GUTACHTEN

Beurteilung des efsta (European Fiscal Standards Association) – Verfahrens aus Informationssicherheitssicht (Datensicherheit und Datenschutz)

University of Applied Sciences – Upper Austria

Fakultät für Informatik, Kommunikation und Medien
Campus Hagenberg, Fachhochschule Oberösterreich

Department für Sichere Informationssysteme

Prof. Dipl.-Ing. Dr. Jürgen Fuß

Ass.-Prof. Dieter Vymazal, M.Sc.

Hagenberg, 03.07.2013

PRÄAMBEL

Das vorliegende Gutachten bezieht sich auf das im efsta-Konzeptdokument „Informationssicherheit im efsta Fiskalsystem“ vom 6.5.2013 beschriebene Verfahren.

ZIELSETZUNG

efsta ist konzipiert als ein Verfahren zur Dokumentation und Archivierung von Geschäftsvorgängen. Eine Softwarekomponente (Register) registriert Transaktionen und meldet diese an ein zentrales Archiv (Cloud). Vom Register wird eine eindeutige Identifikationsnummer (Fiskalnummer) vergeben, über welche eine Überprüfung (Einzelnachweis) im Archiv möglich ist. Daten im Archiv können nicht nachträglich verändert werden. Zur Prüfung der Geschäftsdaten kann Prüfern die Berechtigung (Ticket) zum Lesen einzelner oder aller Datensätze erteilt werden.

Auf diese Weise soll sichergestellt werden, dass:

1. eingemeldete Daten nicht nachträglich vom Besitzer der Daten verändert werden können,
2. Daten nur nach Autorisierung durch den Besitzer der Daten gelesen werden können und
3. auf Rechnungen ausgewiesene Beträge unverändert im Archiv gemeldet werden.

ANFORDERUNGEN

Das Register soll als reine Softwarekomponente realisiert werden. Das bedeutet, dass

1. das Register vom Administrator des Systems, auf dem es läuft, beliebig verändert werden kann. Insbesondere ist es möglich, das Register komplett durch andere Software zu ersetzen;
2. Registerdaten (bspw. Schlüsselmaterial) ausgelesen kann, wenn Zugriff auf das System erlangt wird; insbesondere können Register dann geklont werden.

Das Archiv soll als Cloud-Service realisiert werden. Das bedeutet, dass

1. die Verfügbarkeit des Archivsystems und die Integrität der Daten vertraglich sichergestellt werden müssen;
2. weder die Besitzer der Daten noch die Betreiber des efsta-Systems Kontrolle darüber haben, wo die Daten liegen.

BEURTEILUNG

REGISTER

Register sind als ein Dienst konzipiert, der Daten zu jedem Geschäftsfall von der Kasse übernimmt und der sicheren Archivierung zuführt. Für das efsta-Konzept wird davon ausgegangen, dass Kassen und Register unter der Kontrolle des Kassenbesitzers sind, Modifikationen dieser Komponenten können erfolgen, dürfen sich jedoch nicht auf die Konsistenz, Vertraulichkeit und Unveränderbarkeit der archivierten Daten auswirken.

CLOUD-DIENSTE

In der Cloud gespeicherte Datensätze sind ausnahmslos verschlüsselt. Das Lesen der Daten ist nur bei Kenntnis des entsprechenden Schlüssels möglich. Die Schlüssel werden nur lokal im Browser der berechtigten Benutzer und nicht in der Cloud verwendet.

Damit ist sichergestellt, dass vom Cloudbetreiber keine Daten gelesen werden können. Andererseits übernimmt der Cloudbetreiber die Archivierung der Daten und das Logging aller Transaktionen; weiterhin können Daten in der Cloud durch User nur geschrieben, aber nicht verändert werden.

KOMMUNIKATION

Register kommunizieren mit dem Cloud-Service über TLS[1] mit Client Authentication.

Initialisierung: Am Register wird im Zuge der Initialisierung ein Schlüsselpaar erzeugt, der öffentliche Schlüssel wird an das Cloud-Service übertragen. Dazu wird eine TLS-gesicherte Verbindung mit serverseitiger Authentifizierung verwendet. Im Client-Zertifikat ist die vom Cloud-Service vergebene Register Access Number (RAN) angeführt, die zur Prüfung der Authentizität des Registers herangezogen wird.

VERSCHLÜSSELUNG DER DATEN

Transaktionsdatensätze

Die Verschlüsselung der Transaktionsdatensätze erfolgt symmetrisch mit dem Verschlüsselungsalgorithmus AES[2]. Als Verschlüsselungsmodus wird AES-CCM[3] eingesetzt. Dieses Verfahren gewährleistet Integrität, Authentizität und Vertraulichkeit der verschlüsselten Daten; Lesen und unbemerkte Veränderung der gespeicherten Daten können dadurch verhindert werden.

Schlüsseldatensätze

Die Schlüssel zur Entschlüsselung der archivierten Datensätze werden von einem Periodenschlüssel abgeleitet, der monatlich wechselt und mit dem Public Key des Datenbesitzers RSA-verschlüsselt in der Cloud abgelegt wird. Als Verschlüsselungsmethode kommt RSA nach PKCS#1v2.1[4][5] zum Einsatz. Die Erzeugung der DataKeys aus dem Periodenschlüssel erfolgt durch vielfaches Verarbeiten des Periodenschlüssels mit einem HMAC[6] unter Verwendung des sog. Period Modifier (PM) als Schlüssel. Auf diese Art und Weise können aus auf einem kompromittierten Register gespeichertem Schlüsselmaterial keine bereits verwendeten Schlüssel abgeleitet werden. Diese Konstruktion erlaubt insbesondere die

---

[1] RFC 5246. The Transport Layer Security (TLS) Protocol Version 1.2, 2008. https://tools.ietf.org/html/rfc5246

[2] Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001.

[3] RFC 3610. Counter with CBC-MAC (CCM), 2003. http://tools.ietf.org/html/rfc3610

[4] RFC 3447. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, 2003. http://tools.ietf.org/html/rfc3447

[5] RSA Laboratories: PKCS #1 v2.1: RSA Cryptography Standard, 2002. https://www.rsa.com/rsalabs/node.asp?id=2125

[6] RFC 2104. HMAC: Keyed-Hashing for Message Authentication, 1997. http://www.ietf.org/rfc/rfc2104.txt

Weitergabe von DataKeys für einzelne Transaktionen. Darüber hinaus können die Schlüssel für alle Datensätze einer Periode durch Freigabe der Periodenschlüssel einfach weitergegeben bzw. verschlüsselt in der Cloud gespeichert werden.

Datenbankschlüssel für Einzelnachweise und Attachmentdatensätze

Für Einzelnachweise wird in einem zweistufigen Verfahren aus Fiskalnummer (FN) und Rechnungsbetrag ein eindeutiger Datenbankschlüssel erzeugt. Dadurch wird sichergestellt, dass durch Einzelnachweisanfragen keine Umsatzstatistiken für Register erstellt werden können.

Die Datenbankschlüssel für Attachmentdatensätze werden als HMACs über FN und Attachment-Typ mit PM als Schlüssel berechnet. Auf diese Weise ist sichergestellt, dass auch aus diesen Werten kein Rückschluss auf den PM möglich ist.

FAZIT

Die im Konzept efsta eingesetzten Verfahren entsprechen dem aktuellen Stand der Technik auf dem Gebiet der Datensicherheit.

Eine sichere Implementierung und regelmäßige Auditierung und Wartung der Komponenten vorausgesetzt erlaubt das vorliegende Konzept die sichere Umsetzung eines Archivierungssystems für Geschäftsfälle. Die Vertraulichkeit der archivierten Daten bzw. der kontrollierte Zugriff auf diese Daten können sichergestellt werden. Die Unveränderbarkeit der archivierten Daten sowie deren Verfügbarkeit kann durch entsprechende Policies beim Cloudprovider sichergestellt werden.