Erfurt, 16. Mai 2003

Stellungnahme des TeleTrusT Deutschland e.V.

zur strategischen Neuausrichtung des BSI bei der Produktzertifizierung

auf Grundlage des Protokolls der 2. Sitzung des Runden Tisches Kryptowirtschaft am 27. März 2003

Als ein Weg zur Vertrauenswürdigkeit von elektronischen Geschäftsprozessen spielt die Evaluierung und Zertifizierung der Sicherheitseigenschaften von IT-Produkten seit langem eine wichtige Rolle in den TeleTrusT-Konzepten. In den letzten Jahren wurden aktive Beiträge für die Evaluierung nach den Common Criteria (CC) geleistet, und es wurden Erkenntnisse über deren Marktrelevanz und Grenzen gewonnen.

Vor dem Hintergrund der Entwicklungen auf den internationalen IuK-Märkten, die dadurch gekennzeichnet sind, dass einerseits

- die Sicherheit komplexer Anwendungsprozesse zu bewerten und dass andererseits
- die Forderung nach modularer, skalierbarer und angemessener Sicherheit im konkreten Anwendungskontext zu erfüllen ist,

sind bei TeleTrusT bereits häufig Vorschläge zu einer Flexibilisierung von Sicherheitsqualitätsprüfungen diskutiert worden.

TeleTrusT hat deshalb das Vorhaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur strategischen Neuausrichtung bei der Produktzertifizierung als ein Schwerpunktthema des Internen TeleTrusT-Workshops am 7. und 8. Mai 2003 zur Diskussion gestellt.

TeleTrusT begrüßt diese Initiative ausdrücklich und setzt in sie hohe Erwartungen. Es ist wichtig, dass neue Wege gesucht werden, die den eingangs beschriebenen Trends entsprechen.

Durch die vorgesehene Erweiterung seines Portfolio soll das BSI besser als bisher in der Lage sein, den Anforderungen des Marktes gerecht zu werden, indem innovative Informationstechnik schnell und kostengünstig dem Markt erschlossen wird, ohne deren vertrauenswürdige Nutzung in Frage zu stellen.

Mit der Einführung der neuen Leistung, der **IT-Produkt-Zertifizierung** (IT Product Certification – IPC), soll die bisherige Prüfung nach CC ergänzt werden. Im VS-Bereich beispielsweise wird die Prüfung der einzelnen Module und Komponenten einer Lösung nach CC weiterhin nötig sein. Wegen des höheren Sicherheitsbedarfs sind in diesem Bereich größere Kosten- und Zeitaufwände akzeptabel.

Für Produkte am Massenmarkt scheint **IPC** deutlich besser geeignet, den Anforderungen der Anbieter nach schneller und kostengünstiger Evaluierung ihrer Produkte sowie nach für den Verbraucher verständlichen Prüfaussagen gerecht zu werden. Ein Grund dafür ist, dass nicht mehr lediglich Sicherheits-Module und –Komponenten sowie OEM-Produkte sondern nunmehr auch komplette IT-Produkt-Lösungen und –Services evaluiert werden sollen. Die Zertifizierungsaussagen zu Produkten und Services dieses deutlich größeren Anwendungsbereiches erschließt sich nicht mehr nur ausgebildeten IT-Sicherheitsexperten sondern können direkt beim Endverbraucher und Entscheider vertrauensbildend wirken.

Entsprechend des aus Sicht von TeleTrusT realistischen Zeitplans des BSI zur Einführung des neuen Prüfverfahrens befindet sich die Machbarkeitsstudie derzeit im Abschluss. In die nun vorgesehene Pilotzertifizierung sollten entsprechend ihrer allgemeinen Anerkennung in Wirtschaft und Verwaltung als technologische Grundlage ISIS-MTT und als Angebot für die PKI-Unterstützung von Anwendungen die European Bridge-CA (EB-CA) in die IPC-Liste aufgenommen werden. TeleTrusT wird in den Boards von ISIS-MTT und der EB-CA dies konsequent unterstützen und sich entschieden für eine IPC-Zertifizierung einsetzen. Auch die neu initiierte AG2 „Personal Security Environ-

ment – PSE“ von TeleTrusT bietet ihre Kompetenz zur aktiven Begleitung des BSI-Vorhabens an. Ein Ansatzpunkt hierfür bietet sich z.B. bei SmartCard Security Bundle als PGP-Ersatz für WIN XP mit Chipkarte.

Die bis zur Freigabe der IT-Produkt-Lösung durchzuführenden Prüfungen im Product Type Approval (**PTA**) sollen deutlich weniger umfangreich sein. Damit könnten die Eingangstests schnell absolviert werden und verursachten relativ wenig Kosten. Innovative deutsche Produkte würden so eher am Markt verfügbar sein (kürzerer Time to Market) und könnten sich dort besser der weltweiten Konkurrenz stellen (längerer Product Lifecycle). Für die Anbieter stellte sich der ROI deutlich früher ein, sie würden ausländischen Mitanbietern gegenüber konkurrenzfähiger. Dies würde durch die vorgesehene Herstellererklärung und den turnusmäßigen Product Quality Check (**PQC**) nicht beeinträchtigt sondern wirksam ergänzt werden.

Dieser Neuansatz im Prüfverfahren des BSI für den Nicht-VS-Bereich kann effektiv für das BSI und die beauftragten Prüfinstitute und effizient für die Hersteller werden.

Der Überlegung des BSI, dass durch die Kombination aus PTA, PQC und der Herstellerverpflichtung zur ggf. notwendigen Nachbesserung zwar nicht alle denkbaren Risiken ausgeschaltet sind (was bei der herkömmlichen CC-Prüfung auch nicht garantiert werden konnte), der Gewinn durch die im Schnitt vertrauenswürdigeren innovativen Produkte und Leistungen am Markt jedoch deutlich größer ist, folgt TeleTrusT vollinhaltlich.

Die vorgesehenen Prüfungen sollen durch Prüfinstitute unter der Aufsicht des BSI durchgeführt und die Prüfkriterien nach „Best Practice“ oder „State-of-the-Art“ permanent angepasst werden. Damit werden die Prüfverfahren stets aktuell und den konkreten Anwendungskontexten angepasst sein.

Der Erfolg der strategischen Neuausrichtung bei der Produktzertifizierung des BSI hängt von der Akzeptanz sowohl beim Anbieter als auch beim Anwender ab. TeleTrusT wird die anstehende Umsetzung der Machbarkeitsstudie des BSI aktiv begleiten und darauf hinwirken, dass das neue Evaluierungskonzept die Marktchancen für deutsche IT-Sicherheitslösungen verbessert.