

Tested. Certified. Secure

Zertifizierung im Bundesamt für Sicherheit in der Informationstechnik



Bundesamt
für Sicherheit in der
Informationstechnik

- Das BSI stellt sich vor
- Zertifizierung im BSI
- Common Criteria Zertifizierungen
- Beschleunigte Sicherheitszertifizierung
- Zertifizierung und CRA
- Fragen und Antworten

01. Das BSI stellt sich vor

Unsere Stakeholder



Staat



Wirtschaft



Gesellschaft



Wissenschaft

Prävention

Detektion

Reaktion



- Übernahme technischer Schutzmaßnahmen
- Nationales IT-Lagezentrum
- Technische Unterstützung und Dienstleistungen
- CERT-Bund und MIRTs
- Beratung und Service-Center
- Kooperation
- Allianz für Cybersicherheit
- UP KRITIS
- Begleitung in der Aus- und Fortbildung
- Technische Richtlinien
- Zertifizierung
- IT-Sicherheitskennzeichen



Gründung
01. Januar 1991



Bundesministerium
des Innern und für Heimat



Bundesamt für Sicherheit
in der Informationstechnik

Stellen 2025

1.791



Stellenbesetzungsquote: 94 %

*ohne Zuläufe

64

Unbefristete
Mitarbeitende
im Zulauf



36 %*
Frauen



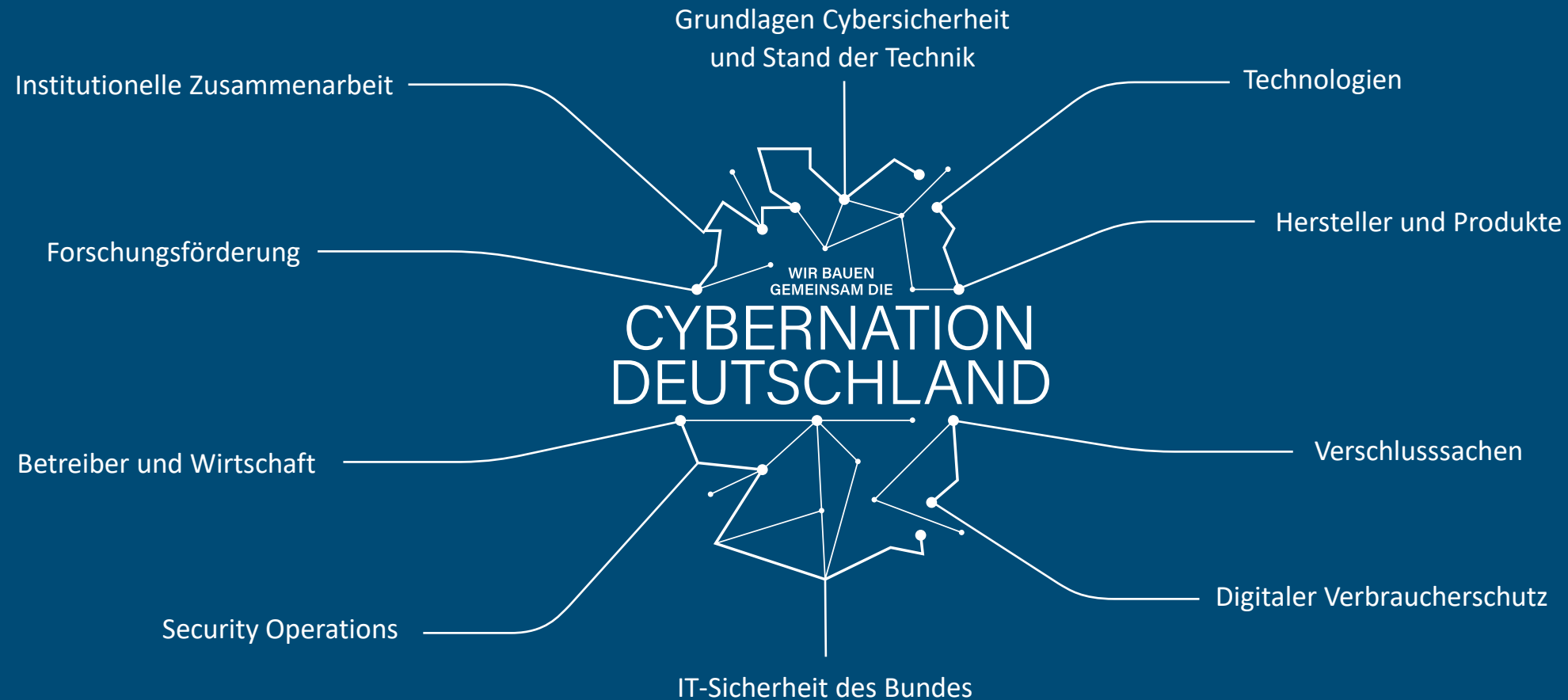
64 %
Männer

*Anteil in Leitungsfunktion: 28 %

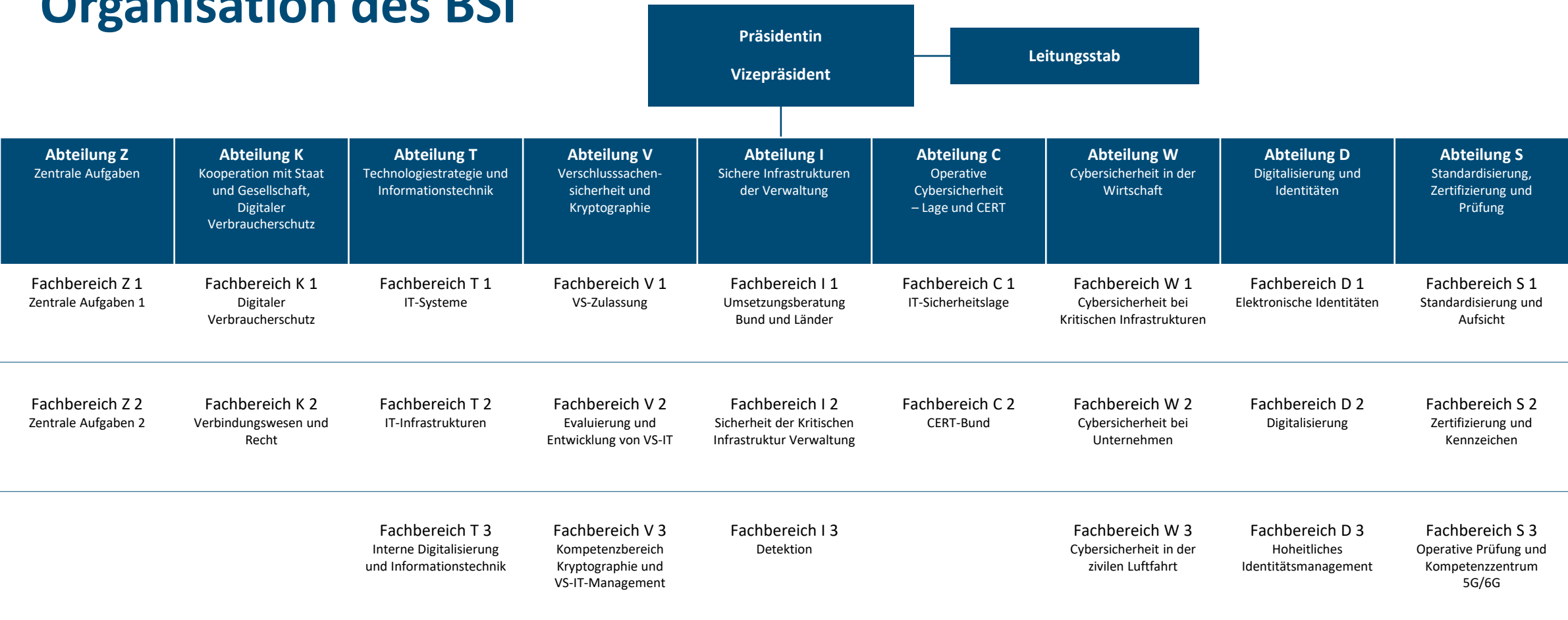
379 Mio.
Euro

Haushalt 2026

Aufgabenschwerpunkte des BSI



Organisation des BSI



02. Hersteller und Produkte: Zertifizierung im BSI

Die Marke des BSI: Hohes Vertrauensniveau

Zertifizierung und Kennzeichnung durch das BSI schaffen Vertrauen in Produkte und Dienstleister für eine sichere Digitalisierung in Deutschland und international.



Zertifizierung im Programm EUCC nach den Common Criteria

Zertifizierung im EUCC- Programm



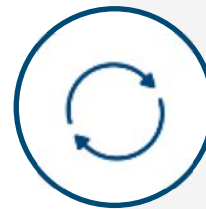
Beantragung

- Hersteller stellt Zertifizierungsantrag nach EUCC
- zugrundeliegende Norm: ISO/IEC 15408:2022



Evaluierung

- Evaluierung wird von notifizierten Prüfstellen (im Drei-Partner-Modell) durchgeführt
- Prüfaspekte u. a.: Entwicklung, Testen (funktional, Penetrationstests), Schwachstellenanalyse, etc.



Aktuelle Entwicklungen

- **seit Ende Februar 2026** agiert das BSI ausschließlich im Programm EUCC
- Maintenance oder Re-Assessment zu gültigen CC-Zertifikaten, die vor dieser Frist erteilt wurden, ist weiterhin möglich



Vorteile

- Vertrauen in Produkte stärken
- Wettbewerbsvorteile für Produkte auf dem europäischen und globalen Markt
- hohe Flexibilität durch anpassbare Evaluierungsstufen 1-7
- entwicklungsbegleitende Evaluierung möglich



Kosten und Dauer

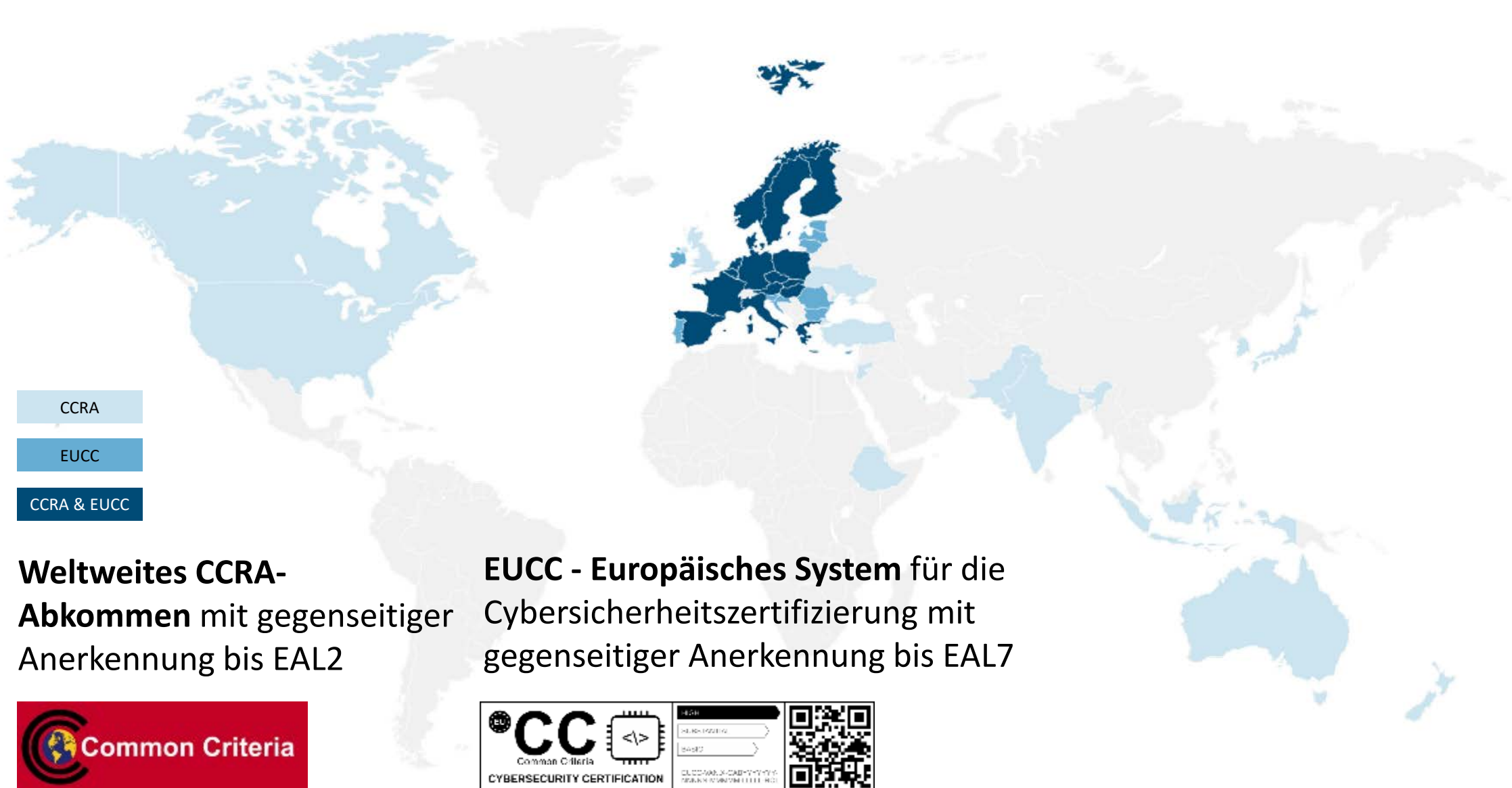
- Kosten nach BMI-Gebührenverordnung zzgl. Evaluierungsaufwände bei der notifizierten Prüfstelle
- Zertifizierungsdauer 6-12 Monate, je nach Prüftiefe und Komplexität des Produktes



Zertifikatserteilung

Nach erfolgreichem Abschluss der Evaluierung wird das EUCC-Zertifikat erstellt und auf der ENISA-Webseite publiziert → Gültigkeit i.d.R. 5 Jahre

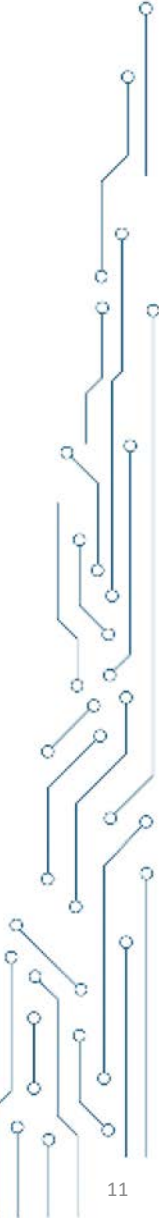
Anerkennung von Common Criteria Zertifikaten



Anforderungen an sichere Hardware

International abgestimmte Vorgaben

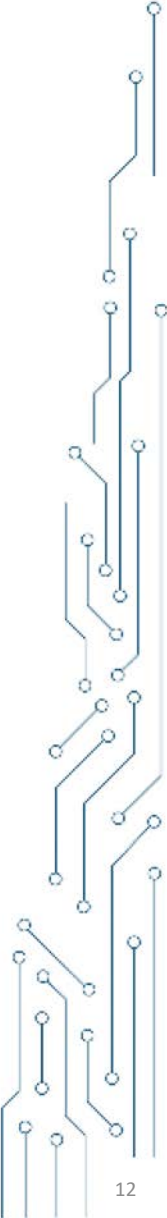
- Hardware wie z.B. Bankkarten, Gesundheitskarten, hoheitliche Dokumente durchlaufen verschiedene Zertifizierungen
- Vorgaben im Bereich der Common Criteria über semiformale Protection Profiles
- Grundlage ist zumeist ein Chip, z.B. Infineon, NXP, STM mit Speicher, Zertifizierung nach BSI-CC-PP-0084/BSI-CC-PP-0125:
 - Schutz der Benutzerdaten vor Fehlfunktionen, Seitenkanalattacken
 - Erkennung und Verhinderungen von Manipulation und Probing-Attacken (Messen von Signalen)
 - Vorgaben für einen Lebenszyklus
 - Zufallszahlengenerierung
- Darauf aufbauend Zertifizierung von Betriebssystem
 - BSI-CC-PP-0099: Java Card System mit Virtual Machine (VM), Runtime Environment (RE), Application Programming Interface (API)
 - BSI-CC-PP-0123: Java-Card System mit Firewall
 - BSI-CC-PP-0082: Anforderungen an Gesundheitskarten



Von den Anforderungen zum Testen mit Sicherheitsbezug

Methodisches Vorgehen kompetenter Labore

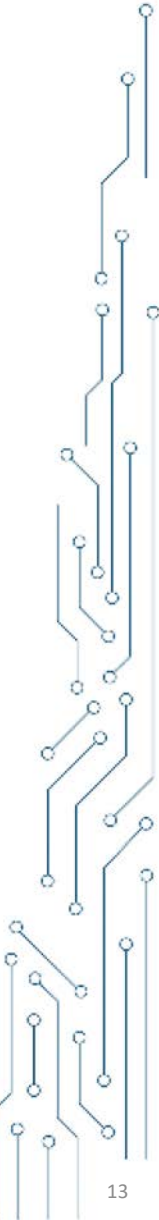
- Evaluierung durch akkreditierte und EU-notifizierte Prüflabore:
 - Akkreditierung nach DIN/ISO 17025 in Zusammenarbeit mit DAKKS und BSI
 - Notifizierung gemäß EUCC-DV durch BSI nach weiterer Kompetenzprüfung u.A. im Bereich Smartcards
 - TÜV IT ist eines der Labore, mit denen BSI zusammenarbeitet
- International harmonisierte Vorgehensweise, zwei internationale Arbeitsgruppen für Methodik
- Teilnehmer sind Prüfstellen, Antragsteller, Organisationen, Zertifizierungsstellen
- JHAS: Kümmert sich vor allem um Angriffsmethodik, Angriffsbewertung
- ISCI WG: Kümmern sich um viele anderen Aspekte
 - Harmonisierung von Sicherheit im Lebenszyklus (MSSR-Dokument)
 - Methodik zur Verbindung von Chip- und Chipbetriebssystem (ETR for Composition)
 - Kommentierung von Protection Profiles
 - Vorgehen bei Audits, insbesondere Wiederverwendung von Auditresultaten (STAR-Methodologie)
 - Soft-IP Zertifizierung
 - Usw.
- Unter EUCC organisiert in der EUCC-ISAC: <https://ccisac.eu/>



Anforderungen an Tests in den Common Criteria

Methodisches Vorgehen, international abgestimmt

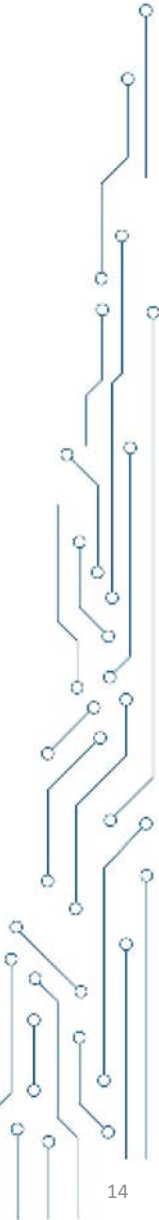
- Anforderungen werden in sog. Klassen formuliert, für das Testen gibt es die Klassen ATE und AVA
- ATE: Ziel ist, basierend auf Testdokumentation des Herstellers die Testtiefe, Abdeckung der Sicherheitsfunktionalität nachzuvollziehen und zu bestätigen
- AVA: Suche nach Schwachstellen für das zu untersuchende Produkt
- Anweisungen für Evaluatoren dokumentiert in der CC Evaluation Methodology, (CEM, ISO 18045)
- CEM beinhaltet für jede Anforderung mehr oder weniger detaillierte Anforderungen, was der Evaluator prüfen muss
- Wichtig: Finden von Gleichgewicht zwischen ausreichendem Testen, sicherem Produkt, Budget und Projektlaufzeit
- Arbeitsgruppen beschäftigen sich insbesondere damit, sinnvolle Ansätze zur Harmonisierung zu finden
- Umfangreiche Literatur entstanden, z.B.:
 - BSI hat in Vorgaben für Kryptographie, Fuzzing, etc. erstellt über Studien
 - Vorgaben zur Bewertung und Methodik von Angriffen
- Neueste Herausforderung mit disruptiven Charakter: Schwachstellensuche mit KI



Testansatz in den Common Criteria

Funktionales Testen

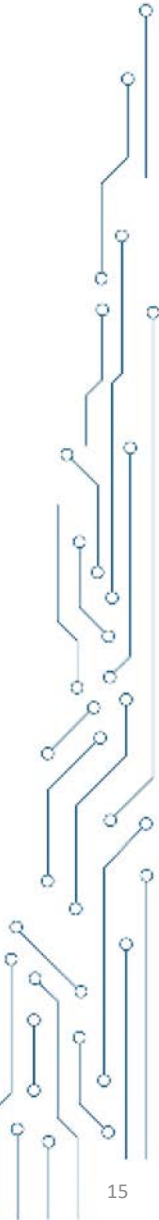
- Funktionales Testen umfasst z.B.
 - Wirksamkeitsprüfung von Rechte- und Rollenmanagent
 - Korrekte Nutzung von Sicherheitsprotokollen wie z.B. IPSEC
 - Implementierung von kryptographischen Algorithmen wie AES, RSA, PQC-Algorithmen
 - Usw.
- Testdurchführung, Dokumentation durch den Hersteller nach Vorgaben der Common Criteria
- Evaluator vollzieht Ausschnitte, wichtig zum Kennenlernen des zu untersuchenden Gegenstands
- Hersteller muss Testtiefe belegen: Tests müssen kleinste dokumentierte Designbestandteile abprüfen
- Hersteller muss Sicherheitsfunktionen abtesten, Mindestmaß an Tests ist vorgegeben
- Abarbeitung ATE ist meistens nicht so ein großes Problem, je nach zu untersuchendem Produkt aber ggf. nur beim Hersteller machbar
- Für Hardware kein Problem, auch in der Prüfstelle nachzuvollziehen



Methodische Suche nach Schwachstellen

Inhalte der Assurance-Klasse AVA

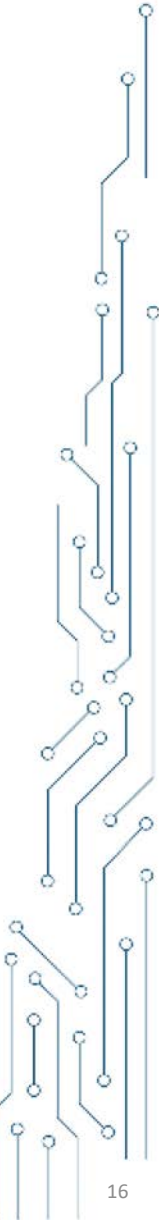
- Untersuchungen auf Schwachstellen hin soll Robustheit der Umsetzung belegen
- Grundsätzlich kein Ende gegeben, man kann immer weiter nach Schwachstellen suchen
- Öffentlich einsehbare Verzeichnisse wie Mitre, etc. sind wertvolle Hinweise
- Verschiedene Projekte im BSI beschäftigen sich mit Sicherheit von Hard- und Software:
 - Nutzung von Fuzzy-Tests
 - Sichere Implementierung von kryptographischen Algorithmen
 - Anleitung zur Umsetzung von PQC-Spezifikationen
- Untersuchung Schwachstellen Hardware:
 - Grundsätzlich unendlich lange ausführbar
 - Minimales Set an Angriffsvektoren werden wegen Mindestaufwänden harmonisiert in Arbeitsgruppen
 - Nutzung verschiedener Möglichkeiten: Oszilloskope, Laser, Abschleifen von Chiplagen, etc., ständige Entwicklung
 - Bewertung nach abgestimmter Punktebewertung
 - Umfänge, Mindestanforderungen immer heiß diskutiert
- BSI hat hohe Kompetenz in Prüfbegleitung, setzt bekannt hohe Anforderungen
- Es ist ein immerwährendes Hase-Igel Verhältnis zwischen Hersteller und Angreifer



Fazit vom Testansatz der Common Criteria

Umfangreiches, abgestimmtes Vorgehen

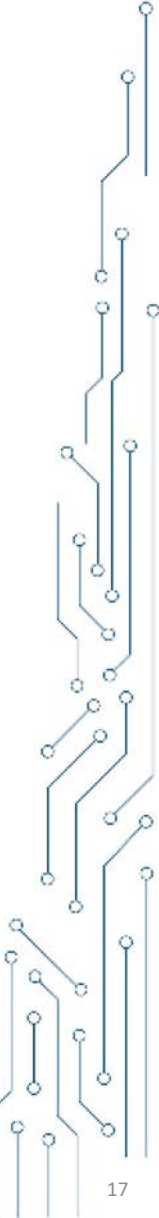
- Erfordert gute Dokumentation vom Hersteller eines Produktes
- Sehr genau beschrieben, möglichst nachvollziehbar -> dadurch etwas starr
- Bei aller Regelung bleibt Fachkompetenz entscheidend
- Kompetente Labore, regelmäßige Überprüfungen, eingespieltes Ökosystem
- Nachvollziehbarkeit und Dokumentationsanforderungen arbeitsintensiv
- Besonderheiten im Hardware-Bereich
 - Seit langer Zeit europaweit harmonisiert
 - Sehr erfolgreich auch in anderen Standards
 - Wird von verschiedenen Organisationen wiederverwendet, z.B. EMVCo-Prüfungen im Finanzumfeld
- KI mit schwierig zu beschreibendem Ansatz stellt große Herausforderung
 - Kriterien ändern sich nicht so schnell, viele Parteien sind beteiligt
 - Zu neuen, disruptiven Technologien keine gute Beschreibung
 - Umfangreiches Werk mit sehr viel Text



Alternativer Ansatz: Beschleunigte Sicherheitszertifizierung

Risikobasiertes Zertifizierungsprogramm mit planbarer Laufzeit

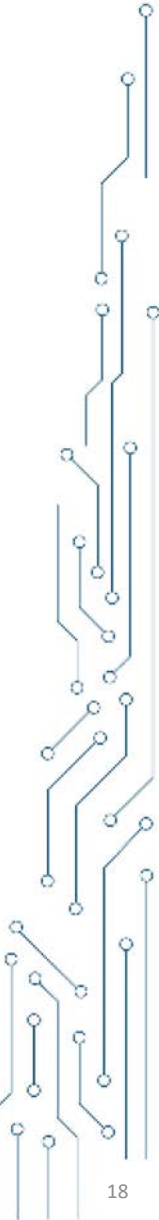
- **Schnelligkeit und Planbarkeit:**
 - Definition der Sicherheitsfunktionalität ähnlich zu Common Criteria
 - Bereitstellung des Produktes
 - Durchführung von Tests in bestimmtem Zeitrahmen, idealerweise 3 Monate
- **Keine umfangreiche Dokumentation:**
 - Aufbau und Inhalt des Produktes müssen nicht so genau beschrieben werden
 - Prüfung weniger Dokumente, kein Lebenszyklus
- **Praxisnaher Fokus**
 - praktische Sicherheits- und Penetrationstests (Angriffstests) an einer oft genutzten Produktkonfiguration.
 - Kein Nachvollziehen von Herstellertests, etc.
- **Europäische Basis:** Die BSZ stützt sich auf die europäische Norm EN 17640 (FiT CEM – Zeitlich festgelegte Cybersicherheitsevaluationsmethodologie für IKT-Produkte)
- **Nur begrenzt international abgestimmt:**
 - Anerkennungsabkommen mit Frankreich besteht
 - Erst seit neuestem in EU-Arbeitsgruppen eingebunden
 - Prüfstellenüberwachung weniger reglementiert, keine internationale Überprüfung



BSZ-Evaluation in a nutshell

Testen steht im Vordergrund

- 3 Geltungsbereiche:
 - Allgemeine Netzwerkkomponenten und eingebettete IP-vernetzte Produkte
 - Highspeed-Konnektoren (Gesundheitsbereich)
 - Komponenten im HAN des SMGW
 - Weitere Geltungsbereiche in Vorbereitung, gerade bei Nutzung von Hardware-Schnittstellen
- Evaluierungsschritte
 - Penetrationstest (risiko-orientierter Fokus auf externe Schnittstellen, Protokolle und Sicherheitsfunktionen)
 - Evaluierungsschritte aus der FiTCEN-Norm, Kompetenz der Prüfstelle wichtig.
 - Konformitätsanalyse (Mindestanforderungen aus den Schemadokumenten an ST, SUG und TOE)
 - Minimale physikalische Evaluierungsschritte (Gehäusetests im GB Komponenten im HAN des SMGW)
 - Gut geeignet für den Einsatz von KI bei der Schwachstellensuche
 - Besonderes Augenmerk auf Kryptographie mit Sourcecodeanalyse
- Für IoT grundsätzlich geeignet, noch nicht erprobt



Zusammenfassung

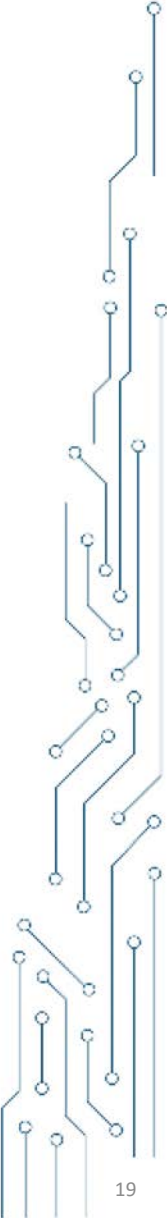
BSI legt Wert auf fundierte Sicherheitsaussagen bei BSZ und CC-Zertifizierung

Beschleunigte Sicherheitszertifizierung:

- Neues Angebot seit 2021 aufbauend auf Erfahrungen aus der Common-Criteria Zertifizierung
- Verwendet für zeitkritische Anwendungen
- Begrenzt auf bestimmte Produkttypen
- Freies Testen, gute Resultate
- Weniger Dokumentation – Weniger Produktkenntnis
- Keine weitgehende internationale Anerkennung

Common Criteria Evaluierungen

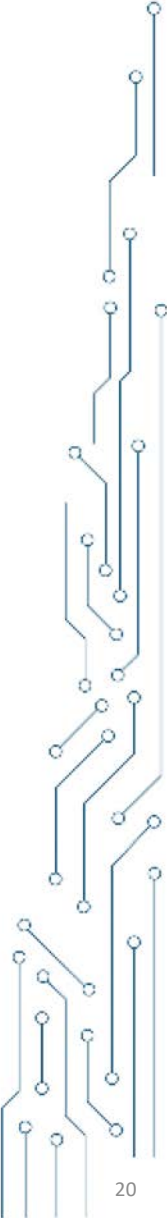
- Etablierter Prüfstandard seit 25 Jahren
- Viel Erfahrung, internationale Anerkennung
- Internationales Engagement in der Kriterienarbeit
- Viel Dokumentation, viele Quellen zum Kennenlernen des Produktes
- International entwickelte Methodologie
- Nachvollziehbarkeit ist ein wichtiger Punkt, umfangreiche Prüfberichte
- Fokus nicht nur auf Testen und Schwachstellen sondern auf ganzheitliche Produktentwicklung



Zertifizierung und CRA

Einbindung in die neue Regulierung

- CRA schafft Möglichkeiten zur Nutzung einer Zertifizierung für Nachweis der Abdeckung
- Abdeckung der Essential Security Requirements:
 - Größere Probleme bei der BSZ wegen fehlender Untersuchungen zum Lebenszyklus von Produkten
 - Nicht abgestimmt auf Anforderungen der Common Criteria
- Anstrengungen nach „Presumption of Conformity“ mit CC-Zertifizierung laufen
 - Erste Studie der ENISA hat gemischtes Bild abgegeben
 - Unterschied zwischen untersuchten Bestandteilen eines Produktes und Herstellererklärung für den Rest
 - Weitere Anforderungen des CRA wie z.B. Datensparsamkeit, Nutzung von Public Clouds sind schwierig abbildbar
- BSI hat ein „Position Paper“ entworfen, eher technisch an den CC und CRA orientiert
- BSI bietet Modul H an außerhalb der Zertifizierung nach BSZ oder Common Criteria
 - Ansatz des BSI basiert auf Ausbau ISO 27001 mit Bewertung der Herstellerprozesse
 - Dargestellt in TR-03183-H als Technische Richtlinie
 - Konformitätsbewertungsstellen müssen sich finden
 - Programm ist im Aufbau, Interesse scheint vorhanden zu sein



Fragen?

Ingo Hahlen

Referatsleiter S 22 -Common Criteria Zertifizierung von Hardwareprodukten

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Godesberger Allee 87

53175 Bonn

Telefon: +49 (0)228 99 9582 -5979

E-Mail: ingo.hahlen@bsi.bund.de



Bundesamt
für Sicherheit in der
Informationstechnik

Follow us:

