

Moderne Ausweisproduktion beim Bundesministerium der Verteidigung



Bild: Bundeswehr-Fotos Wir.Dienen.Deutschland / flickr

Derzeit werden in der Pass- und Ausweisstelle des Bundesministeriums der Verteidigung (BMVg) neue hybride Zutritts- und Zeiterfassungs-Ausweise für alle Mitarbeiter der Standorte Bonn und Berlin produziert. Nach monatelanger Planungs- und Abstimmungsphase konnte nun die bestehende Ausweis-Personalisierungs-Software durch das neue Ausweis-Verwaltungssystem StigmaTag der Vision ID Engineering GmbH ersetzt werden.

Planung

Das Bundesministerium der Verteidigung plant bereits seit einiger Zeit die Einführung neuer Zutritts- und Zeiterfassungsausweise auf Basis einer modernen und hochsicheren Technologie*, da das bisher eingesetzte System nicht mehr dem Stand der Technik in einem Hochsicherheitsbereich entspricht. Dabei muss das bestehende Alt-System solange parallel unterstützt werden, bis schließlich alle Terminals auf die neue Technologie umgerüstet worden sind.

Die neu zum Einsatz kommende Technologie wurde ausgewählt, um die folgenden zwingenden Anforderungen erfüllen zu können:

- Verschiedene Applikationen können auf dem gleichen Chip vollkommen unabhängig voneinander betrieben werden
- Zukünftige Erweiterungen müssen ggf. im Feld aufgebracht werden können
- Es sollen offene Verschlüsselungs-Standards mit hohem Sicherheits-Level zum Einsatz kommen
- Zertifizierung nach Common Criteria EAL4+ (Hardware und Betriebssystem)

Um den gleichzeitigen Betrieb von Alt- und Neu-Anlage in der Übergangszeit sicherzustellen, hat sich das BMVg für den Einsatz einer Hybrid-Karte entschieden, welche die zwei verschiedenen RFID-Technologien in einem Kartenträger vereint.

Die Karte

Bedingt durch die verschiedenen Standorte des BMVg in Bonn und Berlin werden im Zutritts- und Zeiterfassungsbereich künftig drei unterschiedliche Systeme verschiedener Anbieter zum Einsatz kommen. Diese drei verschiedenen Zutritts- und Zeiterfassungssysteme können zwar alle mit der neu

eingesetzten Technologie arbeiten, haben aber völlig unterschiedliche Anforderungen und Vorgaben an die gespeicherten Strukturen und Daten auf der Karte.

Die Vision ID Engineering GmbH wurde damit beauftragt, die Anforderungen der verschiedenen Systeme zu analysieren und dafür eine maßgeschneiderte Kartenstruktur für den zukünftig eingesetzten Karten-Chip zu erstellen.

In Abstimmung mit den Lieferanten der Zutritts- und Zeiterfassungs-Systeme wurde schließlich eine umfassende Spezifikation der Kartenstruktur entworfen, welche alle Informationen für die Codierung und den Betrieb der neuen Karten enthält.

Letztlich war es notwendig, dass jedem System auf dem Karten-Chip eine eigene Applikation zugewiesen wurde, was durch den eingesetzten Chip natürlich problemlos unterstützt wurde.

Im Zuge der Definition der Kartenstruktur wurden von der Vision ID Engineering GmbH auch diverse Musterkarten mit Test-Schlüsseln erstellt und mit den Zutritts- und Zeiterfassungs-Anbietern ausgetauscht, um im Vorfeld bereits

mögliche Kompatibilitäts-Probleme auszuschließen und einen reibungslosen Start des Echtbetriebs zu ermöglichen.

Zusätzlich zu den drei Applikationen der Zutritts- und Zeiterfassungssysteme wurden auch noch zwei andere Standard-Applikationen auf den Chip aufgebracht, welche die zukünftige Nutzung der Karte durch andere Anbieter erheblich erleichtern werden:

- NXP Generic Access Control Data Model - eine Standard-Zutritts-Datenstruktur
- openCashfile-Kartenstandard des Industrieverbands für einheitliche Smartcard-Lösungen e.V. - eine Standard-Geldbörse für geschlossene Zahlungssysteme

Dabei kann die Applikation Generic Access Control Data Model von zukünftigen System-Lieferanten im Bereich der Zutritts- und Zeiterfassung genutzt werden.

Die standardmäßige Aufbringung des openCashfile Kartenstandards ermöglicht Anbietern von geschlossenen Zahlungssystemen (Kantinen, Verpflegungsautomaten) die einfache Nutzung der vorhandenen Zutritts- und Zeiterfassungs-Ausweise als virtuelle Geldbörse.

Ausweis-Verwaltung

Eine zentrale Anforderung an das neue Ausweis-Verwaltungssystem war die eigenständige Generierung und Verwaltung der Zugriffs-Schlüssel durch das BMVg. Nur die für den Betrieb der jeweiligen Applikation notwendigen Schlüssel werden dann bei Inbetriebnahme aus der Schlüssel-Verwaltung exportiert und an den jeweiligen System-Anbieter ausgegeben.

Aber auch der weitere erforderliche Funktionsumfang war nicht trivial. Nachfolgend ein Überblick über die Haupt-Anforderungen, die vom neuen Ausweis-Verwaltungssystem zu erfüllen waren:

- Generierung und gesicherte Schlüssel-Verwaltung der Zugriffs-Schlüssel auf die einzelnen Applikationen
- Auslesen bzw. Codieren von zwei unterschiedlichen Technologien ver-

schiedener Frequenzbereiche in einem Arbeitsgang

- Freie Konfiguration von verschiedenen Applikationen mit unterschiedlichen Sicherheitsmerkmalen (z.B. Schlüssel-Diversifikation, Signatur, etc.)
- Einbindung einer beigegebenen Codier-DLL in den Codierungs-Ablauf: Von einem Anbieter wurde eine Software-Bibliothek in Form einer DLL bereitgestellt, welche die entsprechende Applikation auf die Karte aufbringt.

- Verschlüsselung der Karten-Laufnummer

nach Vorgabe des Bundesministeriums der Verteidigung

- Zugriff auf vorhandene Ausweis-Datenbank IBM DB2 mit vorgegebener Datenbank-Struktur und separater Bildtabelle: Die Datenbank-Anbindung und -Struktur musste aus Kompatibilitätsgründen zu anderen Systemen beibehalten werden.

- Verwaltung des Kartenstatus und Schnittstelle zu Fremdsystemen: Bei der Ausgabe der Karte muss ein sofortiger Export der relevanten Karten-Daten an den Server des Zutrittskontroll-Systems erfolgen, um die Karte dort freizuschalten.

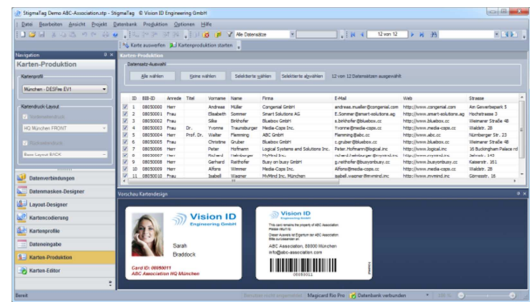
Zusammengefasst ergab sich ein vielschichtiges Anforderungsprofil an die Kartenverwaltungs- und Codierungs-Software, welches aber optimal durch die Kartenmanagement-Lösung StigmaTag in der Enterprise-Edition abgedeckt werden konnte. So waren auch an einigen Stellen Erweiterungen und Anpassungen notwendig, welche durch die offene Struktur jedoch problemlos durchgeführt werden konnten.

Toni Hülsbeck, der Leiter der Pass- und Ausweisstelle des Bundesministeriums der Verteidigung, fasst die Umsetzung mit folgenden Worten zusammen: „Wir haben mit der Vision ID einen kompetenten Partner gefunden, der unsere komplexen Anforderungen mit viel Engagement und Einsatz problemlos zu unserer vollsten Zufriedenheit umsetzen konnte.“

Aktueller Stand

Derzeit werden in der Pass- und Ausweisstelle des BMVg neue hybride Zutritts- und Zeiterfassungs-Ausweise für die Standorte Bonn und Berlin produziert und sukzessive gegen die alten Ausweise getauscht.

Sobald alle Ausweisleser komplett auf die neue, hochsichere Technologie



Ausweis-Verwaltungssystem StigmaTag

umgerüstet sind, wird der kostengünstigere, reine Neu-Technologie-Ausweis die bisherigen Hybrid-Ausweise ersetzen.

Damit wird dann schließlich die Migration der bisherigen Systeme auf die neue Technologie erfolgreich abgeschlossen werden können.

Über Vision ID

Engineering GmbH

Vision ID Engineering GmbH ist Software-Hersteller und Lösungsanbieter von Kartenmanagement- und Kartenpersonalisierungs-Systemen, sowie intelligenter Middleware für kontaktlose Smartcard-Systeme (RFID/NFC). Darüber hinaus bietet Vision ID umfangreiche Beratungsleistungen in den Bereichen kontaktlose Smartcard-Systeme und Embedded Systems.

* Die Namen der jeweiligen Alt- und Neu-Technologien werden auf Wunsch des BMVg aus Sicherheitsgründen in diesem Artikel nicht genannt.

Vision ID Engineering GmbH

Am Rottwerk 34
D-94060 Pocking

Tel.: +49 (85 31) 98 40 74
FAX: +49 (85 31) 98 40 68

E-Mail: info@vision-id.de
Web: www.vision-id.de