PPI AG

TRAVIC-Sign

Sichere Authentifizierung mit digitaler Unterschrift in Internet Portalen

TRAVIC-Sign ist einfach und komfortabel in Portale integrierbar. Deshalb ist die PPI-Lösung in Kreditinstituten so verbreitet.

Überblick

Die Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI) werden kurzfristig zu einem Boom der starken Sicherheitsverfahren mittels Chipkarte oder Token führen. Mit TRAVIC-Sign können Portale einfach erweitert werden. TRAVIC- Sign bietet:

- einfache Integrierbarkeit
- Übernahme des Look & Feel
- FinTS-, EBICS- und Secoder-Signaturen
- Nachladen von Zertifikaten
- umfangreiches Chipkarten-PIN-Management

TRAVIC-Sign richtet sich an Kreditinstitute und Rechenzentren, die Kunden ihrer Web-Anwendungen durch starke Sicherheitsverfahren mehr Sicherheit vor Missbrauch und Datenmanipulation bieten wollen.

TRAVIC-Sign erweitert den Browser so, dass auf einen Chipkartenleser oder ein Sicherheitstoken zugegriffen werden kann. So können Kunden die starken Sicherheitsverfahren der Deutschen Kreditwirtschaft (DK) nutzen.

PPI AG

Unterstützung aller wichtigen Verfahren

TRAVIC-Sign ist das Plugin für chipkartenbasierte Sicherheitsverfahren mit digitaler Signatur in Portalen und HTML-Applikationen.TRAVIC-Sign unterstützt den Secoder und die Signaturverfahren von HBCI/FinTS und EBICS.

Der Secoder-Chipkartenleser und der aktuelle TAN-Generator der DK bieten Datensicherheit auf höchstem Niveau: Die zu signierenden Daten werden im separaten Display angezeigt, das gegen Manipulation geschützt ist; die Signatur wird im Chipkartenleser erzeugt, der wiederum gegen Viren geschützt ist. Secoder und ZKA-TAN-Generator unterscheiden sich nur durch das jeweils verwendete Kryptografieverfahren.

Digitale Signaturen und TANs sichern Auftragsdaten – z. B. Zahlungen, Bestandsänderungen oder Produktverkäufe – mit Hilfe der fortgeschrittenen Signatur personengebunden ab. Signierte Daten können zweifelsfrei einer bestimmten Person zugeordnet werden. TRAVIC-Sign ermöglicht für eine Web-Anwendung die Zwei-Faktor-Autorisierung: Faktor 1 ist dabei das Wissen (PIN), Faktor 2 der Besitz (Chipkarte oder Token).

Web-Anwendungen von Kreditinstituten benötigen TRAVIC-Sign stets dann, wenn es darum geht, eine EBICS- oder FinTS-Signatur zu erzeugen. Auch für eine sichere Secoder-Signatur im Portal führt kein Weg an TRAVIC-Sign vorbei.

Mit TRAVIC-Sign sind auch beliebige Chip-Anwendungen, die per Secure-Messaging-Kommunikation genutzt werden können, in Web-Anwendungen integrierbar.

Manipulationsschutz

Hinsichtlich Aufrufsicherheit und Anzeige ist TRAVIC-Sign eine gehärtete Anwendung. Jeder Funktionsaufruf der Web-Anwendung an TRAVIC-Sign kann mit einer Signatur der Web-Anwendung gesichert werden. Die Signatur sichert ausgewählte Aufruf- und Anzeigedaten. TRAVIC-Sign prüft die verwendete Signatur und lässt nur Aufrufe der bekannten Quelle zu. Falls die Signatur falsch ist, weil ein falscher Schlüssel verwendet worden ist oder weil die Aufrufdaten manipuliert sind, zeigt TRAVIC-Sign den Fehler an und beendet die Session. Auf diese Weise wird eine gesicherte Verbindung der TRAVIC-Sign-Instanz und der zugeordneten Web-Anwendung geschaffen.

TRAVIC-Sign zeigt darüber hinaus die übergebenen Anzeigetexte im Display des Chipkartenlesers an. Dabei überprüft TRAVIC-Sign zum einen, ob das Browserfenster durch einen Trojaner auf dem lokalen Arbeitsplatz überlagert wird, und zum anderen, ob der Text vollständig angezeigt wird. Im Fehlerfall gibt TRAVIC-Sign einen Hinweis aus und arbeitet erst weiter, sobald das Problem behoben ist.

Diese elementaren Eigenschaften machen es Angreifern nach derzeitigem Stand der Technik unmöglich, dem Benutzer unbemerkt manipulierte Texte anzuzeigen.

Funktionsumfang

Aus Performance-Gründen ist TRAVIC-Sign nativ für die Betriebssysteme Windows, MacOS und Linux in der Programmiersprache C/C++ entwickelt. Jede Variante wird als eigenständiges Plugin ausgeliefert. Es wird kein Java Runtime Environment benötigt.

Als Standard für die Einbindung wird die Netscape-Plugin-Schnittstelle (NPAPI) genutzt, die von den relevanten Browsern unterstützt wird. Für den Internet Explorer verwendet TRAVIC-Sign die spezifische Microsoft-Schnittstelle. Für den Zugriff auf Chipkartenleser wird die PC/SC-Schnittstelle

Fotos: Heiko Klotz

PPI AG

Einfache Integration in Portale

TRAVIC-Sign ist einfach und komfortabel in Portale integrierbar. Deshalb ist die PPI-Lösung in Kreditinstituten so verbreitet.

genutzt. TRAVIC-Sign arbeitet auch mit treiberlosen Chipkartenlesern der DK-Norm.

Unter Windows unterstützt TRAVIC-Sign neben Chipkarten über den angeschlossenen Chipkartenleser auch Schlüsselpaare, die sich im Windows-Zertifikatspeicher befinden bzw. dort angemeldet sind (z. B. USB-Token). Auf diese Weise kann u. a. die Signatur über einen 3SKey von SWIFT gebildet werden.

Integrationsfähigkeit

TRAVIC-Sign nutzt in einer Browsersession den Bildschirm zur Anzeige und für die Steuerung durch den Endbenutzer.

Das individuelle Look & Feel der Web-Anwendung unterstützt TRAVIC-Sign durch folgende optionale Funktionen:

- Die Web-Anwendung kann den Aufruf sämtlicher Anzeigetexte bestimmen. Damit kann ein beliebiger Text in beliebiger Landessprache angezeigt werden.
- Die Web-Anwendung kann alle Schaltflächen über grafische Elemente im Aufruf übergeben. Damit können die Stilelemente der Web-Anwendung auch in TRAVIC-Sign genutzt werden.

Werden die Mechanismen zur individuellen Gestaltung nicht genutzt, werden die Standardschaltflächen des jeweiligen Betriebssystems und die Standardtexte von TRAVIC-Sign zur Benutzerführung verwendet.

Sicherheitsverfahren

Die von TRAVIC-Sign unterstützten Sicherheitsverfahren entsprechen den Standards der DK und sind in den HBCI-, FinTS- und EBICS-Spezifikationen beschrieben und definiert.

TRAVIC-Sign unterstützt folgende Sicherheitsverfahren:

- RDH-1 bis RDH-10 (FinTS, HBCI)
- RAH-7 bis RAH-10 (FinTS)
- A004, A005, A006 (EBICS)
- ZKA-TAN-Generator (HHD 1.4) per USB bzw. Bluetooth

Die genannten Sicherheitsverfahren sind z. T. an bestimmte Sicherheitsmedien gebunden. TRAVIC-Sign hält sich an die Spezifikationen für Sicherheitsmedien.

Die Sicherheitsfunktion für den ZKA-TAN-Generator dient dazu, die Transaktionsanzeige zu übermitteln, diese im Chipkartenleser anzuzeigen und die errechnete TAN an die Web-Anwendung zurückzugeben.

Zertifikatsmanagement

TRAVIC-Sign bietet den universellen Zugriff auf Chipkarten auch im Browserkontext.Daher unterstützt TRAVIC-Sign auch den Prozess, dass nicht nur der öffentliche Schlüssel der eingelegten Chipkarte sondern auch das zugehörige Zertifikat, das durch eine Certificate Authority (CA) erzeugt wurde, auf dieser abgelegt werden kann.

Dieser komplexe Vorgang wird mit Hilfe von Secure-Messaging-Nachrichten mehrschrittig mit einer beliebigen Web-Anwendung (Kartenherausgeber) durchgeführt. Im ersten Schritt übermittelt TRAVIC-Sign auf Anfrage (Funktionsaufruf) den im Aufruf angeforderten öffentlichen Schlüssel an die adressierte Web-Anwendung.

PPI AG

TRAVIC-Sign

Umfangreiche Servicefunktion für Chipkarten

Die Web-Anwendung kann weitere Attributdaten ermitteln oder abfragen, die für den CSR-Prozess (Request for Certificate) notwendig sind, und der CA den Auftrag zur Erstellung eines X509-Zertifikats erteilen. Die CA erstellt den autorisierten Schreibauftrag für das beglaubigte Zertifikat und übergibt diesen über die Web-Anwendung als Secure-Messaging-Auftrag an TRAVIC-Sign. TRAVIC-Sign leitet den Auftrag an die Chipkarte weiter. Die Chipkarte autorisiert den Schreibauftrag und speichert bei positiver Prüfung das so erhaltene Zertifikat auf der Chipkarte. Der Kunde muss den Zugriff auf die Chipkarte durch PIN-Eingabe autorisieren.

Weitere Möglichkeiten

Die Secure-Message-Kommunikation von TRAVIC-Sign erlaubt es, beliebige Anwendungen der eingelegten Chipkarte durch die zugehörigen Kommandos zu steuern. So sind auch native Geldkarten-Bezahlfunktionen oder das Management von Pre-Paid-Karten über TRAVIC-Sign möglich.

Servicefunktionen

Chipkarten benötigen eine Reihe von Servicefunktionen. Zum Beispiel wollen Benutzer jederzeit ihre persönliche PIN einstellen können. Diese Funktion wird von TRAVIC-Sign nativ unterstützt. Ein Benutzer kann beliebig häufig seine persönliche PIN wechseln.

Auch die erstmalige Nutzung der Chipkarte (wobei eine vorgegebene Transport-PIN durch eine individuelle PIN ersetzt werden muss) erkennt TRAVIC-Sign selbstständig und leitet den Benutzer mit Anweisungen durch diesen Prozess.

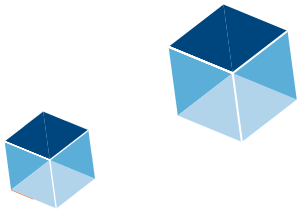
Chipkarten, die aufgrund von Fehleingaben gesperrt sind, können mit der PUK-Eingabe entsperrt werden. TRAVIC-Sign erkennt gesperrte Chipkarten automatisch und fragt in diesem Fall die PUK vom Benutzer ab. Diese Funktion kann optional von der Web-Anwendung abgeschaltet werden.

Das EF-Notepad und die Hash-Werte der Bankschlüssel auf der Chipkarte können über die Web-Anwendung bearbeitet werden. So können z. B. bei Fusionen von Kreditinstituten die gespeicherten Daten auf der Chipkarte angepasst werden.

Treiberlose Chipkartenleser nach DK-Norm erkennt TRAVIC-Sign automatisch.

Signaturen können nur dann sicher geleistet werden, wenn alle zu signierenden Daten tatsächlich am Ort der Signaturbildung vorliegen. Aus diesem Grund unterstützt TRAVIC-Sign für das Firmenkundengeschäft die Signaturbildung von Zahlungsauftragsdateien im Browser am Arbeitsplatz. Dabei liest TRAVIC-Sign die ZV-Auftragsdatei direkt von der Festplatte ein, prüft den syntaktischen Aufbau, erzeugt eine Inhaltskontrollanzeige, bildet den Datei-Hash-Wert und die Signatur und sendet alle lokal erzeugten Teilwerte zusammen an die Web-Anwendung. So ist es unmöglich, die Datei auf dem Weg vom Kundenarbeitsplatz zur Web-Anwendung zu manipulieren.

TRAVIC-Sign bietet die Möglichkeit, eine Chipkarte per EF-ID zur Signaturbildung anzufordern. Auch kann die Web-Anwendung bestimmte Klassen (I, II, III, Secoder) von Chipkartenlesern zur Signaturbildung anfordern. Nicht passende Klassen werden in diesem Fall abgelehnt.



Bei Fragen und für weitere Informationen

Michael Schunk
Tel.: +49 40 227433-1315
Mobil: +49170 8527526
michael.schunk@ppi.de

PPI AG
Moorfuhrtweg 13
22301 Hamburg
www.ppi.de