

### macmon TP Nutzen

- > Verbesserung des Sicherheitsstatus durch fälschungssichere Endgeräte-Authentifizierung
- > Hochsicherheitslösung mit Standard-komponenten
- > Einfache Implementierbarkeit
- > Keine Zertifizierungsstelle nötig
- > In Verbindung mit dem Windows BitLocker ist erstmals die Bestätigung der Integrität der Systemkonfiguration gegenüber einem Dritten möglich („remote attestation“).

### \*Trusted Computing Group

Die Trusted Computing Group ist eine non-Profit Organisation der führenden IT-Firmen. Sie entwickelt, definiert und fördert offene, herstellerneutrale Industrie-Standards für das *trusted computing*.

Die Basis ihrer Sicherheitskonzepte ist eine manipulationssichere Hardware-Komponente, zur Härtung gegen Software-basierte Angriffe. Die Sicherheit eines Systems lässt sich so auf die Sicherheit eines Moduls reduzieren.

## Hochsicherheits-Technologie für zuverlässige Geräte-Identifizierung

Die Authentifizierung von Endgeräten im Netzwerk erfolgt heute mit den gängigen Verfahren über MAC-Adresse, Fingerprint oder - bei Einsatz des Standards 802.1X - über ein auf Zertifikaten basierendes System.

Jeder dieser Ansätze bietet einen guten bis sehr guten Grundschutz, allerdings sind diese Verfahren nicht fälschungssicher. Jüngste Angriffe haben gezeigt, dass die Abwehrmechanismen erweitert werden müssen, denn alle aktuellen Verfahren beruhen auf fälschbaren oder kopierbaren Informationen und können auf dem Gerät eines Angreifers überwunden werden.

Ausgangspunkt der Hochsicherheitskomponente macmon TP zur zuverlässigen Geräte-Identifizierung ist das "Trusted Platform Module" (TPM)\*.

### Manipulationssichere Hardware-Komponente

TPM wird bereits von allen namhaften PC- und Notebook-Herstellern in den Produktreihen für professionelle Anwendungen eingebaut. Es handelt sich hier um eine fest mit der Hauptplatine verbundene, auch gegen Hardware-Angriffe geschützte Hardware-Komponente.

Der TPM-Chip enthält einen eindeutigen kryptografischen Schlüssel. Damit wird die sichere Identifizierung eines Rechners, die sogenannte "Platform Authentication", ermöglicht. Darüber hinaus unterstützt der TPM-Chip eine über Prüfsummen erzeugte Aufzeichnung, um bereits beim Ladevorgang des Betriebssystems die Integrität der Betriebssoftware zu validieren ("Integrity Measurement").

### Fälschungssichere Authentifizierung

Die Produktoption **macmon TP** enthält eine Client- und eine Server-Komponente. Die Client-Komponente ist Teil des macmon-Agents. Sie führt zum einen die Initialisierung der TPM-Chips durch und ist zum anderen für die Endgeräte-Authentifizierung durch Signierung von Zufallswerten mit dem TPM-Chip verantwortlich.

Die Server-Komponente von macmon TP übernimmt die Verwaltung der öffentlichen und privaten Schlüssel wie auch die Validierung. Damit das TPM beliebige Daten signieren kann, wird ein non-migratable Signing Key (2048-Bit RSA) erzeugt. Dieses asymmetrische Schlüsselpaar wird zum Signieren von Prüfpaketen genutzt. Non-migratable (nicht migrierbar) bedeutet, dass der so erzeugte Schlüssel nur in Verbindung mit diesem TPM-Chip benutzt werden kann.

Somit wird sichergestellt, dass nur der TPM-Chip Zugriff auf den privaten Schlüsselteil erhält, mit dem er generiert wurde. Der öffentliche Schlüsselteil kann normal exportiert und gehandhabt werden. Damit nicht jede Applikation Daten signieren kann, wird der Schlüssel zusätzlich mit einem Passwort geschützt.

# macmon TP

## PRODUKT-INFORMATION

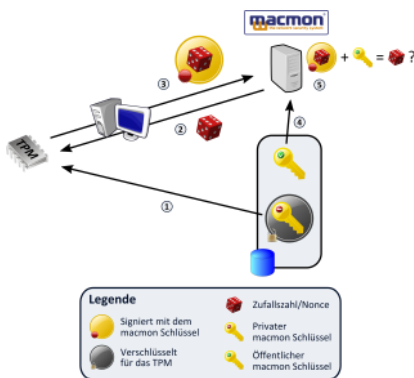


Abb. 1: Ablauf macmon TP

### macmon TP Ablauf

- > 1. Der macmon-Server schickt den privaten macmon-Schlüssel aus der Datenbank zum macmon-Agenten.
- > 2. Der macmon-Server erzeugt eine zufällige Zahl (Nonce) und sendet sie ebenfalls zum Agenten.
- > 3. Der Agent signiert die Nonce mit dem privaten macmon-Schlüssel und sendet die signierte Nonce zum macmon-Server zurück.
- > 4. Der macmon-Server lädt den öffentlichen macmon-Schlüssel aus der Datenbank.
- > 5. Die Signatur wird mit Hilfe des öffentlichen macmon-Schlüssels überprüft.

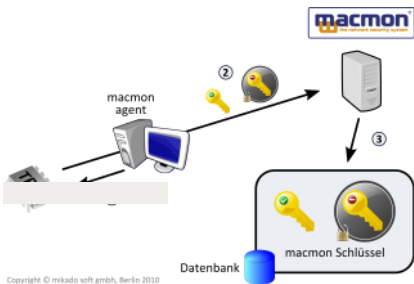


Abb. 2: Speicherung des privaten macmon-Schlüssels

### Zentrale Schlüsselverwaltung

Um ein Gerät eindeutig zu identifizieren, muss macmon den öffentlichen Teil des Schlüssels kennen, mit dem die Signatur angefertigt wird. Neben dem öffentlichen Teil des Schlüssels kann macmon auch für alle Geräte, die sich fälschungssicher im Netz identifizieren sollen, den privaten Teil des „signing keys“ in seiner Datenbank speichern. Da der private Teil nur in Verbindung mit dem TPM-Chip funktional ist, ist die Kenntnis oder der Verlust dieses Schlüssels nicht als sicherheitskritisch zu bewerten.

Im Gegensatz zu anderen Ansätzen wird keine "Public Key Infrastructure" (PKI) zur Erstellung und Verwaltung der Zertifikate benötigt. Die Anforderungen an die Sicherheit des macmon-Servers sind in keiner Weise mit den extrem hohen Sicherheitsanforderungen an die Zertifizierungsstelle einer CA (Certification Authority) vergleichbar.

Der Diebstahl des macmon-Schlüssels durch einen Angreifer ist folgenlos, da das Verfahren nur in Verbindung mit den "richtigen" Endgeräten funktioniert. Der macmon-Schlüssel kann beim ersten Kontakt mit dem macmon-Server erzeugt und in der Datenbank gespeichert werden.

In dieser Produktoption wird das zentrale Management der macmon-Schlüssel von macmon durchgeführt. Eine Identifizierung der Geräte kann nun unabhängig vom installierten Betriebssystem und ohne das erneute Erzeugen von Schlüsseln nach einer Neuinstallation des Betriebssystems erfolgen. Dies wird den administrativen Aufwand für den Betrieb von macmon TP deutlich reduzieren.

macmon TP ist als Option zum System macmon zu erwerben. Es werden die Produktoptionen macmon basic und macmon vlan manager benötigt, die Option macmon client compliance ist Teil der Lizenz macmon TP. Im Client-Bereich werden die Betriebssysteme Windows Vista und Windows 7 unterstützt, Linux ist in Vorbereitung. Die Lizenzierung erfolgt nach Anzahl der abzuschließenden Clients.

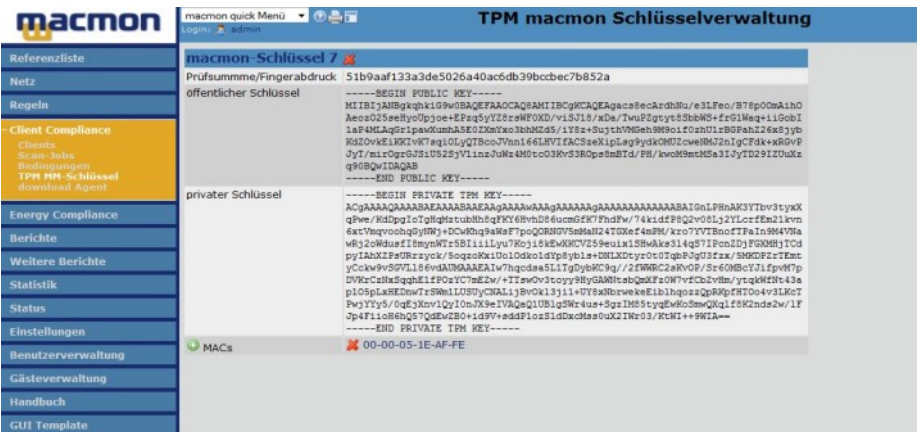


Abb. 3: Management der macmon-Schlüssel