eident

elektronische Identifikation

Online Lösung zur elektronischen Identitätsprüfung

Identifizieren, Authentisieren, Autorisieren

Medium

- Amtliches Dokument: neuer (nationaler) Personalausweis (nPA) mit integriertem RFID-Chip
- Zugriff auf Personendaten des Kunden über Kontaktlos Kartenleser am PC oder Handy oder POS
- Nutzung der Online-Ausweisfunktion des Personalausweises über Internet VPN-Verbindung

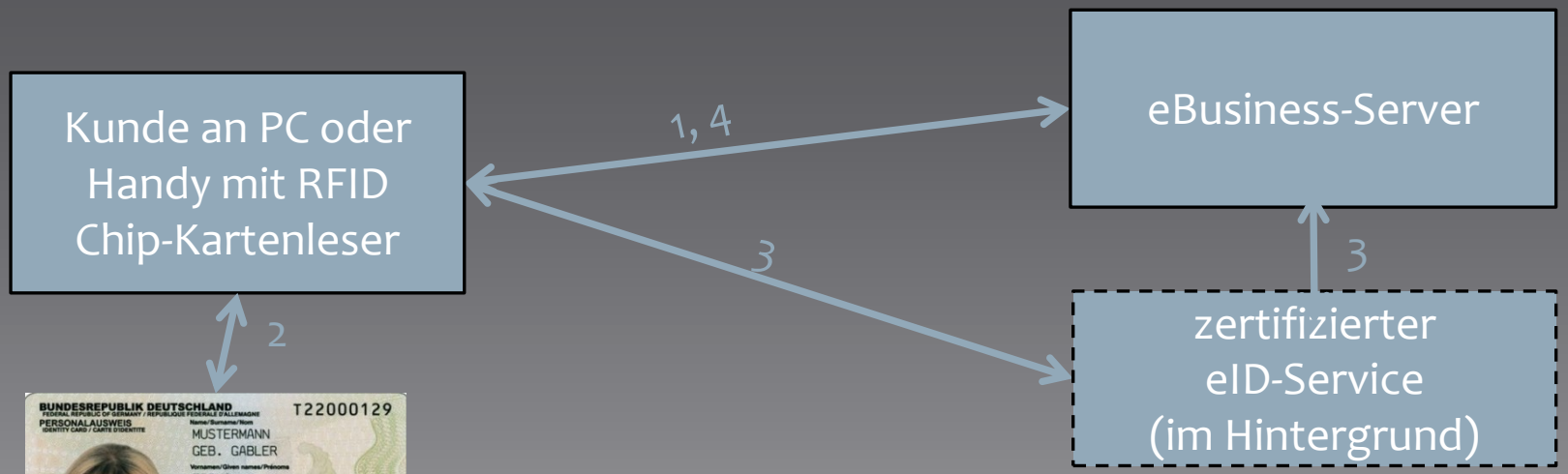
Funktionen

- Online-Ausweisfunktion zur elektronischen Identitätsprüfung mit der eID-Funktion des Personalausweises (Standard-Funktion bei Ausstellung des nPA im integrierten Chip)
- Online-Authentisierung nach dem Prinzip der Gegenseitigkeit durch Berechtigungszertifikat des Anbieters und persönlicher 6-stelliger PIN des Kunden
- Altersnachweis ebenfalls über eID-Funktion möglich

Mögliche Geschäftsvorfälle

- Elektronischer Identitätsnachweis in E-Commerce und E-Government Anwendungen
- Ersetzen von postident (papiergebunden) durch eIdent (elektronisch), z.B. bei Kontoinhaberüberprüfung nach dem GW-Gesetz im Online-Banking
- Überprüfung der Identität von Kunde und Anbieter beim Session-Aufbau mittels Verknüpfung des Kunden-Account mit unique Anbieter-Zertifikat
- Elektronischer Altersnachweis

Beispiel: Online-Registrierung am PC mit elektronischer Identitätsprüfung



1. Kunde wählt Registrierung, der E-Commerce Server startet eine Registrierungs-Transaktion und sendet eine eindeutige Transaktionsnummer an den Kunden PC über VPN-Verbindung.
2. Im Verlauf der Registrierung wählt der Kunde optional für den Identitätscheck das eident-Verfahren und legt seinen Personalausweis auf den Kartenleser (oder zukünftig auf sein Smartphone) und bestätigt mit Transaktionsnummer und 6-stelliger PIN .
3. Der E-Commerce Server startet den Online-Check, indem er sein Berechtigungszertifikat an den eID-Service (z.B. T-Systems) übermittelt. Es werden die Personendaten vom Chip gelesen und verschlüsselt an den E-Commerce Provider weitergeleitet, der den Abgleich mit den eingegeben Kundendaten durchführt.
4. Am PC erscheint dann eine Meldung für den Kunden, bei erfolgreicher Identitätsprüfung bestätigt der E-Commerce Betreiber die Kunden-Registrierung.

eident

Sicherheit und technische Grundlagen

Sicherheit durch

- Kryptographische Sicherheitsmechanismen (PACE, Terminal- und Chip-Authentisierung) gemäß BSI Richtlinien (BSI: Bundesamt für Sicherheit in der Informationstechnik)
- Die im Chip des Personalausweis gespeicherten Daten des Inhabers sind fälschungssicher (u.a. Name, Vorname, Geburtsdatum, Geburtsort, Adresse).
- Prinzip der Gegenseitigkeit: der Kunde kann mit der Online-Ausweisfunktion des nPA seine Identität nachweisen ohne persönlich anwesend zu sein, auf der anderen Seite können nur autorisierte eBusiness-Partner diese Funktion anbieten (Autorisierung läuft im Hintergrund) und erst durch Bestätigung mit seiner 6-stelligen PIN gibt der Kunde die Erlaubnis seine persönlichen Daten zu lesen.
- Es kommen ausschließlich zertifizierte Verfahren, eine abgesicherte Infrastruktur und VPN-Verbindungen zum Einsatz, der Zugriff auf den Personalausweis erfolgt durch einen zertifizierten eID-Server.
- Personendaten sind im gesamten Ablauf durch BSI-konforme kryptographische Sicherheitsverfahren geschützt und werden ausschließlich auf dem Server des Dienstanbieters verarbeitet, auf der Client-Seite treten die Daten nie im Klartext auf.
- Die sog. Privacy des Ausweisinhabers ist mittels seines amtlichen Personalausweises und seiner persönlichen eID-PIN immer gewährleistet.

Technische Grundlagen

- Realisierung der eident-Applikation gemäß den technischen Richtlinien und Vorgaben des BSI, u.a. eCard-API-Framework, Technical Directive of the Federal Office for Information Security Nr. 03112, BSI TR-03112, TR-03127
- Identification cards – Integrated circuit cards programming interfaces, ISO/IEC 24727
- Sichere Infrastruktur und Internet-Kommunikation über VPN-Verbindungen und SSL

eident

Lieferumfang

eIdent Client

- Gekapselter eId-Client, geliefert als jar-File, die Clientsoftware ist Voraussetzung für alle eident-Lösungen. Als Plug-In Komponente installiert sich die Software weitgehend selbst auf dem jeweiligen Endgerät.
- Die Client-Software kann ganz unterschiedliche Interfaces zur Verfügung stellen: Schnittstelle zu allen gängigen Browsern, Java-Schnittstelle zu kundenspezifischer Applikations-Software z.B. für den Einsatz an POS-Terminals oder bei Einbindung des eident-Client in eine Kunden-Webanwendung. Die Web-Interfaces zum Backend-System des Dienstanbieters sowie zu einen kommerziellen externen eID-Service Provider (z.B. T-Systems, Bundesdruckerei, u.a.) sind ebenfalls implementiert. Das Chip-Interface ist vorbereitet für einen kommerziellen kontaktlosen Kartenleser, der mittels PCS-Treiber im System installiert ist oder optional über ein Java-Interface für kundenspezifische Kartenleser beispielsweise an einem Geldautomaten.
- Das im Lieferumfang enthaltene BSI-konforme Benutzer-Interface ist je nach Einsatzzweck voreingestellt für die Benutzung am PC oder POS-Terminal oder eFinance –Transaktionsterminals, je nach Wunsch mit neutralem Design oder auch spezifischem Customer Design.

Konfigurierbare Web-Schnittstellen

- Für spezielle Anwendungsfälle können die Web-Schnittstellen (Webservices, Web Calls, oder Sockets) an die kundenspezifische Infrastruktur angepasst werden, so dass eine Kommunikation mit unterschiedlichsten Backend-Systemen und Web-Portalen möglich ist.
  Im Lieferumfang immer enthalten sind die Web-Services für den Server des Dienstanbieters zur Kommunikation mit dem externen eID-Service Provider sowie dem (remote) eident-Client.

Beratungs- und Serviceleistungen

- Die Realisierung von kundenspezifischen Installationen und Projekten wird durch ein umfassendes Angebot an Beratung, Service-Leistungen , Programmieranleitungen und Programmierbeispielen unterstützt.
  Das Angebot beinhaltet auf Wunsch auch Beratung und Support bei der Beantragung der Berechtigungen zum Betrieb des eident-Verfahrens. Auf Wunsch bieten wir den kompletten technischen Betrieb des eident-Verfahrens an.