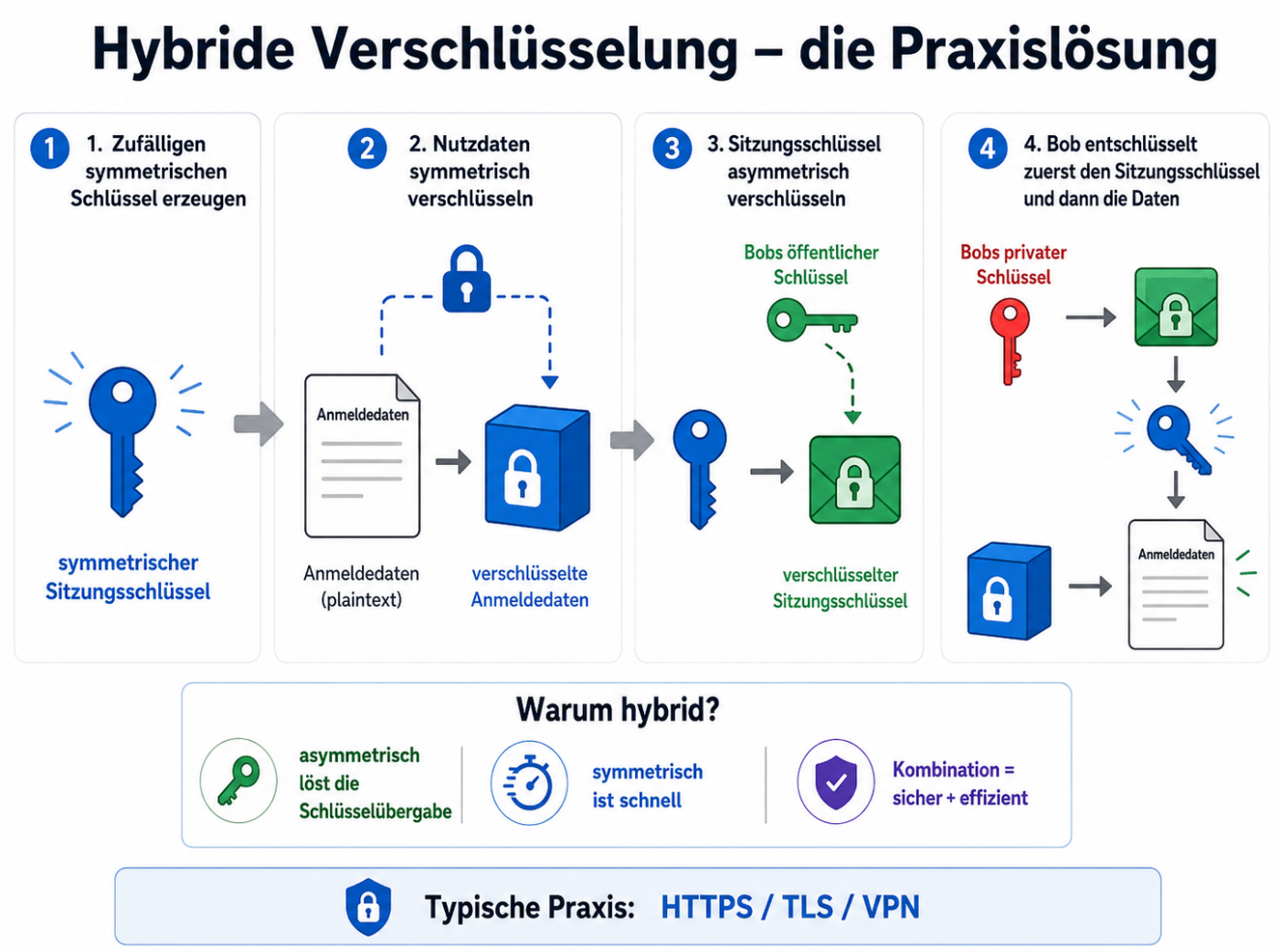
13.4 Hybride Verschlüsselung



Kurzüberblick

Die **hybride Verschlüsselung** kombiniert zwei Verfahren:

- **asymmetrische Verschlüsselung** für den sicheren Schlüsselaustausch
- **symmetrische Verschlüsselung** für die schnelle Verschlüsselung der eigentlichen Daten

> **IHK-Merksatz:**
> Hybrid = asymmetrisch für den sicheren Schlüsselaustausch, symmetrisch für die schnelle Datenverschlüsselung.

Quelle 11.3.5 – Lösung: Übergabe des symmetrischen Schlüssels

Das Problem aus der symmetrischen Verschlüsselung war:

> Alice und Bob brauchen denselben geheimen Schlüssel.
> Aber wie bekommt Bob diesen Schlüssel sicher?

Die Lösung:

Man überträgt nicht direkt ein Geheimnis mit asymmetrischer Verschlüsselung, sondern nutzt asymmetrische Verschlüsselung, um den **symmetrischen Schlüssel sicher zu übergeben**.

Danach wird mit diesem symmetrischen Schlüssel die eigentliche Nachricht schnell verschlüsselt.

Warum braucht man ein hybrides Verfahren?

Symmetrische Verschlüsselung ist schnell, hat aber ein Problem bei der Schlüsselübergabe.

Asymmetrische Verschlüsselung löst die Schlüsselübergabe, ist aber langsamer.

Hybrid kombiniert beide Vorteile.

Verfahren	Vorteil	Nachteil
symmetrisch	sehr schnell	Schlüssel muss sicher übergeben werden
asymmetrisch	Schlüsselübergabe ist einfacher	langsamer
hybrid	sicherer Schlüsselaustausch + schnelle Datenverschlüsselung	etwas komplexerer Ablauf

> **Kurz gesagt:**
> Hybrid nutzt asymmetrisch nur für den Schlüssel.
> Die Nutzdaten werden danach symmetrisch verschlüsselt.

Grundidee

Alice möchte Bob Daten sicher senden.

Dafür passiert Folgendes:

1. Alice erzeugt einen zufälligen symmetrischen Sitzungsschlüssel.
2. Alice verschlüsselt die eigentlichen Daten mit diesem Sitzungsschlüssel.
3. Alice verschlüsselt den Sitzungsschlüssel mit Bobs öffentlichem Schlüssel.

4. Alice sendet die verschlüsselten Daten und den verschlüsselten Sitzungsschlüssel an Bob.
5. Bob entschlüsselt den Sitzungsschlüssel mit seinem privaten Schlüssel.
6. Bob entschlüsselt die Daten mit dem Sitzungsschlüssel.

Begriffe

Begriff	Bedeutung
Sitzungsschlüssel	einmaliger oder zeitlich begrenzter symmetrischer Schlüssel
Nutzdaten	die eigentlichen Daten, zum Beispiel Datei, Text, Login-Daten
öffentlicher Schlüssel	wird genutzt, um den Sitzungsschlüssel für Bob zu verschlüsseln
privater Schlüssel	wird von Bob genutzt, um den Sitzungsschlüssel zu entschlüsseln
hybride Verschlüsselung	Kombination aus asymmetrischem Schlüsselaustausch und symmetrischer Datenverschlüsselung

---

Ablauf Schritt für Schritt

Schritt	Was passiert?	Genutztes Verfahren
1	Alice erzeugt einen zufälligen Sitzungsschlüssel.	symmetrisch
2	Alice verschlüsselt die Nutzdaten mit dem Sitzungsschlüssel.	symmetrisch
3	Alice verschlüsselt den Sitzungsschlüssel mit Bobs öffentlichem Schlüssel.	asymmetrisch
4	Alice sendet verschlüsselte Nutzdaten und verschlüsselten Sitzungsschlüssel.	Übertragung
5	Bob entschlüsselt den Sitzungsschlüssel mit seinem privaten Schlüssel.	asymmetrisch
6	Bob entschlüsselt die Nutzdaten mit dem Sitzungsschlüssel.	symmetrisch

---

Beispiel

Alice möchte Bob WLAN-Anmeldedaten senden.

Die eigentlichen Daten sind:

SSID: Firma-WLAN

Passwort: geheim123

Revision #2
Created 2 June 2026 23:33:22 by Admin
Updated 3 June 2026 06:18:12 by Admin