# Lastenheft CryptDiary

Im Open-Source-Bereich gibt es bis jetzt keine Tagebuch-Software, die es einem erlaubt, die Inhalte in verschlüsselter Form abzulegen. Da es sich bei Tagebuch-Einträgen grundsätzlich um sehr sensible Informationen handelt, verbietet sich der Einsatz von Closed-Source-Software quasi von selbst. Daher habe ich mich entschlossen, mich dieses Problems anzunehmen und nach dem Vorbild von RedNotebook eine Tagebuch-Software zu entwickeln, die als Kernfunktionalität die verschlüsselte Ablage der Einträge anbietet. Sobald das umgesetzt ist, kann die Software beliebig mit weiteren Komfort-Funktionen erweitert werden.

## Kernfunktionalitäten

* Die Tagebuch-Einträge werden als XML-Dateien abgelegt, je eine XML-Datei pro Tag, Header-Informationen wie Datum, Uhrzeit etc. bleiben unverschlüsselt, die Eintrags-Inhalte werden AES-256-verschlüsselt abgelegt.
* Der Benutzer muss beim Öffnen des ersten Beitrags sein Kennwort eingeben, dieses bleibt zur Laufzeit im Speicher und wird später zum Verschlüsseln der Einträge benutzt.
* Nach einer Inaktivitätszeit (einstellbar) wird das Tagebuch geschlossen oder in einen gesperrten Zustand versetzt (PW wird aus Speicher entfernt) und muss durch Wiedereingabe des Passworts reaktiviert werden.
* Der Benutzer kann in den Optionen die Anzahl der Iterationen für die Schlüsselerzeugung einstellen, um Brute-Force-Angriffe zu erschweren. Eine eingebaute Stoppuhr hilft ihm dabei, einen vernünftigen Wert zu finden (Vorbild KeePass). Dieser Iterationswert muss auch in den XML-Dateien gespeichert werden, dass sonst frühere Einträge nach Ändern der Option nicht mehr geöffnet werden können.
* Eine Kalenderfunktion sowie Next- ,Previous- und Today- Buttons erlauben das Navigieren zwischen den Einträgen.

## Benutzeroberfläche

* RichTextBox, in der die Einträge geschrieben und gelesen werden.
* MonthCalendar, auf dem Daten mit hinterlegten Einträgen farblich oder mit Fettdruck markiert werden.
* Vor-, Zurück- und Today-Button, um zwischen den Einträgen zu blättern.
* Lock-Button, um das Tagebuch in einen gelockten Zustand (bei kurzfristiger Abwesenheit) zu versetzen, dann wird die TextBox ausgeblendet
* Menü-Leiste: Laden und Speichern, Optionen, (Statistik), About. Mehr ist glaube ich nicht notwendig.

## Zusatzfunktionalitäten

* Statistikfunktion: Anzahl der Wörter, Sätze, Absätze pro Beitrag. Durchschnitt über alle Beiträge. Durchschnittliche Zeit zw. den Beiträgen. Bevorzugte Wochentage. Was einem noch so einfällt. Zu überlegen ist, ob die dafür nötigen Informationen im Klartext in den XML-Dateien der Beiträge stehen oder auch verschlüsselt in einer separaten Datei. Spontan bevorzuge ich letzteres.
* Tagging-Funktion: Man kann Stichworte in seinen Einträgen mittels #Hashtag taggen und sich später Einträge nach diesen Hashtags filtern lassen. Dafür könnte man ein Dictionary<string, datetime[]> verwenden. Sobald ein Tag gesetzt wird, wird im Dictionary danach gesucht und das entsprechende Datum dem eventuell vorhandenen Eintrag hinzugefügt, ansonsten ein neuer Eintrag im Dictionary angelegt.
* Wortwolke: Die am meisten benutzten Worte werden in einer Wortwolke dargestellt, die Schriftgröße proportianal zur relativen Häufigkeit. Steht prioritätsmäßig ganz ganz hinten, da man sehr viele Wörter ausfiltern müsste, um zu einem sinnvollen Ergebnis zu kommen.
* Cloud-Anbindung/Backup: Die Xml-Dateien können noch einmal zusätzlich in einen verschlüsselten Container geworfen werden und dann an anderer Stelle oder z.B. bei GoogleDrive gesichert werden.