

# Verschlüsselungsadapter – Kurzbeschreibung

Moritz Marc Beller  
24.10.2005

## Idee

In einem Jahrzehnt, in dem die Portabilität von Informationen immer wichtiger wurde, stellen sich bei wachsenden Kapazitäten der USB-Festplatten und Speichersticks nicht nur Firmen immer öfter sicherheitsrelevante Fragen. Wie etwa können sensible Daten auf einer externen Festplatte zwar einerseits schnell zugreifbar sein, andererseits aber auch im Falle des Verlusts oder beim Diebstahl des Geräts vor den Augen Dritter geschützt gelagert werden? Um dies zu erreichen, ist eine Verschlüsselung der Daten unabdingbar. Da sie jedoch ausschließlich mit etlichem Fachwissen in den Chiffrierungstechniken softwareseitig möglich ist, scheuen viele Unternehmen trotz ihrer eindeutigen Vorteile den Einsatz derartiger mobiler Massenspeicher. Begründungen: „Zu unsicher“ oder „zu viel Aufwand“.

Die Anforderungen an die Chipentwicklung lauten nun also, die algorithmischen Verfahren der Verschlüsselung in einen USB-Adapter zu integrieren, der physikalisch als Bindeglied zwischen USB-Port des Rechners und dem benutzten Endgerät, also zum Beispiel der USB-Festplatte, fungiert. Dieser soll den Benutzer während des Mount-Prozesses nach einem Passwort fragen und dann, zwecks einfacher Benutzung, in den Hintergrund treten, so dass es für den Anwender so aussieht, als existiere er nicht.

## Gerätebeschreibung

Eine LED auf dem Chip könnte den Status der Passwortverifizierung anzeigen: Lässt sich mit dem beim Mounten eingegebenen Passwort eine gültige Partitionstabelle aus den verschlüsselten Daten des Endgerät konstruieren, muss die *pass phrase* korrekt sein. Es wird ergo stets nicht nur eine einzelne Partition



verschlüsselt, sondern gleich das gesamte Festplattensystem. Weil die Festplatte selbst immer nur Sektor für Sektor liest oder schreibt, wird sie sich nicht über den scheinbaren Datenmüll, der zu ihr gesendet und von ihr gelesen wird (und der erst durch die Dechiffrierung nutzbar gemacht wird), beschweren.

## Übersicht über zu lösende Probleme

- Verschlüsselungstiefe und -verfahren abhängig von der Rechenpower, die sich auf einen solchen (nach Möglichkeit kompakten Chip) integriert lässt
- Stromversorgung und -weitergabe an das Endgerät
- Erkennung des Endgerätes, softwareseitige Passwortabfrage beim Mounten, Auslesen der Partitionstabelle, Weiterleitung der Daten an das Betriebssystem

## Algorithmus

Als Algorithmus kann ein symmetrisches Verschlüsselungsverfahren, z.B. AES, zum Einsatz kommen: Es bedarf vergleichsweise wenig CPU-Time und gilt heutzutage trotzdem noch als recht sicher, obwohl sicherlich nicht „unknackbar“. Meine Messungen mit einer 900 MHz-CPU ergaben einen Geschwindigkeitsverlust von circa 7% mit einer Keygröße von 256 Bits beim Verschieben einer Datei von einer unverschlüsselten Partition auf eine verschlüsselte (der selben Festplatte). Bei Keygrößen < 256 Bits ließ sich kein Verlust mehr erkennen, und 64 Bit waren sogar mit 233 MHz uneingeschränkt möglich.