AuthCryptor NE - Funktionsbeschreibung

Was ist AuthCryptor NE?

- AuthCryptor NE ist eine **Ende-zu-Ende Verschlüsselungssoftware mit integrierter Authentifizierung**, die Verbindungen in Netzwerken bestehend aus **beliebig vielen Teilnehmern** absichert. Ein vorheriger Informationsaustausch zwischen den Netzwerkteilnehmern wird nicht benötigt.

- AuthCryptor NE ist ein **hybrides Verfahren**, das auf bekannten und bewährten Prinzipien **sowohl asymmetrischer als auch symmetrischer Kryptographie** basiert und den Richtlinien des BSI und NIST folgt. Die Verschlüsselung erfolgt mittels **AES-GCM mit 256-Bit Schlüsseln**, die Schlüsselberechnung wird mit Hilfe von elliptischen Kurven (z.B. secp384r1) durchgeführt.

- Das Verfahren ist vom **Europäischen Patentamt patentiert** und ist als zu testendes Produkt für die geplante „Beschleunigte Sicherheitszertifizierung (BSZ)“ des BSI vorgemerkt.

Welche Funktion hat AuthCryptor NE?

- AuthCryptor NE gewährleistet **selbst in unsicheren Netzen** (z.B. Internet, offenes WLAN) die **Integrität, Herkunft und Vertraulichkeit** der versandten Daten.

- AuthCryptor NE **verknüpft Ende-zu-Ende-Verschlüsselung und Authentifizierung ohne vorherigem Informationsaustausch** zwischen den Netzwerkteilnehmern zu einem Verfahren und schützt somit Verbindungen zwischen beliebigen Endgeräten.

Welche Eigenschaften hat AuthCryptor NE?

- AuthCryptor NE kann **unabhängig von Dritten** betrieben werden und ist nicht auf die öffentliche Zertifikatsinfrastruktur angewiesen. Jährlicher **Kauf und Austausch von Zertifikaten entfällt** dadurch.

- AuthCryptor NE ist zur **Integration in Endgeräte und Systemkomponenten** prädestiniert und kann auch **in bestehende Netzwerke und Prozesse nachgerüstet** werden.

SDT-Solutions GmbH
Erb 10
D-77876 Kappelrodeck

Tel.: +49 (0) 7842 98856
EMail: info@sdt-solutions.de
Internet: www.sdt-solutions.de

- AuthCryptor NE **schützt die Kommunikation von dedizierten Applikationen**, z.B. spezifische Webservices, ohne dass, im Gegensatz zu einer VPN-Lösung, der Nutzer vollwertiger Netzwerkteilnehmer sein muss.

- Der **Verwaltungsaufwand ist minimiert** und kann von einer zentralen Stelle aus erfolgen.

- Die zentrale Stelle, auch „Vermittler“ genannt, **wird nicht zum Kommunikationsaufbau benötigt**. Selbst bei Ausfall des Vermittlers können registrierte und aktive Netzwerkteilnehmer **weiterhin miteinander kommunizieren** und auch neue Verbindungen aufbauen (**kein Single-Point-Of-Failure**).

- Der „Vermittler“ kann **weder die Kommunikation** zwischen Endgeräten direkt **belauschen, noch enthält er sicherheitsrelevante Daten** von Endgeräten.

- Am „Vermittler“ **registrierte Netzwerkteilnehmer konfigurieren sich beim Start selbst**, das heißt alle notwendigen Verbindungsinformationen, Schlüsselnachweise etc. werden vom „Vermittler“ abgerufen.

- **Registrierung neuer Netzwerkteilnehmer** ist mit **konstantem Aufwand** durchführbar und wächst nicht mit der Größe des Netzwerks.

- Netzwerkteilnehmer können gleichzeitig sowohl Sender („Client“) als auch Empfänger („Server“) sein.

- **Ende-zu-Ende-Verschlüsselung** ist **bis in die Endgeräte** hinein möglich. **Insider-Risiken werden so eliminiert**.

- Durch **beidseitige Authentifizierung** bei Verbindungsaufbau und Kommunikation werden **Man-In-the-Middle-Angriffe erkannt und abgewehrt**.

- Die Eigenschaft der „**perfect forward secrecy**“ (PFS) wird erfüllt.

- Mehrere **Netzwerkdienste können in eine Verbindung gebündelt** werden. AuthCryptor NE übernimmt das interne Routing. Die nach außen **offenen Ports können so auf ein Minimum reduziert** werden.

- Die Funktionsbibliothek ist **plattformunabhängig** (x86-64, arm64 etc.).

- Verbindungen sind auch auf **Hostnamebasis und zwischen IPv4- und IPv6-Hosts** möglich.

SDT-Solutions GmbH
Erb 10
D-77876 Kappelrodeck

Tel.: +49 (0) 7842 98856
EMail: info@sdt-solutions.de
Internet: www.sdt-solutions.de