Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Nationales Metrologieinstitut

http://dx.doi.org/10.7795/520.20160913F (Fassung vom 20.12.2013)

Stellungnahme zur Frage der Manipulierbarkeit signierter Falldateien[1]

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 Signaturprüfung wird neben dem zugelassenen 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.

[1] *Zitiervorschlag für die Quellenangabe:*
Stellungnahme zur Frage der Manipulierbarkeit signierter Falldateien. Stand: 20. Dezember 2013 / Physikalisch-Technische Bundesanstalt, Braunschweig und Berlin. DOI: 10.7795/520.20160913F

Verfügbar unter: *http://dx.doi.org/10.7795/520.20160913F*

Eine zweite Möglichkeit für die korrekte Zuordnung des öffentlichen Schlüssels zum betrachteten Messgerät bietet das Abrufen (d. h. Herunterladen oder Anzeigen) des öffentlichen Schlüssels am geeichten Messgerät selbst. Beide Methoden – Abrufen des öffentlichen Schlüssels am Messgerät oder beim Eichamt – werden als „Direct Trust“ bezeichnet.

Liegen nun öffentlicher Schlüssel und signierte Falldatei vor, so kann mit dem Referenz-Auswerteprogramm die Signaturprüfung durchgeführt werden. Nach einer erfolgreichen Signaturprüfung sind Authentizität und Integrität der Falldatei sichergestellt und das Referenz-Auswerteprogramm stellt die Messdaten, Bilddaten und ergänzenden Daten der Falldatei dar.

Der Weg, auf dem Falldatei und zugehöriger öffentlicher Schlüssel in die Auswertestelle gelangen, ist nicht entscheidend für die Signaturprüfung. Für die unterschiedlichen Geschwindigkeits-überwachungsgeräte und Rotlichtüberwachungsanlagen haben die Hersteller verschiedene Wege realisiert.

Zusammenfassend bleibt festzuhalten, dass alle Manipulationen an einer signierten Falldatei zweifelsfrei erkannt werden können, wenn das zugelassene Referenz-Auswerteprogramm und der zum geheimen Schlüssel zugehörige öffentliche Schlüssel des Messgerätes verwendet werden.

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 dem betrachteten Messgerät 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.

Manipulationsmöglichkeiten und deren Entdeckung

Auf dem Weg der Falldatei zwischen Messgerät und Auswertestelle ergeben sich theoretisch zwei Manipulationsmöglichkeiten, die bereits bei der Erteilung der Bauartzulassung berücksichtigt wurden:

1. Der Dateiinhalt oder die Signatur werden gezielt oder zufällig (bei Kopier- und/oder Speichervorgängen) verfälscht.

2. Der Dateiinhalt wird gezielt verfälscht und dabei zusätzlich auch die Signatur an den verfälschten Dateiinhalt entsprechend angepasst.

Im ersten Fall sorgt das von der PTB zugelassene Referenz-Auswerteprogramm dafür, dass derartig manipulierte Daten nicht zur Anzeige gelangen, da die Signaturprüfung dies zuverlässig verhindert.

Während das im ersten Fall geschilderte Manipulationsszenario für Personen mit hohem technischen Sachverstand noch durchführbar erscheint (wenn auch ohne Erfolg, da das Referenz-Auswerteprogramm dies wie erwähnt ja nicht unentdeckt ließe), bleiben die im zweiten Fall skizzierten Angriffsszenarien Personen mit dem Niveau eines Informatikers vorbehalten. So wird in zweifelhaften Gutachten seit dem Jahre 2011 die folgende Vorgehensweise praktiziert: Entfernung der vom Messgerät gebildeten Signatur aus der Falldatei, Durchführung einer Manipulation mit Bildung einer neuen Signatur, Anhängen der neuen Signatur an die manipulierte Falldatei. Am Ende eines solchen Gutachtens wird immer demonstriert, dass das Referenz-Auswerteprogramm die falsche Signatur und damit auch weitere Manipulationen (z.B. Änderung des Messwerts) an der Falldatei nicht erkennt. Gern wird von den Sachverständigen aber verschwiegen, dass in einem solchen Fall für die Signaturprüfung nicht der zum betreffenden Messgerät zugehörige öffentliche Schlüssel verwendet werden kann. Vielmehr ist für die Bildung und Prüfung der manipulierten Signatur ein eigenes Schlüsselpaar nötig.

Den Auswertestellen sind die öffentlichen Schlüssel aller verwendeten Messgeräte bekannt, so dass es ihnen durch eine einfache Überprüfung des verwendeten öffentlichen Schlüssels jederzeit möglich ist, die durchgeführte Manipulation zu enttarnen.

Schlüssellängen

Bei jeder Erstzulassung eines Geschwindigkeitsüberwachungsgerätes bzw. einer Rotlicht-überwachungsanlage, oder einer Neuzulassung einer kryptografischen Komponente eines dieser Messgeräte wird geprüft, dass das vorgestellte Messgerät dem aktuellen – vom Bundesamt für Sicherheit in der Informationstechnik (BSI) definierten – Stand der Technik entspricht. Auch wenn die zum Zeitpunkt der Erstzulassung gewählten Schlüssellängen heute nicht mehr dem aktuellen Stand der Technik entsprechen, so bestehen auf Grund der Qualität der verwendeten Verschlüsselungs-algorithmen (insbesondere RSA) keine Bedenken hinsichtlich der Manipulationssicherheit der signierten Falldateien.

Hash-Algorithmen

Das BSI hat von der Verwendung bestimmter Hash-Algorithmen abgeraten. Der Grund hierfür ist, dass es möglich ist, zwei Dateien mit unterschiedlichem Inhalt zu erzeugen, die denselben Hashwert besitzen (eine sogenannte Kollision). Das heißt aber nicht, dass man von einer beliebigen vorhandenen signierten Datei einfach ein Duplikat mit gezielten Verfälschungen erzeugen kann. Es ist vielmehr erforderlich, dass das Original eine gewisse Struktur und gewisse Inhalte aufweisen muss, damit eine solche Fälschung überhaupt gelingen kann. Der Fälscher muss also sowohl das Original als auch die Fälschung verändern können, um eine Kollision zu erzeugen. Deshalb wird vom BSI auch

http://dx.doi.org/10.7795/520.20160913F

klargestellt, dass die Fälschung einer bereits signierten Datei nicht möglich ist. Übertragen auf Geschwindigkeitsüberwachungsgeräte und Rotlichtüberwachungsanlagen bedeutet dies, dass Falldateien, die vom Messgerät signiert wurden, nachträglich nicht durch Kollision gefälscht werden können. Dass der Fälscher vor der Signierung in den Besitz der Falldateien kommt, ist ausgeschlossen, weil sich diese im Innern des Messgerätes befinden. Der Zugang ist durch diverse Sicherungsmaßnahmen verhindert. Der Zugang wäre nur unter Verletzung der eichtechnischen Sicherungen möglich.

Sowohl die Softwareexperten der PTB, als auch die Fachleute des BSI verfolgen die Entwicklungen auf den Gebieten der Informationstechnik und Kryptografie mit größter Aufmerksamkeit. Bereits bei sich abzeichnenden ernsthaften Bedenken bezüglich der Manipulationssicherheit signierter Falldateien würde die PTB die Initiative ergreifen, um gemeinsam mit dem BSI und dem betreffenden Zulassungsinhaber geeignete Abwehrmaßnahmen zu ergreifen. Die Sicherheit bestehender Regelungen bestätigt die PTB hiermit gern nochmals ausdrücklich.