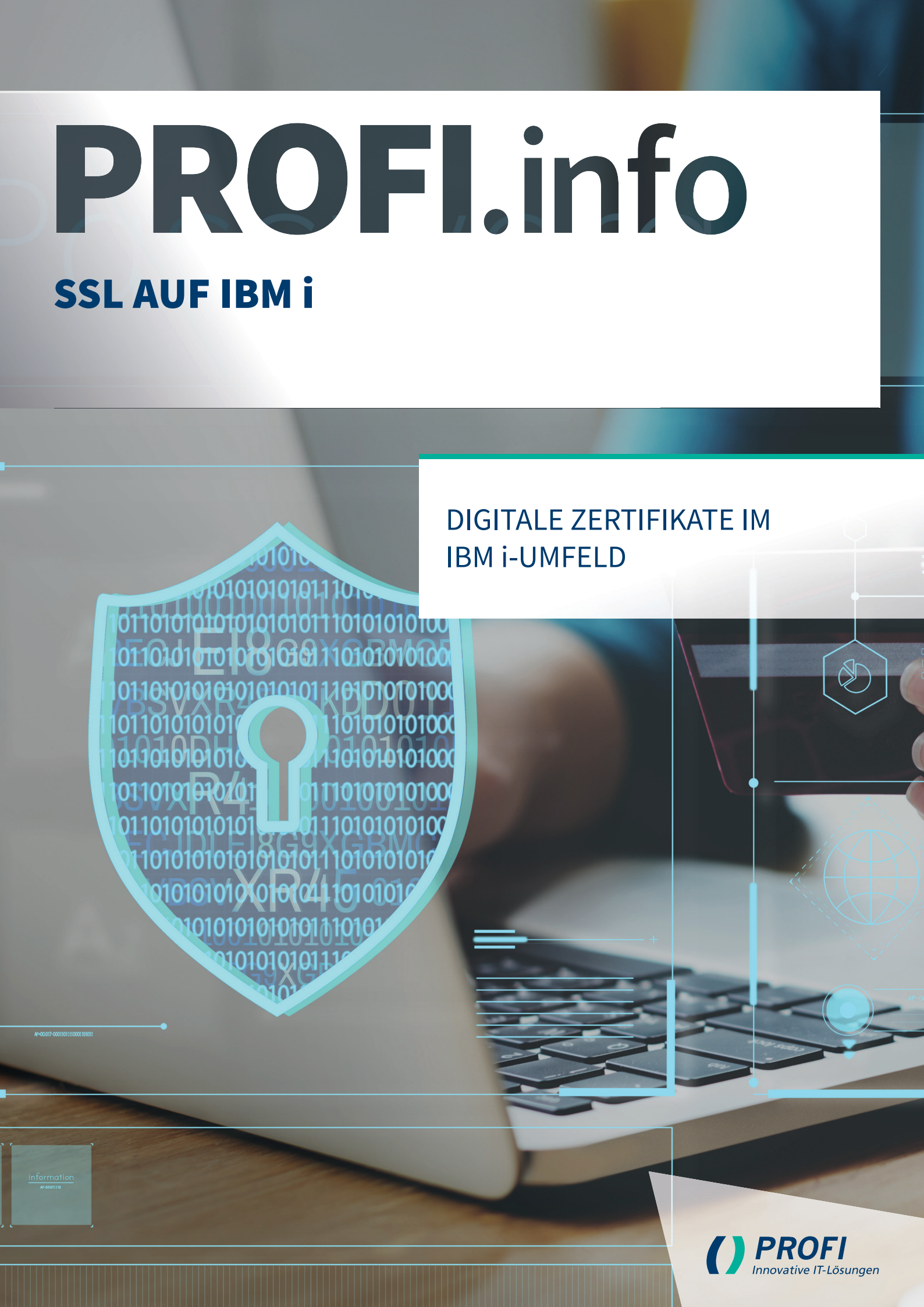
PROFI.info

SSL AUF IBM i

DIGITALE ZERTIFIKATE IM
IBM i-UMFELD



PROFI
Innovative IT-Lösungen

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

Wir, die PROFI Engineering Systems AG sind ein mittelständisches Familienunternehmen. Als finanzkräftiges IT-Lösungshaus mit Hauptsitz in der Wissenschaftsstadt Darmstadt sind wir seit über 35 Jahren der IT-Dienstleister für unsere Kunden, mit individuellen hochwertigen Lösungen zur Optimierung von IT-Prozessen und Systemlandschaften.

Wir begleiten Unternehmen bei der digitalen Transformation – von der IT-Strategie über die Implementierung bis einschließlich des Betriebes der Systeme und Plattformen. Unsere erfahrenen Berater und Architekten beschäftigen sich seit vielen Jahren intensiv mit der Digitalisierung aller Geschäftsabläufe und Unternehmensbereiche. Gestalten Sie mit den PROFI-Fokusthemen schon heute Ihre digitale Zukunft. Profitieren Sie von unserem Know-how vor allem im Kontext von Managed Services, Digital Workplace, SAP HANA, Business Continuity, Agile Software-Entwicklung, Netzwerk & Security, Cloud Solutions, SDDC & Agile Plattformen, Speicherlösungen und Server-Lösungen.

Wir übernehmen für Sie Projektmanagement und Implementierung, einschließlich dem Betrieb Ihrer Systeme und Plattformen. Unser Anspruch ist höchste Kompetenz, Zuverlässigkeit und Qualität, mit messbarem Erfolg und direktem Beitrag zur Wertschöpfung und Wettbewerbsfähigkeit unserer Kunden.

Seit vielen Jahren gehören wir zu Deutschlands erfolgreichsten IT-Lösungsanbietern und pflegen langjährige Partnerschaften mit führenden IT-Herstellern. Die PROFI Engineering Systems AG beschäftigt über 300 Mitarbeiterinnen und Mitarbeiter an 12 Standorten.

Unsere IT-Lösungen für Ihren Erfolg

- **Agile Software-Entwicklung**
- **Business Continuity**
- **Cloud Solutions**
- **Digital Workplace**
- **Managed Services**
- **SAP HANA**
- **SDDC & Agile Plattformen**
- **Security & Netzwerk**
- **Server-Lösungen**
- **Speicherlösungen**

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

11/2021

UNSERE PARTNER

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

Bildnachweise

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

PROFI
Innovative IT-Lösungen