

sc/interface mit IGEL Endpoints

Technology Solution Paper



Eine Terminal-Server-Verbindung nur mit einem Passwort abzusichern ist äußerst riskant – es könnte ein Einfallstor für Hacker entstehen. Daher lohnt es sich, zusätzlich Smartcards einzusetzen. IGEL Endpoints im Zusammenspiel mit der Smartcard-Middleware sc/interface von cryptovision ist eine ideale Lösung für diesen Zweck.

Die Endpoint-Lösungen von IGEL Technology zählen zu den leistungsfähigsten am Markt. Sie sind Europas Nummer 1 bei Linux-basierten Thin Clients und seit 2006 deutscher Marktführer (laut IDC Thin Client Tracker 2016). Zusätzlich hat IGEL mit dem Produkt Universal Desktop Converter und dem UD Pocket Endpoint-Lösungen für Drittanbieter-Hardware im Programm. IGEL OS, IGELs eigenes, Linux-basiertes Betriebssystem, läuft auf jedem kompatiblen 64-Bit x86-Gerät.

IGEL Endpoints sind eine interessante Alternative zu PCs. Für sie spricht nicht nur der günstige Anschaffungspreis, sondern auch die Fernadministration, die zu geringen Wartungskosten führt. IGEL Endpoints sind für klassische Büroapplikationen genauso geeignet wie für Videos, multimediale Präsentationen und Echtzeitkommunikation.

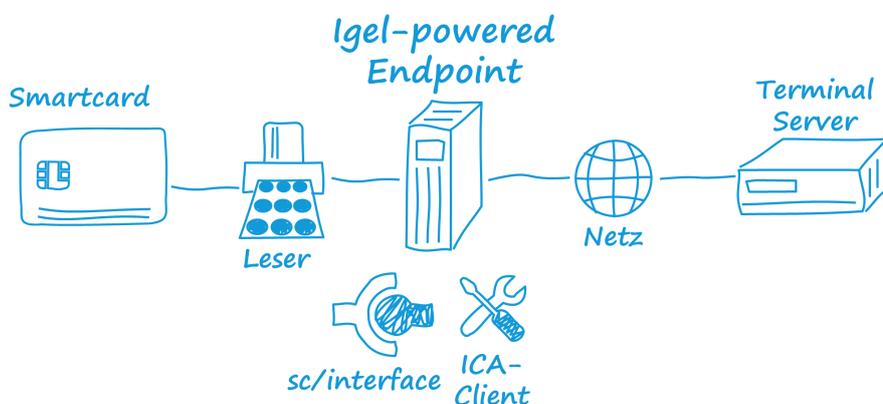
Endpoint-Sicherheit

Auch wenn es um die Sicherheit geht, schneiden IGEL-powered Endpoints gut

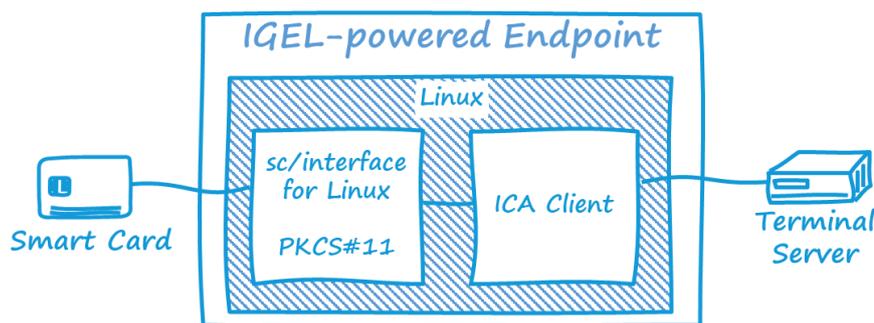
ab. Vertrauliche Daten speichern diese Geräte nicht auf einer Festplatte, sondern gut geschützt auf einem zentralen Server. IGELs Universal Management Suite (UMS) ermöglicht ein zentrales Endpoint-Management mit automatisierter Backend-Steuerung für die IT-Abteilung und eine störungsfreie Arbeitsumgebung für die Anwender.

Das IGEL IOS unterstützt zudem eine große Menge von Smartcards und Smartcard-Readern. Der Reader am Client wird hierbei über das Netz zum Server durchgeschleift. Dort kann sich der Anwender beispielsweise mit seiner Smartcard an einem Web-Portal einloggen, E-Mails entschlüsseln oder Daten signieren.

Der Vorteil hierbei ist offensichtlich: Smartcards sind deutlich sicherer als Passwörter. So wurden in den letzten Jahren Fälle bekannt, in denen Hacker Dutzende von Millionen von Passwörtern stehlen konnten. Bei einer Smartcard kann dies nicht passieren, da das zur Authentifizierung genutzte Geheimnis unauslesbar auf einem



IGEL-powered Endpoints unterstützen Smartcards. Diese können mit der Middleware sc/interface von cryptovision angesprochen werden.



Auf dem IGEL Endpoint läuft ein Linux-basiertes Betriebssystem. Das sc/interface-PKCS#11-Modul für Linux spricht die Smartcard an.

Krypto-Chip gespeichert ist. Nahezu alle Hacker-Einbrüche, die in den vergangenen Jahren die Schwächen von Passwörtern nutzten, hätten nicht funktioniert, wenn die betroffenen Organisationen Smartcards eingesetzt hätten.

sc/interface für IGEL Endpoints

Gemeinsam mit cryptovision hat IGEL zudem eine Sicherheitslücke geschlossen, die in Endpoint-Umgebungen weit verbreitet ist: Die Verbindung zwischen Endpoint und Terminal Server ist im Regelfall nur durch ein Passwort gesichert – selbst wenn Smartcards im Einsatz sind. Dadurch kann ein Hacker mit einem gestohlenen oder erratenen Passwort einen enormen Schaden anrichten.

Die Lösung: Die Smartcard kommt bereits beim Verbindungsaufbau zum Einsatz, nicht erst danach. IGEL Endpoints unterstützen dies, und zwar mit Hilfe der Smartcard-Middleware sc/interface von cryptovision. Diese ist auf verschiedenen Betriebssystemen

lauffähig und hat einen großen Funktionsumfang – inklusive der Unterstützung mehrerer Krypto-Schnittstellen.

IGEL-powered Endpoints nutzen die Linux-Version von sc/interface. Genauer gesagt, handelt es sich um dessen PKCS#11-Modul. PKCS#11 ist die auf Linux übliche Schnittstelle für den Zugriff auf eine Smartcard.

sc/interface ermöglicht die Smartcard-Authentifizierung eines Endpoints gegenüber dem Terminal-Server bereits beim Verbindungsaufbau. Da sc/interface alle gängigen Smartcard-Typen unterstützt (statt einer Smartcard kann auch ein anderer Formfaktor genutzt werden), ist der Betreiber der Endpoints bei der Kartenauswahl völlig flexibel.

sc/interface ist in IGEL's eigene Linux-basierte Firmware IGEL OS integriert. Der Nutzer bekommt beim Einschalten des Geräts einige zusätzliche Module angezeigt, die er nutzen kann – darunter sc/interface. Für dessen Nutzung

ist eine Lizenz von cryptovision notwendig.

Bei zahlreichen Kunden im Einsatz

Die Kombination aus IGEL-powered Endpoints und sc/interface ist bereits seit Jahren bei zahlreichen Kunden im Einsatz. Beispielsweise nutzen Einzelhandelsunternehmen diese Technik zur Absicherung der Kommunikation zwischen Filiale und Firmenzentrale. Im Finanzwesen sichern zahlreiche Unternehmen den Zugriff auf wichtige Daten mit IGEL Endpoints und sc/interface ab.

Ein weiterer Kunde von IGEL und cryptovision ist die Signal Iduna Versicherung. Das Unternehmen mit Sitz in Dortmund hat seine Mitarbeiter mit IGEL Endpoints statt mit PCs ausgestattet und nutzt Smartcards, die über sc/interface angesprochen werden. Auf diese Weise ist der Zugriff eines Endpoints auf den Terminal-Server gut geschützt. Außerdem steht die Smartcard auch für Anwendungen auf dem Terminal Server (z. B. E-Mail-Verschlüsselung und sicherer Web-Zugriff) zur Verfügung. Dabei ist Signal Iduna nicht auf ein bestimmtes Kartensystem festgelegt, da sc/interface über 80 Kartentypen unterstützt.

Die zahlreichen Kunden belegen, dass die Thin Clients von IGEL Technology zu den leistungsfähigsten und sichersten ihrer Art am Markt zählen – nicht zuletzt dank der Smartcard-Unterstützung durch sc/interface von cryptovision.

cv cryptovision GmbH · Munscheidstr. 14 · 45886 Gelsenkirchen · Deutschland

www.cryptovision.com · Tel.: +49 (209) 167 2450 · Fax: +49 (209) 167 2461

cv cryptovision Inc. · 100 Park Avenue · Suite 1600 · New York, NY 10017 · USA