DG VERLAG

Partner im genossenschaftlichen Verbund

CeBIT 2010 Genossenschafts-Tag

Das neue ZKA Kartenterminal **Secoder 2**

Sicheres Signieren im Online-Banking

Christian Adler
Deutscher Genossenschafts-Verlag eG
Wiesbaden

DG VERLAG

Vortragsübersicht: Vorstellung des neuen ZKA-Internet-Kundenterminals

- Anwendungsbereiche
- Technischer Ansatz
- Konzeptionelle Bestandteile der Leserarchitektur
- Funktionalität
- Stufenkonzept der Einführung
- Die Signaturfunktionalität des Secoder 2
- Produktzulassung
- Zusammenfassung

DG VERLAG

Das neue ZKA Internet Kundenterminal - Anwendungsbereiche

- **Ziel: *Ein* multifunktionaler Leser für den Kunden**
  - **GeldKarte-Transaktionen im Internet**
  - **Browserbasiertes Online-Banking**
  - **Kundensystem-basiertes Online-Banking**
    - **FinTS / HBCI**
  - **DFÜ mit Kunden / EBICS**
  - **Qualifizierte Signatur (mit SAK)**

Das neue ZKA Internet Kundenterminal – Technischer Ansatz

- **Ein „schlanker“ Leser, um Stückkosten zu begrenzen**
  - **Klasse 3 Leser für kontaktbehaftete Karten**
    - **kein SAM (Security Authentication Module)**
  - **PC/SC API-Schnittstelle (evtl. USB CCID)**
  - **zweizeiliges Display á 16 Zeichen (Minimum)**
  - **14 Tasten**
  - **keine kryptographischen Funktionen im Leser (außer für Firmware Update)**
  - **nur begrenzter Datenpuffer**
  - **Datenkompression durch Hashing (unter Nutzung der Chipkartenfunktionalität)**
  - **keine Unterstützung von Gesamtabläufen im Secoder** (Beispiel: GeldKarte-Zahlung)
    - **es sind nur die sicherheitsrelevanten Teilabläufe im Secoder realisiert (z.B. Anzeige/Bestätigung des Betrags)**
    - **Gesamtablaufsteuerung wird der PC-seitigen Software überlassen**

Die konzeptionellen Bestandteile der Leserarchitektur

- **Leserfunktionen: < 10 Kartenterminalkommandos**
  - Beispiele: Applikationsmodusselektion, Datenvisualisierung und Bestätigung, Signatur- bzw. Kryptogrammbildung, GeldKarte-Zahlung, PIN-Handling
- **Zustandsraum des Kartenterminals: < 20 Zustandsvariablen**
  - Beispiele: Typ der eingesteckten Karte, aktuell selektierter Applikationsmodus, Status der PIN-Verifikation, visualisierte Daten, Status der Datenbestätigung durch den Nutzer
- **Firewall des Kartenterminals: ca. 50 Filterregeln**
  - Chipkarten- und Kartenterminalkommandos werden applikationskontextabhängig zugelassen bzw. blockiert.
  - Beispiel: Das GeldKarte ABBUCHEN EINLEITEN Chipkartenkommando ist global blockiert und nur lokal im Applikationsmodus GeldKarte Zahlung zugelassen. Das GeldKarte ABBUCHEN Chipkartenkommando ist generell blockiert und kann nur über das Kartenterminalkommando GK PAYMENT im Applikationsmodus GeldKarte Zahlung an die Chipkarte hindurchgeleitet werden; der abzubuchende Betrag (bzw. bei inkrementellem Abbuchen der Maximalbetrag) wird am Secoder angezeigt und muss vom Nutzer bestätigt werden.

➢ **Der Secoder ist auch konzeptionell ein relativ „schlanker“ Leser**

Funktionalität des Secoders – Die universell einsetzbare Basis (I)

- Im **Standardmodus** ist der Secoder ein Klasse 2/3-Leser – mit einigen Besonderheiten:
  - Der Standardmodus erlaubt einen (fast uneingeschränkten) transparenten Zugriff auf die Chipkarte
    - keine Bindung an ein bestimmtes Chipkartenbetriebssystem
      - auch andere als die kreditwirtschaftlichen SECCOS Karten sind einsetzbar
    - Etablierte kreditwirtschaftliche Verfahren können unverändert genutzt werden (z.B. FinTS/HBCI)
    - gesicherte PIN-Eingabe und -Verwaltung werden unterstützt (wie bei einem Klasse 3 Leser)
    - allerdings sind einige sicherheitskritische Spezialkommandos kreditwirtschaftlicher Chipkartenapplikationen gesperrt, z.B.:
      - Abbuchen von der GeldKarte (Ergänzungskommando ABBUCHEN)
      - Bildung eines EMV-Applikationskryptogramms (EMV-Kommando GENERATE AC)

Funktionalität des Secoders – Die universell einsetzbare Basis (II)

- Der Standardmodus erlaubt jedoch der Anwendung aus Sicherheitsgründen keinen transparenten Zugriff auf Tastatur und Display des Secoders.
  - Die Tastatur wird zur trojanersicheren PIN (und PUK) Eingabe genutzt.
  - Auf dem Display werden nur in der Secoder-Spezifikation vordefinierte Texte zur Unterstützung der PIN-Eingabe bzw. der PIN-Verwaltung angezeigt.
  - Um entsprechende Angriffe (z.B. Vortäuschung einer sicheren PIN-Eingabe) zu verhindern, können im Standardmodus somit Display und Tastatur des Secoders von der PC-seitigen Software in keiner Weise direkt angesteuert werden.
  - Zusätzlich blockiert der Secoder 2 bei Nutzung kreditwirtschaftlicher Karten jegliche transparente – also für den Kunden nicht sichtbare – PIN-Operationen (Chipkartenkommandos VERIFY, CHANGE REFERENCE DATA, RESET RETRY COUNTER): Damit wird bei Verwendung von SECCOS-Karten die sichere PIN-Eingabe über die Secoder-Tastatur erzwungen, d.h. die Anwendungssoftware muss sich diesem Regime unterwerfen.

Funktionalität des Secoders – Dedizierte Applikationsmodi

- Darüber hinaus unterstützt der Secoder bestimmte Anwendungsmodi, die auf die entsprechenden kreditwirtschaftlichen Chipkartenapplikationen zugeschnitten sind:
  - **GeldKarte-Zahlung**
  - **symmetrische und asymmetrische Authentisierungsverfahren**
    - symmetrisch: EMV AC
    - asymmetrisch: AUT und DS
  - **Die Abläufe in den Secoder-Anwendungsmodi sind eng verzahnt mit der Funktionalität der entsprechenden Chipkartenapplikationen der kreditwirtschaftlichen SECCOS 5 bzw. SECCOS 6-Karten**
    - elektronische Geldbörse
    - EMV AC / TAN Anwendung
    - Signaturanwendung

Funktionalität des Secoders – Applikationsmodi zur Authentisierung (I)

- In den Anwendungsmodi zur Authentisierung können beliebige Informationen von der PC-seitigen Software am Display angezeigt werden.
- Zusätzlich können beim symmetrischen Authentisierungsverfahren an der Secoder-Tastatur auch nummerische Daten eingegeben werden (z.B. Transaktionsdaten wie Beträge, Kontonummern oder auch vertrauliche Authentisierungsdaten wie z.B. ein Geburtsdatum oder eine Online-Banking-PIN).
- Über Funktionstasten können angezeigte Informationen vom Nutzer bestätigt oder verworfen werden.
- Durch gesicherte PIN-Eingabe wird vom Nutzer (wenn erforderlich) die dem jeweiligen Anwendungsmodus entsprechende Chipapplikation zur Authentisierung freigeschaltet.
- Die visualisierten Informationen bzw. Daten werden vom Secoder mithilfe der entsprechenden SECCOS-Chipkartenfunktionalität signiert.
  - unidirektionale kryptographische Absicherung visualisierter Daten sowie der Leser- und Kartenidentität
    - Signatur: Leser -> Hintergrundsystem

Funktionalität des Secoders – Applikationsmodi zur Authentisierung (II)

- Nur die Signaturen (bzw. Applikationskryptogramme) werden der PC-seitigen Software – und damit letztlich dem Hintergrundsystem – zugänglich gemacht, nicht aber die an der Secoder-Tastatur eingegebenen bzw. am Display angezeigten Daten.

- Das Hintergrundsystem (Bank-Server) überprüft die Signatur (bzw. im Falle der symmetrischen Authentisierung das Applikationskryptogramm) durch Rekonstruktion der am Secoder visualisierten Informationen sowie ggf. weiterer, zur Absicherung in die Signaturbildung einbezogener (nicht visualisierter) Daten wie z.B. Karten- und Leseridentitäten.

- Während das Hintergrundsystem in der Regel die auf dem Display zur Anzeige gebrachten Informationen kennt, da es die Funktionalität der PC-basierenden Software – und damit die zur Visualisierung am Secoder eingestellten Daten – steuert, muss es bei etwaigen, vom Nutzer an der Secoder-Tastatur hinzugefügten (nummerischen) Eingaben auf getrenntem Wege diese Daten in Erfahrung bringen:

  - Auf am Secoder eingegebene vertrauliche Daten (z.B. vom Anwendungsprozess geforderte Authentisierungsmerkmale) muß das Hintergrundsystem zur Verifikation des Kryptogramms auf anderem Wege zugreifen können.

  - Transaktionsparameter (wie z.B. ein Überweisungsbetrag oder eine Zielkontonummer) sind vom Kunden (zusätzlich) direkt am PC einzugeben.

    - Eine im Anwendungsprozess ggf. geforderte Eingabe von nicht vertraulichen Daten (z.B. von Transaktionsparametern) an der Tastatur des Secoders würde also lediglich der Aufmerksamkeitsbindung des Nutzers dienen.

Das ZKA Secoder Vorhaben: Stufenkonzept der Einführung

- **Secoder 1**
  - Spezifikation Ende 2007 finalisiert
  - unterstützt drei Modi:
    - **Standardmodus**
    - **GeldKarte-Zahlung**
    - **symmetrisches Authentisierungsverfahren** (EMV AC)
  - seit Frühjahr 2008 bei der GAD im Browser-gestützten Online Banking im Einsatz
  - derzeit am Markt: 4 Leserprodukte von 2 Herstellern (REINER SCT, KOBIL)
- **Secoder 2**
  - Spezifikation (Version 2.0) im Juli 2009 verabschiedet
  - unterstützt zusätzliche Anwendungsmodi:
    - **asymmetrische Authentisierungsverfahren**
      - AUT Signatur
      - DS Signatur
  - Spezifikation zur Secoder-Einbindung in **FinTS** im Dezember 2009 fertiggestellt
  - neue Spezifikationsversion 2.1 voraussichtlich noch in diesem Monat verfügbar
    - ermöglicht die optionale Integration einer kontaktlosen Leserschnittstelle zum neuen Personalausweis (Standardleservariante CAT-S gemäß BSI TR-03119)
      - ➢ Unterstützung der **eID-Funktionalität des nPA** auf Klasse 2 Leserniveau: Online-Authentisierung mit sicherer PIN-Handhabung

Die Signaturfunktionalität des Secoder 2 (I)

❖ **Transparente Verwendung der Standard-Chipkartenkommandos INTERNAL AUTHENTICATE und COMPUTE DIGITAL SIGNATURE:**

- Wie der Secoder 1, so kann auch der **Secoder 2 im Standardmodus** wie ein „normaler“ Leser zur transparenten Erstellung von Signaturen (d.h. ohne Datenvisualisierung am Secoder) mit allen – also insbesondere auch den kreditwirtschaftlichen SECCOS-Karten – eingesetzt werden.

  ➢ Damit ist die **Kompatibilität zu den bisherigen Verfahren** gewährleistet (z.B. zu dem derzeitigen FinTS/HBCI ohne Secoder-Unterstützung).

Die Signaturfunktionalität des Secoder 2 (II)

❖ **Standardkonforme elektronische Signatur mit zusätzlichem Visualisierungsnachweis**

- In den **Signaturanwendungsmodi des Secoder 2** (AUT bzw. DS Signatur) mit Datenvisualisierung und Bestätigung kann neben der standardkonformen Signaturbildung (fortgeschrittene bzw. auch qualifizierte elektronische Signatur) mit einem der Signaturschlüssel (hier dem Authentifikationsschlüssel) zusätzlich eine nicht-standardkonforme Signatur als Visualisierungsnachweis erstellt werden.
- Filtermechanismen verhindern, dass ein derartiger Visualisierungsnachweis im **Standardmodus des Secoder 2** nachgebildet werden kann.

➢ Das Hintergrundsystem hat damit die Möglichkeit zu prüfen, ob die vorgelegte Signatur tatsächlich am Secoder in einem Signaturanwendungsmodus unter Datenvisualisierung und Bestätigung erstellt wurde (vorausgesetzt, dass kundenseitig ein zugelassener Secoder 2 eingesetzt wird).

- Das vom ZKA spezifizierte Authentifizierungsverfahren zur Bildung des Visualisierungsnachweises nutzt lediglich Standard-Chipkartenkommandos und setzt leserseitig keinerlei kryptographische Algorithmen, Schlüssel oder gar geheime Verfahren bzw. Daten voraus (Konzept des „schlanken“ Lesers).

➢ Dieses patentgeschützte Verfahren wäre prinzipiell – auch unabhängig von dem spezifischen Lesertyp Secoder 2 – in analoger Weise bei Nutzung anderer als kreditwirtschaftlicher Karten einsetzbar (z.B. HBA, eGK mit QES).

Das ZKA Zulassungsverfahren für den Secoder 2

- **Herstellererklärung**
  - Zusicherung der Konformität mit der Spezifikation
- **Funktionstest**
  - ZKA-akkreditierte Testlabore:
    - VÖB-ZVD GmbH, Bonn
    - CETECOM ICT Services GmbH, Saarbrücken
  - Testbereitschaft ab Q2/2010
- **Sicherheitsgutachten**
  - Untersuchung gewisser sicherheitskritischer Eigenschaften

➢ **ZKA-Siegel**

- als Nachweis der Produktzertifizierung

Zusammenfassung

Sicherheit

Motto: **what you see is what you sign**

- Am Secoder eingegebene Daten sind vor Ausspähung geschützt: **Vertraulichkeit**
- Bestätigung visualisierter Daten unter ausschließlicher Kundenkontrolle: **Authentizität** und **Integrität** der Transaktionen gewährleistet
- Der Secoder im Zusammenspiel mit der SECCOS-Chipkarte:
  Eine vertrauenswürdige Signierkomponente mit Datenvisualisierung

Preis

- Dank „schlankem“ Leserkonzept hinreichend gering

DG VERLAG

Partner im genossenschaftlichen Verbund

Gelegenheit zu Fragen und Stellungnahmen