Secure Logon HiCrypt™ 2.0

Produktsicherheit in der Automobilindustrie

Sicherer Anmeldeprozess mittels USB Smartcard-Token
und Schutz von vertraulichen Daten

Herausforderung

Automobilhersteller müssen konsequent Ihre Zulieferer auditieren, um sicher zu stellen, dass diese Betriebe die hohen automobilspezifischen Standards erfüllen. Die Rahmenanforderungen der ISO 27001 sind dadurch gekennzeichnet, dass bei der Entwicklung oder beim Testbetrieb von Prototypen oder Fahrzeugkomponenten ein besonderer Schutz des Designs und der Innovation erforderlich ist. Die Unternehmen haben somit sicher zu stellen, dass die der Geheimhaltung unterliegenden Prototypen sowie die sich in der Entwicklung befindlichen Konzepte sicher in unterschiedlichen Zertifizierungen des Prototypenschutzes in Ergänzung zur ISO Umgebung entwickelt uns getestet werden können. Die 27001 umfasst drei Säulen, wobei der Schwerpunkt klar auf die ersten beiden Punkte zu legen ist:

- Strategische und organisatorische Kriterien des Informationsschutzes (Verfügbarkeit, Vertraulichkeit, Integrität)
- Technische Kriterien der IT-Systeme (Verfügbarkeit, Vertraulichkeit, Integrität)
- Klassische Sicherheitsaspekte: Prototypenschutz

Was wir Ihnen bieten

digitronic® stellt ein Authentifizierungssystem bereit, welches aus einer clientbasierten Software Komponente Secure Logon (2-Faktor-Authentifizie- rung) und einem digitronic USB Smartcard-Token besteht und somit die Rahmenanforderungen der ISO 27001 erfüllt. Zusätzlich wird durch die Software Komponente HiCrypt™ 2.0 der Schutz von vertraulichen Daten gewährleistet.

Lösung

Secure Logon ermöglicht die sichere Anmeldung am Windows Betriebssystem mittels des eingesetzten digitronic Security Smartcard-Token. Die Windows-Anmeldedaten werden verschlüsselt auf dem Token hinterlegt. Erst nach Freischaltung des Tokens durch die Eingabe der korrekten PIN, werden die Anmeldedaten vom Token gelesen und der Nutzer wird erfolgreich am System angemeldet. Da der Benutzer weder Benutzernamen noch Passwort eingibt, diese ihm nicht einmal bekannt sein müssen, können die Zugangsdaten so komplex gewählt werden, dass sie möglichen Angriffen standhalten und damit die hohen Sicherheitsanforderungen in Unternehmen erfüllen. Verlässt der Benutzer kurzfristig seinen Arbeitsplatz und zieht dabei seinen Token ab, wird dieser standardmäßig gesperrt. Eine Vielzahl von individuellen Einstellungen lässt aber auch andere Reaktionen, wie Abmelden des Benutzers oder Herunterfahren der Arbeitsstation zu. Eine weitere Zusatzoption erlaubt die Deaktivierung der Standardanmeldung.

Secure Logon HiCrypt™ 2.0

Produktsicherheit in der Automobilindustrie

Sicherer Anmeldeprozess mittels USB Smartcard-Token
und Schutz von vertraulichen Daten

Mit HiCrypt™ 2.0 werden vertrauliche Daten auf Netzlaufwerken verschlüsselt, ermöglicht aber den Benutzern durch seine Architektur den gemeinsamen Zugriff auf verschlüsselte Dateien und Ordner. Die Ver- und Entschlüsselung findet am Arbeitsplatz-Computer statt. Dadurch ist sowohl die Datenübertragung zum Ablageort, als auch die Dateiablage selbst verschlüsselt. Unberechtigte Personen (z.B. IT-Administratoren) haben keine Möglichkeit die verschlüsselten Informationen einzusehen. Die IT-Administration stellt nur die IT-Infrastruktur bereit, übernimmt aber nicht die Schlüsselvergabe. HiCrypt™ 2.0 unterstützt mehrere Authentifizierungsmethoden, standardisierte Kennwortabfragen, 2-Faktor- Authentifizierung mittels Security-Token und 4-Augen-Prinzip.

Umsetzung

Mit dem PC wird die digitronic Secure Logon Software installiert. Für die korrekte Funktion des Token mit Secure Logon sind zusätzlich 3 Installationspakete für den Gerätetreiber zu installieren. Nach Abschluss der Installtion der Treiber kann der USB Smartcard-Token mit dem System verbunden werden.

Bevor eine Anmeldung mit einem Token als Authentifizierungsmittel durchgeführt werden kann, müssen die Anmeldeinformationen darauf gespeichert werden. Dies erfolgt mit dem Token-Manager. Sobald der Token korrekt initialisiert ist und die Anmeldeinformationen auf ihm gespeichert sind, kann der Token zur Anmeldung am Betriebssystem verwendet werden.

Mit Secure Logon können Aktionen festgelegt werden, die beim Entfernen des Tokens ausgeführt werden sollen. Vom einfachen Sperren des Computers, bis zum Herunterfahren.

Die Erkennung des Tokens erfolgt durch den PC.

	Secure Logon	HiCrypt™ 2.0
Betriebssysteme:	ab Windows 2000	ab Windows XP (x86 & x64)
Standards:	PKCS #11	CIFS/SMB
Verschlüsselungsalgorithmen:		AES, Blowfish, IDEA
Preis:	www.digitronic.net	www.hicrypt.com
Download:	www.digitronic.net	www.hicrypt.com

	USB Smartcard-Token
Betriebssysteme:	Windows, Linux, Mac OS X
Standards:	MS CAPI, PKSC#11
Smartcard Chip Zertifizierungen:	EAL 5+, EMV, ISO7816
Elektrische Zertifizierung:	FCC, CE, RWTÜV

Jakobsoftware
Robert-Bosch-Breite 10
D-37079 Göttingen

Telefon +49 551 305 604-33
Fax +49 551 305 604-55

vertrieb@jakobsoftware.de
https://www.jakobsoftware.de