Revisionssichere Archivierung mit sonoGDT

Eine revisionssichere Archivierung ist für Ultraschallbilder nicht vorgeschrieben, Sie müssen diese lediglich 10 Jahre aufbewahren, um der KV auf Anfrage nachweisen zu können, dass eine abgerechnete Untersuchung auch stattgefunden hat. Dazu genügt es, die Bilder in einem üblichen Format einzureichen. sonoGDT speichert die Bilder als JPG-Grafiken und erfüllt damit diese Anforderung. Dennoch können Sie mit sonoGDT ab Version 22.0 die revisionssichere Archivierung aktivieren und damit später nachweisen, dass ein Bild ab dem Zeitpunkt seiner Aufnahme nicht verändert wurde. Im Folgenden wird erklärt, auf welche Weise dieser Nachweis erbracht wird.

Jede Bilddatei wird im sonoGDT-Bildarchiv unter der Patientennummer abgelegt. Gleichzeitig wird in der Datei **..\Bildarchiv\Hashes\Hashes.ini** ein SHA256-Hash dieser Bilddatei gespeichert. Ein solcher Hash ist eine 64-stellige Zahl, welche mit anerkannten kryptographischen Verfahren gebildet wird und für jede Datei einzigartig ist. Solange eine Datei unverändert ist, wird eine erneute Anwendung dieses Verfahrens immer wieder den gleichen Hash erzeugen. Er ist damit wie ein Fingerabdruck geeignet, eine Datei eindeutig zu identifizieren.

Der wesentliche Inhalt der Textdatei mit den Hashes zweier Beispielbilder könnte so aussehen:

```
[Hashvalues]
20200725_193317:0000000001__20200725-193315_11.jpg=14f776e53cc485698e1ddfdc03794ad2945715d5fa5362f9f16b48b44f2bdc87
20200725_193318:0000000001__20200725-193316_12.jpg=633472e79b96b6e311ea1b5e9054bc099c3d0b35d126dc001e43f548faf87465
```

Das Format ist leicht zu erkennen:

```
Datum___Uhrzeit:Dateiname____________________.jpg=64-stelliger Hashwert________________________________________
```

Wird zu einem späteren Zeitpunkt der Nachweis gefordert, dass eine der Dateien nicht manipuliert wurde, dann müsste man lediglich den SHA256-Hash für das angezweifelte Bild erneut bilden und mit dem gespeicherten Wert vergleichen. Ist der Fingerabdruck identisch, wurde die Datei nicht verändert.

Da diese Fingerabdrücke in einer Textdatei gespeichert sind, wäre es allerdings einfach, ein Bild unbemerkt zu manipulieren, man müsste danach lediglich den in der Datei gespeicherten Fingerabdruck durch den neuen Fingerabdruck des manipulierten Bildes austauschen und keiner würde etwas merken.

Um das auszuschließen, wird in regelmäßigen Abständen aus dieser Textdatei ein PDF-File erzeugt, die Werte werden also ‚fixiert'. Danach wird die Textdatei geleert, um die Fingerabdrücke der nächsten zu speichernden Bilder aufzunehmen. Ist der eingestellte Turnus (z.B. nach 14 Tagen) erreicht, wird auch diese neue Textdatei wieder in ein PDF-gewandelt und anschließend geleert. So entstehen nach und nach PDF-Dateien, die die jeweiligen Fingerabdrücke der Bilder eines Zeitraumes zwischen ‚Fixierungen' enthalten.

Nun könnte man auch ein PDF nachträglich verändern. Um dies auszuschließen, wird auch von diesem PDF-File ein Hashwert gebildet und als erster Wert in der leeren Textdatei, welche die Fingerabdrücke der künftigen Bilder aufnehmen wird, gespeichert. Spätestens wenn diese Textdatei später wieder zu einem PDF gewandelt wird, ist auch dieser Hashwert nicht mehr manipulierbar.

Sie haben also in jedem PDF-File den Nachweis, dass die jeweils zuvor erzeugte PDF-Datei unverändert ist, bis hin zur ersten erzeugten PDF-Datei.

Zweifelt nun jemand die Unverändertheit eines vor 3 Jahren erstellten Bildes an, kann er mit öffentlich zugänglichen Tools den Hash dieses Bildes erstellen und mit dem im damaligen PDF gespeicherten Hash vergleichen. Gleichzeitig kann er in allen darauf folgenden PDF-Dateien nachweisen, dass die Inhalte im jeweils vorhergehenden PDF nicht manipuliert wurden.

Dieses Verfahren wurde aus der Blockchain-Technologie bekannt und gilt, trotz aller hypothetischen Manipulationszenarien, als sicher, da der zeitliche Aufwand für eine rückwirkende Manipulation aller Dateien zu groß wäre.