Universität Hamburg
Fachbereich Informatik

Bachelorarbeit

Prototypische Erstellung eines Online-Bestellmoduls für Schließanlagen

vorgelegt von

Tim Krämer
geb. am 22. April 1987 in Lübbecke
Matrikelnummer 5945287

eingereicht am 22. September 2012

Betreuer: Jochen Körtner (*Körtner & Muth GmbH*)
Erstgutachter: Prof. Dr.-Ing. Hannes Federrath
Zweitgutachter: Dr. Andreas Günter

Inhaltsverzeichnis

Abstract

Sicherungskarten als Identifikationsmittel befinden sich seit vielen Jahren weltweit im Praxiseinsatz in der Schließanlagenproduktion. Eine ausreichende Identifikation ist aber nur mit zusätzlichem Unterschriftsbeleg oder persönlichem Kontakt zwischen Händler und Endnutzer gegeben. Ziel dieser Bachelorarbeit ist, ein Konzept zu erarbeiten, welches einen komfortablen und den Sicherheitsanforderungen der Schließanlagenindustrie entsprechenden digitalen Bestellvorgang für Endnutzer, Händler und Hersteller von Schließanlagen ermöglicht. Im Mittelpunkt steht dabei die Anbindung an die bestehende Schließanlagensoftware *LOCKBASE* der *Körtner & Muth GmbH*. In dieser Bachelorarbeit wird die aktuelle Praxis beschrieben, aktuelle Anforderungen des Marktes untersucht, die Möglichkeit einer Identifikation mit Hilfe von Software diskutiert und ein technisches Konzept für die Anbindung an die bestehende Schließanlagensoftware *LOCKBASE* geschaffen.

1 Einleitung

Bei einer Schließanlage handelt es sich um ein aus mehreren Schließzylindern mit zugehörigen Schlüsseln bestehendes Schließsystem. Schließzylinder werden meist in Türen verbaut und Schlüssel jeweils an befugte Personen ausgegeben, um Zugang zu diesen Türen zu ermöglichen. Der Unterschied zu einem einzelnen Schlüssel- und Schließzylinderpaar besteht darin, dass in einer Schließanlage die Schließzylinder so eingerichtet werden, dass mehrere unterschiedliche Schlüssel in ihnen schließen. Dies wird durch einen bestimmten Bestiftungsmodus der Schließzylinder ermöglicht. Allgemein werden Schließanlagen verwendet, um unter Einhaltung der individuellen Zutrittsberechtigungen mehreren Personen Zugang zu verschiedenen Türen zu geben, ohne dass für jeden Schließzylinder ein individueller Schlüssel existieren muss (siehe Abb. 1). Die Schlüsselinhaber bekommen im Regelfall nur einen Schlüssel für alle von ihnen zu öffnenden Türen.

Schließzylinder sind neben den Schlüsseln die Hauptbestandteile von Schließanlagen. Große Schließanlagen müssen häufig modifiziert werden, da sich die Anzahl der Schlüssel und der Türen schnell verändern kann. Prominente Beispiele für solche Situationen sind die Einstellung und Entlassung von Mitarbeitern oder der Anbau von neuen Gebäudeabschnitten. Das wohl kritischste Ereignis ist der Diebstahl eines hierarchisch hoch eingeordneten Schlüssels einer Schließanlage, denn daraufhin sollten schnellstmöglich alle verbundenen Schließzylinder modifiziert werden, sodass der verlorene Schlüssel vollständig aus der betroffenen Anlage ausgeschlossen und ein neu hergestellter Schlüssel integriert wird.

Während die sog. Umstiftung von Schließzylindern, also die Veränderung der möglichen Schließkombinationen für einen Schließzylinder, i. d. R. vom Fachhändler vollständig übernommen wird (inklusive Aus- und Einbau vor Ort), werden neue Schlüssel und Schlüsselkopien häufig telefonisch vom Endnutzer bestellt. Schon jetzt besteht die Möglichkeit, Bestellungen via E-Mail oder Websites aufzugeben, und die Nachfrage

nach komfortableren Bestellmöglichkeiten wird in naher Zukunft deutlich ansteigen. Dabei ist es wichtig zu beachten, dass diese sicherheitskritischen Bestellungen nicht von unbefugten dritten Personen in Auftrag gegeben oder manipuliert werden können.

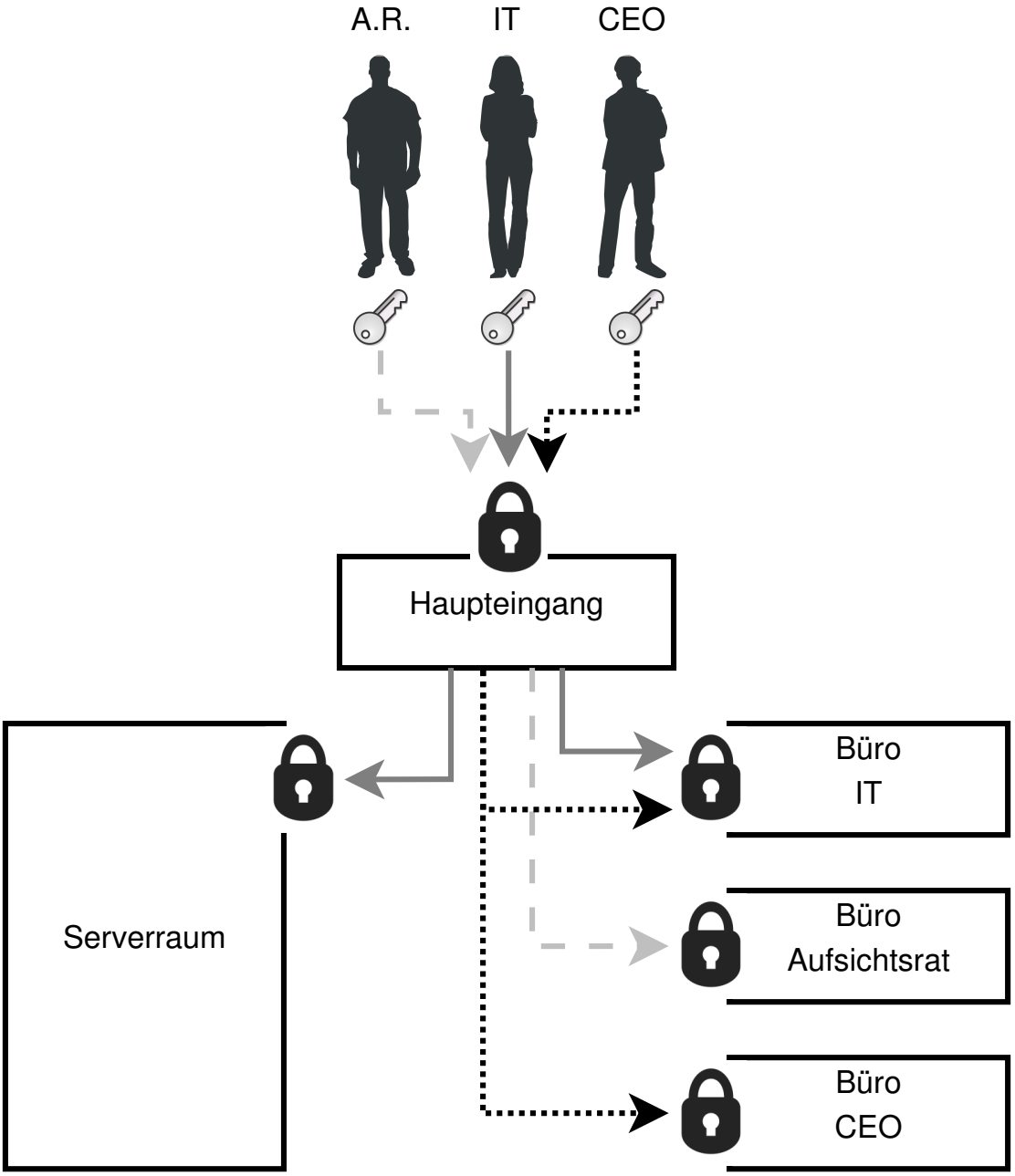

Abbildung 1: Schematischer Aufbau einer Schließanlage

1.1 Aufgabenstellung

Die *Körtner & Muth GmbH* entwickelt Software zur Planung, Berechnung und Verwaltung von Schließanlagen. Zielgruppen sind die Schlossindustrie, Schließanlagenhändler und Endnutzer mit spezifischen Modulen für die jeweiligen Anwendungen. Die Aufgabe dieser Arbeit besteht darin, ein Softwarekonzept für die Kommunikation und Datenübertragung zwischen zwei Benutzern der *LOCKBASE* Software zu ermöglichen. Bei der Kommunikation sollen die Schutzziele Integrität[1], Vertraulichkeit[2] und Verfügbarkeit[3] erfüllt werden. Die konkrete Implementation des Konzepts soll die Möglichkeit eines Bestellvorgangs für neue und Erweiterungen bereits bestehender Schließanlagen schaffen. Um eine Identifikation des bestellenden Nutzers zu gewährleisten, sollen Methoden aus der Informatik eingesetzt werden. Für die Akzeptanz einer Bestellsoftware in der Schließanlagenindustrie ist es besonders wichtig, dass die bereits eingesetzten Identifikationverfahren nicht aufgegeben werden müssen. Im Vordergrund steht dabei, dass die resultierende Anwendung einen Mehrwert an Komfort für Endnutzer, Händler und Hersteller bietet. Um die Vereinbarkeit und Verbesserung des Nutzerkomforts zum derzeitigen Stand der Praxis zu untersuchen, soll dieser zunächst vorgestellt und mit Hilfe von Angreifermodellen auf potentielle Sicherheitsrisiken untersucht werden.

Die Konzipierung soll einen idealtypischen Bestellablauf beinhalten und anhand diesem sollen Anforderungen an die Funktionalität der darauf basierenden Software erarbeitet werden. Außerdem sollen notwendige Veränderungen an den vorhandenen *LOCKBASE*-Modulen vorgeschlagen werden, um eine Anbindung eines Bestellmoduls zu realisieren.

Das folgende Beispielszenario mit den bekannten Protagonisten Alice und Bob soll dem Leser eine Vorstellung vermitteln, durch welche Ausgangslage der Wunsch nach einer Schließanlagenerweiterungen entstehen könnte. Um das Augenmerk auf den Komfortaspekt einer Bestellung zu legen, wird hier die Perspektive des Endnutzers einer Schließanlage beschrieben:

Eine Person namens Alice arbeitet als Personalleiterin einer Firma und stellt regelmäßig neue Mitarbeiter ein. Alle Mitarbeiter bekommen von Alice einen eigenen Schlüssel, mit dem sie genau zu den Räumen Zugang erhalten, die sie für ihre Arbeit betreten müssen. Bob, der neue Mitarbeiter aus der IT, benötigt einen Schlüssel mit Zugang zum Haupteingang und den Serverräumen, die Tür zu Alices Büro soll er allerdings nicht aufschließen können. Diese Schlüsselkonfiguration ist üblich für die Mitarbeiter der IT, sodass Alice in Ihrer Verwaltungssoftware bereits einen Gruppenschlüssel mit der Bezeichnung „IT“ und den entsprechenden Berechtigungen angelegt hat. Sie kann

[1] Die Integrität einer Nachricht liegt vor, wenn diese Nachricht unverändert zugestellt wurde [BSI2009].

[2] Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein [BSI2009].

[3] Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können [BSI2009].

nun einfach bei ihrem Schließanlagenhändler einen weiteren „IT“-Gruppenschlüssel bestellen. Sobald der Schlüssel gefertigt und geliefert ist, händigt Alice diesen an Bob aus.

1.2 Begriffserläuterungen

Der besseren Lesbarkeit halber werden die Akteurinnen und Akteure aller Beispiele gemeinsam durch folgende Begriffe bezeichnet:

- Der **Endnutzer**, in dem o. g. Beispiel Alice, ist direkter Kunde des Händlers, außerdem initialer Auftraggeber von Bestellungen und somit der legitime Empfänger der bestellten Ware. Er besitzt und verwaltet die physische Schließanlage und vertraut seinem Händler.
- Der **Händler**, in der Schließanlagenindustrie häufig als „Errichter“ bezeichnet, agiert in den meisten Fällen als Fachberater für mehrere Endnutzer, bestellt die benötigte Ware beim Hersteller und lässt diese an den Endnutzer direkt ausliefern. In selteneren Fällen kann er die bestellten Artikel auch selbst anfertigen und entsprechend ausliefern. In diesem Fall besitzt er die Daten für den Bau und Erweiterungen der Schließanlagen seiner Endnutzer und ist vertraglich verpflichtet, die Berechtigung für Schlüsselfertigungen und Zugriff auf die Kundendaten zu überprüfen.
- Der **Hersteller** kann Händler mit vorgefertigten Teilen und Schlüsselrohlingen für Schließanlagen versorgen und durch Auftrag eines Händlers auch Endnutzer direkt mit Endprodukten für spezifische Schließanlagen beliefern, auch hier wird die Zugangsberechtigung zu Kundendaten und Schlüsselfertigungen überprüft.

Der Übersichtlichkeit zu Gunsten wird in den nachfolgenden Beispielen und Szenarien der Empfänger nur als Schließanlagenhändler oder kurz, als Händler bezeichnet. Wobei es sich auch, je nach Größe der Schließanlage, um den Schließanlagenhersteller handeln kann. In späteren Kapiteln wird dieser Unterschied nochmal genauer differenziert.

2 Identifikation

Um bei der Entwicklung eines neuen digitalen Bestellverfahrens eine Vereinbarkeit mit den derzeitigen Praktiken der Schließanlagenindustrie zu erreichen, wird in den folgenden Abschnitten zunächst beschrieben, wie der Händler überprüft, ob die bestellende Person berechtigt ist Ware für die entsprechenden Schließanlage zu erhalten.

Der Vorgang eine Person eindeutig zu erkennen anhand dessen, was er ist, hat oder weiß, wird Identifikation genannt (vgl. [FP2012]).

Der Schließanlagenhändler ist verpflichtet zu überprüfen, dass die gefertigte Ware nur an eine befugte Person ausgehändigt wird, dies gilt besonders für Schlüssel von Schließanlagen. Die Überprüfung sollte möglichst vor der Fertigung der bestellten Ware stattfinden, damit unbefugt bestellte Ware gar nicht erst hergestellt wird. Denn ein geschnittener Schlüssel kann nicht wiederverwendet werden und stellt als unbefugte Kopie ein hohes Sicherheitsrisiko für den Besitzer der zugehörigen Schließanlagen dar. Deshalb muss dieser sofort zerstört werden.

Die Überprüfung erfolgt in der Praxis durch Identifikation des Bestellers anhand einer eigenhändigen Unterschrift oder über den Besitz einer Sicherungskarte. Auf die Vor- und Nachteile beider Lösungen wird im folgenden Kapitel näher eingegangen.

3 Sicherungskarte und Unterschriftsbeleg

Der Schließanlagenhändler identifiziert den Besteller, vor der Fertigung von sicherheitskritischen Komponenten einer Schließanlage, anhand der eigenhändigen Unterschrift des Bestellers mit Hilfe eines **Unterschriftsbelegs** oder einer vom Besteller vorgelegten **Sicherungskarte**. Das populärste Beispiel für eine sicherheitskritische Komponente ist die Fertigung eines passenden Schlüssels zu einer bestehenden Schließanlage. Dieser darf nur von einem befugten Endnutzer in Auftrag gegeben werden.

Bei einem **Unterschriftsbeleg** handelt es sich um ein Abbild der Unterschrift des berechtigten Endnutzers, der bei jeder Bestellung mit der eigenhändigen Unterschrift des Bestellers verglichen wird.

Sicherungskarten sehen je nach Hersteller, Händler und Qualität der Schließanlage unterschiedlich aus. Alle Variationen enthalten mindestens eine Schließanlagenbezeichnung, die für den Händler eine eindeutige Zuordnung zu einer Schließanlage ermöglicht. Häufig werden Plastikkarten im Kreditkartenformat verwendet, auf denen die Schließanlagenbezeichnung sowohl in Hochprägung aufgebracht als auch in kodierter Form auf einem Magnetstreifen gespeichert ist. Die Berechtigungskontrolle eines Bestellers geschieht mit einer Sicherungskarte über die, auf dem Magnetstreifen kodierte, Schließanlagenbezeichnung. Vor der Bestellung muss dem Schließanlagenhändler die Sicherungskarte vorgelegt werden, die daraufhin mit einem Kartenleser eingelesen und dekodiert wird. Anhand der dekodierten Schließanlagenbezeichnung wird diese dann der bestehenden Schließanlage zugeordnet. Bei anderen Versionen der Sicherungskarte

werden Abrollbelege benutzt um zu quittieren, dass die Sicherungskarte bei der Bestellung vorlag. Anhand des Abdrucks der Schließanlagenbezeichnung in Hochprägung geschieht hier die äquivalente Zuordnung zu einer bestehenden Schließanlage.

Vereinzelt wird bei der Kommunikation zwischen Händler und Hersteller via Internet eine Identifikation mittels Magnetstreifenkartenleser beim Händler durchgeführt. Die Händler lesen dazu die Sicherungskarten der Endnutzer ein und können so Schlüssel oder Erweiterungen für die zugehörige Schließanlage beim Hersteller bestellen. Dieses Verfahren wird dann eingesetzt, wenn sich die Hersteller verpflichtet haben, die Endnutzer nicht direkt zu bedienen, sondern Fachgeschäfte als Zwischenhändler und Ansprechpartner für Endnutzer agieren zu lassen. Da es sich hierbei um ein geschlossenes und undokumentiertes Verfahren der Hersteller handelt, kann dieses nicht im Rahmen dieser Arbeit untersucht werden.

Häufig wird eine Kombination aus beiden Identifikationsmöglichkeiten eingesetzt. Um den Vorteil dieses hybriden Verfahrens zu verdeutlichen, werden in der folgenden Tabelle die Merkmale von Unterschriftsbelegen und Sicherungskarten gegenübergestellt.

Unterschriftsbeleg	**Sicherungskarte**
biometrisch global eindeutig	oft nur unternehmensintern eindeutig
üblicherweise keine Verlustgefahr	kann leicht verloren werden
nur mit viel Übung fälschbar	nur mit großem Aufwand fälschbar, aber i. d. R. leicht kopierbar
personengebunden	übertragbar
müssen persönlich hinterlegt werden	Übergabe auch postalisch möglich
lassen sich nur aufwändig digital verwahren	digitale Speicherung beim Händler einfach und günstig

Tabelle 1: Unterschriftsbeleg und Sicherungskarte im Vergleich

Der Einsatz von beiden Identifikationsmöglichkeiten bietet den Vorteil für den Endnutzer, dass auch bei Verlust der Sicherungskarte, durch die eigenhändige Unterschrift, eine neue Sicherungskarte ausgestellt werden kann, ohne dass andere aufwändige Identifikationsverfahren eingesetzt werden müssen. Der Händler kann seinen Kunden bei der Bestellung schnell anhand einer Sicherungskarte identifizieren und diese automatisch der entsprechenden Schließanlage zuordnen, dies spart viel Zeit bei der Auftragsbearbeitung. Zusätzlich kann er sich die Ausgabe der bestellten Ware mit einer eigenhändigen Unterschrift quittieren lassen, sodass er die erfolgte Warenausgabe im Zweifelsfall nachweisen kann.

Aus den in Tab. 1 gegenübergestellten Merkmalen beider Identifikationsmittel sorgt besonders die Übertragbarkeit der Sicherungskarte für große Beliebtheit bei Endnutzern aus großen Firmen. So kann ein Bote für die Bestellung von neuen Schlüsseln gesandt werden, ohne das sich die verantwortlichen Personalleiter selbst zum Schließanlagenhändler begeben müssen. Dabei handelt es sich um ein Beispiel, wo zu Gunsten des Komforts Sicherheitsrisiken eingegangen werden. Dieses und weitere Szenarien werden im folgenden Kapitel im Rahmen von Angreifermodellen untersucht.

4 Angreifermodell

In diesem Kapitel werden die Angriffsmöglichkeiten an den dargestellten Identifikationsverfahren mit Unterschriftsbeleg und Sicherungskarte betrachtet. Um eine strukturierte Übersicht zu erstellen, aus denen daraufhin Sicherheitsanforderungen für die zu konzipierende Bestellsoftware ableitbar sind, werden in diesem Abschnitt Angriffsszenarien formuliert um die Stärken und Schwächen von Sicherungskarten und Unterschriftsbelegen aufzuzeigen.

Zunächst können die potentiellen Angreifer zwischen Mitarbeitern des Endnutzers und Außenstehenden unterschieden werden. Entsprechend ihrer Position haben diese unterschiedliche Möglichkeiten, um die Identifikationverfahren zu manipulieren oder zu missbrauchen.

Mitarbeit des Händlers brauchen im Rahmen ihrer alltäglichen Arbeit Zugriff auf die Schließanlagendaten ihrer Kunden, um diese fachgerecht beraten zu können. Ähnlich zum Beruf eines Bankmitarbeiters, genießen die Mitarbeiter des Händlers das Vertrauen ihrer Kunden. Da es nicht Bestandteil dieser Arbeit sein soll, dieses Vertrauensverhältnis durch Software abzulösen, wird im Folgenden angenommen, dass nur vertrauenswürdige Mitarbeiter bei der Herstellung und Erweiterung von Schließanlagen involviert sind und nicht zum Schaden der Endnutzer oder des Händlers agieren.

„Ein **Angreifermodell** definiert die Stärke eines Angreifers, gegen den ein bestimmter Schutzmechanismus (z. B. ein ganz bestimmtes Verschlüsselungsverfahren) gerade noch sicher ist“ [FP2012].

Bei Schlüsseln handelt es sich um spezielle Gegenstände, deren Besitz Zugang zu wichtigen und wertvollen Objekten ermöglichen kann. In hierarchisch strukturierten Schließanlagen existieren Schlüssel, mit denen sich alle Türen der Schließanlage öffnen lassen. Diese speziellen Schlüssel werden als Hauptschlüssel bezeichnet. Schlüssel und insbesondere Hauptschlüssel sind ein besonders begehrtes Diebesgut.

Besonders kritisch ist es, wenn ein Einbruch und Diebstahl mit Hilfe eines passenden Schlüssels in einer Schließanlage erfolgte, ohne dass ein Schlüsselverlust gemeldet wurde. Sofern der Diebstahl nicht vorgetäuscht wurde, um Versicherungsbetrug zu begehen, ist davon auszugehen, dass ein weiterer, unbekannter Schlüssel für die Schließanlage existiert. Diese Schlüssel werden auch als „schwarze Schlüssel“ bezeichnet [Abu2012].

Neben ggf. hergestellten Schlüsseln handele es sich bei allen Informationen in den folgenden Beispielen um sensible Daten, zu denen unbefugten Personen keinen Zugriff erhalten dürften.

Allgemein wird in dieser Arbeit davon ausgegangen, dass der Besitzer der Schließanlagendaten, also den Schlüsselschneidwerten und Zylinderbestiftungsplänen vertrauenswürdig ist und damit als „befugt“ gilt. Das gleiche gilt für den legitimen Empfänger der bestellten Ware. Damit wird hier eine bewusste Weitergabe der sensiblen Daten und Schlüssel ausgeschlossen.

Es wird weiterhin vorausgesetzt, dass der Händler entweder über eine Kopie der Unterschrift des Endnutzers der Schließanlage verfügt oder beim Errichten der Schließanlage dem Endnutzer eine Sicherungskarte mit einer Schließanlagenbezeichnung ausgehändigt hat. Diese Schließanlagenbezeichnung speichert der Händler zusammen mit den Schlüsselschneidwerten und Zylinderbestiftungsplänen. Außerdem können beide Methoden kombiniert eingesetzt werden, um den Endnutzer zu identifizieren.

Nachfolgend sind Angriffsszenarien aufgelistet, die mit den oben genannten Einschränkungen realistische Bedrohungen darstellen und aus denen, in späteren Kapiteln, Sicherheitsanforderungen für das Konzept des softwarebasierten Bestellverfahrens ermittelt werden.

4.1 Angriffsszenario: Fälschung der Unterschrift

Ein Außenstehender mit Wissen über den Ablauf könnte die Unterschrift von Alice üben und direkt im Geschäft des Schließanlagenhändlers einen passenden Schlüssel bestellen, Alices eigenhändige Unterschrift vor Ort fälschen und den Schlüssel an sich nehmen.

Aufwand / Risiko: Während der Aufwand eine Unterschrift zu lernen nicht unrealistisch hoch wäre, ginge der Angreifer in diesem Szenario ein großes Risiko ein. So wäre es denkbar, dass der Händler Alice persönlich kennt und den Betrug sofort bemerkt. Außerdem könnten bei Zweifel an der Legitimität der Unterschrift weitere Identifikationsmerkmale gefordert werden, wie z. B. ein Personalausweis. Des Weiteren müsste sich der Angreifer für mehrere Minuten im Geschäft des Händlers aufhalten, während der Schlüssel gefertigt würde.

Konsequenz im Erfolgsfall: Sollte der Angreifer den Händler erfolgreich täuschen können und einen bestellten Hauptschlüssel ausgehändigt bekommen, hätte er nun vollen Zugriff auf die Räumlichkeiten von Alices Firma.

Konsequenz des Scheiterns: Ließe sich der Händler nicht täuschen, könnte der Angreifer relativ einfach gestellt werden, da er sich im Geschäft des Händlers befände.

4.2 Angriffsszenario: Diebstahl der Sicherungskarte

Ein Außenstehender hätte große Schwierigkeiten an die Sicherungskarte heranzukommen, da sich diese an einem sicheren Ort oder zumindest im direkten Besitz von Alice befindet. Üblicherweise wird Nutzern geraten, die Sicherungskarte in einem Tresor oder einem anderen sicheren Ort innerhalb des Gebäudes zu verwahren. Bei einer großen Firma hingegen könnte ein Einbruch für einen Außenstehenden mit der Aussicht auf einen Hauptschlüssel lohnen. Mitarbeitern von Alice wäre es mit gleicher Motivation noch leichter möglich sich die Sicherungskarte anzueignen und mit deren Hilfe einen Schlüssel für die betreffende Schließanlage zu bestellen und im Geschäft abzuholen.

Aufwand / Risiko: Der Aufwand, um an die Sicherungskarte zu gelangen, hängt ganz davon ab, wie sicher Alice diese verwahrt hat. Das eingegangene Risiko der Bestellung

ist gering, selbst wenn bei Abholung eine Unterschrift verlangt würde, könnte der Mitarbeiter leicht angeben er handele im Auftrag von Alice und mit beliebigem Namen unterschreiben.

Konsequenz im Erfolgsfall: Sollte der Angreifer die Sicherungskarte unbemerkt benutzen können, um einen Hauptschlüssel zu bestellen, hätte er nun vollen Zugriff auf die Räumlichkeiten von Alices Firma.

Konsequenz des Scheiterns: Ließe sich der Händler nicht überzeugen, einen Schlüssel nur anhand der Sicherungskarte auszugeben, hätte der Angreifer zwar keinen Erfolg, jedoch gäbe es keinen Grund für den Händler dem Angreifer gegenüber skeptisch zu sein, sodass der Angreifer unidentifiziert bliebe und ihm keine direkten Konsequenzen drohten.

4.3 Angriffsszenario: Kopie der Sicherungskarte

Realistischer als der Diebstahl einer Sicherungskarte durch einen Mitarbeiter von Alice ist, dass sie diesem die Sicherungskarte freiwillig aushändigt um eine Bestellung beim Händler zu tätigen. Da es sich bei den Sicherungskarten üblicherweise um Magnetstreifenkarten handelt, ist es nicht sehr aufwändig diese zu vervielfältigen. Die fehlende Hochprägung und das wahrscheinlich unterschiedliche Aussehen einer Kartenkopie würden jedem Schließanlagenhändler jedoch sofort auffallen. Selbst bei der oben erwähnten Identifikation via Internet und Magnetstreifenkartenleser, ist es sehr wahrscheinlich, dass zusätzlich vorher eine Authentifikation mittels Benutzername und Passwort erfolgt, sodass der Zugriff für Außenstehende nicht einfach erfolgen kann.

Aufwand / Risiko: Sowohl für einen außenstehenden Angreifer, als auch für einen Angreifer aus den Reihen von Alices Mitarbeitern dürfte es äußerst schwierig sein einen Sicherungskartenrohling im Layout des Schließanlagenherstellers zu bekommen, um diesen mit einer passenden Hochprägung und den kopierten Daten der originalen Sicherungskarte zu versehen. Hier gelten die gleichen Risiken, wie bei dem Diebstahl der Sicherungskarte mit dem Unterschied, dass in diesem Fall kein Verlust der originalen Karte vorliegt und somit erst auffällt, nachdem der Händler den gefertigten Schlüssel Alices Firma in Rechnung stellt.

Konsequenz im Erfolgsfall: Sollte es dem Angreifer gelingen eine Sicherungskarte ausreichend gut genug zu kopieren, hätte er damit die Möglichkeit einen Hauptschlüssel für die zugehörige Schließanlage zu bestellen und mit diesem Zugriff auf die Räumlichkeiten von Alices Firma.

Konsequenz des Scheiterns: Sollte der Händler die Kopie als solche identifizieren, drohte dem Angreifer die Strafe für diese Art von Betrug.

4.4 Angriffsszenario: Verändern der Daten beim Händler

Anstatt Alice direkt anzugreifen, könnte ein Angreifer das hinterlegte Abbild von Alices eigenhändiger Unterschrift oder die Sicherungskarteninformation manipulieren. Damit wäre es ihm möglich, selbst Bestellungen aufzugeben, indem er die entsprechend hergestellte Unterschrift oder Sicherungskarte nutzt.

Aufwand / Risiko: Der Aufwand, um die Daten des Händlers zu manipulieren, ist stark davon abhängig, wie gut geschützt der Händler diese Kundendaten verwahrt. Ein außenstehender Angreifer hingegen müsste zuerst physischen Zugang zum Geschäft des Händlers bekommen, oder im Falle einer digitalen Speicherung Zugriff zu dem entsprechenden Computersystem. Da es sich um die Örtlichkeiten von Schließanlagenhändlern und i, d. R. um Sicherheitsfachgeschäften handelt, ist davon auszugehen, dass diese Gebäude überdurchschnittlich gut abgesichert sind. Das Risiko eines physischen Einbruchs in so ein Geschäft ist in den meisten Fällen ähnlich hoch, wie der direkte Einbruch in Alices Gebäude. Unter Umständen ist der Zugriff auf digital hinterlegte Daten jedoch wesentlich einfacher und bietet ein realistisches Ziel.

Konsequenz im Erfolgsfall: Die Veränderung der Kundendaten beim Händler würde dem Angreifer die Möglichkeit bieten Hauptschlüssel für alle Schließanlagenkunden des angegriffenen Händlers anzufertigen zu lassen. Die Folgen wären für den Händler katastrophal.

Konsequenz des Scheiterns: Sollte der Angreifer beim Einbruch in das Gebäude des Händlers erwischt werden, drohte ihm eine entsprechende Strafe. Unter Umständen wäre allerdings ein nicht rückverfolgbarer Angriff auf das Computersystem des Händlers möglich, sodass dem Angreifer im Fall des Scheiterns keine direkten Konsequenzen drohten.

4.5 Angriffsszenario: Mitlesen der Sicherungskarteninformation

Falls Alice eine Bestellung via E-Mail aufgibt, müsste Sie dafür entweder ihre Unterschrift als Bild mit übertragen, oder in der E-Mail die Informationen der Sicherungskarte angeben. In beiden Fällen wäre der Inhalt und Anhang der E-Mail leicht sichtbar, sowohl für Mitarbeiter im gleichen Netzwerk als auch für Außenstehende, die am Transfer der E-Mail beteiligt sind. Auch die Adressauswahl beim Versand einer E-Mail ist fehleranfällig, so könnte durch einen falschen Klick, einen Fehler im Computer oder einer Manipulation des Systems schnell ein falscher Empfänger adressiert werden, dem daraufhin die sensiblen Daten zur Verfügung stehen.

Aufwand / Risiko: An dem Versand einer E-Mail sind wesentlich mehr Instanzen beteiligt, als an den vorher vorgestellten Verfahren, damit erhöht sich die Anzahl der potentiellen Angreifer signifikant. Der Aufwand, eine E-Mail während der Übertragung zu lesen, verfälschen, oder verwerfen ist für einen Angreifer im gleichen Netzwerk sehr gering. Es sind viele, leicht bedienbare Programme erhältlich, die diese Aufgaben automatisiert erfüllen können. Für außenstehende Angreifer besteht die Möglichkeit,

Zugriff auf einen der beteiligten E-Mailserver zu bekommen. Jedoch ist dieser Aufwand wesentlich höher. Das Risiko entdeckt zu werden ist für die vorgestellten Methoden denkbar gering.

Konsequenz im Erfolgsfall: Sollte der Angreifer eine E-Mail mit einer gültigen Bestellung verändern oder verwerfen können, hätte er Alice zwar ggf. finanziellen Schaden zugefügt, jedoch käme er damit nicht unmittelbar in den Besitz eines Schlüssels. Dennoch besteht die Möglichkeit, dass die bestellte Ware nach Fertigung via Paketdienst versandt würde. Falls es sich um einen Mitarbeiter von Alice handelt, könnte er diese bei der Ankunft in Alices Firma abfangen. Ein außenstehender Angreifer könnte die Bestellung so manipulieren, dass sie eine von ihm ausgewählte Postanschrift enthält. Da es sich bei Schließanlagen um ortsgebundene Produkte handelt, würde der Händler jedoch einen Versand an eine fremde Adresse höchstwahrscheinlich nicht ohne Nachfrage akzeptieren.

Könnte der Angreifer die E-Mail lediglich mitlesen, wäre er im Besitz eines Abbilds von Alices eigenhändiger Unterschrift oder der Sicherungskarteninformation. Damit könnte der Angreifer unabhängig von Alice weitere Bestellungen in Auftrag geben, stünde aber vor dem gleichen Problem, dass er nicht unmittelbar in Besitz eines Schlüssels käme.

Konsequenz des Scheiterns: Das Scheitern beim Mitlesen, Verändern oder Verwerfen hätte für den Angreifer keine direkten Konsequenzen, da die Wahrscheinlichkeit dass der Versuch des Mitlesens entdeckt wird, vernachlässigbar gering ist.

4.6 Zusammenfassung

Zusammengefasst kann festgehalten werden, dass es bei dem derzeitigen Identifikationsverfahren für den Händler leicht möglich ist, den bestellenden Endnutzer ausreichend sicher zu identifizieren, sofern er dem Endnutzer persönlich gegenüber steht und die Echtheit der Unterschrift oder Sicherungskarte prüfen kann. Jedoch ist diese Notwendigkeit für den Endnutzer sehr unkomfortabel, sodass häufig der Wunsch besteht, ein Bestellverfahren mit ausreichend sicherer Identifikation, aber ohne physische Anwesenheit einzusetzen. Oft reagieren die Händler darauf, indem sie Bestellungen via E-Mail, Fax oder Telefon entgegennehmen. Da bei diesen Übertragungswegen die Schutzziele Vertraulichkeit und Integrität nicht gewährleistet sind, entstehen inakzeptable Sicherheitsrisiken. Auch Boten, meist Praktikanten und Auszubildene, denen Sicherungskarten zur Bestellung von Schlüsseln oder Schließanlagenerweiterungen ausgehändigt werden, wird ein unverhältnismäßig hohes Vertrauen entgegengebracht, so wäre es einem Boten mit Hilfe der Sicherungskarte möglich auch Hauptschlüssel für die Schließanlage zu bestellen. Wenn dies von der Geschäftsführung anhand der Abrechnung des Schließanlagenhändlers auffällt, ist dies möglicherweise bereits zu spät.

Der klare Wunsch nach Komfort soll im Folgenden durch ein softwarebasiertes Bestellverfahren erfüllt werden, welches die Schutzziele Vertraulichkeit und Integrität gewährleisten kann, aber ähnlich einfach und komfortabel wie eine E-Mail benutzbar ist. Weitere Voraussetzungen und die Konzipierung so einer Lösung werden im folgenden Kapitel erarbeitet.

5 Konzept einer Softwarelösung

Die Ziele der Softwarelösung zur Bestellung von Schließanlagenkomponenten sollen, neben Komfort und Akzeptanz für alle Beteiligten auch die Erfüllung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit sein.

Der wahrgenommene Komfort der Software ergibt sich aus der Vereinbarkeit der Funktionalität und den Arbeitsgewohnheiten der Nutzers. Aus den oben diskutierten Angreifermodellen ergibt sich neben den Sicherheitsanforderungen auch der Wunsch nach einer Bestellmöglichkeit ohne physische Anwesenheit beim Händler, an deren Verfahren aber nur befugte Personen beteiligt sind, also keine anderen Mitarbeiter oder Boten. Für den Schließanlagenhändler als Empfänger der Bestellung soll eine unkomplizierte Identifikation des Bestellers ermöglicht werden, die außerdem eine automatische Zuordnung zu der entsprechenden Schließanlage vornehmen kann.

Die Akzeptanz des Konzepts steigt mit dem wahrgenommenen Komfort bei dem Einsatz der Software, aber auch mit der Vereinbarkeit mit den derzeitig angewandten Identifikationsverfahren. Bereits vorhandene Sicherungskarten und Unterschriftsbelege sollten auch weiterhin nutzbar bleiben und den gleichzeitigen Einsatz eines softwarebasierten Bestellverfahrens nicht verhindern.

Um Hersteller und Händler zu überzeugen, ein weiteres neues Verfahren einzusetzen, müssen aber vor allem die, durch den Einsatz einer digitalen Bestellmöglichkeit, gewonnenen Sicherheitsmerkmale klar ersichtlich sein. Während die Technik des Verfahrens zu Gunsten der einfachen Bedienbarkeit für den Nutzer möglichst transparent und im Hintergrund bleiben sollte, ist es wichtig, dass der Schutz der Vertraulichkeit und Integrität in der Software entsprechend visualisiert wird. So soll dem Benutzer zu jeder Zeit ersichtlich sein, dass die Integrität der Bestellung geprüft wurde, das konkrete Prüfverfahren sollte allerdings möglichst automatisch, ohne unnötige Eingabeaufforderungen im Hintergrund ablaufen.

Um ein geeignetes Umsetzungskonzept zu entwerfen, wird zunächst ein idealtypischer Ablauf einer Schließanlagenbestellung angeschaut, mit dessen Hilfe konkret benötigte Funktionen erarbeitetet werden.

5.1 Idealtypischer Workflow

Ein softwarebasiertes Verfahren, dessen Sicherheit nicht auf der physischen Anwesenheit des bestellenden Endnutzers basiert, hat mehre Anforderungen, die anhand eines Workflow-Diagramms gefunden und beschrieben werden sollen.

Um ein aussagekräftiges Diagramm eines Bestellvorgangs abzubilden, muss im Voraus klar sein, welche Instanzen im Idealfall kommunizieren müssen, damit eine Bestellung ausgeführt werden kann. Ausgehend vom o. g. Beispiel, kommuniziert Alice ihrem Schließanlagenhändler, um bei diesem die gewünschten Schließanlagenkomponenten zu bestellen. Allgemein formuliert, basiert das grundlegende Konzept auf der

Voraussetzung, dass die Kommunikation und Datenübertragung immer zwischen genau zwei Instanzen der Software stattfindet, da in der Schließanlagenindustrie für die Bestellungen jeweils eindeutige Kommunikationspartner existieren.

Wie im Rahmen der Begriffsdefinitionen erwähnt, besteht die Möglichkeit, dass der Händler von Alice die Ware nicht selbst herstellen kann und diese stattdessen bei einem Hersteller bestellt. Aber auch in diesem Fall handelt es sich um eine Kommunikation zwischen genau zwei Parteien, sodass sich für das Konzept der Bestellsoftware nichts verändert.

Mit dieser Voraussetzung kann nun die zeitliche Abfolge des geplanten Konzepts visualisiert werden.

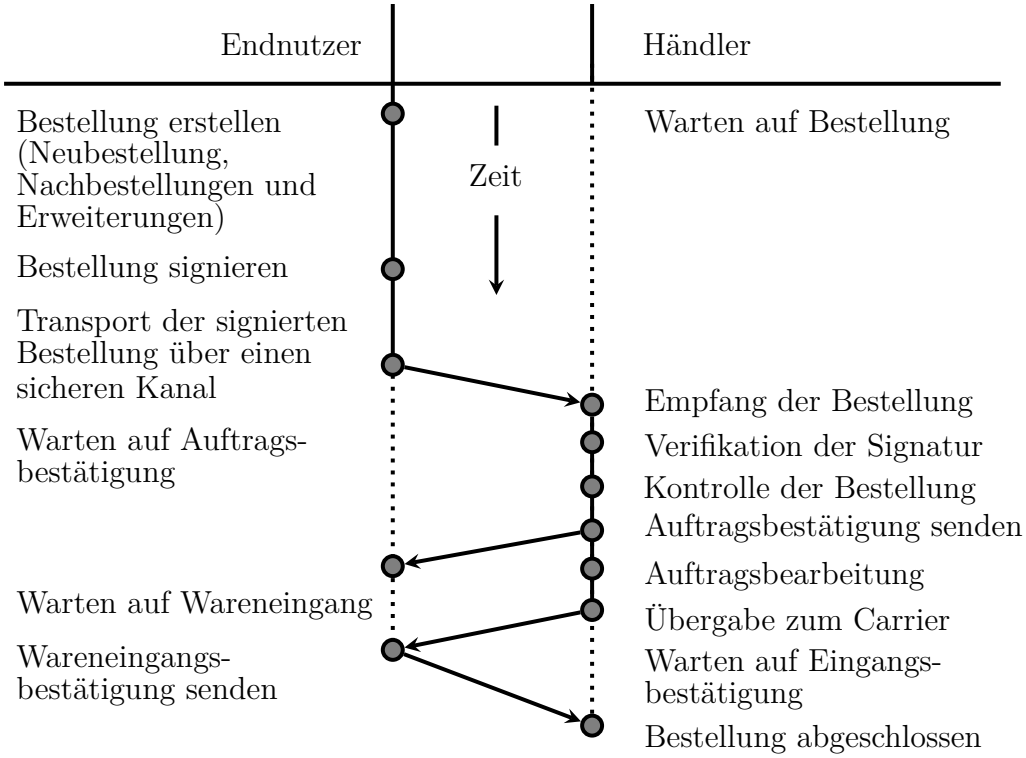

Abbildung 2: Zeitliche Abfolge eines idealtypischen Bestellvorgangs

Die in Abb. 2 dargestellten Schritte eines idealtypischen Bestellvorgangs, werden in den folgenden Abschnitten genauer thematisiert und in Hinblick auf neue Anforderungen an die Software untersucht.

5.1.1 Bestellung

Im ersten Schritt des Bestellvorgangs erstellt der Endnutzer die Bestellung. Sowohl für die erstmalige Einrichtung als auch für die Verwaltung von Schließanlagen existieren bereits entsprechende *LOCKBASE*-Softwaremodule der *Körtner & Muth GmbH.*

Nachdem der Endnutzer in der jeweiligen Software die zu bestellende Ware ausgewählt hat, soll daraus eine Bestellung generiert werden. Das vorliegende Konzept geht davon aus, dass bereits ein Bestellungsdatensatz vorliegt mit dem der Bestellvorgang begonnen werden kann. Dieser Bestelldatensatz sollte mit anderer Software, die auf die Erstellung eines solchen Datensatzes optimiert ist, erstellt werden.

5.1.2 Eigenhändige Unterschrift

Die im Ablaufdiagramm (siehe Abb. 2) nachfolgende Signatur der Bestellung erfordert ein geeignetes digitales Signaturverfahren.

Bruce Schneier beschreibt in seinem Buch *Angewandte Kryptographie* [Sch1996] die Problematik von eigenhändigen Unterschriften:

> ”
>
> - Eine Unterschrift ist **authentisch**. Sie überzeugt den Empfänger des Dokuments davon, dass der Unterzeichner das Dokument willentlich unterschrieben hat.
> - Eine Unterschrift ist **fälschungssicher**. Sie beweist, dass der Unterzeichner und kein anderer das Dokument unterschrieben hat.
> - Eine Unterschrift ist **nicht wiederverwendbar**. Sie ist Bestandteil des Dokuments und kann in kein anderes Dokument übertragen werden.
> - Das unterzeichnete Dokument ist **unveränderbar**. Nachdem das Dokument unterschrieben ist, kann es nicht mehr geändert werden.
> - Die Unterschrift **kann nicht zurückgenommen werden**. Unterschrift und Dokument liegen physisch vor. Die Unterzeichnerin kann später nicht behaupten, dass sie das Dokument nicht unterschrieben hat.
>
> In der Realität trifft keine dieser Aussagen über Unterschriften uneingeschränkt zu. Unterschriften können gefälscht oder von einem Dokument in ein anderes übertragen werden; man kann Dokumente auch nach ihrer Unterzeichnung noch ändern. Wir finden uns mit diesen Unzulänglichkeiten im allgemeinen ab, da Betrug schwierig ist und aller Wahrscheinlichkeit nach aufgedeckt wird. “
>
> [Sch1996, p. 41]

5.1.3 digitale Signatur

Um eine geeignete digitale Signatur zu erstellen, können verschiedene Methoden verwendet werden. Eigenhändige Unterschriften, wie die aus dem bisher eingesetzten Verfahren, können nicht trivial von Computern überprüft werden, daher werden für die

Kommunikation im Internet in der Regel kryptographische – und damit mathematisch verifizierbare – Methoden benutzt, um Daten zu signieren (vgl. [FP2012]).

„Eine digitale Signatur einer Nachricht ist eine Zahl, berechnet aus einem, nur dem Unterzeichner bekannten Geheimnis in Abhängigkeit zur signierten Nachricht“ [MOVR1997].

Um eine digitale Signatur zu berechnen, wird ein asymmetrisches kryptographisches Verfahren benutzt. Dafür wird ein Schlüsselpaar verwendet, dass aus einem privaten und einem öffentlichen Schlüssel besteht. In der Informatik wird dieses häufig mit den englischen Begriffen *Private-* und *Public-Key* bezeichnet. Bei einem digitalen Signaturverfahren wird der Private-Key genutzt, um mit Hilfe einer eindeutigen Rechenvorschrift eine Signatur zu berechnen.

Die Software soll die Bestellungen vor dem Versenden digital signieren, damit der adressierte Empfänger überprüfen kann, dass die Bestellung wirklich vom angegebenen Absender stammt und außerdem bei der Übertragung nicht verändert wurde. Dafür wird beim Absender die gewünschte Bestellung signiert und zusammen mit dem Public-Key des Absenders an den Empfänger versendet. Während die Integrität der Bestellung durch den signierten Hashwert automatisch sichergestellt werden kann, ist es dem Empfänger noch nicht möglich aus dem enthaltenen Public-Key auf die Identität des Absenders zu schließen.

Für die Zuordnung eines Public-Key zu einer Identität – einer bestimmten Person oder Firma – wird in der Informatik üblicherweise eine dritte Instanz genutzt, die von allen beteiligten Kommunikationspartnern als *vertrauenswürdig* angesehen wird. Häufig wird diese dritte Instanz als Trusted Third Party, kurz *TTP* bezeichnet. Die TTP könnte dem Empfänger nun anhand des Public-Keys die Identität des Absenders bestätigen.

Sofern keine TTP existiert, könnte der Empfänger die zugehörige Identität zum empfangenen Public-Key auch selbst überprüfen, indem er sich von dem Absender die Korrektheit des Public-Keys über einen sicheren Kanal bestätigen lässt. Dies erfordert allerdings, dass bereits ein sicherer Kanal besteht. Während diese Anforderung für die weltweite Kommunikation im Internet nicht haltbar ist, wäre sie hingegen für den Kontext einer Schließanlagenbestellung und dem häufig bereits bestehenden persönlichen Kontakt zwischen Endnutzer und Händler erfüllbar.

Als Anforderung soll dem softwarebasierten Bestellverfahren ein initialer persönlicher Austausch des Public-Keys ohne eine zusätzliche TTP genügen.

Des Weiteren ergibt sich die Anforderung an das Softwarekonzept, dass auch weiterhin Bestellungen ohne verifizierbare digitale Signatur empfangen werden können, da zum Zeitpunkt des Bestelleingangs dem Empfänger der Public-Key des Absenders noch unbekannt sein könnte. In diesem Fall muss der Empfänger die manuelle Überprüfung des Public-Keys nachholen oder mit anderen Identifikationsverfahren dafür Sorge tragen, dass die Bestellung beabsichtigt, unverändert und legitim ist. Außerdem soll es einem Händler möglich sein, eine Bestellung für einen Endnutzer selbst anzulegen,

damit es weiterhin möglich ist, dass ein Endnutzer die Bestellung persönlich im Geschäft des Schließanlagenhändlers tätigt. Die Software soll folgende Methoden für das Benutzerinterface bereitstellen:

- Bestelleingang mit einer **automatisch** verifizierten Signatur,
- Bestelleingang mit einer **manuell** zu verifizierenden Signatur (z. B. bei Verifikation über andere Verfahren),
- Bestelleingang **ohne** Signatur (z. B. wenn der Endnutzer persönlich bestellt).

5.1.4 Schlüsselmedium

Das beschriebene Verfahren geht davon aus, dass bei der Installation der Software ein Schlüsselpaar, ein Public- und ein Private-Key, erzeugt werden und entsprechend der o.g. Schritte verwendet werden, um Daten zu signieren. Das bedeutet aber auch, dass von nun an der Private-Key direkt mit der Identität des Benutzers in Verbindung gebracht wird. Gemeinsam mit dem Namen und der Adresse des Benutzers kann dies als eine Art digitale Sicherungskarte angesehen werden. Genau wie bei der bisher häufig verwendeten Sicherungskarte für Schließanlagen sollte dem Benutzer auch hier geraten werden, diese Daten an einem sicheren Ort aufzubewahren. Vor allem für unerfahrenere Computerbenutzer ist es oftmals einfacher, einen physischen Gegenstand als „wichtig“ zu betrachten und entsprechend sicher zu verwahren. Deshalb sollte es möglich sein, dass der Private-Key auf einem externen, physischen Speichermedium erzeugt werden kann.

Um der fortlaufenden Entwicklung der Datenträger gerecht zu werden, soll es dabei keine Rolle spielen, welche Art von Medium genutzt wird. Auch einmalig beschreibbare Medien, bzw. „read-only“ Medien sind geeignet, da der Private-Key sich nicht verändert und lediglich ausgelesen wird. Aktuell sind USB-Speichersticks, SD-Karten oder Chipkarten geeignete Beispiele. Problematisch an diesen Datenträgern ist jedoch, dass der Private-Key von Computerviren und jedem ausgelesen und kopiert werden kann der Zugriff auf diese (auch für nur kurze Zeit) hat, deshalb werden für solche Anwendungen spezielle Chipkarten mit Kryptoprozessor eingesetzt, der ein autonomes Signaturverfahren ermöglicht, dass ausschließlich durch die Hardware der Chipkarte ausgeführt wird. Ein Nutzer erhält nach Übertragung von Daten durch eine Schnittstelle an die Chipkarte, die signierten Daten auf dem gleichen Weg zurück. Bei dieser Art von Chipkarte sollte es nicht möglich sein, den genutzten Private-Key auszulesen. Durch den hohen Sicherheitgrad der Karten begründet sind diese Art von Chipkarten allerdings teurer, als die anderen vorgestellten Datenträger. Möchte man dennoch die auslesbaren Datenträger verwenden, sollte zumindest eine zusätzliche symmetrische Verschlüsselung des Private-Keys erfolgen, um einen erhöhten Schutz gegen unberechtigte Nutzung und gegen manche Computerviren zu erreichen. So könnte der User seinen Private-Key zusätzlich durch die Eingabe eines Passworts schützen.

Während grundsätzlich sinnvoll und wichtig ist, dass der Private- und Public-Key bei den jeweiligen Benutzern lokal generiert wird, könnte diese Regel zu Gunsten der

einfacheren Benutzbarkeit und erhöhten Akzeptanz im Einzelfall auch aufgehoben werden. Denn zumindest im Kontext der Schließanlagenbestellung besitzt der Händler alle Schlüsselschneidwerte und Zylinderbestiftungspläne des Endnutzers und hat damit Zugriff auf alle sensiblen Schließanlagendaten. Der Händler genießt in der Praxis demnach volles Vertrauen seiner Kunden. Vor diesem Hintergrund ist es unbedenklich, dass der Händler mit Errichtung der Schließanlage ein Schlüsselmedium mit bereits generierten Private-Key an den Endnutzer aushändigt. Dies hätte den weiteren Vorteil, dass dem Händler der Public-Key seines Kunden sofort bekannt wäre und kein zusätzlicher Aufwand für den Abgleich des Public-Keys betrieben werden müsste. Dennoch sollte jedem Benutzer jederzeit die Möglichkeit geboten werden, ein neues Schlüsselpaar zu generieren und den gewünschten Kommunikationspartnern den neuen Public-Key zukommen zu lassen.

Das Lesen von Private-Keys aus externen Datenquellen, die Ansteuerung von Kartenlesern u. ä. Geräten und die symmetrische Entschlüsselung durch ein eingegebenes Passwort sind somit weitere Anforderungen an die Bestellsoftware.

5.1.5 Übertragung

Für die Übertragung muss der Software der gewünschte Empfänger bekannt sein. In der Schließanlagenindustrie hat der Endnutzer für jede Schließanlage üblicherweise genau einen Schließanlagenhändler, der die benötigten Daten zur Fertigung von neuen Schlüsseln oder Erweiterungen besitzt. Dieser Händler soll beim Ausliefern der Software mit den entsprechenden Schließanlagendaten im Adressbuch des Endnutzers bereits angelegt werden können.

Die als nächstes zu übertragende Bestellung besitzt zwar eine digitale Signatur und ist somit vor Verfälschung geschützt, kann aber dennoch auf dem Übertragungsweg leicht mitgelesen werden. Da es sich bei den übertragenen Daten laut Aufgabenstellung um sensible Daten handelt (siehe Abschnitt 4 auf Seite 8), ist dies kein akzeptabler Zustand. Um das Schutzziel Vertraulichkeit zu erfüllen, müssen die Daten über einen nicht abhörbaren Kanal übertragen oder vor der Übertragung verschlüsselt werden. Für die Software *LOCKBASE* existiert bereits das Modul *B2B*, welches einen sicheren Kanal zur Verfügung stellt, sodass dieser direkt genutzt werden könnte. Da dieses Verfahren bereits die Verwendung von Private- und Public-Keys vorsieht, kann damit leicht eine asymmetrische Verschlüsselung der Daten erreicht werden, sodass die verschlüsselten Daten auch über unsichere Kanäle, wie z. B. via E-Mail, übertragen werden könnten. Eine weitere Anforderung an das softwarebasierte Bestellverfahren ist demnach, dem Nutzer mindestens eine der genannten Möglichkeiten zum Versand anzubieten.

Auf der Seite des Empfängers soll dem Übertragungsweg entsprechend der Eingang der versandten Bestellung gestaltet werden. Auch hier kann das existierende *LOCKBASE B2B* Softwaremodul genutzt werden, um die Bestellung in das Postfach des Empfängers zu importieren. Damit jedoch jeder beliebige Übertragungsweg gewählt werden kann, besteht die Anforderung an die Software, dass dem Benutzer auch ein manueller

Import der signierten Daten ermöglicht wird. Die Entschlüsselung sollte allerdings je nach Übertragungsweg im Voraus durchgeführt werden, da nur der Import von Daten im Klartext vorgesehen wird.

5.1.6 Verifikation

Nachdem die Bestellung beim Empfänger eingegangen ist, soll die Signatur der Bestellung verifiziert werden. Bei einer Verifikation handelt es sich um den mathematischen Beweis, dass Daten der vorgegebenen Spezifikation entsprechen. Die übertragene Bestellung besteht, wie oben beschrieben, aus den Bestelldaten in Klartext, dem signierten Hashwert der Bestelldaten und dem Public-Key des Absenders (siehe Abschnitt 5.1.3 auf Seite 16). Auf technischer Seite wird für die Verifikation der signierte Hashwert mit dem Public-Key des Absenders zurückgerechnet und das Ergebnis mit dem selbst gebildeten Hashwert der Bestelldaten verglichen. Sind beide Hashwerte gleich, dann kann davon ausgegangen werden, dass es sich um die vom Absender gewollte und unveränderte Bestellung handelt. Dies basiert auf der Annahme, dass es ohne den Besitz des Private-Keys des Absenders nicht möglich ist, eine Signatur für den Hashwert der Bestellung zu berechnen, die mit dem Public-Key des Absenders zurückgerechnet werden kann, und dass es bei der angewandten Hashfunktion nicht möglich ist, eine zweite sinnvolle Bestellung zu finden, die den gleichen Hashwert der originalen Bestellung hat. Damit beide Kommunikationspartner die gleichen Rechenoperationen verwenden, muss vorher ein spezifisches Verfahren festgelegt werden. *RSA*[4] ist ein populäres Beispiel für so ein kryptographisches Verfahren.

5.1.7 Auftragsbearbeitung

Nachdem sichergestellt wurde, dass es sich um eine unverfälschte Bestellung von dem angegeben Endnutzer handelt, folgt die eigentlich Auftragsbearbeitung auf Seiten des Empfängers. Hierzu gehören unter anderem die Kontrolle auf Vollständigkeit und Umsetzbarkeit der eingegangenen Bestellung. Erst nach einer manuellen Bestätigung wird eine Auftragsbestätigung an den Kunden versendet. Dies soll über den vom Endnutzer favorisierten Kommunikationskanal geschehen, z. B. via E-Mail, SMS oder telefonischer Benachrichtigung. Als weitere Anforderung für die Software sollte der Händler eine Bestellung als „überprüft“ markieren, und für den Endnutzer eine gewünschte Benachrichtigungsart definieren können.

Häufig können Händler die Artikel aus der eingegangene Bestellung nicht selbst fertigen und bestellen diese stattdessen beim Schließanlagenhersteller. Für diesen Fall kann der Händler eine Bestellung an den Hersteller erstellen und benötigte Teile und Anfertigungen bei diesem in Auftrag geben. In der Praxis wird der Händler möglichst

[4] RSA (Rivest, Shamir und Adleman) ist ein asymmetrisches kryptographisches Verfahren, dass sowohl zur Verschlüsselung als auch zur digitalen Signatur verwendet werden kann. [RSA1978]

viele der bestellten Ware aus dem eigenen Bestand verkaufen und bei dem Hersteller nur solche Ware bestellen, die der Händler selbst nicht fertigen kann oder nicht mehr auf Lager hat. Häufig werden auch Artikel aus den Bestellungen von verschiedenen Endnutzern gleichzeitig beim Hersteller bestellt, um unnötige Versandkosten zu sparen. Die Möglichkeit einer schlichten „Weiterleitung“ der Bestellung ist damit in den meisten Fällen nicht sinnvoll und kann als optionale Anforderung an die Software betrachtet werden.

Nachdem der Händler die bestellte Ware zusammengestellt hat, übergibt er diese, adressiert an seinen Kunden, einem Carrier, z. B. einem Spediteur. Weitere Geschäftsprozesse, wie Abrechnung und Buchhaltung sollen nicht Inhalt dieses Konzepts sein. Abschließen sollte der Händler den Bestellprozess allerdings erst, nachdem er eine Wareneingangsbestätigung von seinem Kunden erhalten hat. Diese soll entweder vom Kunden mit Hilfe der Bestellsoftware versandt werden, oder vom Händler manuell eingetragen werden können. Diese zusätzliche Kontrolle stellt sicher, dass die bestellte Ware nicht z. B. verloren gegangen ist. Die Bestätigung des Kunden kann als zusätzliche Sicherheitseinrichtung betrachtet werden, deren Anforderung ebenfalls optional ist.

5.2 Zusammenfassung der Anforderungen

Durch die Untersuchung der einzelnen Schritte des Bestellablaufs ergeben sich einige Anforderungen an das Konzept für die Software. Zuerst muss ein Bestelldatensatz vorliegen, der danach von der Bestellsoftware signiert wird. Es soll sich also um kein alleinstehende Anwendungen handeln, sondern um ein Modul dass nach der Auswahl der zu bestellenden Ware aufgerufen wird. Mit dem Aufruf des Bestellmoduls sollen zunächst der vorliegende Bestelldatensatz signiert werden. Das setzt voraus, dass bereits ein Private-Key existiert, der im Signaturvorgang genutzt werden kann. Das Modul soll Methoden für die Erstellung eines Schlüsselpaars, das Einlesen eines passwortgeschützten Private-Keys und die Ansteuerung von externen Signaturgeräten bieten mit denen der Bestelldatensatz signiert wird. Um die signierten Daten an den korrekten Absender zu versenden, soll die Möglichkeit bestehen den gewünschten Empfänger aus einem Adressbuch auszuwählen. Dies hat den Vorteil, dass keine Fehler bei der Eingabe der Empfangsadresse passieren können, und bietet zusätzlichen Komfort für den Benutzer. Die Übertragung der signierten Daten an den ausgewählten Empfänger soll über ein sicheres externes Verfahren geschehen. Zu Gunsten des Komforts soll die Übergabe an ein konfiguriertes Verfahren transparent für den Benutzer passieren.

Für den Empfang von Bestellungen existieren weitere Anforderungen, die für die Gruppe der Endnutzer jedoch nicht relevant sind. Aus diesem Umstand ergibt sich, dass der bestellende Endnutzer eine andere Benutzeroberfläche benötigt, als der empfangende Händler. Für den Händler sind die vorher genannten Anforderungen jedoch genauso notwendig, da auch hier Bestellungen an Hersteller oder andere Händler getätigt werden können.

Zunächst sollen eingehende Bestellungen automatisch und transparent für den Benutzer von den konfigurierten Übertragungswegen importiert werden. Trotzdem soll es dem Benutzer möglich sein, Bestellungen auch manuell zu importieren. Nach Empfang einer Bestellung, soll zuerst die Signatur verifiziert werden, dafür ist notwendig, dass die Software Zugriff auf eine Datenbank mit Public-Keys von Kommunikationspartnern verfügt. Mit Hilfe des entsprechenden Public-Keys kann daraufhin die Gültigkeit der Signatur verifiziert werden. Das Ergebnis soll dem Benutzer entsprechend visualisiert werden. Außerdem sollte es möglich sein, dass der Benutzer die Signatur auch zu einem späteren Zeitpunkt nochmals verifizieren kann, z.b. nach Erhalt des korrekten Public-Keys. Mit Beginn der Bearbeitung der eingegangen Bestellung sollte dem Benutzer ermöglicht werden, die verschiedenen Bestellungen mit einem Auftragsstatus zu versehen. Dies soll ebenfalls entsprechend visualisiert werden.

Nach Erhalt der Ware besteht die optionale Anforderung, dass der Besteller den Wareneingang in der Software bestätigt, sodass auf Seite des Händlers schnell ersichtlich ist, dass beim Transport der Ware keine Fehler aufgetreten sind.

Bei den beschriebenen Anforderungen handelt es sich um die Mindestanforderungen um ein softwarebasiertes Bestellverfahren umzusetzen zu können, das dem diskutierten Wunsch nach Komfort im Bestellprozess nachkommt, als auch den Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit genügt. Das vorgestellte Konzept bietet zusätzlich Potential für Erweiterungen, die in dem folgenden Abschnitt diskutiert wird.

5.3 Erweiterungspotential

5.3.1 Schlüsselmedium mit unterschiedlichen Rechten

Basierend auf dem Konzept der Sicherungskarte ist es naheliegend, dass es nicht nur einen bevollmächtigten Benutzer gibt, sondern verschiedenen Benutzern individuelle Rechte definiert werden können. So könnten für eine große Schließanlage mehrere Personen für die Bestellung und Ausgabe von Schlüsseln zuständig sein. Ein Beispiel dafür sind Universitätsgebäude mit verschiedenen Arbeitsbereichsleitern, die ihren neuen Mitarbeitern selbst Schlüssel aushändigen wollen, aber weder die Schlüssel von anderen Arbeitsbereichen, noch Erweiterungen durch zusätzliche Schließzylinder bestellen dürfen.

Das bisherige Konzept kann leicht auf mehrere legitime Besteller mit jeweiligen Public-Keys ausgeweitet werden. In den Schließanlagendaten beim Händler werden die Bestellberechtigungen den einzelnen Personen, bzw. deren Public-Keys zugeordnet. So kann beim Bestelleingang, nach der Verifikation der Signatur, automatisch entschieden werden, ob der Besteller berechtigt ist die jeweilige Ware zu erhalten. Da die Rechtevergabe technisch innerhalb der Schließanlagendaten gespeichert wird, und diese i. d. R. beim Schließanlagenhändler hinterlegt sind, sollte der Händler ebenfalls innerhalb der Rechte-Hierarchie platziert sein, mit der Berechtigung zur Rechtevergabe.

In der Praxis werden vor allem große Schließanlagen für überregionale Institute oder Firmen häufig von den Herstellern der Schließanlagen direkt beliefert und durch per-

sönliche Vertreter oder Zwischenhändler an den jeweiligen Orten betreut. Derzeit können komplexere Handelsketten nur aufwändig realisiert werden, sodass die Hersteller große Endkunden häufig im Direktvertrieb beliefern. Dies schadet vor allem den örtlichen Fachgeschäften und reduziert langfristig die individuelle Beratungsleistung. Durch eine digital verwaltete Rechte-Hierarchie wäre es möglich, dass die jeweiligen Bereiche einer überregionalen Schließanlage bei den örtlichen Händlern Bestellungen aufgeben, die Händler ihren Möglichkeiten entsprechend Ware ausliefern und den Rest der Bestellung an die überregionalen Schließanlagenhersteller weiterleiten. Dadurch könnten die Schließanlagenhändler den Kontakt zu ihren regionalen Kunden stärken, und weiterhin eine Fachberatung anbieten.

5.3.2 PIN / TAN Verfahren

Im Rahmen dieser Arbeit wurde hauptsächlich der Einsatz von digitalen Signaturen zur Identifikation der befugten Besteller genutzt. Eine andere Möglichkeit wäre der Einsatz von PIN / TAN Verfahren, wie es beim Homebanking und vielen anderen Anwendungen ebenfalls üblich ist. Die Bekanntheit und das bereits vorhandene Vertrauen in dieses Verfahren wäre ein großer Vorteil zum Erhöhen der Akzeptanz innerhalb der Schließanlagenindustrie. Bei den ausgegeben individuellen TAN-Bögen handelt es sich einmalig verwendbare Geheimnisse mit denen die Bestellungen authentifiziert werden könnten und die, durch den zusätzlichen Schutz eines PINs, nicht von unbefugten Personen benutzt werden können, trotzdem gelten auch die diese die gleichen Sicherheitsrisiken wie für Sicherungskarten. Jedoch mit dem Vorteil, dass TANs nur einmal verwendet werden können und somit gegen die Gefahr von Kopien geschützt sind. So könnte ein Bote diesen zwar einfach kopieren, allerdings nicht wiederholt zur Bestellung nutzen. Die komplexe Verwaltung der TAN-Listen auf Seite der Schließanlagenhändler, wäre hingegen ein großer Nachteil. Auch Endnutzer mit mehreren Schließanlagen müssten für jeden adressierten Händler eine eigene TAN-Liste nutzen.

5.3.3 Webshop

Das vorgestellte Konzept ist auch hinsichtlich der Unabhängigkeit der Plattform erweiterbar. So könnte durch den Betrieb auf einem Webserver ein Online-Shop für Schließanlagen entstehen. Durch die Anbindung von weiteren Modulen der *LOCKBASE*-Software steht eine umfangreiche und komfortable Verwaltung von Schließanlagen in Aussicht.

6 Fazit

In dieser Arbeit wurde ein Konzept für eine Software zur Bestellung von Schließanlagenkomponenten erarbeitet, den Sicherheitsanforderungen der Schließanlagenindustrie angepasst und durch bekannte Sicherheitsaspekte aus der Informatik verbessert. Es wurden Überlegungen und Vorschläge zum Aufbau der Benutzeroberfläche vorgestellt und in Ausrichtung auf die zu erwartende Akzeptanz und Komfortabilität in der Benutzung angepasst.

Bei dem vorgestellten Prinzip der signierten und verschlüsselten sicheren Kommunikation handelt es sich um ein spezielles Verfahren, das den besonderen Umständen der Schließanlagenindustrie angemessen entwickelt wurde.

Literatur

[Abu2012] Abus: *Der Schlüssel, täglicher Gebrauchsgegenstand für Häuser, Wohnungen, Autos, Fahrräder, Motorräder usw.* `http://abus.de/de/main.asp?ScreenLang=de&select=0212`, 2012. – zuletzt abgerufen am 23.08.2012

[BSI2009] BSI: *Online-Glossar des Bundesamtes für Sicherheit in der Informationstechnik.* `https://www.bsi.bund.de/cln_174/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html`, 2009. – zuletzt abgerufen am 17.09.2012

[FP2012] Federrath, Hannes ; Pfitzmann, Andreas: *Datenschutz und Datensicherheit In: Uwe Schneider, Dieter Werner (Hrsg.): Taschenbuch der Informatik.* 7. Carl Hanser Verlag GmbH & CO. KG, 2012

[MOVR1997] Menezes, Alfred J. ; Oorschot, Paul C. V. ; Vanstone, Scott A. ; Rivest, R. L.: *Handbook of Applied Cryptography.* 1997

[RSA1978] Rivest, Ronald L. ; Shamir, Adi ; Adleman, Leonard M.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. In: *Commun. ACM* 21 (1978), Nr. 2, S. 120–126

[Sch1996] Schneier, Bruce: *Angewandte Kryptographie - Protokolle, Algorithmen und Sourcecode in C.* Addison-Wesley, 1996

Erklärung

Ich versiche, dass ich die Arbeit selbstständig verfasst und keine anderen, als die angegebenen Hilfsmittel – insbesondere keine im Quellenverzeichnis nicht benannten Internetquellen – benutzt habe, die Arbeit vorher nicht in einem anderen Prüfungsverfahren eingereicht habe und die eingereichte schriftliche Fassung der auf dem elektronischen Speichermedium entspricht.

Ich bin mit der Einstellung der Bachelor-Arbeit in den Bestand der Bibliothek des Fachbereichs Informatik einverstanden.

Hamburg, 22. September 2012

Tim Krämer