that unsafe, unverified or out-of-date systems don't connect to a corporate network and provides a cost effective, built in hardware root of trust that can be used to authenticate devices and users.

Addressing Global Demand for Data Security Best Practices

The TPM 2.0 specification responds to the exponential explosion of devices that require protection from cyber threats both inside and outside the traditional enterprise system firewalls. With growing market demand for enhanced security and privacy, TPM 2.0 offers comprehensive protections based on hardware roots of trust. Together with support for upgraded cryptographic algorithms, the TPM 2.0 specification is designed with cryptographic agility to allow support for more algorithms in the future.

Lastly, TPM 2.0 offers the flexibility for industry implementations across a broad range of platforms including servers, desktops, embedded systems, mobile devices and network equipment. In order to accommodate all of these different platforms, the new specification is written in a way that enables TCG to develop platform specific specifications utilizing TPM 2.0 to meet the requirements of their platform.

Hier steht die Spezifkation TPM 2.0 zur Verfügung: http://www. trustedcomputinggroup.org/resources/tpm_library_specification

"Common-elD" für leichtere Nutzbarkeit der Online-Ausweisfunktion

Technologieanbieter im Umfeld elektronischer Identitäten (eID) haben ihre Kräfte im "Common-eID"-Projekt (http://Common-eID.org) gebündelt, um die Interoperabilität in diesem Bereich zu verbessern und dadurch diese wichtige Schlüsseltechnologie noch leichter nutzbar zu machen. Auf Basis der Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sollen systematische Tests mit den Client- und Server-Komponenten der unterschiedlichen Anbieter für das reibungslose Zusammenspiel sorgen.

Online-Ausweisfunktion als wirkungsvolles Mittel gegen Identitätsdiebstahl im Internet

Die jüngst bekannt gewordenen Fälle millionenfachen Identitätsdiebstahls[1] verdeutlichen eindrucksvoll, wie riskant und unsicher
die Passwort-basierte Authentisierung im Internet tatsächlich ist.
Auf der anderen Seite stehen mit der Online-Ausweisfunktion des
Personalausweises und den Authentisierungsfunktionen der weiteren Chipkarten der eCard-Strategie, wie z.B. der elektronischen
Gesundheitskarte, heute bereits sehr sichere und benutzerfreundliche Alternativen für das Login bereit, die nur noch in die im Internet angebotenen Anwendungsdienste integriert werden müssen.

Technische Richtlinien des BSI als Grundlage für interoperable eID-Systeme

Damit die sicheren elektronischen Ausweise leicht mit den verschiedenen Komponenten und Diensten der unterschiedlichen Anbieter genutzt werden können, sind einheitliche Standards und interoperable Implementierungen notwendig. "Mit den auf internationalen Standards basierenden Technischen Richtlinien des BSI existiert eine ausgezeichnete Grundlage für die Realisierung von interoperablen elD-Systemlösungen", so Marc Gurov, CEO der OpenLimit SignCubes AG. "Die Umsetzung dieser Technischen

Richtlinien inklusive der Konformitätstests ist sicherlich notwendig für die Interoperabilität im eID-Bereich, aber möglicherweise auf Grund der hohen Systemkomplexität alleine nicht hinreichend", so Jürgen Ruf, CEO der media transfer AG.

elD-Technologieanbieter starten "Common-elD"-Projekt

Mit dem Ziel den neuen Personalausweis und ähnliche elektronische Ausweise noch leichter in verschiedenen Anwendungen nutzbar zu machen, haben sich die elD-Technologieanbieter ecsec GmbH, Governikus GmbH & Co. KG, media transfer AG und OpenLimit SignCubes AG unter dem Dach des gemeinnützigen TeleTrusT – Bundesverband IT-Sicherheit e.V. zusammengefunden und das "Common-eID"-Projekt gestartet. In diesem Projekt sollen auf Basis der einschlägigen Technischen Richtlinien des BSI systematische Tests mit den Client- und Server-Komponenten der unterschiedlichen Anbieter durchgeführt werden, um das reibungslose Zusammenspiel der unterschiedlichen Systemkomponenten gewährleisten zu können. "Ergänzend zur Umsetzung der einschlägigen BSI-Richtlinien sollen im ,Common-eID'-Projekt zusätzlich systematische Tests mit den verschiedenen Client- und Server-Komponenten der unterschiedlichen Anbieter durchgeführt werden", so Dr. Holger Mühlbauer, Geschäftsführer TeleTrusT - Bundesverband IT-Sicherheit e.V. "Hierdurch wird die Interoperabilität im eID-Umfeld gesteigert und elektronische Ausweise können leichter in Anwendungen genutzt werden, was letztlich für mehr Sicherheit im Internet sorgt."

TeleTrusT-Innovationspreis 2014: Bewerbungen bis 31.08.2014

TeleTrusT ruft zu Bewerbungen für den diesjährigen TeleTrusT-Innovationspreis auf. Einreichungen sind bis 31.08.2014 möglich. Das Bewerbungsformular ist unter http://www.teletrust.de/innovationspreis/teletrust-innovationspreis/ abrufbar.

Seit 1999 verleiht der TeleTrusT – Bundesverband IT-Sicherheit e.V. den "TeleTrusT-Innovationspreis". Der Preis ist für Unternehmen und Institutionen bestimmt, die innovative, vertrauenswürdige und praxistaugliche IT-Sicherheitslösungen für Wirtschaft und Verwaltung entwickelt haben oder selbst einsetzen.

Eine Jury wählt den Preisträger anhand folgender Kriterien aus:

- Ist der Sicherheitslevel dem Schutzbedarf der Anwendung angemessen?
- Sind die Sicherheitsfunktionen integrierter Bestandteil des angebotenen oder genutzten Produktes?
- Sind die integrierten Sicherheitsfunktionen für den Anwender transparent und bedienerfreundlich?
- Ist die Anwendung interoperabel, idealerweise mit europäischer Reichweite?
- Trägt die Anwendung zur wirtschaftlichen Stabilität des Unternehmens bei?

Traditionell wird der Preis im Rahmen der "Information Security Solutions Europe Conference" (ISSE) überreicht.

Die 16. ISSE, ein Gemeinschaftsprojekt der EEMA (European Association for e-Identity and Security) und TeleTrusT, findet am 14. und 15.10.2014 in Brüssel statt, um internationale Experten aus Forschung und Wirtschaft zum fachlichen Austausch über aktuelle IT-Sicherheitsthemen, IT-Sicherheitsszenarien, Studienergeb-