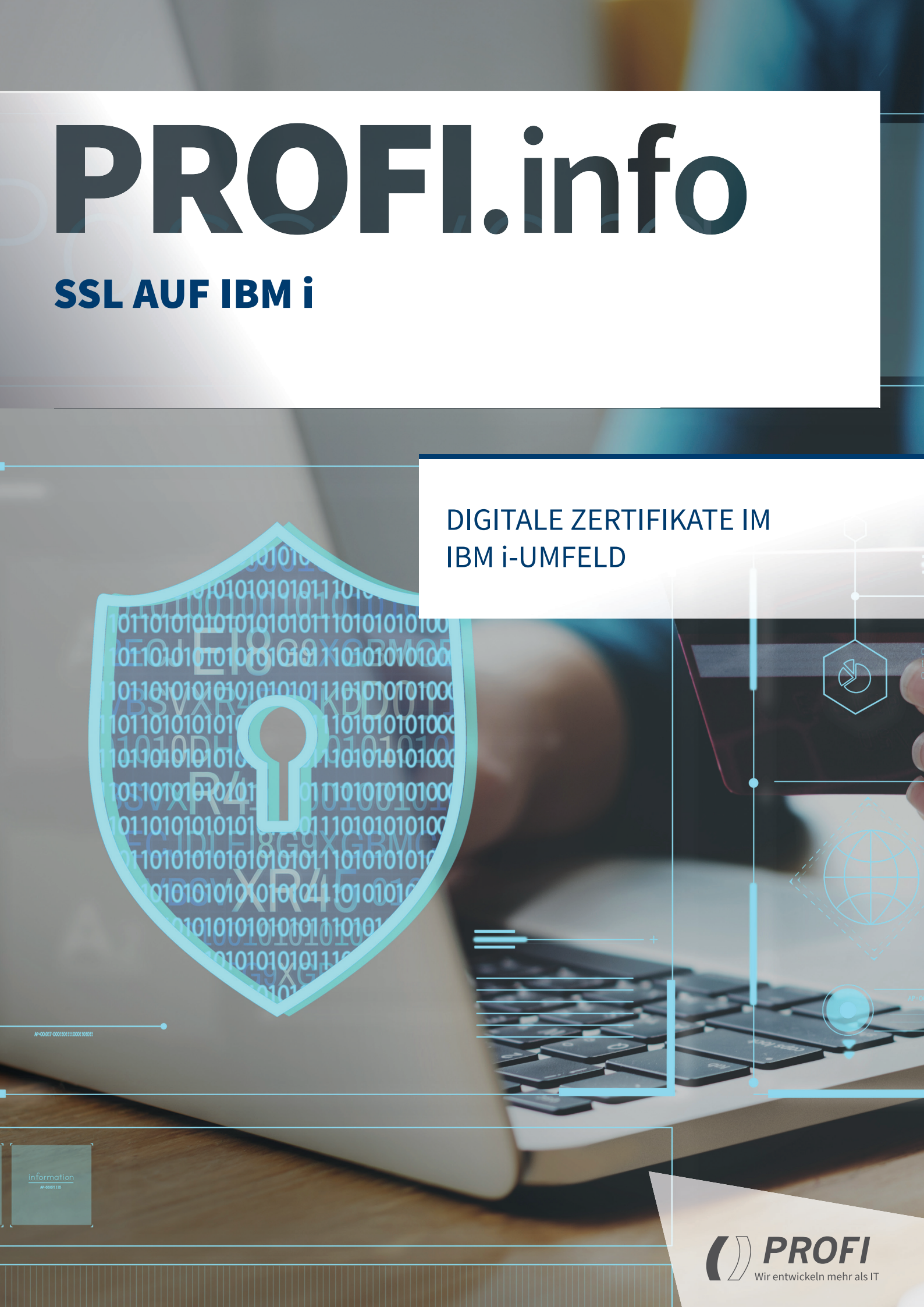
PROFI.info

SSL AUF IBM i

DIGITALE ZERTIFIKATE IM
IBM i-UMFELD



PROFI
Wir entwickeln mehr als IT

DIGITALE ZERTIFIKATE IM IBM i-UMFELD

Ein digitales Zertifikat ist ein elektronischer Berechtigungsnachweis, den Sie bei elektronischen Transaktionen zur Belegung Ihrer Identität verwenden können. Sie sind z. B. bei der Konfiguration und der Verwendung von Secure Sockets Layer (SSL) von zentraler Bedeutung. Durch den Einsatz von SSL können gesicherte Verbindungen zwischen Benutzern und Serveranwendungen innerhalb eines nicht anerkannten Netzwerks wie z. B. dem Internet herstellt werden.

Zahlreiche IBM® i-Plattformen und -Anwendungen wie FTP, Telnet oder HTTP-Server stellen SSL-Unterstützung zur Gewährleistung der Vertraulichkeit von Daten zur Verfügung. Digitale Zertifikate und die zugehörigen Sicherheitsschlüssel können auch zum Signieren von Objekten eingesetzt werden. Damit wird unterbunden, dass Nachrichten verfälscht werden oder mehrere Nachrichten über denselben Schlüssel verfügen können.

Digitale Signaturen verwenden das Prinzip der Kryptografie und nutzen Hash-Werte – und das über die Plattformgrenzen hinaus. Wichtig ist, dass die Standards für die digitalen Signaturen eingehalten werden und die notwendigen Schlüsselpaare für den Zugriff existieren und genutzt werden können.

Ein mögliches Beispiel für den Einsatz von Zertifikaten ist das Verschlüsseln der Datenverbindung. Der 5250-Datenstrom beispielsweise wird bei den klassischen 5250-Greenscreen-Oberflächen genutzt. Die Kommunikation mit dem Host (dem System i) ist dabei unverschlüsselt. Durch den Einsatz von Zertifikaten kann die Datenverbindung durch SSL verschlüsselt werden und dadurch für mehr Sicherheit in der Datenübertragung sorgen.

Das Lizenzprogramm SC1 (Basis und Option1) muss installiert sein. Die Konfiguration und die Administration der digitalen Zertifikate erfolgen mittels der HTTP-Administrationsoberfläche.

Dort lassen sich auch die unterschiedlichen Bereiche für die digitalen Zertifikate verwalten. Diese sind:

- Zertifizierungsinstanz (CA),
- Zertifikatsspeicher,
- Chiffrierung und
- Schlüsselpaare.

Zertifizierungsinstanz
Es ist gängige Praxis, dass Zertifikate von öffentlichen und privaten Zertifizierungsinstanzen (vertrauenswürdigen!) genutzt werden.

Zertifikatsspeicher
Beim Zertifikatsspeicher handelt es sich um eine spezielle Datenbank für das Speichern und Bereitstellen der Schlüssel. Er wird im Speziellen vom Digital Certificate Manager der System i genutzt und erlaubt es, unterschiedliche Bereiche einzurichten und eine Verwaltungshilfe für die genutzten Zertifikate einzusetzen. In diesem Bereich werden z. B. folgende Zertifikate unterschieden:

- lokale Zertifikate,
- *SYSTEM-Zertifikate,
- *OBJECTSIGNING-Zertifikate,
- *SIGNATUREVERIFICATION-Zertifikate und
- Speicher für andere Systemzertifikate.

Die Zertifizierungskomponenten, die mit dem DCM verwaltet werden, müssen im Regelfall im IFS abgelegt sein.

Chiffrierung
Beim Einsatz der Schlüsselpaare sind Chiffrierungen gegen unberechtigte Zugriffe wichtig. Im Zusammenspiel mit den Schlüsseln kommen auf dem System i folgende Chiffrierverfahren zum Einsatz:

- symmetrische Chiffrierung und
- asymmetrische Chiffrierung.

Die symmetrische Chiffrierung wird für die gemeinsamen Schlüssel verwendet. Zwei Teilnehmer nutzen denselben (geheimen) Schlüssel.

Die asymmetrische Chiffrierung wird mit öffentlichen Schlüsseln genutzt. Dabei wird für das Verschlüsseln und Entschlüsseln jeweils ein anderer Schlüssel eingesetzt. Die Schlüsselpaare bestehen jeweils aus einem öffentlichen und einem privaten Schlüssel, die sich auch mit der System i erzeugen und verwenden lassen. Der öffentliche Schlüssel wird in der Regel mittels eines digitalen Zertifikats weitergeleitet, während das Gegenstück – der private Schlüssel – sicher vom Empfänger aufbewahrt und eingesetzt wird.

PROFI bietet Ihnen an

- Sie in die Theorie des Zertifikats-Managements und der SSL-Verbindungen einzuführen.
- Ersatz für proprietäre unverschlüsselte Protokolle zu finden.
- Ihre Systeme auf SSL-Verbindungen umzustellen.
- Sie zu unterstützen Zertifikate zu etablieren.
- Alle Verbindungen können und sollten verschlüsselt werden. PROFI bietet dies für IBM-, Dell- und NetApp-Produktlinien an. Das beinhaltet auch die IBM i mit Ihren interaktiven und Datenbank-Anbindungen. Sollte eine proprietäre Anbindung tatsächlich kein SSL nativ unterstützen, so weiß PROFI auch das verschlüsselt zu übertragen.

Haben wir Ihr Interesse geweckt?
Dann sprechen Sie mich gerne an:

Ingo Rothermel
System Engineer
i.rothermel@profi-ag.de

DIE PROFI ENGINEERING SYSTEMS AG

Die PROFI AG ist ein mittelständischer IT-Dienstleister mit Unternehmenssitz in Darmstadt. Das Unternehmen begleitet seine Kunden in allen Belangen der digitalen Transformation mit einem spezialisierten Portfolio von IT-Lösungen, Dienstleistungs- und Beratungsangeboten rund um die Themen Server- und Speichersysteme, Hybrid Cloud, Business Continuity, Cyber Resilience, IT-Automation, Virtualisierung, Digital Workplace, Software-Entwicklung und Managed Services.

Der Anspruch ist höchste Kompetenz, Zuverlässigkeit und Qualität, mit messbarem Erfolg und direktem Beitrag zur Wertschöpfung und Wettbewerbsfähigkeit der Kunden.

PROFI beschäftigt über 300 Mitarbeitende an bundesweit 12 Standorten. Seit vielen Jahren gehört das Unternehmen zu Deutschlands erfolgreichsten IT-Lösungsanbietern und pflegt langjährige Partnerschaften mit allen führenden IT-Herstellern.

Unsere IT-Lösungen für Ihren Erfolg

- **Business Continuity**
- **Cyber Resilience**
- **DevOps**
- **Digital Workplace**
- **Managed Services**
- **Netzwerk / IT Security**
- **Platforms**
- **SDDC / IT-Automation**
- **Software-Entwicklung**

PROFI Engineering Systems AG
Otto-Röhm-Straße 18
64293 Darmstadt
Telefon: +49 6151 8290-0
Telefax: +49 6151 8290-7610
E-Mail: profi@profi-ag.de
www.profi-ag.de

05/2024

UNSERE PARTNER

Gemeinsam mit unseren starken Partnern setzen wir Ihre optimalen Lösungen um.

IBM Platinum Partner
BROADCOM PREMIER PARTNER VMware Reseller VMWARE DIVISION
DELL Technologies TITANIUM PARTNER
NetApp PREFERRED PARTNER
FUJITSU SELECT Expert
Red Hat Premier Business Partner
Data Center Partner Platinum Lenovo
Microsoft Partner
CISCO Partner Premier Certified
SAP Partner
NUTANIX PARTNER Champion Reseller
plusserver EXPERT PARTNER
veeAM Value-Added Reseller Gold

Bildnachweise:
shutterstock.com
© Rawpixel: Titelbild
© SFIO CRACHO: S. 2

PROFI
Wir entwickeln mehr als IT