Physikalisch-Technische Bundesanstalt

Braunschweig und Berlin

Stellungnahme zur Frage der Manipulierbarkeit signierter Falldateien

Ausgabe Oktober 2012

Alle mit Digitalkameras ausgestatteten Geschwindigkeitsüberwachungsgeräte und Rotlichtüberwachungsanlagen erzeugen signierte Falldateien. Ziel der Signierung ist es die Authentizität und Integrität der Falldateien zweifelsfrei verifizieren zu können. Diese Anforderung ist ein zentraler Bestandteil der PTB-Anforderungen und ermöglicht es, alle Formen der Manipulation an den Falldateien nachweisen zu können.

Erzeugung signierter Falldateien

Die von Geschwindigkeitsüberwachungsgeräten und Rotlichtüberwachungsanlagen erstellten Digitalfotos werden zusammen mit den Messdaten und ergänzenden Daten in einer so genannten Falldatei zusammengefasst.

Anschließend berechnet das Messgerät einen Hashwert über die gesamte Falldatei. Dieser Hashwert wird danach mit Hilfe eines asymmetrischen Verschlüsselungsalgorithmus‘ (insbesondere RSA) verschlüsselt. Asymmetrische Verschlüsselungsalgorithmen basieren auf einem Schlüsselpaar, bestehend aus einem geheimen und einem öffentlichen Schlüssel. Der geheime Schlüssel wird für die Verschlüsselung des Hashwertes verwendet. Er befindet sich in einer Komponente des Messgerätes und kann nicht ausgelesen werden. Der öffentliche Schlüssel, der zum Entschlüsseln benötigt wird (s.u.), kann am Messgerät abgerufen werden.

Man bezeichnet den verschlüsselten Hashwert der Falldatei als Signatur der Falldatei. Diese Signatur wird an die Falldatei angehängt. Optional darf die signierte Falldatei anschließend mit einem anderen Algorithmus verschlüsselt werden, um die Falldatei aus Gründen des Datenschutzes nur autorisierten Benutzern zugänglich zu machen. Diese optionale Verschlüsselung ist nicht Bestandteil der Zulassung

Auswertung signierter Falldateien

Die signierte Falldatei wird in der Messeinheit bereit gehalten und kann von dort heruntergeladen werden, um sie in der Auswertestelle auszuwerten. Für die Auswertung zeigt das Referenz-Auswerteprogramm die Messdaten, Bilddaten und ergänzenden Daten der Falldatei an. Diese Anzeigen erfolgen nur, wenn zuvor eine erfolgreiche Signaturprüfung durchgeführt wurde.

Für die Signaturprüfung wird neben dem Referenz-Auswerteprogramm und der zu prüfenden Falldatei der zum geheimen Schlüssel zugehörige öffentliche Schlüssel benötigt. Der Eichbeamte registriert bei der Ersteichung eines jeden Messgerätes den zugehörigen öffentlichen Schlüssel. Er ist auch für die Verwaltung der von ihm registrierten öffentlichen Schlüssel verantwortlich. In Zweifelsfällen kann daher ein Gutachter über das zuständige Eichamt rekonstruieren, welcher öffentliche Schlüssel tatsächlich zu dem betrachteten Messgerät gehört.

Der Weg, auf dem Falldatei und zugehöriger öffentlicher Schlüssel in die Auswertestelle gelangen, ist nicht entscheidend für die Signaturprüfung. Für die unterschiedlichen Geschwindigkeits-

Hausadresse, Lieferanschrift:
Bundesallee 100
38116 Braunschweig
DEUTSCHLAND

Telefon (Zentrale): 0531 592-0
Telefax (Zentrale): 0531 592-9292
E-Mail (Zentrale): poststelle@ptb.de
Internet: http://www.ptb.de

Achtung! Neue Bankverbindung:
Deutsche Bundesbank
Filiale Halle (BBk Halle)
Kto-Nr.: 800 010 20 BLZ: 800 000 00
IBAN: DE 58 80000000 0080001020
BIC: ZBNS DE 21800
VAT-Nr.: DE 811 240 952

PTB Berlin-Charlottenburg
Abbestraße 2-12
10587 Berlin
DEUTSCHLAND

überwachungsgeräte und Rotlichtüberwachungsanlagen haben die Hersteller verschiedene Wege realisiert.

Details der Signaturprüfung

Nachdem die optional verschlüsselte Falldatei entschlüsselt wurde, wird mit dem öffentlichen Schlüssel die Signatur der Falldatei entschlüsselt. Man erhält damit den Sollhashwert der Falldatei. Anschließend wird ein Hashwert über die Falldatei berechnet. Nur wenn dieser neu berechnete Hashwert mit dem in der Signatur enthaltenen Sollhashwert übereinstimmt, ist die Signaturprüfung erfolgreich. Eine erfolgreiche Signaturprüfung garantiert, dass die Falldatei von der betrachteten Messeinheit stammt (Authentizität) und unverfälscht vorliegt (Integrität). Das Ergebnis der Signaturprüfung wird dem Auswerter auf der grafischen Benutzeroberfläche des Referenz-Auswerteprogramms dargestellt. Nähere Hinweise dazu sind der jeweiligen Gebrauchsanweisung zu entnehmen.

Das hier beschriebene Auswerteverfahren ist Teil des standardisierten Messverfahrens und kann in Zweifelsfällen mit Hilfe des Referenz-Auswerteprogramms jederzeit wiederholt werden. Nur die signierte Falldatei gilt als unveränderliches Beweismittel. Ein Ausdruck des Inhalts der signierten Falldatei oder ein Ausdruck der grafischen Benutzeroberfläche des Referenz-Auswerteprogramms gelten nicht als unveränderliches Beweismittel.

Auf Grund der hier vorgestellten Sicherung der Authentizität und Integrität der Falldatei werden alle Manipulationen an Falldateien zweifelsfrei erkannt.