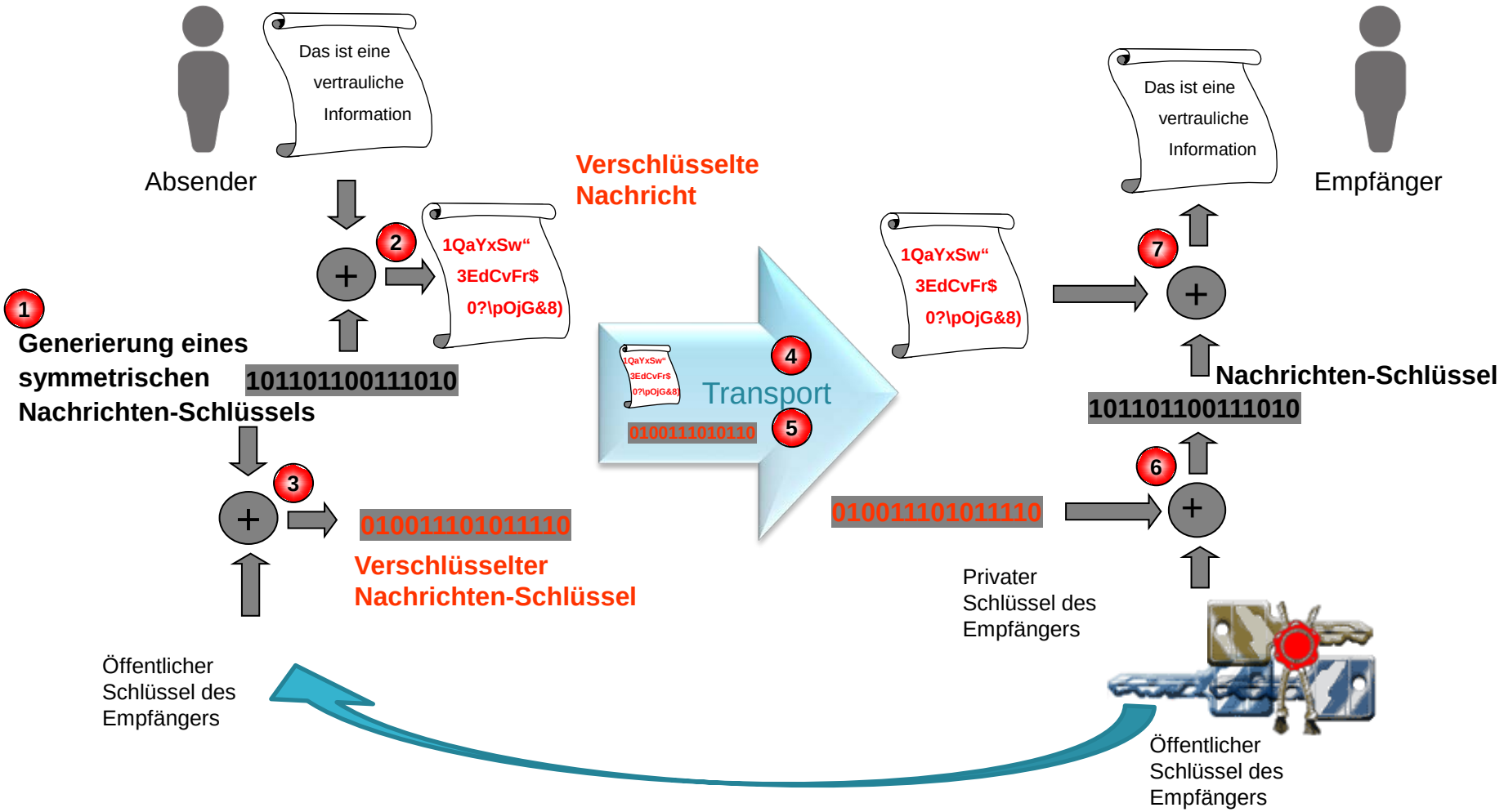
Ende-zu-Ende Verschlüsselung im besonderen elektronischen Anwaltspostfach (beA)

Berlin, 08.07.2015

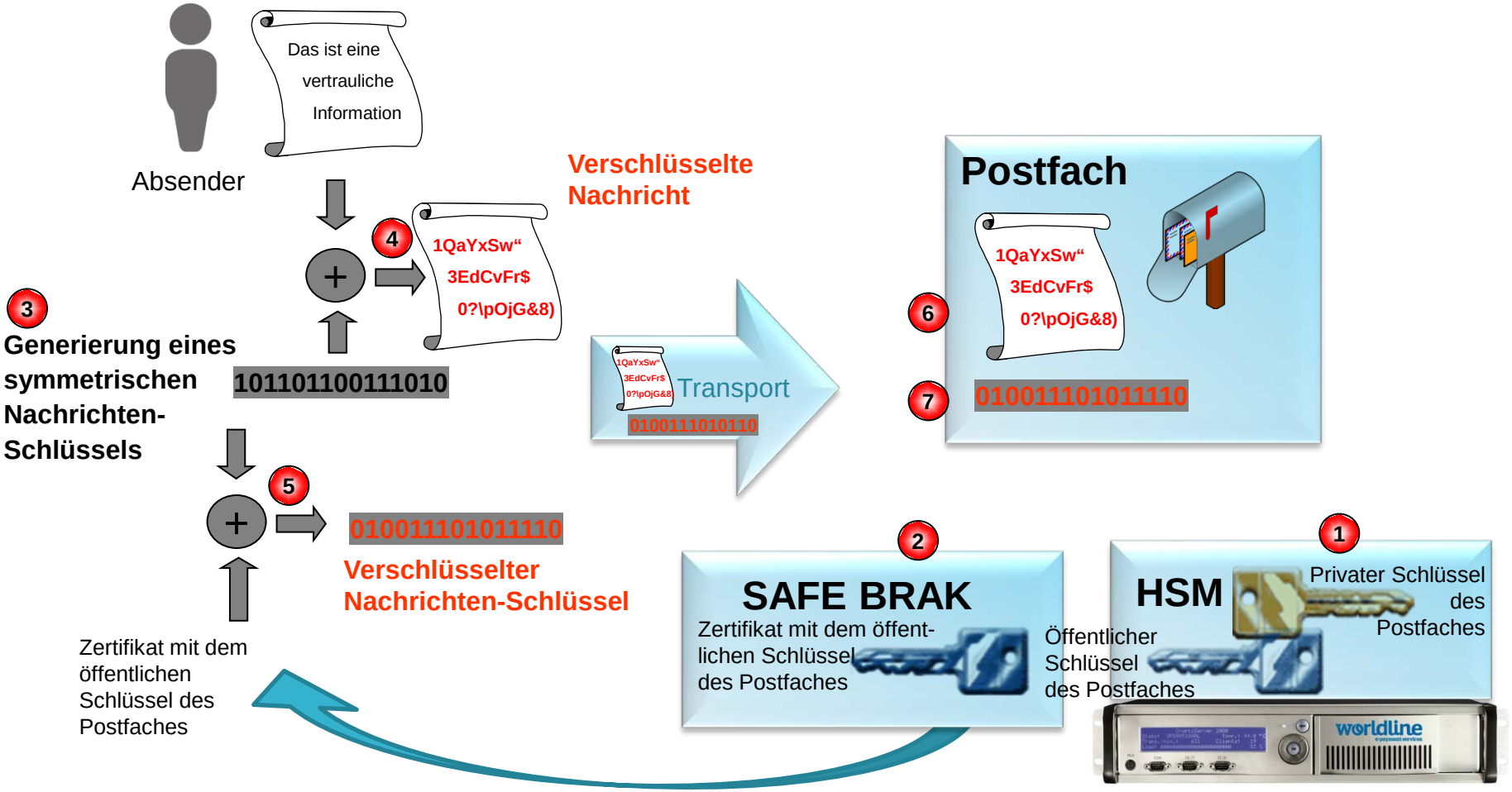
Ende-zu-Ende-Verschlüsselung wird durch eine Kombination aus symmetrischen und asymmetrischen Schlüssel realisiert

Ende-zu-Ende-Verschlüsselung – Grundprinzip (graphisch)



Im beA wird ein Nachrichtenschlüssel mit dem öffentlichen Postfachschlüssel verschlüsselt

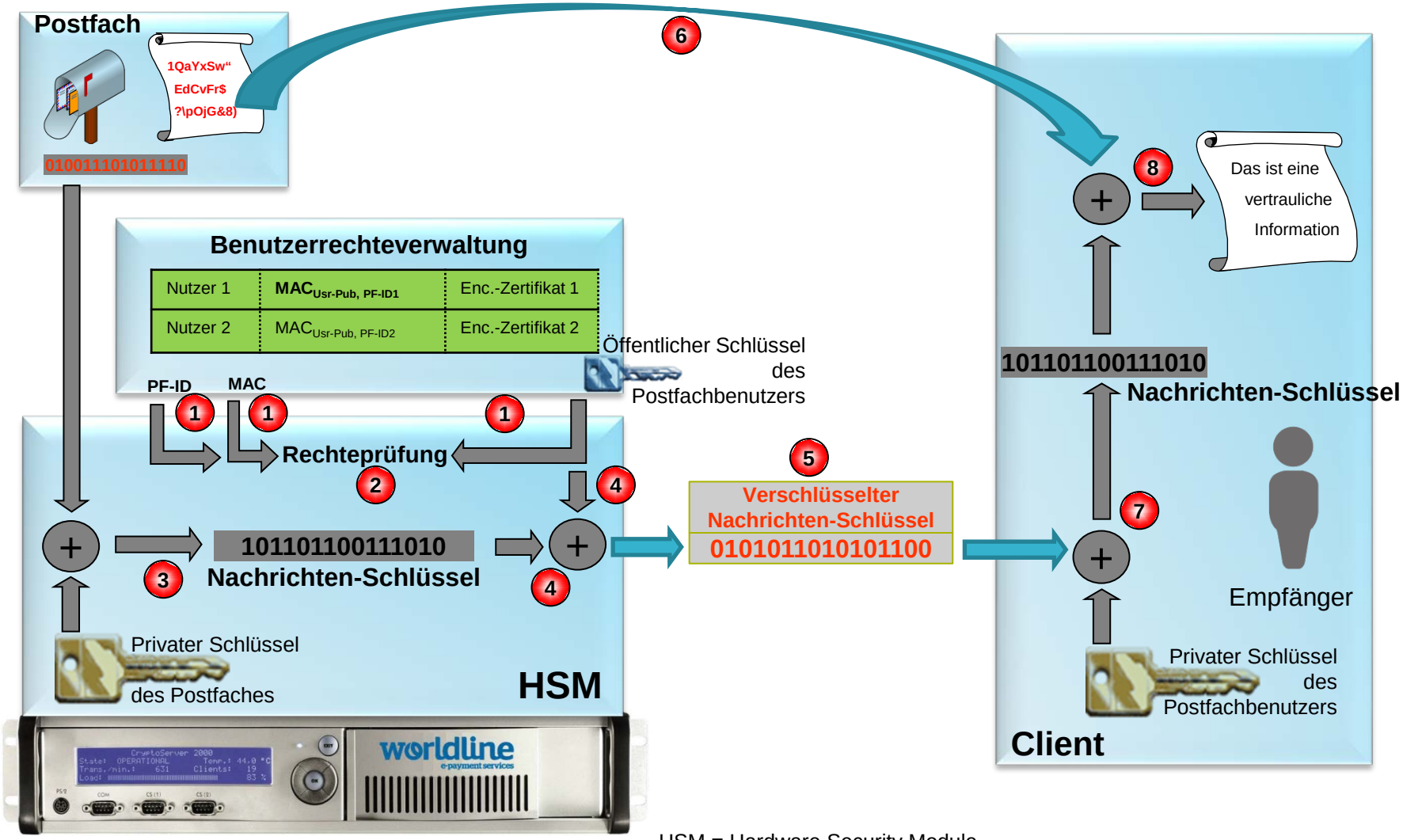
Ende-zu-Ende-Verschlüsselung – Verschlüsselung einer Nachricht (graphisch)



HSM = Hardware Security Module

beA-Postfächer erlauben Zugriff durch mehrere Benutzer. Die Berechtigungsprüfung ist durch das HSM abgesichert

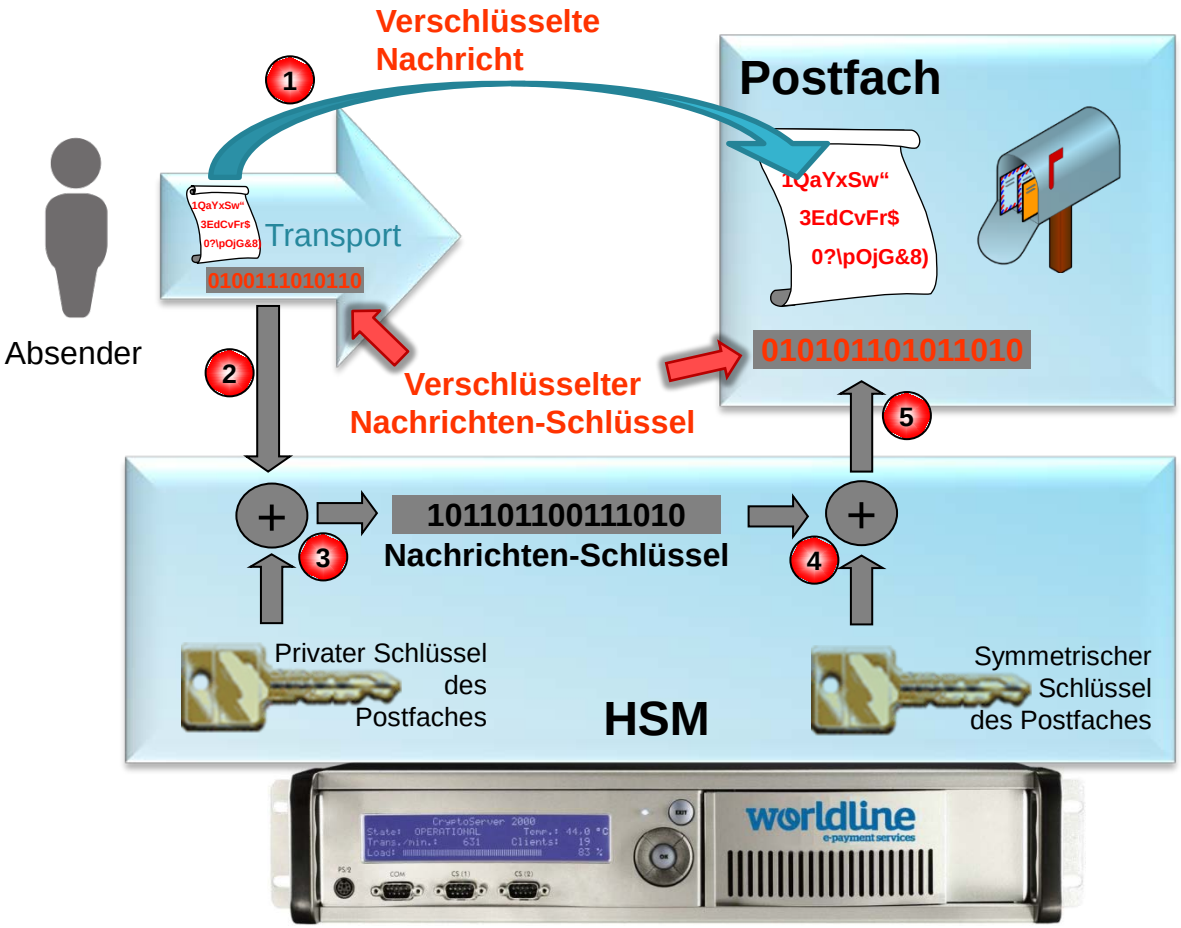
Ende-zu-Ende-Verschlüsselung – Entschlüsselung einer Nachricht (graphisch)



HSM = Hardware Security Module

Das Umschlüsseln mittels symmetrischer Postfachschlüssel macht die weitere Verarbeitung performanter und komfortabler

Ende-zu-Ende-Verschlüsselung – Ablage einer Nachricht in einem beA (graphisch)



- Jedes Postfach verfügt über
  - ein Schlüsselpaar zur **asymmetrischen Verschlüsselung** und
  - einen Schlüssel zur **symmetrischen Verschlüsselung**.
- Die asymmetrische Verschlüsselung dient zum sicheren Transport der Nachrichtenschlüssel ins Postfach.
- Vorteil 1: Durch die Umschlüsselung auf den symmetrischen Schlüssel können **Nachrichtenzugriffe deutlich schneller** erfolgen.
- Vorteil 2: Der Einsatz eines symmetrischen Postfachschlüssels ermöglicht die verschlüsselte Ablage von Betreffzeilen der einzelnen Nachrichten. Dadurch können die **Betreffzeilen in der Nachrichten-übersicht** en Block angezeigt werden.

Das Umschlüsseln mittels symmetrischer Postfachschlüssel macht die weitere Verarbeitung performanter und komfortabler

Ende-zu-Ende-Verschlüsselung – Ablage einer Nachricht in einem beA (graphisch)

Symmetrische kryptografische Operationen sind um ein vielfaches performanter als asymmetrische kryptografische Operationen.

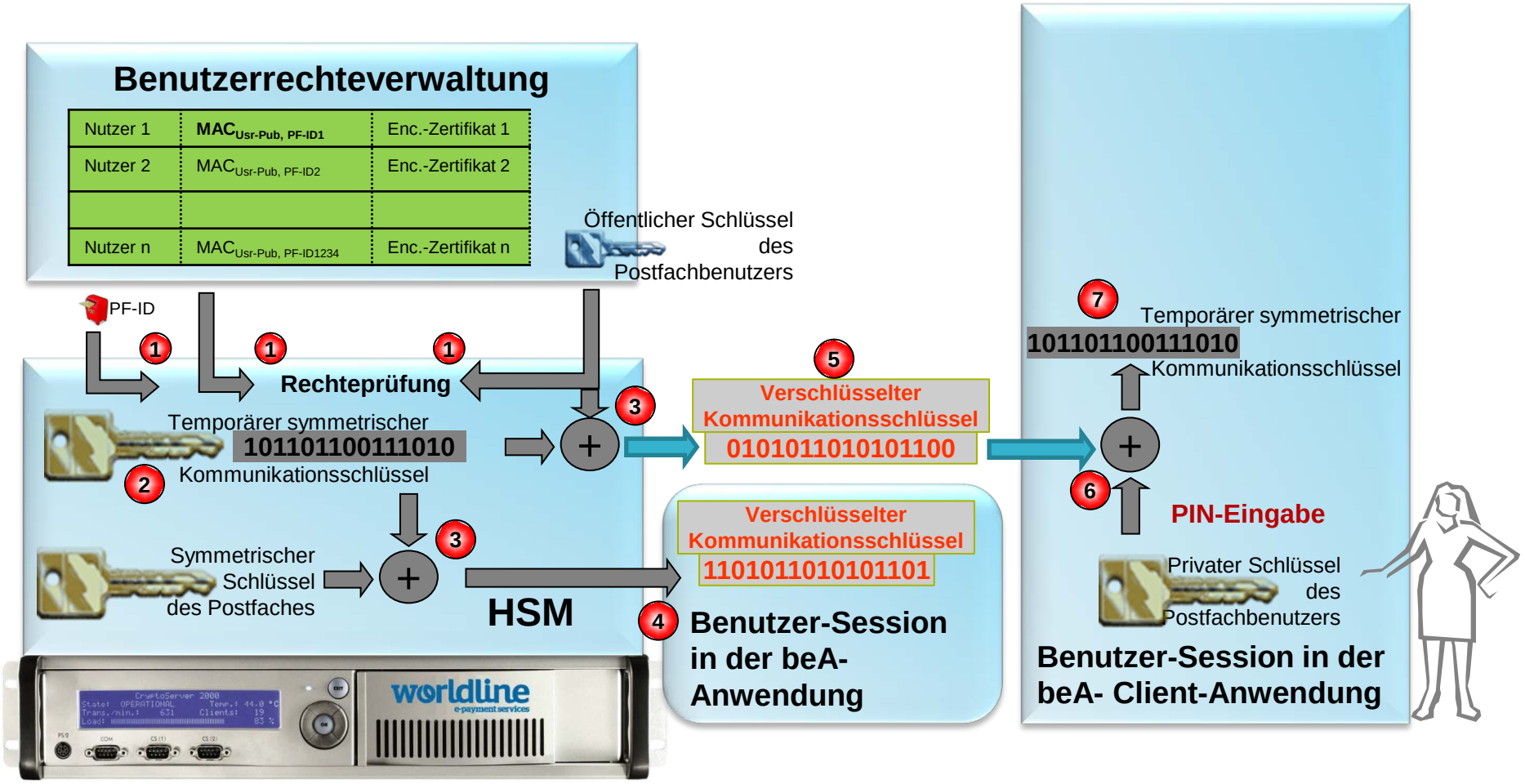
Der symmetrische Postfachschlüssel wird auch zur Ver- und Entschlüsselung der im Postfach abgelegten verschlüsselten Betreffzeilen verwendet.

Ablauf der Ablage einer empfangenen Nachricht im Postfach.

1. Ein verschlüsselter Nachrichtencontent wird ohne Veränderung im Postfach gespeichert.
2. Der zugehörige mit dem öffentlichen Postfachschlüssel verschlüsselte Nachrichtenschlüssel wird an das HSM zur Umschlüsselung übergeben.
3. Entschlüsselung des mit dem öffentlichen Postfachschlüssel verschlüsselten Nachrichtenschlüssels mittels privaten Postfachschlüssels.
4. Verschlüsselung des Nachrichtenschlüssels mit dem symmetrischen Schlüssels des Postfaches.
5. Speicherung des mit dem symmetrischen Schlüssel des Postfaches verschlüsselten Nachrichtenschlüssels im Postfach.

Erstellung und Verteilung eines temporären Kommunikationsschlüssels

Ende-zu-Ende Verschlüsselung – beA-Entschlüsselung für berechtigte Benutzer



Erstellung und Verteilung eines temporären Kommunikationsschlüssels

Ende-zu-Ende Verschlüsselung – beA-Entschlüsselung für berechtigte Benutzer

Wenn ein Nachrichtenschlüssel für den Transport aus dem beA zum Benutzer mit dem öffentlichen Schlüssel des Benutzers verschlüsselt wird und der Benutzer zur Entschlüsselung eine Signaturkarte benutzt auf der sein privater Schlüsse gespeichert ist, so ist er gezwungen bei jeder Entschlüsselung eines Nachrichtenschlüssels die Karten-PIN einzugeben.

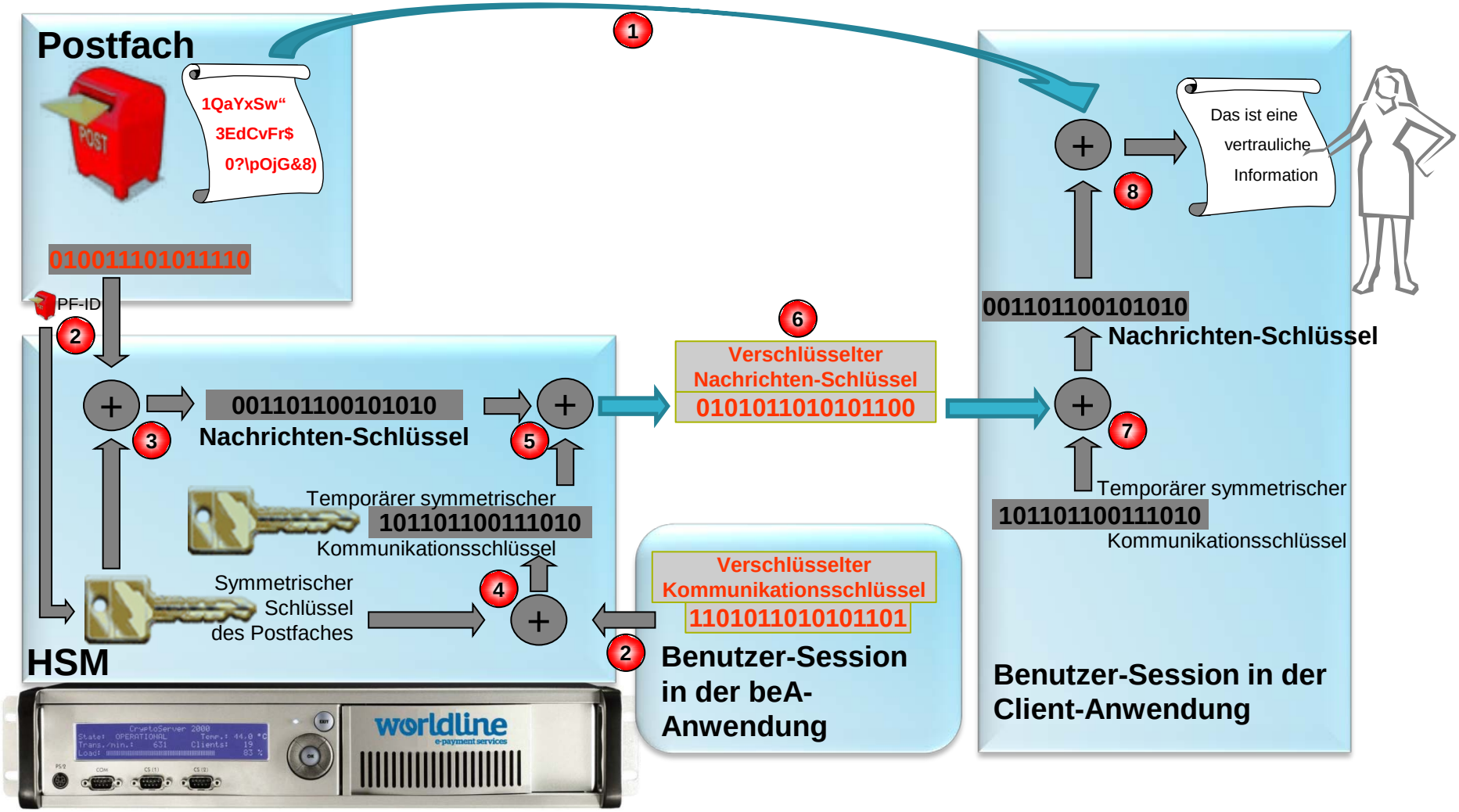
Diese für die Usability des beA nachteilige Eigenschaft von Crypto-Chipkarten wird durch die Nutzung eines temporären symmetrischen Sitzungsschlüssels für die Verschlüsselung des Nachrichtenschlüssels auf dem Transport zwischen beA und dem Client aufgehoben.

Ablauf der Erstellung eines symmetrischen Kommunikationsschlüssels, der Speicherung, der Übertragung und der Entschlüsselung auf dem Client:

1. Prüfung der Berechtigung der Nachrichtenentschlüsselung eines bestimmtes Postfaches für einen Benutzers des beA durch das im HSM
2. Nach der Anmeldung eines Benutzers am System wird beim ersten Zugriff auf ein Postfach ein temporärer symmetrischer Kommunikationsschlüssel (AES-256) im HSM gebildet.
3. Dieser Kommunikationsschlüssel wird mit dem öffentlichen Schlüssel des Benutzers und den symmetrischen Postfachschlüssel im HSM verschlüsselt.
4. Zwischenspeicherung des entschlüsselten Kommunikationsschlüssels in der Benutzer-Session der beA-Applikation.
5. Übertragung des mit dem öffentlichen Schlüssel des autorisierten Benutzers verschlüsselten Kommunikationsschlüssels an den Client des Benutzers.
6. Entschlüsselung des Kommunikationsschlüssels mit dem privaten Schlüssel des Benutzers.
7. Zwischenspeicherung des entschlüsselten Kommunikationsschlüssels in der Client-Session.

Entschlüsselung von Nachrichten auf dem Client

Ende-zu-Ende Verschlüsselung – beA-Entschlüsselung für berechtigte Benutzer



Entschlüsselung von Nachrichten auf dem Client

Ende-zu-Ende Verschlüsselung – beA-Entschlüsselung für berechtigte Benutzer

Ablauf der Abholung einer Nachricht aus dem Postfach und Entschlüsselung auf dem Client mit dem temporären symmetrischen Kommunikationsschlüssel.

1. Ein verschlüsselter Nachrichtencontent wird ohne Veränderung aus dem Postfach an den Client übertragen.
2. Die PF-ID, der zugehörige mit dem Postfachschlüssel verschlüsselte Nachrichtenschlüssel und der mit dem Postfachschlüssel verschlüsselte symmetrische Kommunikationsschlüssel wird an das HSM zur Umschlüsselung übergeben.
3. Entschlüsselung des mit dem symmetrischen Postfachschlüssel verschlüsselten Nachrichtenschlüssels.
4. Entschlüsselung des mit dem symmetrischen Postfachschlüssel verschlüsselten Kommunikationsschlüssels.
5. Verschlüsselung des Nachrichtenschlüssels mit dem symmetrischen Kommunikationsschlüssel.
6. Übertragung des mit dem symmetrischen Kommunikationsschlüssel verschlüsselten Nachrichtenschlüssels an den Client.
7. Entschlüsselung des Nachrichtenschlüssels mit dem Kommunikationsschlüssel.
8. Entschlüsselung der Nachricht mit dem Nachrichtenschlüssel.

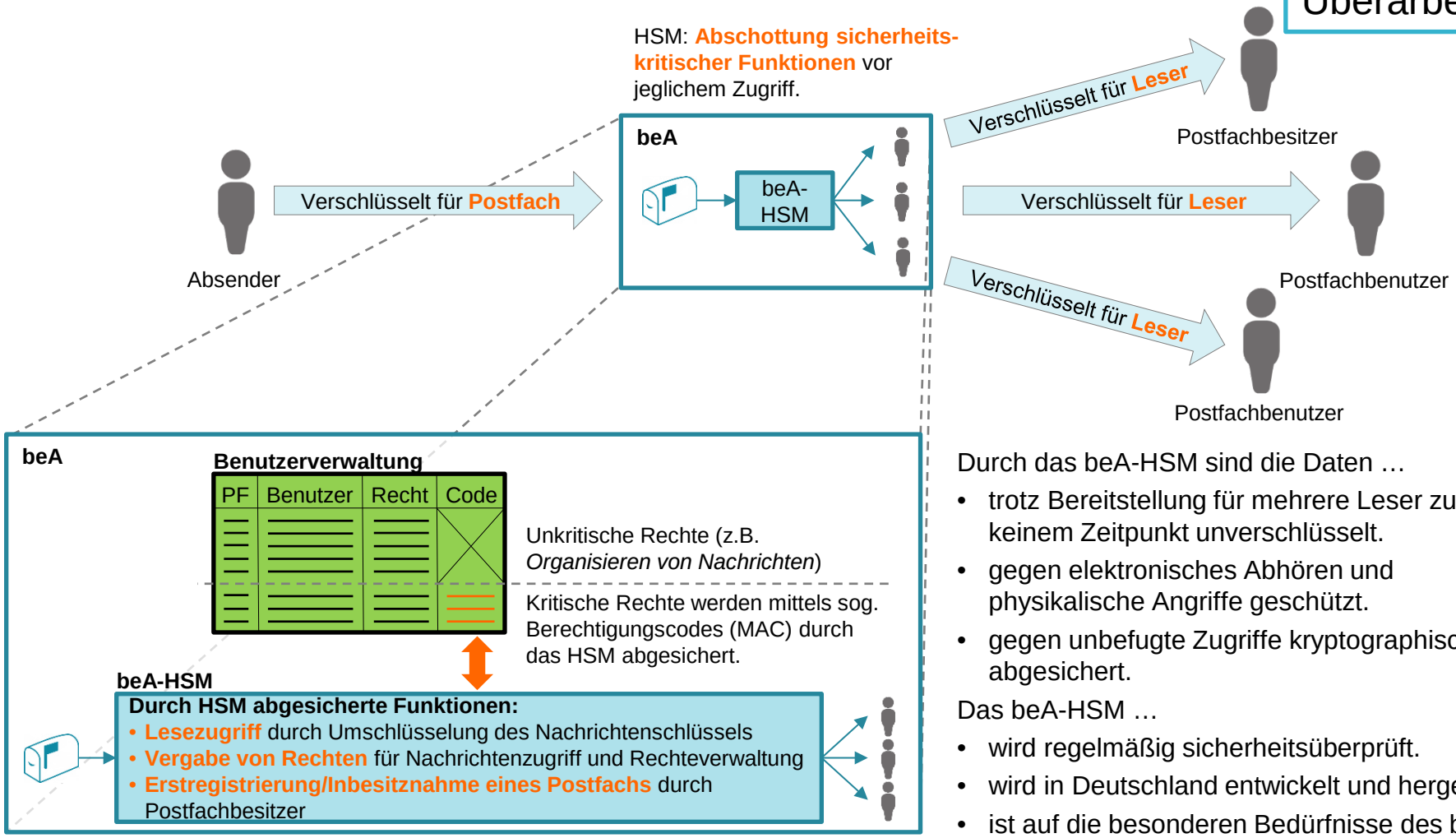
Das beA-HSM wahrt die Ende-zu-Ende-Verschlüsselung auch beim Nachrichtenzugriff durch mehrere Leser

Absicherung des Nachrichtenzugriffs mittels HSM – Überblick

BUNDESRECHTSANWALTSKAMMER

Atos

Überarbeitet



HSM = Hardware Security Module, PF = Postfach

Durch das beA-HSM sind die Daten …

- trotz Bereitstellung für mehrere Leser zu keinem Zeitpunkt unverschlüsselt.
- gegen elektronisches Abhören und physikalische Angriffe geschützt.
- gegen unbefugte Zugriffe kryptographisch abgesichert.

Das beA-HSM …

- wird regelmäßig sicherheitsüberprüft.
- wird in Deutschland entwickelt und hergestellt.
- ist auf die besonderen Bedürfnisse des beA angepasst.

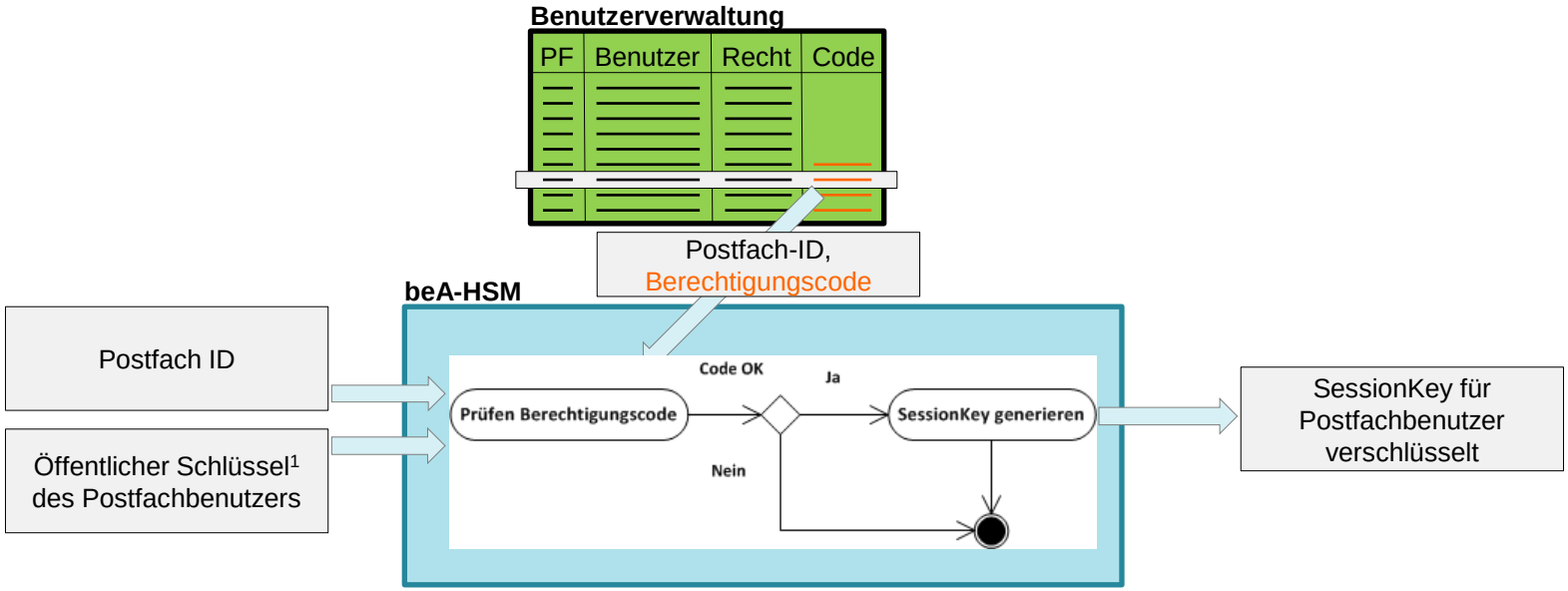
Lesezugriff benötigt individuellen Kommunikationsschlüssel, den das HSM nur nach Berechtigungsprüfung erstellt

Absicherung des Postfachzugriffs mittels HSM – Lese Recht und Session Key

BUNDESRECHTSANWALTSKAMMER

Atos

Überarbeitet

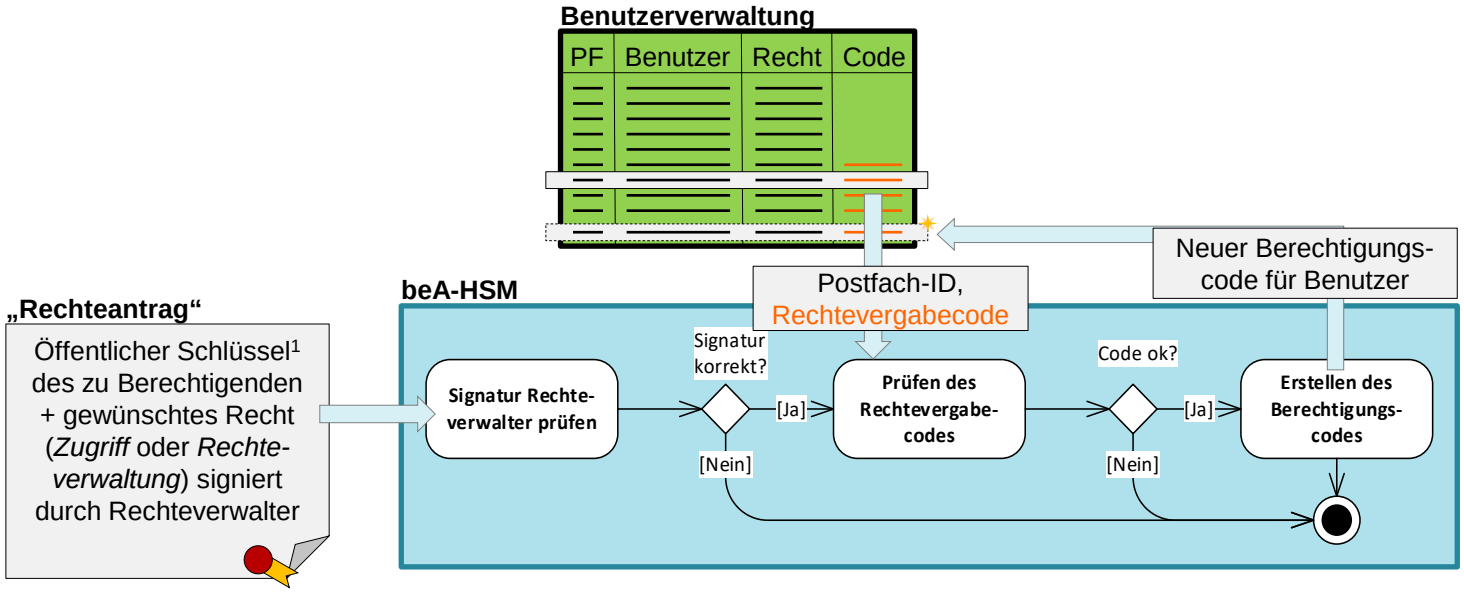


- Das HSM ermittelt bei der Session Key Anfrage, was für einen Berechtigungscode (MAC) der Leser benötigt.
- Nur wenn in der Benutzerverwaltung für den öffentlichen Schlüssel des anfragenden Postfachbenutzers ein passender Berechtigungscode vorliegt, wird der SessionKey für den Leser verschlüsselt mit dem öffentlichen Schlüssel des Benutzers bereitgestellt.

1 Es wird der öffentliche Schlüssel des Verschlüsselungszertifikats verwendet, mit dem der Nachrichtenschlüssel umgeschlüsselt werden soll.

Berechtigungscodes werden nur durch das HSM erzeugt. Zur Rechteverwaltung wird ein eigener Code benötigt

Absicherung des Postfachzugriffs mittels HSM – Vergabe von Rechten

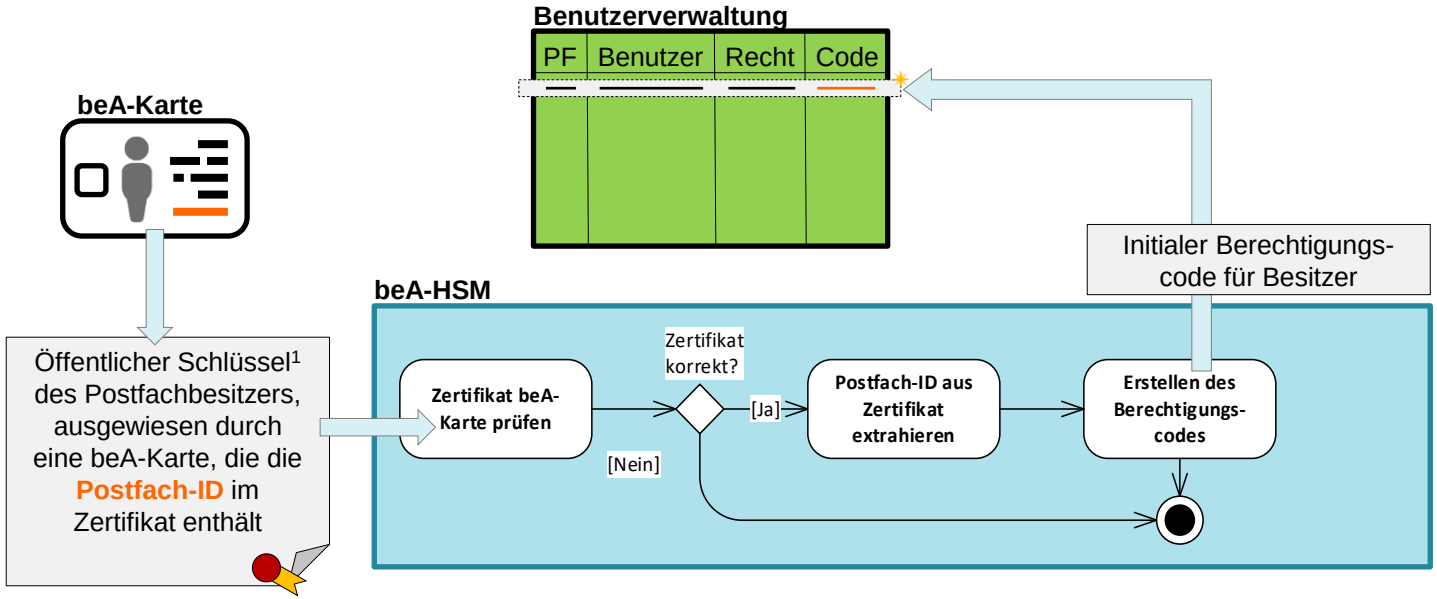


- Nur Benutzer, für die in der Benutzerverwaltung ein Berechtigungscode zur Vergabe von Rechten (Rechtevergabecode) vorliegt, können vom HSM neue Berechtigungscodes für andere Benutzer erstellen lassen.
- Dieser Vorgang muss durch vom Rechteverwalter fortgeschritten signiert werden.

1 Je nach Rechtetyp (Nachrichtenzugriff bzw. Rechteverwaltung) wird der öffentliche Schlüssel des Verschlüsselungszertifikats bzw. des Authentifizierungszertifikats verwendet.

Zur Inbesitznahme eines Postfaches wird eine speziell für das Postfach erstellte beA-Karte benötigt

Absicherung des Postfachzugriffs mittels HSM – Inbesitznahme eines Postfaches

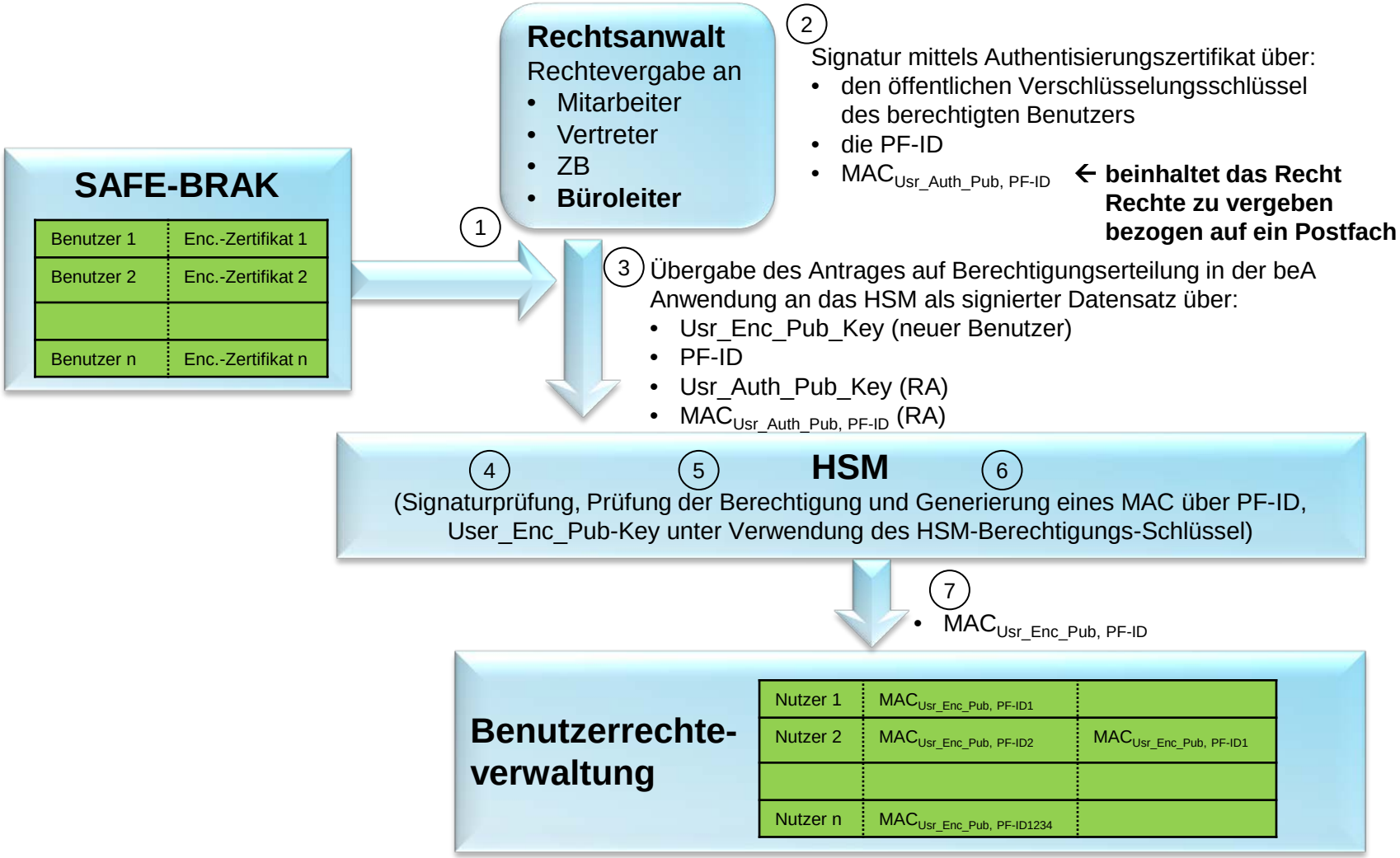


- Zur Erstellung des initialen Berechtigungscodes (Rechtevergabecodes) eines Postfaches wird das Zertifikat der beA-Karte benötigt, das die Postfach-ID enthält.
- Durch die Einbettung von Postfach-ID in dem für den Postfachbesitzer ausgestellten Zertifikat erfolgt eine eineindeutige Zuordnung zum Postfach in der Rechteverwaltung.
- Nur mittels dieser speziell für das Postfach erstellten Karte wird sichergestellt, dass ausschließlich der berechtigte Benutzer (= Postfachbesitzer) Zugriff auf das Postfach erlangt.

1 Öffentlicher Schlüssel des Authentifizierungszertifikats

Der verschlüsselungsrelevanter Zugriff auf ein Postfach wird über ein kryptografische abgesicherte Recht erteilt

Ende-zu-Ende Verschlüsselung – Rechtevergabe in der Benutzerverwaltung



Bei der Rechtevergabe zur Entschlüsselung von Nachrichten werden die öffentlichen Schlüssel der Verschlüsselungszertifikate der Benutzer abgesichert.

Verschlüsselungsrelevanter Zugriff auf ein Postfach werden über kryptografische abgesicherte Rechte erteilt

Ende-zu-Ende Verschlüsselung – Rechtevergabe in der Benutzerverwaltung

Das Recht zum Lesen der verschlüsselten Daten eines Postfaches wird bei der Rechtevergabe kryptografisch abgesichert und bei der Ausübung des Rechtes kryptografisch geprüft.

(1) Zusammenstellung des Datensatzes zur Berechtigungsvergabe
- PF-ID des Postfaches für das ein Benutzer die Berechtigung zum Lesen der verschlüsselten Daten erhalten soll
- öffentlicher Entschlüsselungsschlüssel des zukünftigen leseberechtigten Benutzers
- Kryptografische Absicherung des eigenen Rechtes zur Rechtevergabe auf ein bestimmtes Postfach MAC[1)] ($MAC_{Usr\_Auth\_Pub,\ PF\text{-}ID}$)

(2) Signatur des Datensatzes zur Berechtigungsvergabe mit dem privaten Schlüssel des Authentisierungszertifikates als Willensbekundung zur Rechtevergabe

(3) Übertragung des signierten Datensatzes mit dem Verschlüsselungszertifikat des zukünftig berechtigten Benutzers und der Postfach-ID (SAFE-ID) an das HSM

(4) HSM: Prüfung der Signatur des Datensatzes

(5) HSM: Prüfung des Rechtes zur Rechtevergabe an Hand der kryptografischen Absicherung des eigenen Rechtes ($MAC_{Usr\_Auth\_Pub,\ PF\text{-}ID}$)

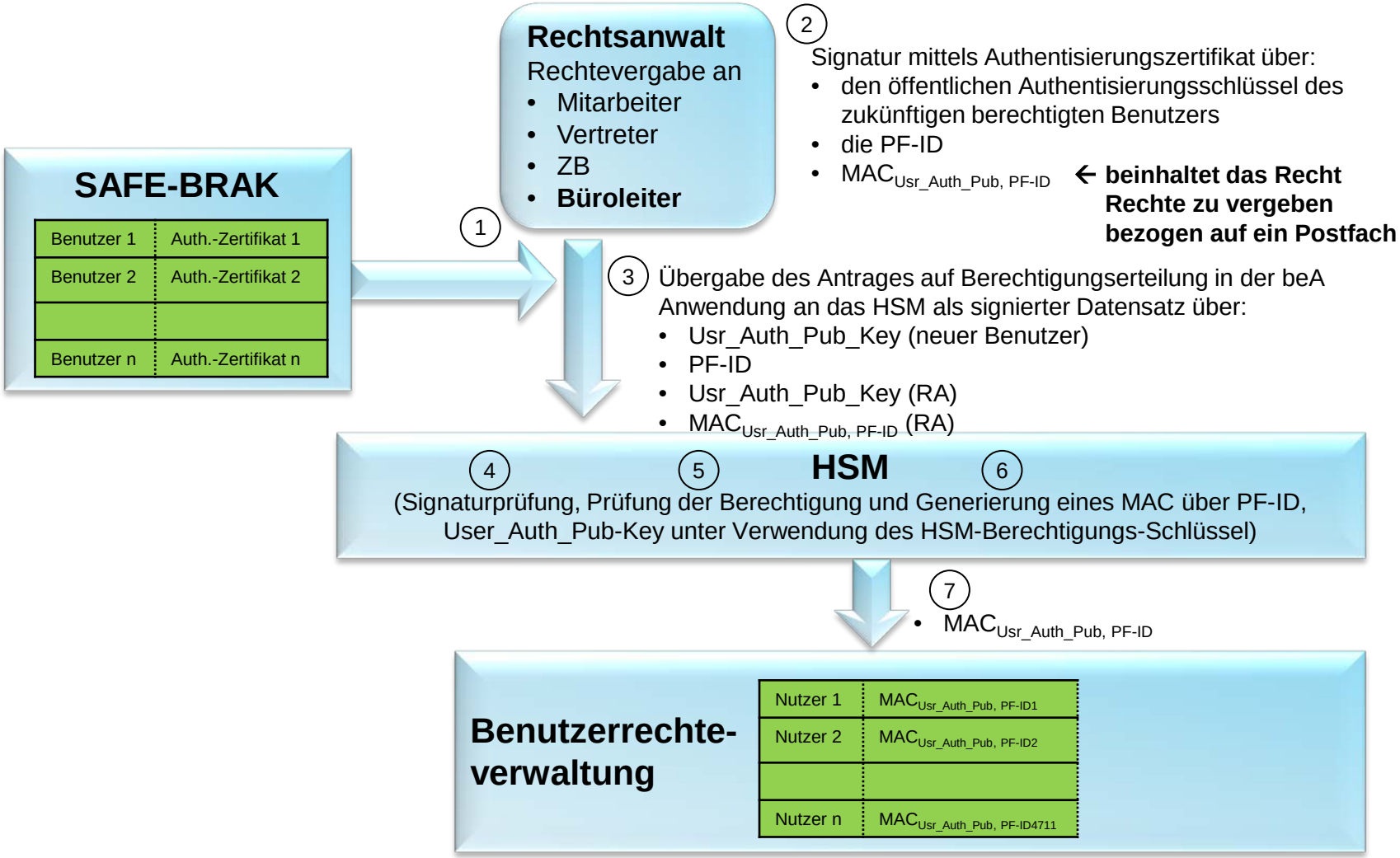
(6) HSM: Erstellung eines MAC über den öffentlichen Entschlüsselungsschlüssel des neuen berechtigten Benutzers für das die Berechtigung erteilt werden soll unter Verwendung eines nur im HSM bekannten Berechtigungs-Schlüssel auf der Basis der Postfach-ID (SAFE-ID).

(7) Hinterlegung des MAC ($MAC_{Usr\_Enc\_Pub,\ PF\text{-}ID}$) in der Benutzerrechteverwaltung der beA Anwendung für den neuen autorisierten Benutzer

1) Message Authentication Code

Das Recht ein Recht auf ein Postfach zu vergeben wird kryptografische abgesicherte vergeben

Rechtedelegierung – Rechtevergabe in der Benutzerverwaltung



Bei der Rechtedelegierung werden die öffentlichen Schlüssel der Authentifizierungszertifikate der Benutzer abgesichert.

Das Recht ein Recht auf ein Postfach zu vergeben wird kryptografische abgesicherte vergeben

Rechtedelegierung – Rechtevergabe in der Benutzerverwaltung

Das Recht zur Delegierung der Berechtigungsvergabe zum Lesen der verschlüsselten Daten eines Postfaches wird bei der Rechtevergabe kryptografisch abgesichert und bei der Ausübung des Rechtes kryptografisch geprüft.

(1) Zusammenstellung des Datensatzes zur Berechtigungsvergabe
   - PF-ID des Postfaches für das ein Benutzer die Berechtigung Vergabe von Rechten zum Lesen der Verschlüsselten Nachrichten erhalten soll
   - öffentlicher Authentisierungsschlüssel des zukünftigen Benutzers, der die Rechte vergeben soll
   - Kryptografische Absicherung des eigenen Rechtes zur Rechtevergabe auf ein bestimmtes Postfach ($MAC^{1)}_{Usr\_Auth\_Pub,\ PF\text{-}ID}$)

(2) Signatur des Datensatzes zur Berechtigungsvergabe mit dem privaten Schlüssel des Authentisierungszertifikates des bereits berechtigten Benutzers (RA) als Willensbekundung zur Rechtevergabe

(3) Übertragung des signierten Datensatzes mit dem Authentisierungszertifikat des zukünftig berechtigten Benutzers und der Postfach-ID (SAFE-ID) an das HSM

(4) HSM: Prüfung des Rechtes zur Rechtevergabe an Hand der kryptografischen Absicherung des eigenen Rechtes ($MAC_{Usr\_Auth\_Pub,\ PF\text{-}ID}$)

(5) HSM: Prüfung der Signatur des Datensatzes

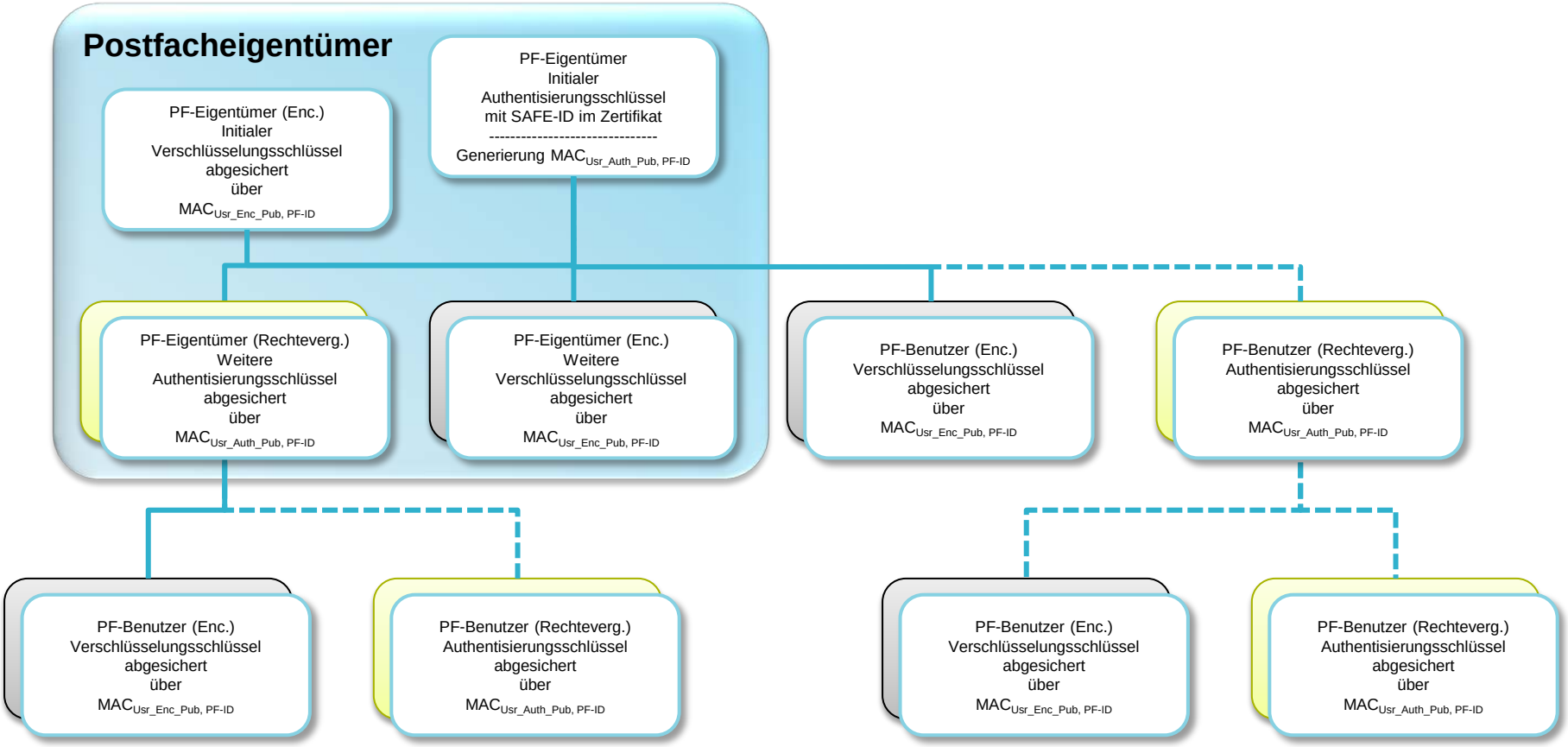
(6) HSM: Erstellung eines MAC über den öffentlichen Authentisierungsschlüssel des neuen berechtigten Benutzers für das die Berechtigung erteilt werden soll unter Verwendung eines nur im HSM bekannten Berechtigungs-Schlüssel auf der Basis der Postfach-ID (SAFE-ID).

(7) Hinterlegung des MAC ($MAC_{Usr\_Auth\_Pub,\ PF\text{-}ID}$) in der Benutzerrechteverwaltung der beA Anwendung für den neuen autorisierten Benutzer

1) Message Authentication Code

Rechtevergabe auf die Postfächer sind durch kryptografische Verfahren (MAC1)) geschützt.

Rechtevergabe aufbauend auf der Erstanmeldung des Postfachinhabers mittels Zertifikat mit SAFE-ID



Postfacheigentümer

PF-Eigentümer
Initialer
Authentisierungsschlüssel
mit SAFE-ID im Zertifikat

Generierung $MAC_{Usr\_Auth\_Pub, PF-ID}$

PF-Eigentümer (Enc.)
Initialer
Verschlüsselungsschlüssel
abgesichert
über
$MAC_{Usr\_Enc\_Pub, PF-ID}$

PF-Eigentümer (Rechteverg.)
Weitere
Authentisierungsschlüssel
abgesichert
über
$MAC_{Usr\_Auth\_Pub, PF-ID}$

PF-Eigentümer (Enc.)
Weitere
Verschlüsselungsschlüssel
abgesichert
über
$MAC_{Usr\_Enc\_Pub, PF-ID}$

PF-Benutzer (Enc.)
Verschlüsselungsschlüssel
abgesichert
über
$MAC_{Usr\_Enc\_Pub, PF-ID}$

PF-Benutzer (Rechteverg.)
Authentisierungsschlüssel
abgesichert
über
$MAC_{Usr\_Auth\_Pub, PF-ID}$

PF-Benutzer (Enc.)
Verschlüsselungsschlüssel
abgesichert
über
$MAC_{Usr\_Enc\_Pub, PF-ID}$

PF-Benutzer (Rechteverg.)
Authentisierungsschlüssel
abgesichert
über
$MAC_{Usr\_Auth\_Pub, PF-ID}$

PF-Benutzer (Enc.)
Verschlüsselungsschlüssel
abgesichert
über
$MAC_{Usr\_Enc\_Pub, PF-ID}$

PF-Benutzer (Rechteverg.)
Authentisierungsschlüssel
abgesichert
über
$MAC_{Usr\_Auth\_Pub, PF-ID}$

---

1) MAC: Message Authentication Code – kryptografisches Verfahren zur Absicherung der Korrektheit einer Information.