Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

"IT-Sicherheit im Deutschland-Stack"

Positionspapier

2026

TeleTrusT-Arbeitsgruppe "Cyber-Nation" [https://www.teletrust.de/arbeitsgremien/cyber-nation/]

Impressum

Herausgeber:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 310
E-Mail: info@teletrust.de
https://www.teletrust.de

Inhaltsverzeichnis

1 Zusammenfassung

1. Der Deutschland-Stack darf nicht als reines Digitalisierungs-, Cloud- oder Plattformprojekt verstanden werden, sondern als sicherheitskritische nationale Infrastruktur.

2. Informations- und Cyber-Sicherheit müssen deshalb von Beginn an als tragende Architektur-, Governance- und Betriebsprinzipien verankert werden.

3. Sicherheit darf nicht auf klassische IT-Sicherheit einzelner Systeme reduziert werden, sondern muss Identitäten, Zugriffe, Daten, Infrastruktur, Lieferketten, Betrieb, Resilienz und Wiederherstellbarkeit ganzheitlich umfassen.

4. Digitale Souveränität entsteht nur dann, wenn kritische Abhängigkeiten technisch, organisatorisch und betrieblich beherrschbar bleiben.

5. Der Deutschland-Stack benötigt daher überprüfbare Mindestanforderungen an Architektur, Beschaffung, Betrieb, Auditierbarkeit und Krisenfähigkeit.

6. Zero Trust ist ein wichtiger Ausgangspunkt, sollte für staatliche und kritische Infrastrukturen jedoch nicht als Endzustand verstanden werden.

7. Für besonders schutzbedürftige Bereiche sollten vom BSI überprüfte Systeme zum Einsatz kommen, die den Umsetzungen z.B. der vollumfänglichen Anforderungen nach VSA genügen und die aktuellen Entwicklungen zu (Post)-Zero-Trust, Identitäten, Authentifizierung etc. bestmöglich berücksichtigen.

8. Entscheidend ist, dass Nutzer und Endgeräte keinen allgemeinen Netzwerkzugang erhalten, sondern nur kontrollierten Zugriff auf konkret freigegebene Anwendungen und Dienste.

9. Resilienz muss außerdem durch belastbare Backup-/Restore- und Site-Recovery-Plattformen ergänzt werden, damit kritische Systeme im Ernstfall nicht erst neu beschafft, installiert und wiederhergestellt werden müssen, sondern kurzfristig weiterbetrieben werden können.

10. Der Erfolg des Deutschland-Stacks wird sich letztlich daran messen lassen, ob er nicht nur im Regelbetrieb funktioniert, sondern auch unter Angriffen, Ausfällen, Lieferkettenstörungen und Krisen souverän, sicher und wiederherstellbar bleibt.

Cyber-Sicherheit darf im Deutschland-Stack nicht als nachgelagerter Baustein oder als Sammlung einzelner Sicherheitsprodukte verstanden werden. Vielleicht besser: Sie ist ein durchgängiges Struktur- und Betriebsprinzip des gesamten Stacks und muss in Governance, Architektur, Standards, Zugriffsmodell, Betriebsmodell und Resilienz verbindlich verankert werden. Der Deutschland-Stack ist nur dann ein belastbares Fundament staatlicher Digitalisierung, wenn Informations- und Cyber-Sicherheit als durchgängige Führungs-, Architektur- und Betriebsaufgabe verankert werden. Ein auf Einzeltechnologien oder stark fragmentierte Strukturen verkürzter Ansatz greift zu kurz. Er erhöht Komplexität, schafft neue Abhängigkeiten und gefährdet Souveränität, Skalierbarkeit und Krisenfestigkeit. Für den Deutschland-Stack braucht es deshalb ein verbindliches Sicherheitszielbild, das föderal tragfähig ist und sich über den gesamten Lebenszyklus erstreckt - von Spezifikation und Beschaffung über Implementierung und Betrieb bis zu Audit, Migration und Außerbetriebnahme und Wiederherstellung.

- Sicherheit ist kein Add-on, sondern ein Architekturprinzip.
- Cloud und Managed Services sind Betriebsformen, keine Sicherheitskonzepte.
- Souveränität entsteht durch Kontrolle über Daten, Zugriffe, Schlüssel, Betriebsprozesse, Schnittstellen und Wechselpfade.
- Resilienz bedeutet nicht nur Prävention, sondern nachweisbare Wiederherstellungsfähigkeit.
- Zero Trust, Defense in Depth, Kryptoagilität und Security by Design müssen verbindliche Leitprinzipien des Deutschland-Stacks werden.
- Relevante Vorgaben des BSI, etablierte Normen und regulatorische Anforderungen müssen konsistent referenziert und operationalisiert werden.

Das vorliegende Positionspapier verdichtet diese Anforderungen zu einem eigenständigen cyber-politischen und architektonischen Zielbild für den Deutschland-Stack.

2 Ausgangslage

Der Deutschland-Stack verfolgt das richtige strategische Ziel: digitale Handlungsfähigkeit, Nachnutzbarkeit, Interoperabilität, Resilienz und Souveränität im öffentlichen Sektor zu stärken. Aus Sicht der Cyber-Sicherheit reicht es jedoch nicht aus, Technologien und Standards aufzuzählen. Entscheidend ist, wie diese in einem beherrschbaren, auditierbaren und resilienten Gesamtmodell zusammenwirken.

Die aktuelle Bedrohungslage durch staatliche Akteure, organisierte Kriminalität, komplexe Lieferketten, Schwachstellen in Cloud- und Software-Ökosystemen sowie steigende Abhängigkeiten von nicht-europäischen Plattformen macht deutlich: Der Deutschland-Stack muss von Beginn an als Sicherheits- und Souveränitätsarchitektur gedacht werden.

Cyber-Sicherheit ist dabei kein eigener Layer neben anderen, sondern eine Querschnittsanforderung an alle Layer des Stacks sowie an Governance und Betrieb, die zudem der regelmäßigen Aktualisierung und Anpassung an den Stand der Technik unterliegt.

3 Leitbild: Informations- und Cyber-Sicherheit statt enger IT-Sicherheit

Der Deutschland-Stack sollte terminologisch und inhaltlich konsequent von "Informations- und Cyber-Sicherheit" sprechen. Der Begriff "IT-Sicherheit" ist zu eng, weil er vorrangig informationstechnische Komponenten adressiert. Für den Deutschland-Stack geht es hingegen um Schutz von Informationen, Infrastrukturen, Netzen, Identitäten, kryptographischen Vertrauensankern, Betriebsabläufen und Wiederherstellung im Angriffs- und Krisenfall als durchgängiges Strukturprinzip.

Ein modernes Sicherheitsverständnis umfasst daher mindestens:

- Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität;
- Schutz digitaler Prozesse, Identitäten und Schlüsselmaterialien;
- Schutz vor hybriden, staatlichen und kriminellen Cyber-Bedrohungen;
- resiliente Reaktions- und Wiederherstellungsfähigkeit;
- kontinuierliche Anpassung an den Stand der Technik.

Das Leitbild des Deutschland-Stacks muss diese Breite ausdrücklich abbilden und zudem mit dem jeweiligen Stand der Technik in Bezug setzen.

4 Strategische Leitprinzipien

Die folgenden strategischen Leitprinzipien sollten dabei handlungsleitend sein und im besten Fall als verbindliche Architektur- und Betriebsprinzipien verstanden werden:

Security by Design und by Default: Sicherheitsanforderungen sind bereits in Zielarchitektur, Referenzdesigns, Schnittstellen und Betriebsmodellen zu verankern.

Zero Trust als Mindestniveau: Kein implizites Vertrauen in Netzsegmente, Standorte oder Plattformen; Zugriff erfolgt identitäts-, kontext- und ressourcenbezogen.

Defense in Depth: Mehrstufige Schutzmaßnahmen aus Identitätskontrolle, Segmentierung, Protokollierung, Detektion und Recovery.

Souveränität durch Kontrolle: Kontrolle über Daten, Schlüssel, Zugriffe, Betriebsprozesse, Schnittstellen, Migrationspfade und Anbieterwechsel.

Beherrschbarkeit: Architekturen dürfen nur so komplex sein wie nötig. Hohe Komplexität senkt das Sicherheitsniveau, Prüf- und Betriebsfähigkeit.

Kryptoagilität: Kryptographische Verfahren, Schlüsselverwaltung und Vertrauensdienste müssen aktualisierbar und regulatorisch anschlussfähig sein.

Resilienz: Weiterbetrieb, Schadensbegrenzung, Wiederherstellung und Wiederanlauffähigkeit müssen gleichermaßen geplant und getestet werden.

Föderale Umsetzbarkeit: Sicherheitsvorgaben müssen für Bund, Länder und Kommunen anschlussfähig, verbindlich und nachnutzbar sein.

5 Kernforderungen für den Deutschland-Stack

Verbindliches Sicherheitszielbild und Target Operating Model
Der Deutschland-Stack braucht ein föderal tragfähiges Zielbild für Governance, Rollen, Betriebsverantwortung, Sicherheitskontrollen, Eskalation, Auditierung und Weiterentwicklung. Ohne ein solches Modell bleibt der Stack ein Technologiekatalog ohne belastbare Betriebsrealität.

Sicherheits-Governance über den gesamten Lebenszyklus
Cyber-Sicherheit muss von Beschaffung und Spezifikation über Implementierung, Betrieb, Monitoring, Audit, Incident Response und Außerbetriebnahme hinweg verbindlich gesteuert werden. Erforderlich sind Risikoanalysen, Schutzbedarfsfeststellung, Sicherheitsreviews, regelmäßige Nachweise und ein kontinuierlicher Verbesserungsprozess.

Architektonisch integrierte Infrastruktur statt Flickenteppich
Eine virtualisierte, softwarebasierte Infrastruktur muss als ganzheitliche Einheit aus Compute, Storage, Netzwerk, Segmentierung, Identitätsbezug, Backup/Recovery, Plattformdiensten und kontrollierter Hardware verstanden werden. Sicherheit darf nicht erst durch nachträgliche Zusatzprodukte kompensiert werden.

Cloud- und Managed-Service-Nutzung nur innerhalb kontrollierter Architektur
Cloud und Managed Services dürfen nicht mit Sicherheit oder Souveränität gleichgesetzt werden. Maßgeblich ist, ob die gleiche Sicherheitslogik, die gleichen Kontrollpunkte und die gleiche Wiederherstellungsfähigkeit unabhängig vom Betriebsort, vom Betreiber und von eingesetzter Technologie erhalten bleiben.

Zero-Trust-Zugriff als Standardmodell
Zugriffe auf Anwendungen, Daten und Administrationsfunktionen müssen identitätsbasiert, gerätebezogen, kontextabhängig und minimal privilegiert gesteuert werden. Netzsichtbarkeit ohne explizite Autorisierung darf nicht Teil des Zielbilds sein.

Wiederherstellungsfähigkeit als Pflichtanforderung
Resilienz umfasst eine mehrstufige Backup- und Recovery-Architektur mit Trennung von Produktiv- und Sicherungsdomänen, begrenzter Erreichbarkeit, regelmäßigen Restore-Tests sowie belastbaren RTO/RPO-Nachweisen. Recovery ist kein Zusatzservice, sondern Kern des Betriebsmodells.

Konsolidierte Referenz auf Normen, Standards und Regulierung
Der Deutschland-Stack sollte relevante Rahmenwerke konsistent referenzieren und in verbindliche Umsetzungsanforderungen übersetzen. Dazu zählen insbesondere ISO/IEC 27001, 27017 und 27018, BSI IT-Grundschutz, BSI C5, DSGVO, NIS2 sowie eIDAS.

BSI-konforme Kryptographie und Kryptoagilität
Eigene pauschale Festlegungen zu einzelnen Algorithmen reichen nicht aus. Kryptographische Anforderungen sollten an aktuelle BSI-Vorgaben, insbesondere TR-02102, anschließen. Zusätzlich sind Kryptoagilität, Schlüsselmanagement und Migrationsfähigkeit - auch im Kontext postquantenfester Verfahren - verbindlich vorzusehen.

Vollständige Security-Bausteine in der Stack-Landkarte
Zur operativen Sicherheitsfähigkeit gehören SIEM, IDS/IPS, Firewalls, sicheres Logging, Zeit- und Protokollierungsinfrastruktur, Backup, Key Management, Monitoring und Alerting. Authentisierungs- und Föderationsmechanismen sowie sichere Protokolle müssen vollständig mitgedacht werden.

Souveränität durch Exit-, Portabilitäts- und Wechselpfade
Souveränität muss technisch und organisatorisch überprüfbar werden, durch offene Schnittstellen, exportierbare Daten, dokumentierte Migrationspfade, mehrfache Anbieteroptionen, kontrollierbare Schlüsselhoheit und klare Regelungen gegen Vendor Lock-in.

KI-unterstützte Schwachstellenanalyse
Ergänzend sollte im Deutschland-Stack auch die KI-unterstützte Schwachstellenanalyse berücksichtigt werden. Sie kann Sicherheitsverantwortliche dabei unterstützen, Schwachstellen in Code, Konfigurationen, Abhängigkeiten und Betriebsumgebungen frühzeitig zu identifizieren, zu korrelieren und risikobasiert zu priorisieren. Ihr Einsatz darf jedoch nur im Rahmen klarer Governance-Vorgaben erfolgen. Dazu zählen insbesondere Anforderungen an Nachvollziehbarkeit, Auditierbarkeit, Datenschutz, Schutz sensibler Informationen, menschliche Validierung kritischer Ergebnisse sowie die souveräne und kontrollierbare Betriebsform der eingesetzten KI-Komponenten. Für das Governance-Modell des Deutschland-Stacks ist sie damit zugleich Werkzeug und Regelungsgegenstand: Sie stärkt die kontinuierliche Risikoerkennung und Sicherheitssteuerung, erfordert aber selbst verbindliche Vorgaben zu Verantwortung, Kontrolle, Qualitätssicherung und Compliance.

6 Operative Schwerpunkte der Cyber-Sicherheit

Die im folgenden genannten Themenfelder stellen die wesentlichen Schwerpunkte aus operativer Sicht dar.

- Identitäts- und Zugriffsmanagement mit starker Authentisierung, privilegiertem Zugriffsmanagement und mandantenfähigen Freigabemodellen.
- Durchgängige Protokollierung, Monitoring und Sicherheitsdetektion mit zentral auswertbaren Logs, Metriken, Alarmierung und forensischer Nachvollziehbarkeit.
- Segmentierung von Netz-, Plattform- und Mandantendomänen sowie klare Trennung von Administrations-, Produktiv- und Sicherungszugängen.
- Sichere Software- und Plattformlieferkette mit Härtung, Patch-Management, Schwachstellenmanagement und reproduzierbaren Deployments.
- Datenklassifizierung, Schutzbedarfsfeststellung und differenzierte Sicherheitsvorgaben je nach Kritikalität.
- Technisch und organisatorisch belastbare Notfallorganisation inklusive Krisenkommunikation, Meldewegen und Wiederanlaufplanung.
- Regelmäßige Audits, Penetrationstests, Schwachstellenanalysen und Reifegradmessungen (auch KI unterstützt).
- Sichere Anbindung von Vertrauensdiensten, Identitätsökosystemen und perspektivisch europäischen Wallet- und Nachweisstrukturen.

7 Föderale Governance und Verantwortlichkeiten

Für die Wirksamkeit des Deutschland-Stacks ist entscheidend, dass Sicherheitsvorgaben nicht nur empfohlen, sondern in ihrer Verbindlichkeit geklärt werden. Bund, Länder und Kommunen benötigen ein gemeinsames Mindestniveau, kompatible Nachweisverfahren und klare Zuständigkeiten.

Dazu gehören insbesondere:

- ein gemeinsamer Mindeststandard für Sicherheitsarchitekturen und Kontrollpunkte;
- einheitliche Anforderungen an Auditierung, Protokollierung, Recovery-Nachweise und Sicherheitsdokumentation;
- klare Verantwortung des Auftraggebers auch bei ausgelagerten Betriebsleistungen;
- Referenzarchitekturen und Referenzimplementierungen zur beschleunigten Nachnutzung;
- Mechanismen für Ausnahmen, aber ohne Aufweichung des Sicherheitsfundaments.

Nur so entsteht ein föderales Sicherheitsregime, das Standardisierung und Handlungsfähigkeit verbindet.

8 Prioritäre Maßnahmen in den nächsten 12 Monaten

1. Erarbeitung eines verbindlichen Sicherheits- und Betriebszielbilds für den Deutschland-Stack.

2. Festlegung eines verbindlichen Mindestkatalogs technischer Kontrollpunkte für Identität, Segmentierung, Logging, Recovery und Schlüsselmanagement.

3. Konsolidierte Referenzierung relevanter BSI-, ISO- und regulatorischer Vorgaben in den Stack-Vorgaben.

4. Aufbau von Referenzimplementierungen und Proofs of Concept für sichere Betriebsmodelle in föderalen Szenarien (D-Stack Reallabor).

5. Definition eines verbindlichen Recovery- und Resilienzrahmens mit Testpflichten.

6. Erweiterung der Tech-Stack-Landkarte um fehlende Security- und Monitoring-Bausteine.

7. Einrichtung eines kontinuierlichen Sicherheits-Review-Prozesses zur Anpassung an neue Bedrohungen und Standards.

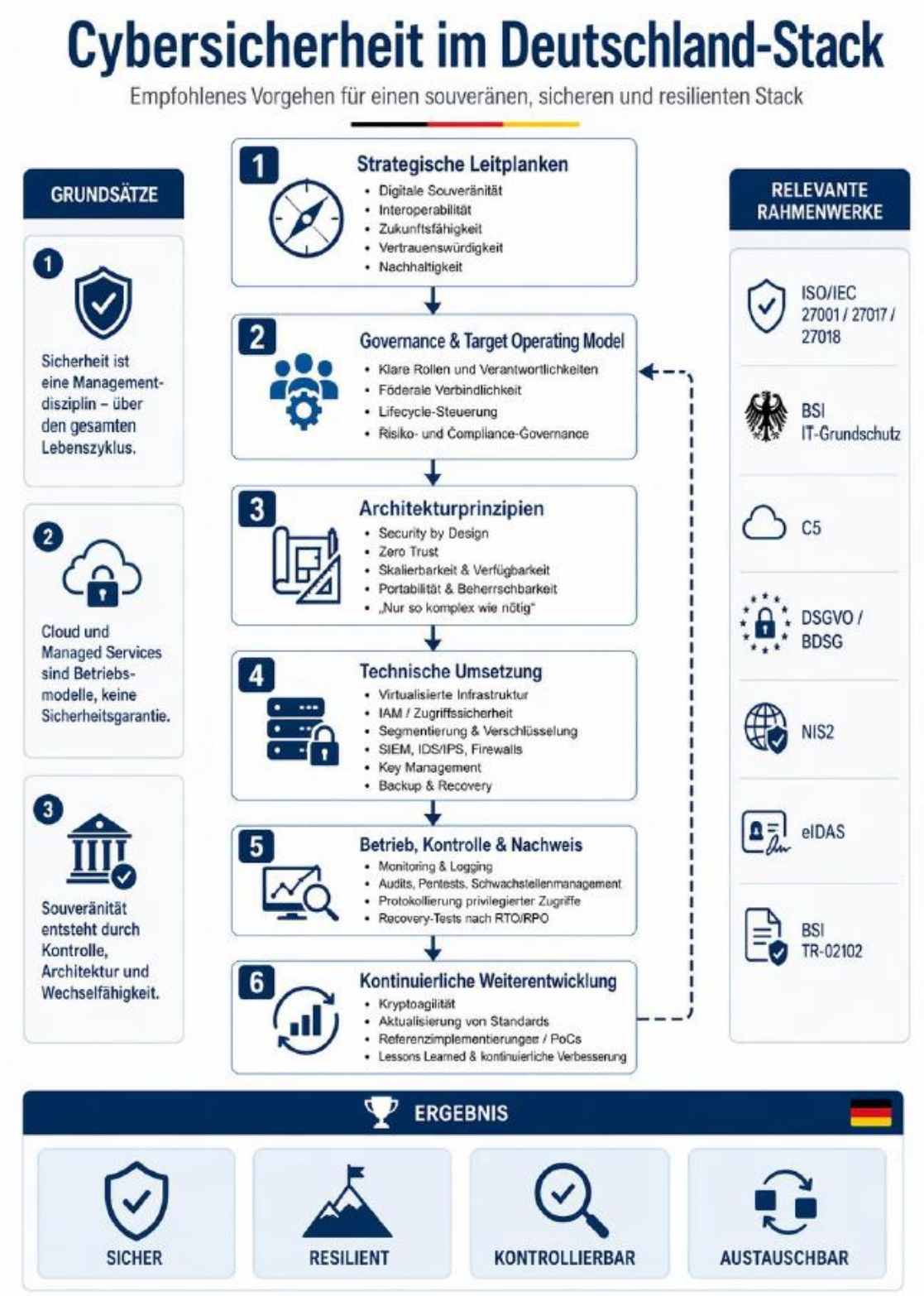
9 Schlussfolgerungen

Der Deutschland-Stack muss zu einem zentralen Baustein digitaler Souveränität und Sicherheit in Deutschland werden und zugleich auch als sicherheitskritische nationale Infrastruktur verstanden werden. Dafür muss Cyber-Sicherheit jedoch als Ordnungsprinzip verstanden werden: nicht als isolierter Sicherheitsblock, sondern als verbindende Logik von Architektur, Betrieb, Kontrolle und Wiederherstellung.

Ein souveräner Deutschland-Stack ist nicht der Stack mit den meisten Technologien, sondern der Stack mit der höchsten Beherrschbarkeit, der klarsten Verantwortungsstruktur und der nachweisbarsten Resilienz. Entscheidend ist, dass der Deutschland-Stack nicht nur funktional, sondern auch im Krisen-, Angriffs- und Ausfallszenario belastbar bleibt.

Das ist die Voraussetzung dafür, dass öffentliche digitale Infrastrukturen auch unter Krisenbedingungen vertrauenswürdig, belastbar funktionsfähig und weiterentwickelbar bleiben.

Abbildung Infografik zum Vorgehens- und Governance-Modell



Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie der Vertrauenszeichen "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de