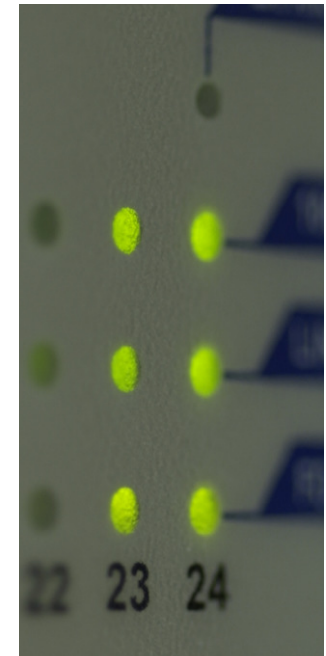


# Übersicht des Altersverifikationssystems „mtG-AVS“

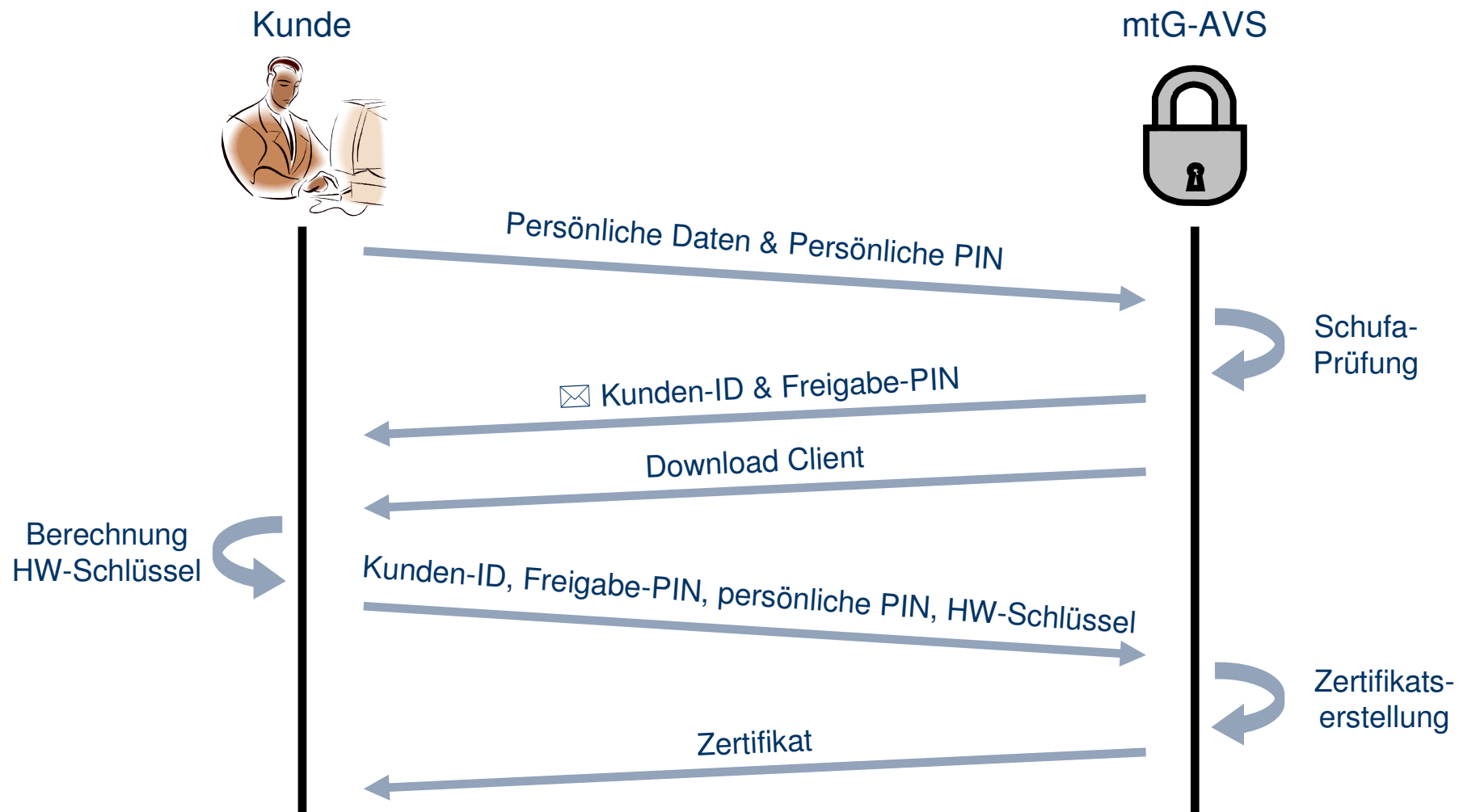
media transfer AG, Darmstadt



## mtG-AVS: sichere Altersverifikation gemäß KJM

- Ziel: Sicherstellung einer geschlossenen Benutzergruppe
- Umsetzung der Eckpunkte der KJM basierend auf dem Jugendmedienschutz-Staatsvertrag (JMStV §4 Absatz 2 Satz 2)
- 2-stufiger Prozess der Altersverifikation gemäss KJM
- Schritt 1: Identifizierung
  - mittels Schufa-Modul „Identitäts-Check mit Q-Bit“
  - Übermittlung der Freigabe-PIN per Einschreiben eigenhändig
- Schritt 2: Authentifizierung
  - Authentifizierung durch persönliche PIN (und Zertifikat)
  - Bindung an ein Hardware-Token, das nicht vervielfältigt werden kann
    - Variante 1: PC des Anwenders
    - Variante 2: USB-Token

# mtG-AVS: Identifizierung (Variante 1, vereinfacht)



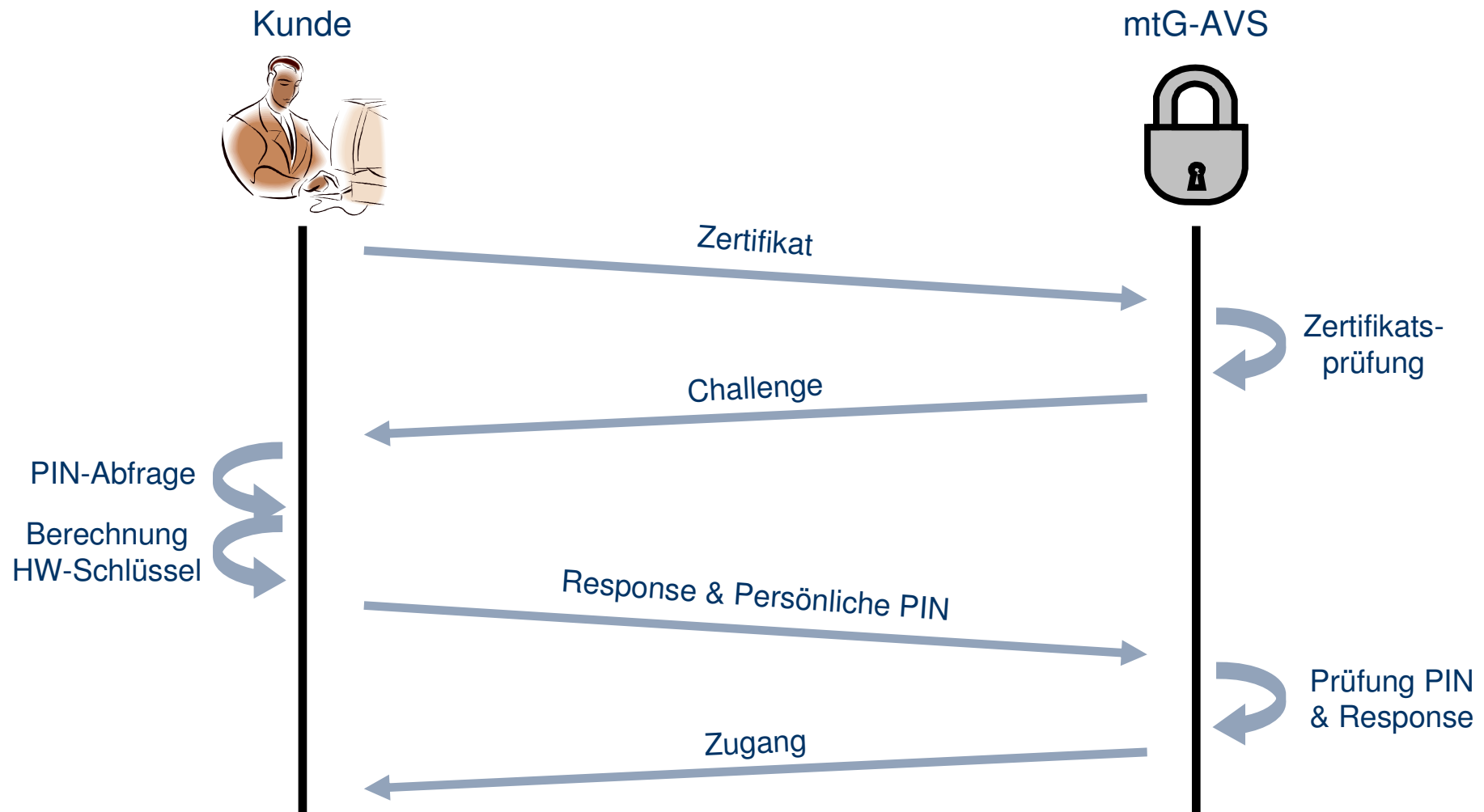
## mtG-AVS: Identifizierung (Variante 1) Teil 1

- Kunde gibt seine persönlichen Daten ein und wählt eine persönliche PIN
- Kundendaten werden in der Datenbank des mtG-AVS gespeichert
- mtG-AVS überprüft die Daten mittels Schufa-Modul „Identitäts-Check mit Q-Bit“
  - Rückgriff auf erfolgte Face-to-Face-Kontrolle und Volljährigkeitsprüfung der Kreditinstitute
- bei negativer Prüfung:
  - Fehlermeldung; Ende des Verfahrens
- bei positiver Prüfung: Auslieferung der Zugangsdaten wie beim Schufa-Modul vorgesehen:
  - per Einschreiben eigenhändig

## mtG-AVS: Identifizierung (Variante 1) Teil 2

- Generierung der Zugangsdaten:
  - Kunde wählt persönliche PIN selbst im ersten Teil der Identifizierung
  - mtG-AVS speichert die persönliche PIN
  - mtG-AVS generiert eine Kunden-ID und eine zufällige Freigabe-PIN
- Auslieferung Kunden-ID und Freigabe-PIN per Einschreiben eigenhändig
- Eingabe der Zugangsdaten, um die Identifizierung abzuschließen
  - Kunden-ID
  - Freigabe-PIN
  - persönliche PIN
- Wenn Zugangsdaten korrekt, wird die Hardware-Bindung hergestellt
  - Berechnung eines hardwarespezifischen Schlüssels und Übermittlung an den mtG-AVS-Server (für Abgleich bei der Authentifizierung)
  - dabei Installation des Zertifikats vom mtG-AVS Server
  - Freigabe-PIN wird danach ungültig

# mtG-AVS: Authentifizierung (Variante 1, vereinfacht)



## mtG-AVS: Authentifizierung (Variante 1)

- Verbindung zum mtG-AVS Server gesichert durch Zertifikat (SSL Protokoll mit Client Authentifizierung)
- Der Server prüft, dass das Zertifikat korrekt ist und nicht gesperrt wurde.
- Server erzeugt Zufallszahl (Salt) und verschlüsselt mit hardware-spezifischem Schlüssel (Challenge)
- Kunde gibt persönliche PIN ein
- Client-Software
  - berechnet hardware-spezifischen Schlüssel
  - entschlüsselt Challenge → Salt
  - modifiziert Salt
  - verschlüsselt das Ergebnis wieder (Response)
- mtG-AVS prüft persönliche PIN und Response
- bei positiver Prüfung erhält der Kunde Zugriff auf Ü18-Inhalte

## mtG-AVS: Positivbewertung durch die KJM

- mtG-AVS erhielt die Positivbewertung der KJM
- Veröffentlichung mit Datum 2.1.2008 unter [www.kjm-online.de](http://www.kjm-online.de) (Rubrik „Pressemitteilungen“)

## Ihr schneller und sicherer Kontakt zu uns

media transfer AG  
Dolivostr. 11  
64293 Darmstadt

Telefon: 0 61 51 / 81 93-0  
E-Mail: [contact@mtg.de](mailto:contact@mtg.de)

[www.mtg.de](http://www.mtg.de)

