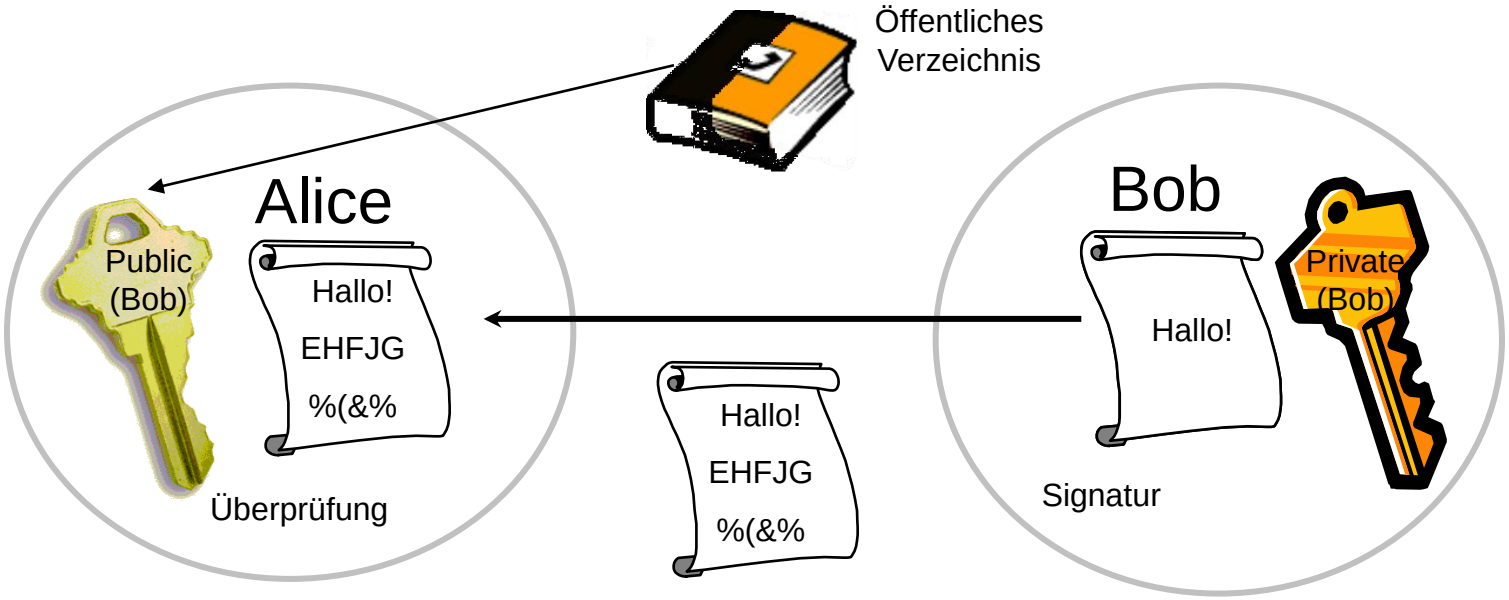
Asymmetrische Schlüssel/Verfahren (2)

- Im Rahmen der Public Key Infrastructure (PKI) erstellt ein sogenanntes TrustCenter als Zertifizierungsdienstleister (Certification Authority, CA) Zertifikate und bestätigt damit die Zugehörigkeit eines öffentlichen Schlüssels zum Zertifikatsinhaber. Die CA dient als vertrauenswürdige Instanz.



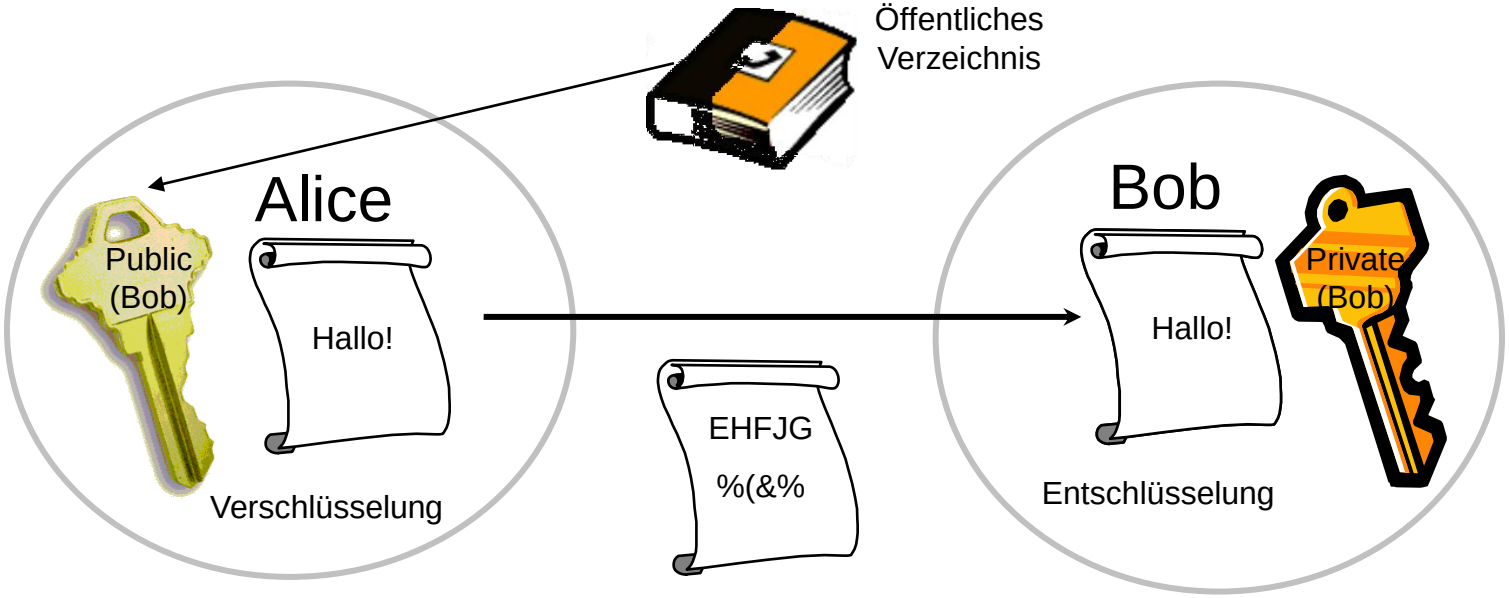
Asymmetrische Schlüssel/Verfahren (3)

- Mit dem privaten Schlüssel wird eine Signatur erzeugt und mit dem öffentlichen überprüft



Asymmetrische Schlüssel/Verfahren (4)

- Mit dem öffentlichen Schlüssel wird eine Nachricht verschlüsselt und mit dem privaten wieder entschlüsselt



Angewendete Verfahren (1)

- Beim Verkaufsprozess wird durch asymmetrische Verfahren, die das Verteilproblem lösen, eine hohe Sicherheit gewährleistet, die aber zeitaufwendig ist
- Bei den Kontroll- und Erfassungsprozessen wird durch symmetrische Verfahren mit wenigen zu verteilenden Schlüsseln eine hohe Sicherheit gewährleistet, die sehr schnell ist

Angewendete Verfahren (2)

- Die dazu erforderlichen symmetrischen und asymmetrischen Schlüssel befinden sich
  - im (((eTicket-Nutzermedium (z.B. Chipkarte),
  - in einem Sicherheitsmodul (Secure Application Module, SAM, vergleichbar mit einer SIM-Karte) in den Terminals und
  - (zur Zeit noch) im Kundenvertragspartner-System (KVP-System, privater Teil des asymmetrischen Schlüsselpaares für SAM-Freischaltung für Verkauf)

    → Spec-Aktivierungsmedium veröffentlicht

Verwendete Schlüssel (1)

- Asymmetrische Schlüsselpaare im (((eTicket-Nutzermedium (Chipkarte) zur
  - Authentisierung zwischen NM und SAM
- Asymmetrische Schlüsselpaare im SAM zur
  - Authentisierung zwischen NM und SAM
  - Signatur von Datensätzen
  - Ver- und Entschlüsselung von Kryptogrammen zur Konfiguration der symmetrischen Schlüssel im SAM

Verwendete Schlüssel (2)

- Asymmetrische Schlüsselpaare für teilnehmende Organisationen zur
  - Signatur von Kryptogrammen zur Konfiguration der symmetrischen Schlüssel im SAM als KVP, DL und PV
  - Freischaltung von SAMs für den Verkauf als KVP
- Symmetrische Schlüssel für teilnehmende Organisationen zur
  - Bildung von MAC‘s bei NM-Transaktionen als KVP und PV

Verwendete Schlüssel (3)

- Systemweite asymmetrische Schlüsselpaare des Applikationsherausgebers
- Systemweite symmetrische Schlüssel des Applikationsherausgebers
  - Erfassungsschlüssel für die Regionen Nord-Ost, West, Süd und Bundesweit zum Erkennen der „Echtheit“ anhand eines MAC‘s
  - Transaktionsschlüssel zur Bildung des MAC-Kontrolle (MAC-Transaktion)

Verwendete Schlüssel (4)

- Jeder Schlüssel ist unter anderem durch eine Organisations-ID (Org-ID) gekennzeichnet
- Abhängig von der Org-ID ergibt sich die Zugehörigkeit zu einem bestimmten **Sicherheitslevel** der VDV-Kernapplikation
- Generell gilt: Die VDV-Kernapplikation ist Org-ID gesteuert

Aufgaben der KA-Systeme (1)

- KOSE-System
  - Sperrlistenhandling
- AH-System
  - Datenrouting
  - Teilnahme am Sperrwesen
  - Monitoring (Applikationen)

Aufgaben der KA-Systeme (2)

- PV-System
  - Datenrouting
  - Teilnahme am Sperrwesen
  - Monitoring (Berechtigungen)
  - Definition von Tarifprodukten und Weitergabe der Definitionen an KVP und DL
  - Produktabrechnung (Finanzclearing)

Aufgaben der KA-Systeme (3)

- KVP-System
  - Teilnahme am Sperrwesen
  - Monitoring
  - Ausgabe/Änderung/Rücknahme/Anzeige von Berechtigungen auf Basis von Tarifprodukten des PV
- DL-System
  - Teilnahme am Sperrwesen
  - Monitoring
  - Kontrolle/Erfassung von Berechtigungen auf Basis von Tarifprodukten des PV