Kanton St.Gallen
Staatskanzlei

Recht und Legistik
Dienst für politische Rechte

Anhang 14
Backup und Löschung der Daten

V1.0

Inhaltsverzeichnis

1 Einleitung

Das vorliegende Dokument definiert das Backup der Daten und die Löschung der sensiblen Daten. Es macht zudem detailliertere Angaben zur Architektur der Datenhaltung als die anderen Dokumente, da das Backup und das Löschen der Daten gewisse Eigenschaften voraussetzen. Die Darstellung folgt den Systemanforderungen in Anhang 6. Die Verweise auf bspw. «K36» beziehen sich ebenfalls auf die Nummerierung in Anhang 6.

2 K36 Separates verschlüsseltes Backup

Die Datenhaltung geschieht mit Vorteil in einer relationalen Datenbank. Wird ein alternatives Modell gewählt, so bleiben die an eine relationale Datenbank gestellten Anforderungen bestehen.

Neben den üblichen Fähigkeiten einer relationalen Datenbank sind explizit die Folgenden, je nach System fortgeschrittenen Fähigkeiten nötig:

- Möglichkeit gesamte Datenbank für das Backup als SQL Dump zu exportieren. Gibt es Konfigurationsoptionen etc., die nicht Teil des Dumps sind, so müssen sie doch auf die eine Art und Weise exportierbar und bei einem Restore wieder lesbar sein.
- Trigger und Stored Procedures, welche es erlauben, das Erstellen von Tabellen und Views aus einer Online Applikation heraus zu initiieren.
- Umfassendes Rollenkonzept, welche es namentlich erlaubt, einzelnen Usern zu erlauben Tabellen zu erstellen und zu löschen und den Zugriff auf diese Tabelle einzuschränken.

Pro Unterschriftensammlung werden die sensiblen Daten in einem eigenen Datenbestand geführt. Diese Datenablage wird als separate Tabelle in einer relationalen Datenbank implementiert.
Für das Backup müssen die verschiedenen sensiblen Tabellen derselben Datenbank seriell einzeln gesichert werden. Das wird automatisiert. Das Backup der übrigen Tabellen mit unsensiblen Daten wird entweder auch selektiv auf Stufe Tabelle durchgeführt oder die sensiblen Tabellen werden aus dem kompletten Datenbank-Backup herausgelöscht. Auch das wird automatisiert.

3 K37 Vorbereitung von verschlüsselbaren Datenablagen

Die Datenablage, respektive Tabelle zur Datenablage, muss zu einem gegebenen Zeitpunkt erstellt werden. Zur Erstellung der Datenablage gehört auch das Erstellen eines spezifischen Schlüsselpaares für die Public-/Private-Key Verschlüsselung des Backups. Die Schlüssel müssen ab diesem Moment manuell in die Schlüsselverwaltung überführt und gesichert werden. Die Erstellung der Datenablage muss interaktiv ausgelöst und das neue Schlüsselpaar manuell gesichert werden.

Die Vorbereitung von verschlüsselten Datenablagen ist damit von der Einrichtung eines Begehrens entkoppelt.

Das System erlaubt es der Staatskanzlei, inaktive Datenablagen und zugehörige Schlüssel vorzubereiten. Bei der Einrichtung eines Begehrens (durch die Staatskanzlei, eine Gemeinde oder ein Komitee) wird jeweils eine dieser vorbereiteten Datenablagen aktiviert und automatisch an das neue Begehren angebunden. Das Schlüsselpaar liegt bereit und ist bereits mit der nun aktivierten Datenablage verbunden. Das Backup funktioniert also ohne weiteres Zutun.

4 K38 Generierung der Schlüssel

Zum Schlüsselpaar pro Datenablage gehört ein Public- und ein Private-Key. Der Public-Key wird zur Verschlüsselung der Backups benötigt und idealerweise in der Datenbank selbst als Teil der unsensiblen Daten abgelegt. Der Private-Key wird dem gegenüber nur beim Restore der Daten eingesetzt.
Beim Erstellen der Datenablage für die Unterschriftensammlung wird auch das zugehörige Schlüsselpaar generiert. Dieses wird aus der Applikation heraus direkt in den lokalen Keystore auf USB Stick geschrieben. Idealerweise wird mehr als ein USB-Stick geschrieben und damit ein Backup miterstellt.

5 K39 Zukünftiger Ersatz der Verschlüsselungsalgorithmen

Es ist denkbar, dass die Verschlüsselung der Backups zukünftig gebrochen werden könnte (Post-Quantum-Kryptographie). Die Verschlüsselungsalgorithmen müssen deshalb – sobald dies absehbar wird – rechtzeitig ersetzt werden können. Das System ist auf dieses mögliche Update hin aufzubauen.

6 K40 Rollenteilung bei der Verwaltung der Backups und Schlüssel

Bei einem Restore der gebackupten Daten wird zunächst die Datenbank mit den unsensiblen Daten als Basis restoriert. Danach werden die einzelnen Datenablagen mit den verschlüsselten Daten entschlüsselt und hinzugefügt. Zur Entschlüsselung ist der Private-Key nötig der zu diesem Zweck übermittelt oder als Kopie übermittelt und nach dem Restore wieder gelöscht werden muss. Wichtig ist bei einer Übermittlung über einen sicheren Kanal, dass der Private-Key nicht plötzlich in einem Email-Backup archiviert wird.
Nach dem Restore muss zwingend sichergestellt werden, dass die übermittelte Kopie des Keystores vernichtet wird.

7 K41 Löschen

Nach Ablauf der gesetzlichen Fristen müssen die Datenablagen wieder gelöscht werden. Dies umfasst einerseits die Datenablage selbst, als auch die Backups. Innerhalb der Datenbank wird die entsprechende separate Tabelle gelöscht.

Das Löschen der Backups wird via das Löschen des zugehörigen Schlüsselpaares und sämtlicher Kopien derselben realisiert.

8 K52 Zugriffsberechtigungen

Es werden nur diejenigen Rollen genannt und beschrieben, welche für die Handhabung der sensiblen Daten nötig sind.

Applikations-Berechtigung: Erstellen und Löschen von Datenablagen für sensible Daten

Rolleninhaber: Dienst für Politische Rechte der Staatskanzlei

Der Dienst für Politische Rechte der Staatskanzlei hat keine Leserechte auf den Datenablagen für sensible Daten.

Applikations-Berechtigung: Lesen und Schreiben der Datenablagen für sensible Daten

Rolleninhaber: Gemeinden

Es ist wichtig sicherzustellen, dass die Gemeinden nur via das System (idealerweise API) auf die sensiblen Daten zugreifen können und das System verhindert, dass auf Daten einer fremden Gemeinde zugegriffen werden kann.

Rolleninhaberin: Staatskanzlei

Die Staatskanzlei braucht Zugriff auf die sensiblen Daten um Stichproben durchführen zu können. Die Applikation darf diesen Zugriff aber immer nur auf einen einzelnen Datensatz erlauben. Das heisst, die Staatskanzlei gibt die Angaben eines Eintrages eines Unterschriftenbogens ein und die Applikation zeigt genau diesen Datensatz an, sofern die Eingabe eindeutig ist. Die Applikation antwortet nie mit einer Auswahl von Datensätzen.

Rolleninhaber: Stimmberechtigte

Es ist wichtig sicherzustellen, dass die Stimmberechtigten nur via das System auf die sensiblen Daten zugreifen können und das System verhindert, dass auf Daten einer fremden Person zugegriffen werden kann.

Datenbank-Berechtigung: Online-Applikationsuser

Rolleninhaber: Applikation

Wichtig: Der Applikations-User wird durch das System (API), Views und Stored Procedures eingeengt. Da er vollen Lesezugriff auf die gesamte Datenbank benötigt, muss sichergestellt werden, dass dieser User wirklich nur via die Applikation und nicht interaktiv eingesetzt wird.

Das Erstellen und Löschen der Datenablagen / Tabellen für die sensiblen Daten sollte durch den Applikationsuser nur angestossen werden (Trigger, Stored Procedure). Aus Sicherheitsgründen sollte es vermieden werden, dass der Applikationsuser die entsprechenden Befehle selbst ausführt (SQL Statements).

Datenbank-Berechtigung: Superuser

Rolleninhaber: Betreiber/in der Applikation und Datenbank

Wichtig: Es muss vertraglich sichergestellt werden, dass der Superuser nur bei separat autorisierten Arbeiten sowie separat autorisierten forensischen Abklärungen und Audits eingesetzt wird und sich der Betreiber dabei auf die autorisierten Arbeiten und Abklärungen beschränkt.