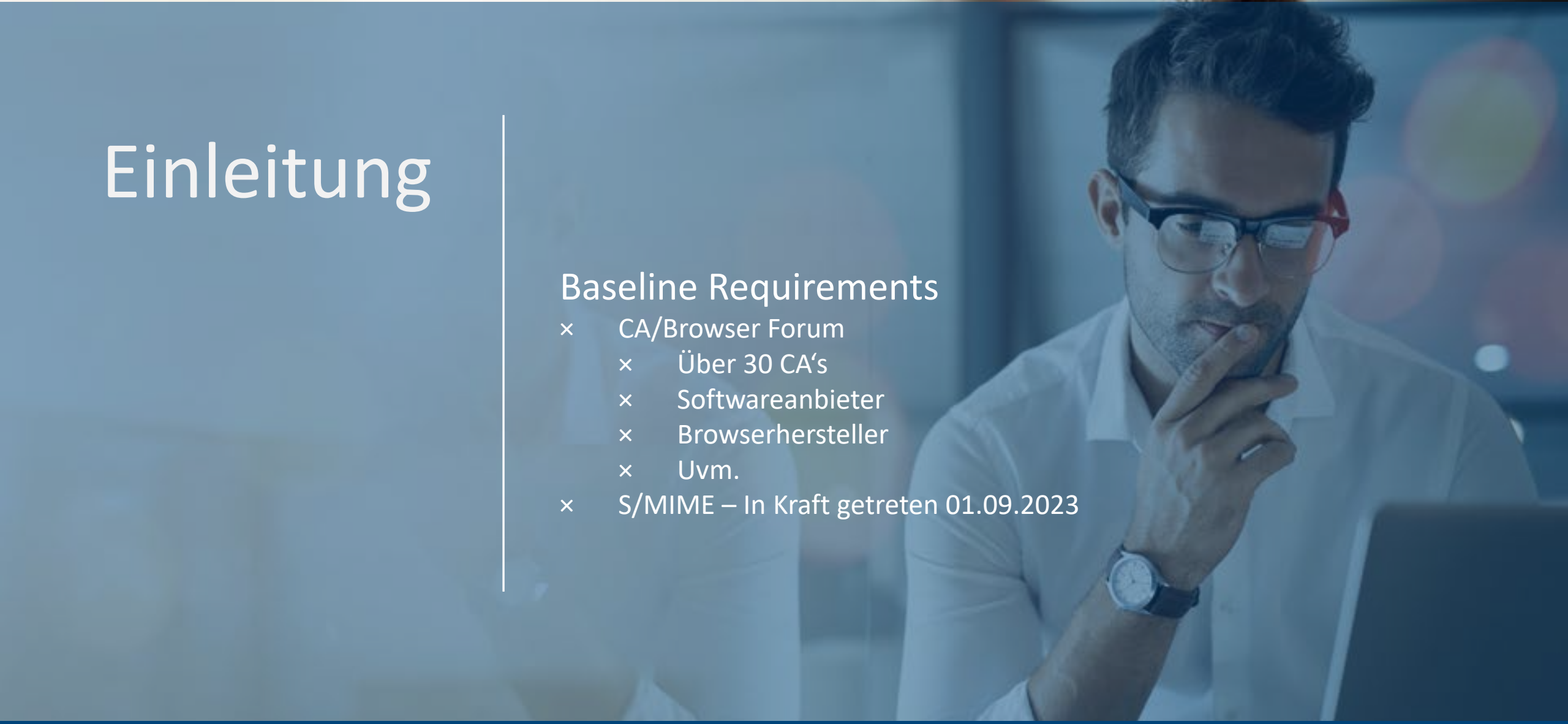
S/MIME-Zertifikate

Laufzeitkürzung auf 2 Jahre

PSW GROUP

Klassifizierung: extern

Einleitung



Baseline Requirements

- CA/Browser Forum
  - Über 30 CA‘s
  - Softwareanbieter
  - Browserhersteller
  - Uvm.
- S/MIME – In Kraft getreten 01.09.2023

Klassifizierung: extern

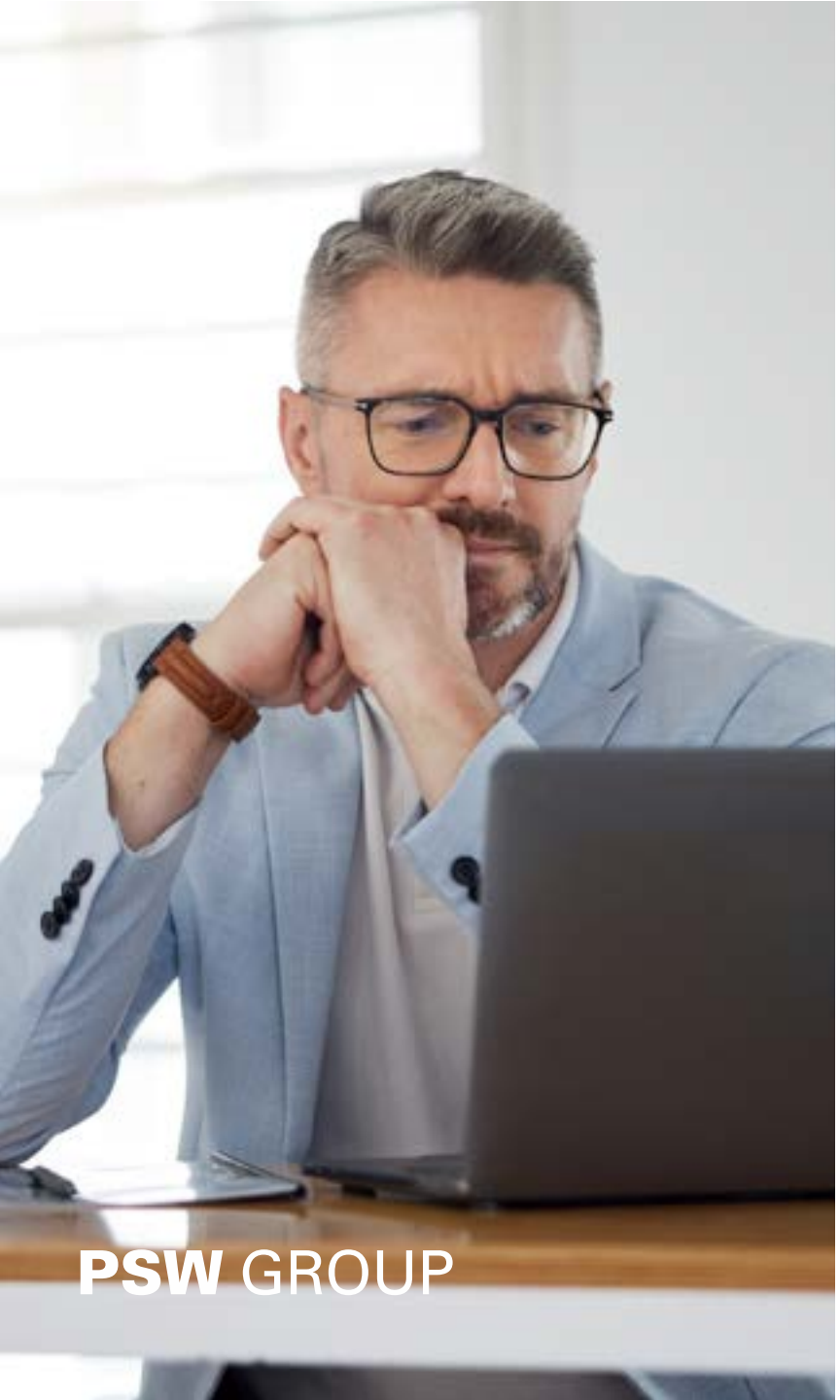
Themen:

- Ziel der Laufzeitverkürzung
- Was ändert sich?
  - Erklärung der Profiltypen
  - Erklärung der Produkttypen
- Änderungen bei D-Trust & DigiCert
- Empfehlungen
- Die wichtigsten Daten

PSW GROUP

Ziel der Laufzeitverkürzung

- Mehr Sicherheit
  - Weniger kompromittierte Schlüssel
  - Neue Algorithmen schneller ausgerollt
- Einheitlicher Standard
  - Gleiche Rahmenbedingungen
- Häufigere Identifizierung
  - Weniger falsche Angaben in gültigen Zertifikaten
- Ende der 3-Jahres Laufzeit / 15.07.2025



Was ändert sich? - Profiltypen

~~Legacy~~

- ✓ Übergangsprofil / fällt nun am 15.07.25 weg
- ✓ 3-Jahre Laufzeit möglich

Multipurpose

- ✓ Zertifikate für mehrere Zwecke
- ✓ Client-Authentifizierung & Office-Signierung

Strict

- ✓ S/MIME nur für E-Mail Signierung/Verschlüsselung
- ✓ Wird auf lange Sicht der einzige Profiltyp werden

Was ändert sich - Produkttypen

Mailbox

- ✓ E-Mail-Adresse

Individual

- ✓ E-Mail-Adresse
- ✓ Vor- und Nachname

Sponsor

- ✓ E-Mail-Adresse
- ✓ Vor- und Nachname
- ✓ Organisationsdaten

Organization

- ✓ E-Mail-Adresse
- ✓ Organisationsdaten

Neue Produkte

- 01.07.2025
- Wegfall 3-Jahres Laufzeit
- Wegfall der Produkte DigiCert Basic & DigiCert Enterprise
- Neue Produkte:
  - DigiCert S/MIME Basic
  - DigiCert S/MIME Business
  - DigiCert S/MIME Sponsor

PSW GROUP

Empfehlungen

Ablaufdatum der aktuellen Zertifikate prüfen

- ✓ Welche Zertifikate laufen ab? Wer nutzt Sie?
- ✓ Zertifikate die in kürze ablaufen ggf. vorzeitig verlängern
- ✓ 3-Jahres Zertifikate behalten auch nach dem 15.07 weiterhin die Gültigkeit

Aktuelle Zertifikate sichern

- ✓ Durch eine Sicherung (.pfx-Datei + Passwort) kann ein Zertifikat auch nach einem Rechnerwechsel etc. wieder installiert werden.
- ✓ Durch einen Austausch würde man ggf. Laufzeit verlieren

Über Automatisierung informieren

- ✓ Automatische Erstellung/Verlängerung mittels MPKI
- ✓ MPKI‘s können mit E-Mail-Gateways verknüpft werden
- ✓ SwissSign MPKI-Webinar am 10.07.2025

Neue Produkte & Zertifikatskette

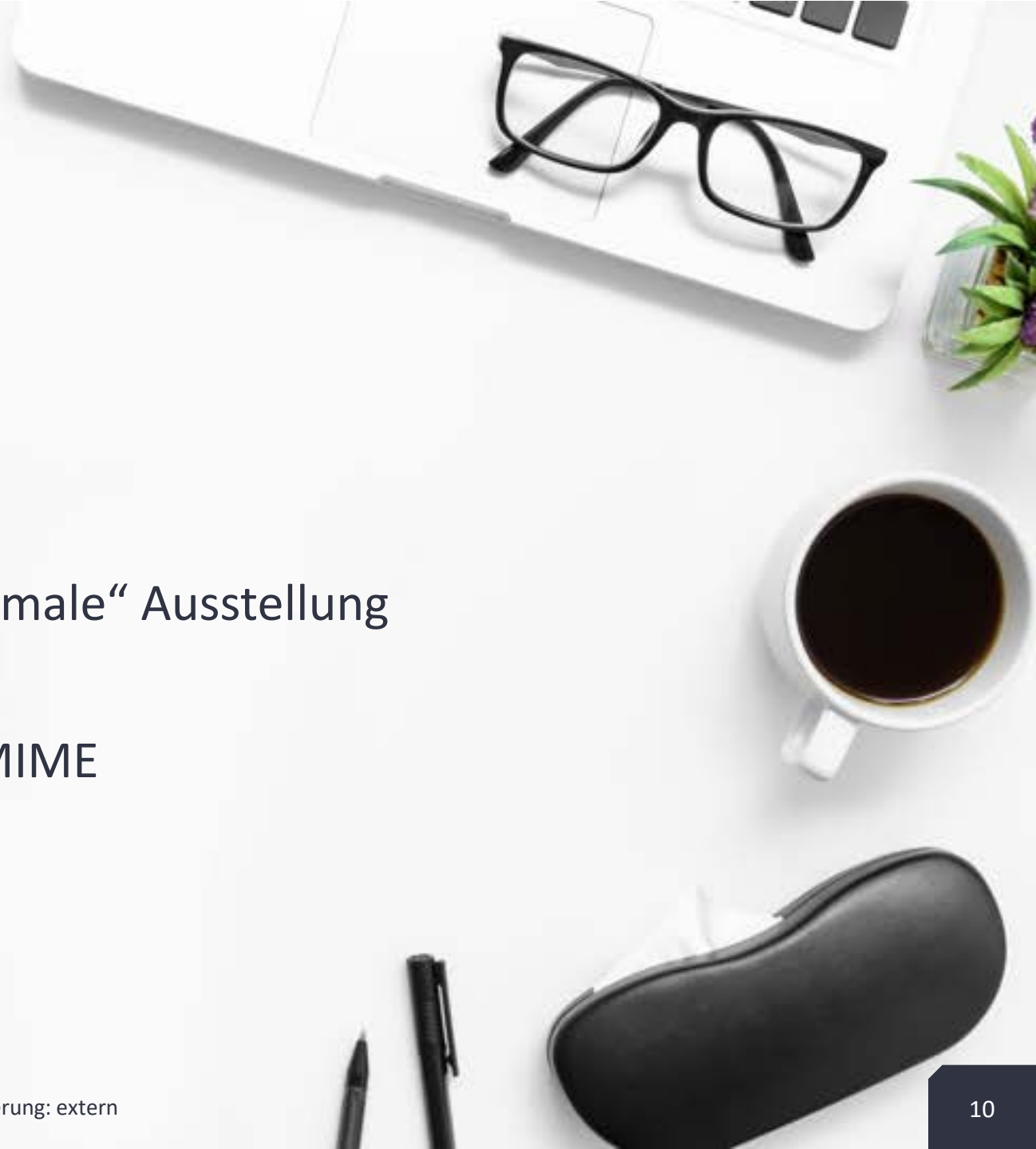
Neue Zwischen- und Root-Zertifikate

- Q3 2025
- RSA / ECC
- Größere Schlüssellängen (3072 / 4096 Bit)
- Nicht im Adobe Truststore enthalten!
- Laufzeit nur 1 Jahr

Auswirkungen

Das ändert sich:

- Kein PDF-Signing mehr möglich
- Bis zur Einführung der neuen Kette „normale“ Ausstellung
- Alte Zertifikate behalten Gültigkeit
- PDF-Signing (eSigning) getrennt von S/MIME

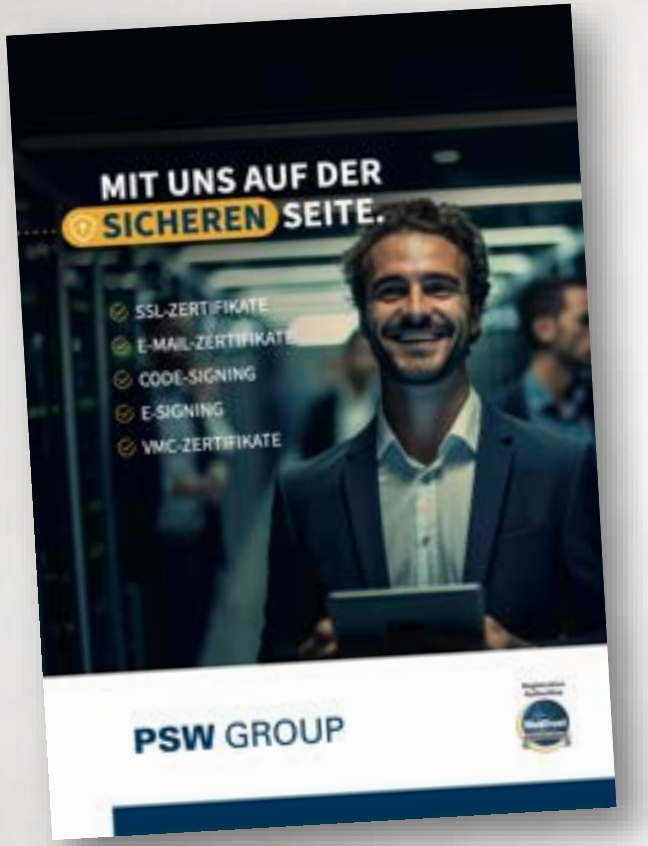


PSW GROUP

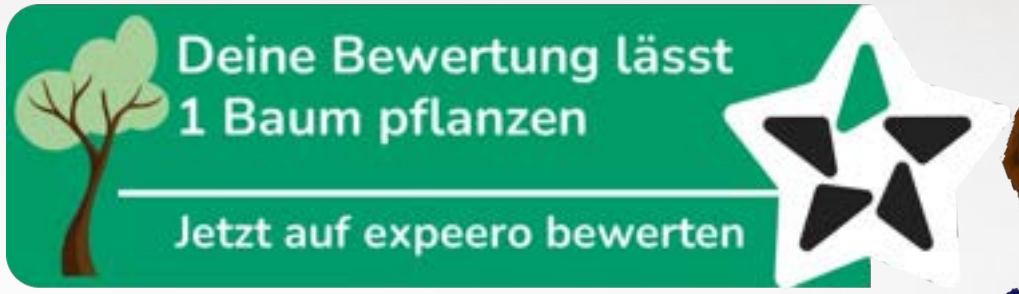
Die wichtigsten Daten:

- S/MIME
  - 27.01.25 – Keine 3 Jahre mehr bei GlobalSign
  - 30.06.25 – Keine 3 Jahre mehr bei SwissSign
  - 01.07.25 – Keine 3 Jahre mehr bei DigiCert
    - Neue S/MIME-Produkte bei DigiCert
  - Q3 2025 – Neue Zertifikatskette bei D-Trust
    - Neue S/MIME-Produkte bei D-Trust

  - 15.07.25 – Keine 3 Jahre mehr (Alle CA‘s)



Unsere neue Broschüre finden Sie unter:
www.psw-group.de/downloads

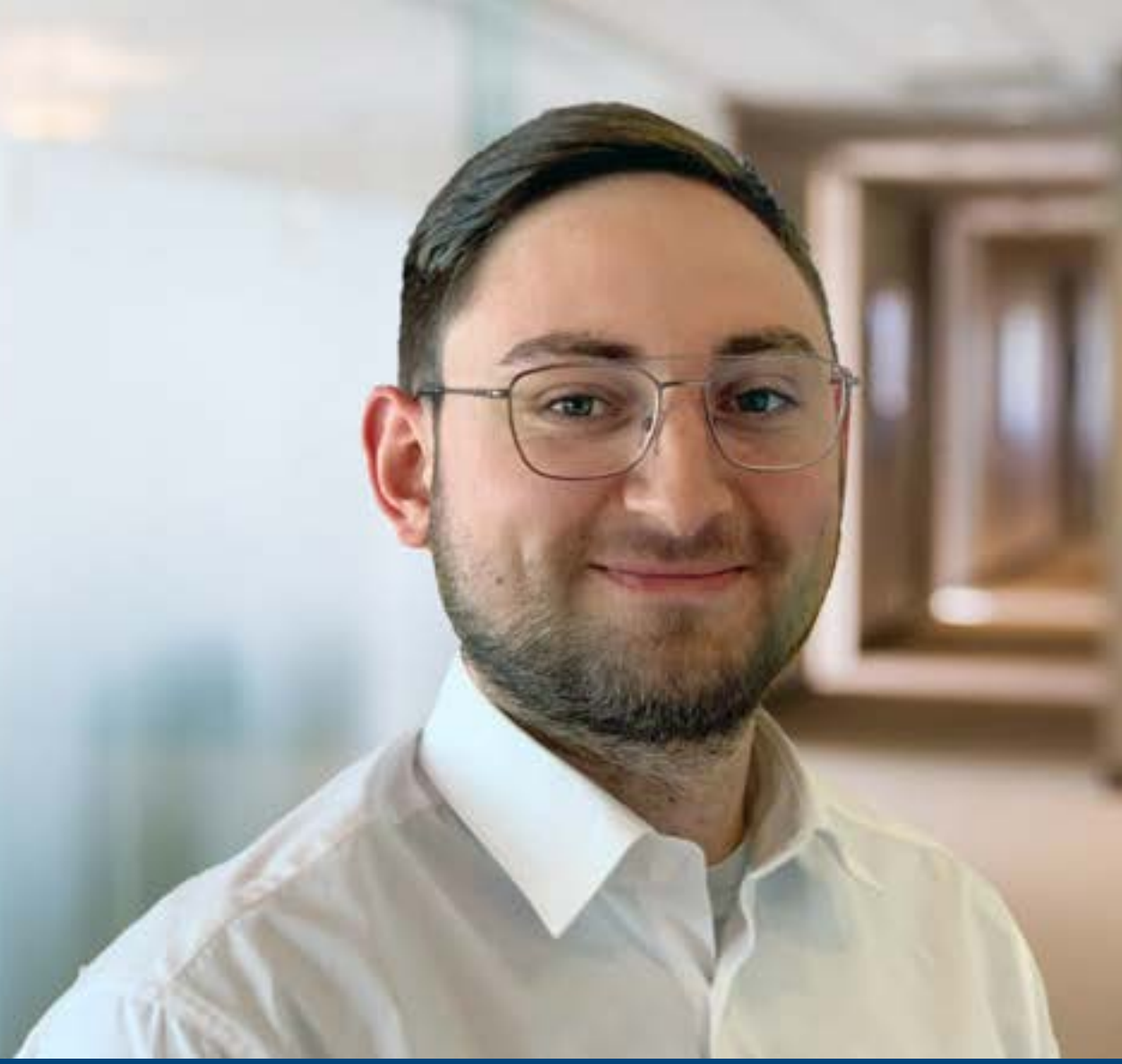


Bewerten Sie uns auf Google

GEPRÜFTER ONLINE-SHOP EHI

Excellent Shop
10 Jahre zertifiziert

Vielen Dank!



PSW GROUP **Newsletter**

Erhalten Sie alle Webinar-Ankündigungen und Informationen aus der Branche per E-Mail.

www.psw-group.de/newsletter-abonnieren/

Klassifizierung: extern