Das BMF gibt folgende Information zur Registrierung von Registrierkassen über FinanzOnline bekannt:

Um Fehleingaben bei der Erfassung von AES-Schlüsseln bei der Registrierung von Registrierkassen über FinanzOnline vermeiden zu helfen, führt das BMF ein Prüfwertverfahren für die Erfassung der AES-Schlüssel über FinanzOnline ein, das ab Ende August 2016 zur Verfügung stehen wird. Das Prüfwertverfahren ist optional und besteht aus einem vierstelligen Prüfwert, der nach vorgegebenen Regeln (Berechnungsalgorithmus) aus dem AES-Schlüssel ermittelt werden kann. Wird der Prüfwert nach dem selben Berechnungsalgorithmus auch von der Registrierkasse ermittelt und vom Unternehmer zusätzlich zum AES-Schlüssel über FinanzOnline erfasst, stellt FinanzOnline durch eine Vergleichsrechnung sicher, dass der AES-Schlüssel fehlerfrei über FinanzOnline erfasst wurde.

Hinweis für Softwaretechniker: die Verwendung des SHA256-Hash-Wertes begründet sich in der Tatsache, dass die Kassensoftware die dafür benötigten Softwarebibliotheken bereits im Einsatz hat. Auch die Extraktion von einer gegebenen Anzahl von Bytes aus dem berechneten Hash-Wert muss bereits im Rahmen der RKSV-konformen Umsetzung vorhanden sein. Die Aufwände für die Implementierung sollen damit minimal gehalten werden.

Berechnungsalgorithmus Prüfwert für AES-Schlüssel:

1. **Eingabewerte**:
    a. **base64AESKey**: BASE64-kodierter AES Schlüssel, mit dem die Kasse initialisiert wurde und der im FinanzOnline gemeldet werden soll.
    b. **N**: Die Anzahl der Bytes, die vom Hash-Wert extrahiert werden. Es wird **N=3** festgelegt.
2. **Berechnung der Prüfsumme**:
    a. Hashberechnung: SHA256-Hash-Wert-Berechnung von **base64AESKey** ➔ **sha256hash** (Byte Array der Länge 32)
    b. Extraktion der ersten **N** Bytes aus **sha256hash** ➔ **sha256hashNbytes** (Byte Array der Länge **N**)
    c. BASE64-Kodierung von **sha256hashNbytes** ➔ **base64sha256hashNbytes**
    d. Entfernen aller „=“ Zeichen aus **base64sha256hashNbytes** ➔ **valSumCalc**
3. **Output:**
    a. **valSumCalc:** Prüfwert der vom Unternehmer im FinanzOnline eingegeben werden kann. FinanzOnline verwendet den gleichen Algorithmus für die Berechnung des Prüfwerts und informiert den Unternehmer, wenn der berechnete und der eingegebene Wert nicht identisch sind.

Code-Snippet, **N=3**.

```
public static boolean checkValSum(int N, String base64AESKey, String userCheckSum) throws
NoSuchAlgorithmException {
```

```
    String calculatedCheckSum = calcCheckSumFromKey(base64AESKey, N);
    return calculatedCheckSum.equals(userCheckSum);
}

public static String calcCheckSumFromKey(String base64AESKey, int N) throws NoSuchAlgorithmException {
    MessageDigest md = MessageDigest.getInstance("SHA-256");

    byte[] sha256hash  = md.digest(base64AESKey.getBytes());
    byte[] sha256hashNbytes = new byte[N];

    System.arraycopy(sha256hash , 0, sha256hashNbytes, 0, N);

    String base64sha256hashNbytes = CashBoxUtils.base64Encode(sha256hashNbytes, false);
    String valSumCalc = base64sha256hashNbytes.replace("=", "");

    return valSumCalc;
}
```