TeleTrusT-EBCA "PKI-Workshop" 2021

Berlin, 30.09.2021

Trust Spaces - Ein Weg den Gordischen Knoten zwischen der EU und den Browsern zu lösen

Enrico Entschew, D-Trust

Was macht einen Vertrauensraum aus?

- Vorgaben
- Technische Umsetzung
- Verantwortlichkeit
- Überwachung

Vertrauensräume existieren gemäß diesem Schema in beiden Welten – sowohl analog als auch digital.

Beispiele für Vertrauensräume

Der Vertrauensraum der Browser

- Vorgaben: Root Store Policy, Baseline Requirements, EV-Guidelines
- Technische Umsetzung: Root Store
- Verantwortlichkeit: Browser
- Überwachung: Qualifizierte Auditoren and CCADB

Der Europäische Binnenmarkt

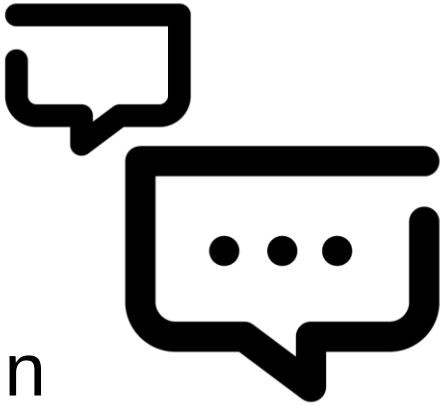
- Vorgaben: EU-Verordnung eIDAS, referenzierte Durchführungsrechtsakte und technische Standards
- Technische Umsetzung: EU Trusted List und nationale eIDAS Trusted Lists
- Verantwortlichkeit: EU Kommission
- Überwachung: Supervisory Bodies und Konformitätsbewertungsstelle

Das qualifizierte Zertifikat für Website-Authentifizierung (QWAC)

- Vertrauensdienst der eIDAS
- Klassisches TLS-Zertifikat gemäß RFC 5280
- Prüfmöglichkeit gegen die eIDAS Trusted List
- Erwägungsgrund 67 "Website-Authentifizierungsdienste geben dem Besucher einer Website die Sicherheit, dass hinter der Website eine echte und rechtmäßige Einrichtung steht. "
- QWAC soll im Einklang mit den Regeln der EU genutzt werden

Im CA/Browser Forum arbeitet D-TRUST zusammen mit anderen europäischen TSPs daran, dass QWACs durch Browser anerkannt werden.

Der aktuelle Status von QWAC in Browsern



- Werden selten mit Browsern genutzt
- Nutzung nur unter Beachtung der EV Guidelines
- Root CA muss im Rootstore des Browsers enthalten sein
- Von CA/B-Forum abweichende oder ergänzende Zertifikatserweiterungen sind nicht zulässig

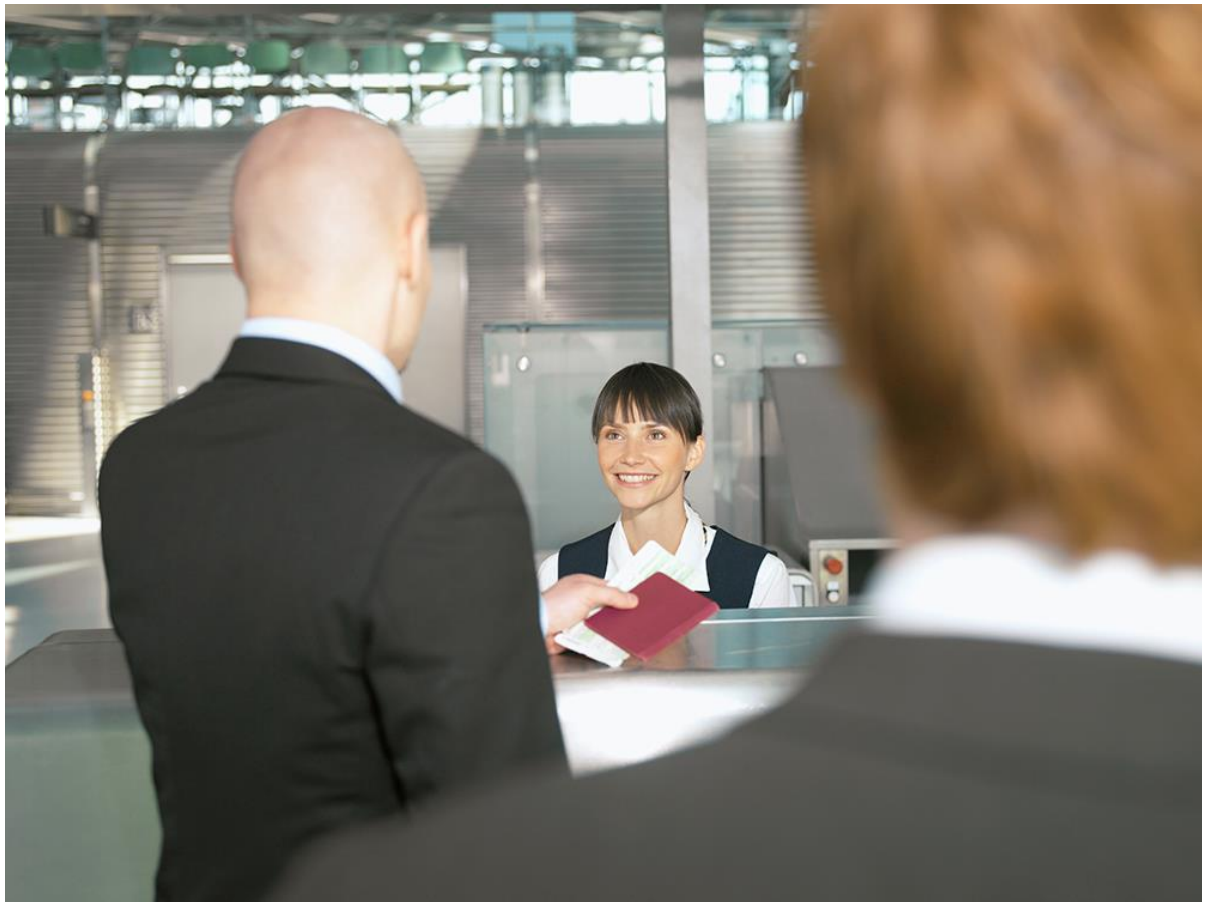
Mehrjähriger intensiver Austausch zwischen EU-Kommission und Browser zur Integration von QWAC.

Wir brauchen eine Brücke zwischen den Vertrauensräumen!

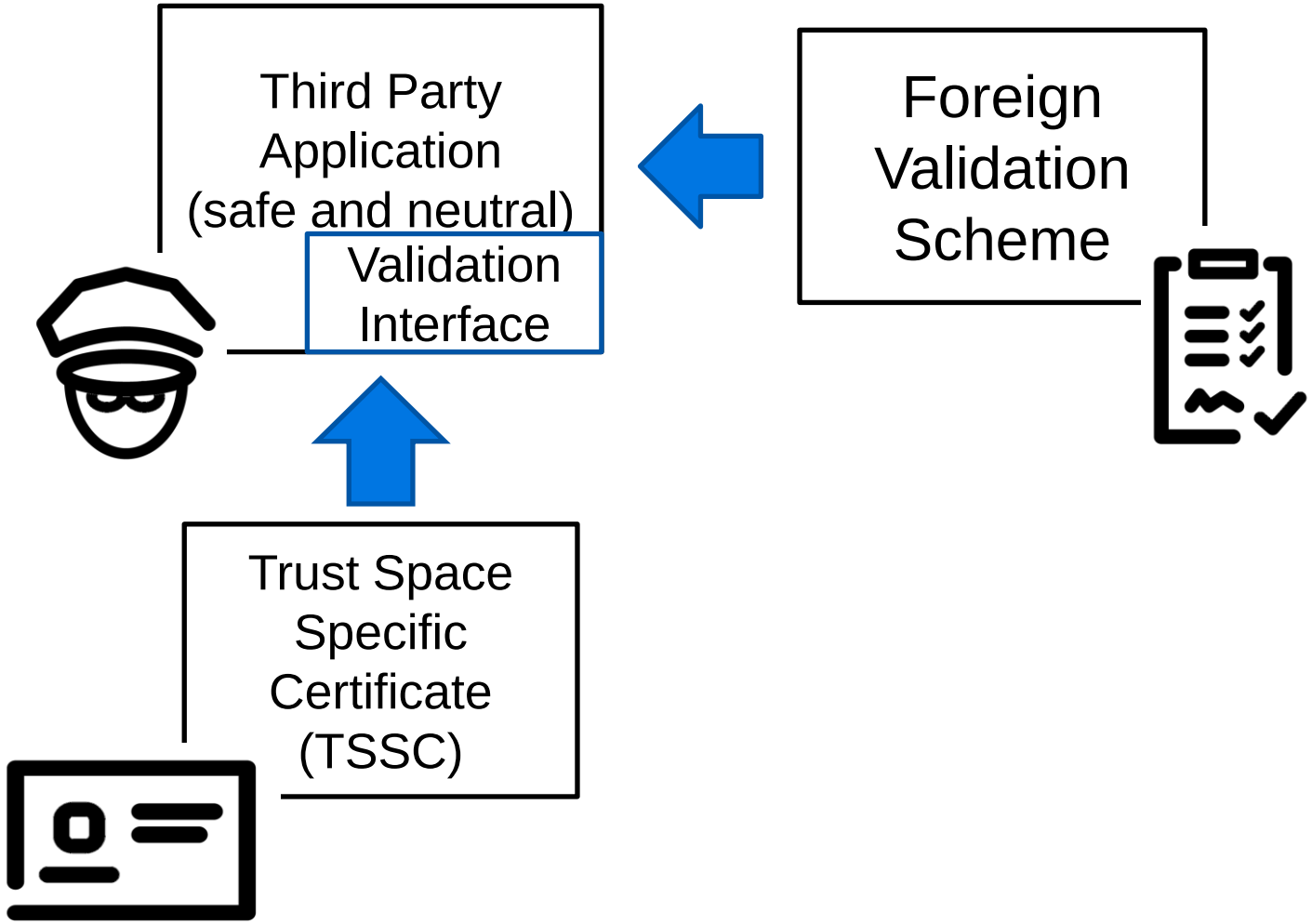
Es muss in allen Anwendungen immer möglich sein, zu erkennen, in welchem Vertrauensraum sich der User aktuell befindet.

Wie eine Brücke im echten Leben gebildet wird...

Wie prüfen wir heute ein Element eines fremden Vertrauensraums?



Was braucht es um eine Brücke zu bauen?



Erinnern Sie sich noch an diese Vertrauensräume?

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Der Vertrauensraum der Browser

- Vorgaben: Root Store Policy, Baseline Requirements, EV-Guidelines
- Technische Umsetzung: Root Store
- Verantwortlichkeit: Browser
- Überwachung: Qualifizierte Auditoren and CCADB

Der Europäische Binnenmarkt

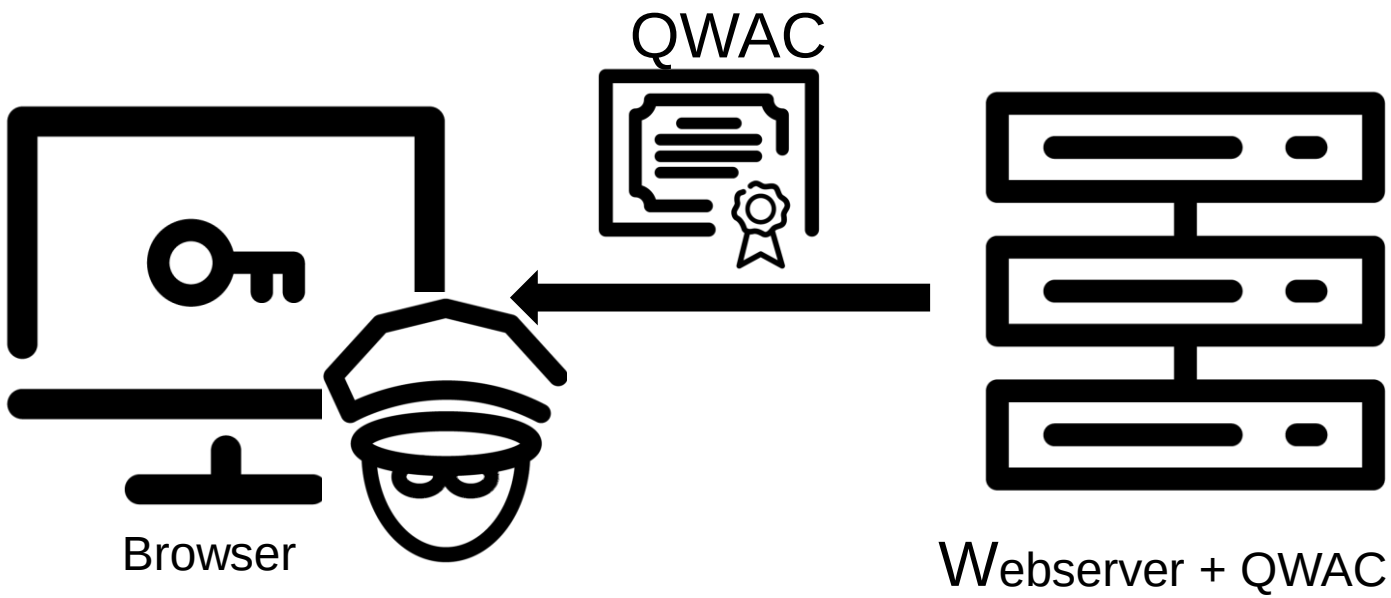
- Vorgaben: EU-Verordnung eIDAS, referenzierte Durchführungsrechtsakte und technische Standards
- Technische Umsetzung: EU Trusted List und nationale eIDAS Trusted Lists
- Verantwortlichkeit: EU Kommission
- Überwachung: Supervisory Bodies und Konformitätsbewertungsstelle

Unser Ziel

- Users und Zertifikatsinhaber sollen das QWAC im Browser nutzen können
- Browser sind nicht verantwortlich für das QWAC Prüfergebnis
- Browser betreiben ihren eigenen Vertrauensraum
- Die EU behält ihre Souveränität über das QWAC

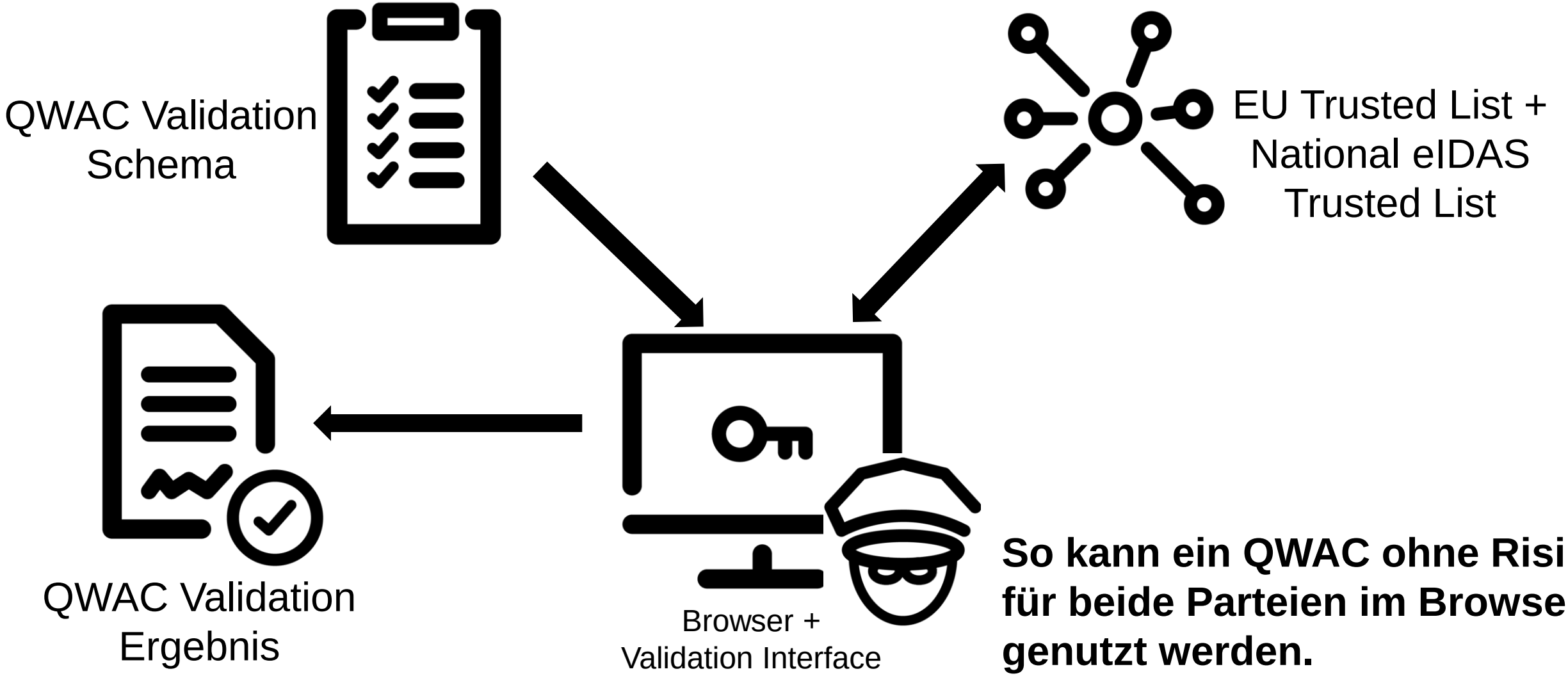
Auf diese Weise könnte ein QWAC im Browser, ohne Risiko für beide Parteien, genutzt werden. Jede Partei behält ihren eigenen Verantwortungsbereich.

Die Integration von QWAC im Browser



Soweit ist alles wie bei einem normalen TLS-Zertifikat.

Die Integration von QWAC im Browser



So kann ein QWAC ohne Risiko für beide Parteien im Browser genutzt werden.

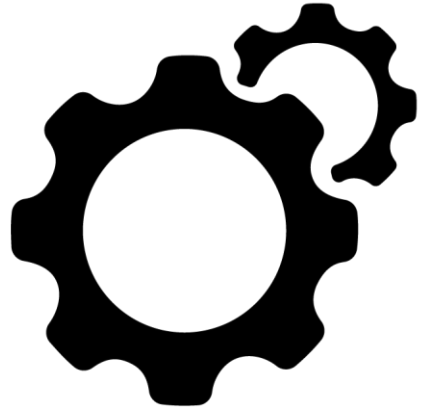
Überprüfung der Zielerreichung für QWAC

- ✓ Users und Zertifikatsinhaber sollen das QWAC im Browser nutzen können
- ✓ Browser sind nicht verantwortlich für das QWAC Prüfergebnis
- ✓ Browser betreiben ihren eigenen Vertrauensraum
- ✓ Die EU behält ihre Souveränität über das QWAC

- ✓ **Auf diese Weise kann ein QWAC im Browser, ohne Risiko für beide Parteien, genutzt werden.**

Take away

- Das Konzept kann dabei helfen, den gordischen Knoten zwischen Browsern und der Nutzung von QWACs zu lösen.
- Das Konzept ist nicht auf die Nutzung von TLS beschränkt und kann auch für andere Zertifikatstypen und Anwendungen genutzt werden.
- Das Konzept erlaubt es Anwendungen, Vertrauensräume zu nutzen, ohne für diese verantwortlich zu sein.
- Dies verleiht Anwendungen ein hohes Maß an Flexibilität und erweitert ihren Anwendungsbereich.



Wir brauchen ein offenes Validierungsinterface für Anwendungen, da …

Die Nutzung von Vertrauensräumen sollte so einfach sein, wie das Reisen mit dem Auto

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

… es in dieser Welt immer unterschiedliche Vertrauensräume geben wird. Anwendungen sollten standardisiert auf unterschiedliche Vertrauensräume zugreifen können.

Vielen Dank!

Enrico Entschew
E-Mail: e.entschew@d-trust.net or enrico.entschew@bdr.de
Telefon:+49 (30) 2598-3070