

# Sicherheit im Bankensektor

Die Schlüssel eines Unternehmens stellen einen der wichtigsten Vermögenswerte dar, denn Schlüssel ermöglichen den Zugang zu Gebäuden, Aktenschränken, Spinden, Fahrzeugen, Tresoranlagen, Serverschränken, Computern und zum Personal. Schlüssel werden benutzt, um Schutz und Sicherheit, Gesundheit und Vertrauen zu gewährleisten. Schlüssel existieren in vielfältiger Form, nicht nur als mechanische Ausführung mit dem berühmten Schlüsselbart, sondern auch als RFID oder Funk-Transponder, Magnetkarten, USB-Security-Sticks und als PIN-Code für Terminals. Nur wer jederzeit exakt und lückenlos darüber informiert ist wo die vielfältigen Schlüssel seines Unternehmens sich befinden, schützt das Unternehmen von Innen nach Außen.

In vielen Banken wird leider immer noch auf der Basis der altbekannten Karteikarte gearbeitet. Die Ausgabe eines Schlüssels erfolgt durch eine Person, wird handschriftlich notiert und alle beteiligten Personen hoffen darauf, dass sich der Schlüssel auch bald wieder einfindet. Nicht selten erfolgt danach eine Suchaktion mit allen bekannten negativen Auswirkungen in finanzieller und personeller Richtung, bis hin zur gravierenden Störungen des Betriebsklimas. Selbst bei einer Zugriffsbeschränkung auf nur 2 oder 3 Personen kann man die Erfahrung einer größeren Bank anführen, in der eines Tages der Zentralschlüssel nicht mehr auffindbar war und nicht nachvollziehbar war, welche Person ihn zuletzt in den Händen hatte. Das Ergebnis war der Austausch von 2000 Türschlössern.

Gelagert werden die Schlüssel meist in Schubladen, Schlüsselkästen oder in sogenannten Schlüsselsafes. Die Schlüsselsafes suggerieren dem Anwender zwar eine höhere Sicherheit als ein Schlüsselkasten, aber letztendlich ist nach der Öffnung des Schlüsselsafes trotzdem jede vorsätzliche oder unbeabsichtigte Manipulation möglich. Nicht selten werden Schlüsselsafes bei Arbeitsbeginn geöffnet und erst wieder am Abend geschlossen, weil die mehrmalige Öffnung im Tagesgeschäft für die beteiligten Personen zu umständlich ist.

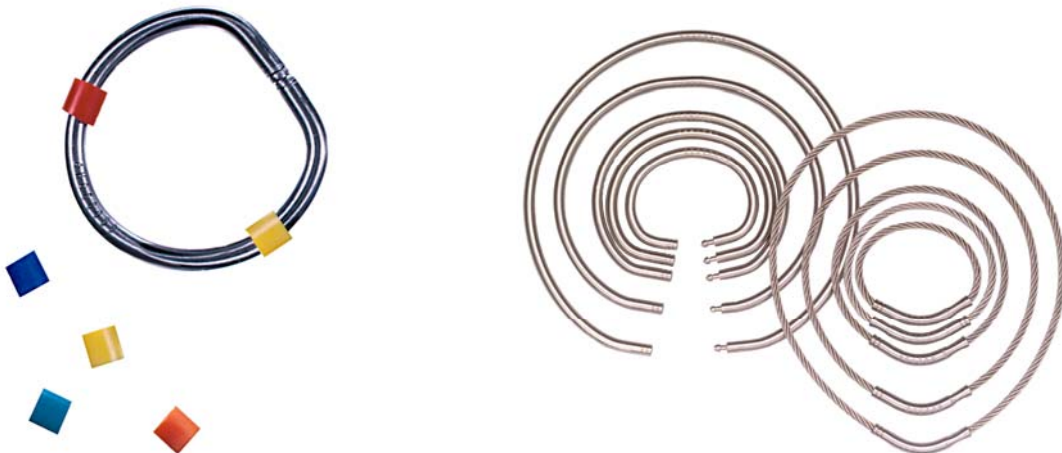
Die einzige Lösung, die eine manipulationsfreie, lückenlose und bequeme Entnahme und Rückgabe von Schlüsseln und Objekten jeglicher Art gewährleistet, sind Rechner gesteuerte Schlüsselschränke und Fachanlagen mit elektronisch einzigartiger Inhaltserkennung, wie sie z.B. von TRAKA in verschiedenen Größen angeboten werden.



## Der Intelligenz-Bolzen



Die Basis der Traka-Systeme ist ein robuster intelligenter Metallstift, der Traka-iFOB. Dank seiner Form besitzt er eine automatische Selbstreinigung. Der Traka-iFOB ist mit einem 2-poligen Mikrochip ausgestattet und benötigt aus diesem Grund nur 2 einfache Kontakte (wartungsfrei) und keine zusätzlichen Komponenten wie z.B. einen Microschalter oder eine Lichtschranke, wie sie bei RFID basierenden Systemen verwendet werden müssen. Zusätzlich zu seiner robusten Konstruktion ergibt sich über den integrierten Datenlogger auch die Möglichkeit, dass er nicht nur ein intelligenter Schlüsselerkennungsstift ist, sondern auch selbst zu einem intelligenten protokollierenden Schlüssel werden kann, dem sogenannten Traka-Immobilisator.



Die Schlüssel oder Objekte werden mit robusten Sicherheitsplomben, verfügbar bis 4mm Edelstahl, mit dem iFOB fest verbunden und können nur durch massive Gewalteinwirkung zerstört werden. Eine optionale Plombennummer in Verbindung mit der automatischen Plombennummerabfrage des Schlüsselschrankes gewährleistet, dass kein Manipulationsversuch unentdeckt bleibt. Aufgrund der Codierung der intelligenten Stecker (iFOB) und der zusätzlichen Einzelplatzverriegelung können berechnete Personen oder Personengruppen nur die Ihnen zugewiesenen Schlüssel, Schlüsselbunde oder Objekte entnehmen. Nicht zugewiesene Schlüssel oder Objekte sind mechanisch über einen Stahlbozen verriegelt und können nicht entnommen werden. Der Sicherheitsverantwortliche kann jeder Person oder Personengruppe für jeden einzelnen Schlüssel oder Schlüsselbund die Zugriffsberechtigung erteilen oder unmittelbar wieder sperren. Die Freigabe der Schlüssel ist individuell und gruppenweise für verschiedene Nutzer zeitabhängig programmierbar. Dies ermöglicht eine permanente, dezentrale



Überwachung sämtlicher Entnahmen und Rückgaben durch den Verantwortlichen, vor Ort und/oder über das Firmen-Netzwerk.

Die Öffnung der Schranktür erfolgt nur mittels Zugangsberechtigung der entsprechenden Person. Diese Berechtigung kann in Form einer Geheimzahl (PIN-Code), einer Magnetkarte, einer Chipkarte, eines Transponders oder durch *biometrische Identifikation*, z.B. der leistungsfähige SAGEM-Fingerprintreader, erteilt werden. Als Novität besteht die Möglichkeit, sämtliche kundenspezifischen Erkennungsmodule in die Kontrolleinheit zu integrieren. Das optimiert die Akzeptanz und senkt signifikant die Kosten, da keine zusätzlichen Erkennungskarten oder Module ausgegeben werden müssen. Durch die Kombination mit einer zusätzlichen PIN-Eingabe wird ein unberechtigter Zugang, bei Verlust der Zugangskarte oder des Zugangsmoduls, verhindert. Damit kann ebenfalls festgelegt werden, daß bestimmte Schlüssel nur in Gegenwart einer zweiten Person entnommen werden dürfen – das sogenannte Vier-Augen-Prinzip.

Im Gegensatz zu anderen Systemen arbeiten die Schlüsselschränke von TRAKA grundsätzlich mit einer festen Ordnung, d.h. die Schlüssel oder Schlüsselbunde werden immer wieder an ihren fest definierten Steckplatz zurückgesteckt. Dadurch wird die Schlüsselorganisation übersichtlicher und die Entnahme und die Rückgabe wesentlich beschleunigt. Eine signifikante Zeitersparnis bei größeren Applikationen und/oder umfangreichen Schichtwechseln. Je nach Anwendungsfall besteht aber auch die Möglichkeit der wahlfreien Rückgabe (Random Return), sowohl innerhalb eines Schrankes als auch über multiple Systemanwendungen (Multiple Random Return) inkl. einer einfachen Oberfläche zur Schlüsselverfolgung und Lokalisierung im System, des sogenannten Traka-KeyWizards.

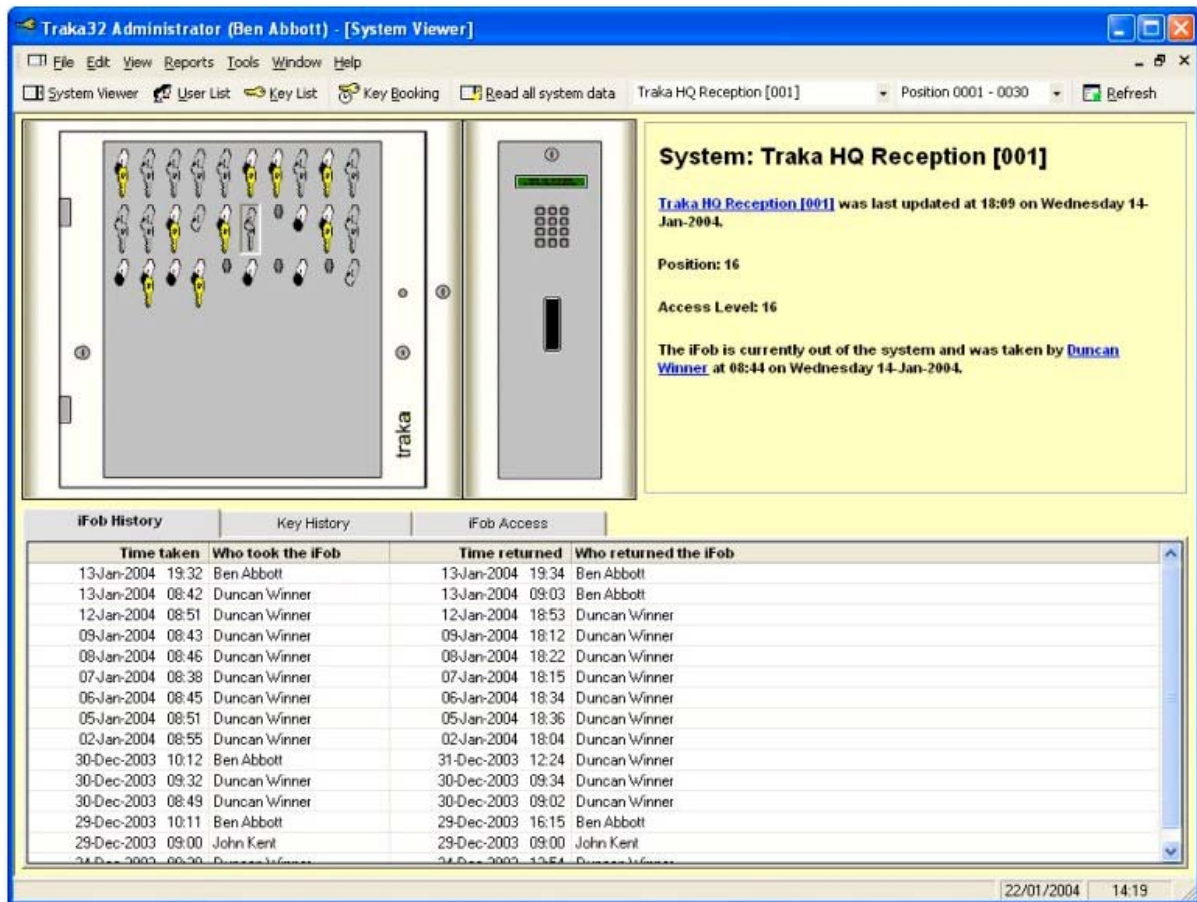
Ein integrierter Akku gewährleistet Netzunabhängigkeit. Je nach Zugriffshäufigkeit ist ein netzstromunabhängiger Betrieb für 10 Tage und mehr gewährleistet. Der integrierte Prozessor kann das komplette Schlüsselsystem über die Kontrolleinheit ebenfalls autark betreiben. Die Displayabfrage ermöglicht die Abfrage der Schlüsselvergabe und letzten Nutzung direkt vor Ort. Mit Hilfe einer Netzwerkkarte und einer entsprechenden TCP/IP-Adresse kann der Datenabgleich auch über das Internet erfolgen, inklusive ferngesteuerter Einzelplatz-Entriegelung und Notfall-Entriegelung. Die Datenübertragung über ein WLAN gewährleistet Ortsunabhängigkeit und vermeidet zusätzliche Kosten für Kabelinstallationen.. Wenn keine Netzwerkverbindung besteht, können die Traka-Systeme die entsprechenden Zugriffsereignisse bis zu 12 Monate zwischenspeichern.

TRAKA - Schlüsselschränke können aber viel mehr kontrollieren als nur Schlüssel – mit den neuen **Depot-Streifen** besitzen sie sogar Fächer in der Größe eines Handys, Kartenhalters, kleine Funksprechgeräte und Pager/Piepser. Für größere Gegenstände wie z.B. Laptops, PDAs und andere mobile Geräte aus dem Computerbereich bieten sich die **intelligenten Fachanlagen** mit elektronischer Fachinhaltserkennung an.



Diese Art von Fachanlagen wird für die kontrollierte Lagerung sensibler Dokumente immer interessanter. Die einzelnen Fächer gibt es in unterschiedlichen Größen, z.B. auch für DIN A4 Ordner und werden mit einer RFID-Fachinhaltserkennung ausgestattet. Die einzulagernden Dokumente erhalten einen RFID-Transponder, welcher fest in das Dokument integriert wird. Die Entnahme und Rückgabe des Dokumentes wird unmittelbar vom Steuerrechner der Fachanlage registriert und dem Sicherheitsverantwortlichen gemeldet. Bei der Rückgabe des Dokumentes wird zusätzlich zum Inhalt auch die Einlagerung in das fest zugewiesene Fach geprüft und bei Unstimmigkeit sofort ein Alarm abgesetzt.

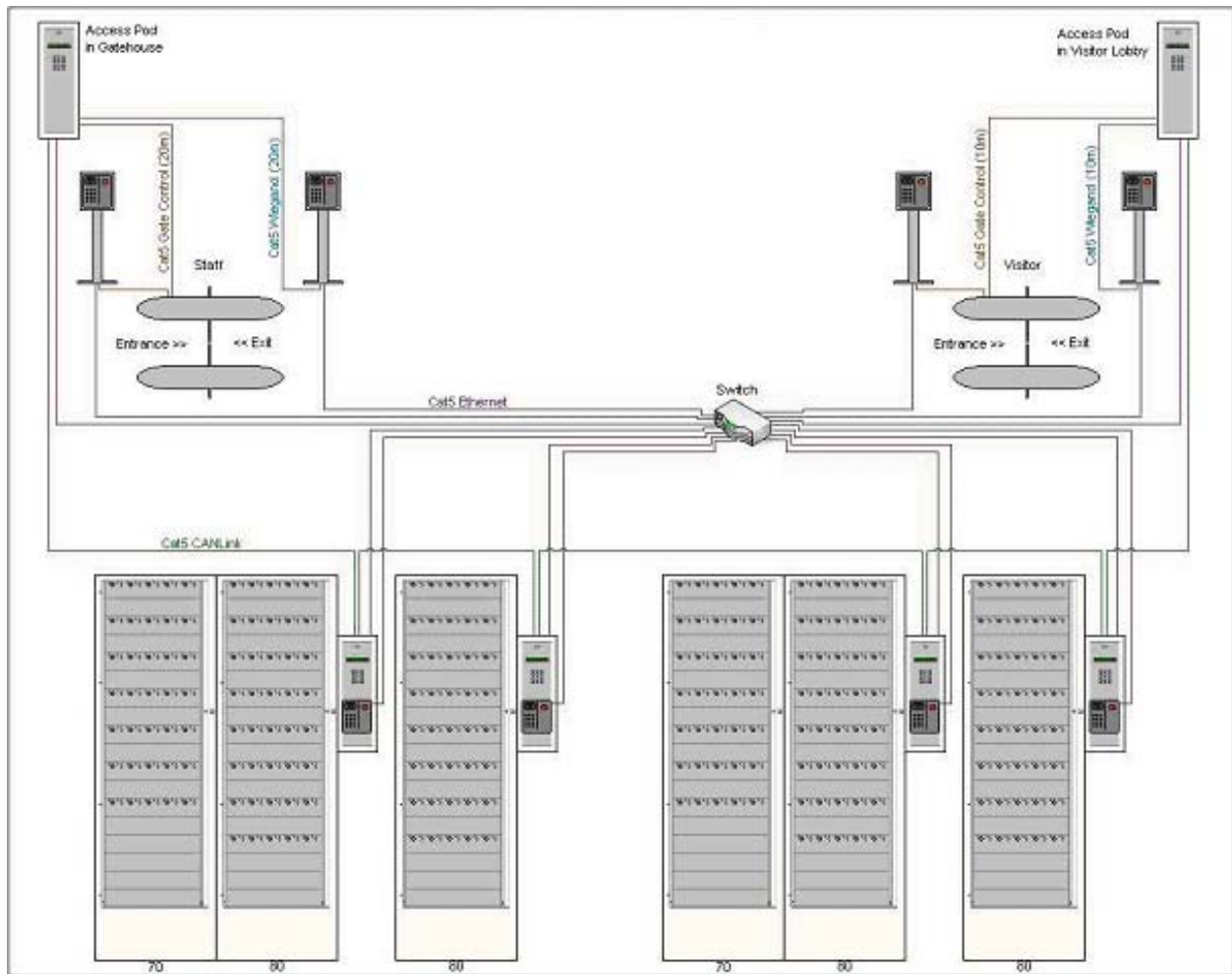
## Client/Server Management Software



Alle Schlüsselschränke und Fachanlagen werden mit der Traka32 Managementsoftware konfiguriert und die entsprechenden Schlüssel- und Objekt-Zugriffe manipulationsfrei protokolliert. Die Traka32 Software ist als Client/Server strukturiert und kann entweder auf einem lokalen Rechner installiert werden, der unmittelbar mit der TRAKA-Kontrolleinheit über die Ethernet-Schnittstelle verbunden ist, oder auf einem beliebigen Host im Unternehmensnetzwerk inkl. Terminal-Server Betrieb. Es ist nicht unbedingt erforderlich, dass sich Traka32 kontinuierlich im "online" Modus befindet. Nur für die Momente der Datenbanksynchronisation, bei Änderungen in der Berechtigungsstruktur und für Schlüssel-Parametrisierungen muß eine Datenverbindung geschaltet werden.



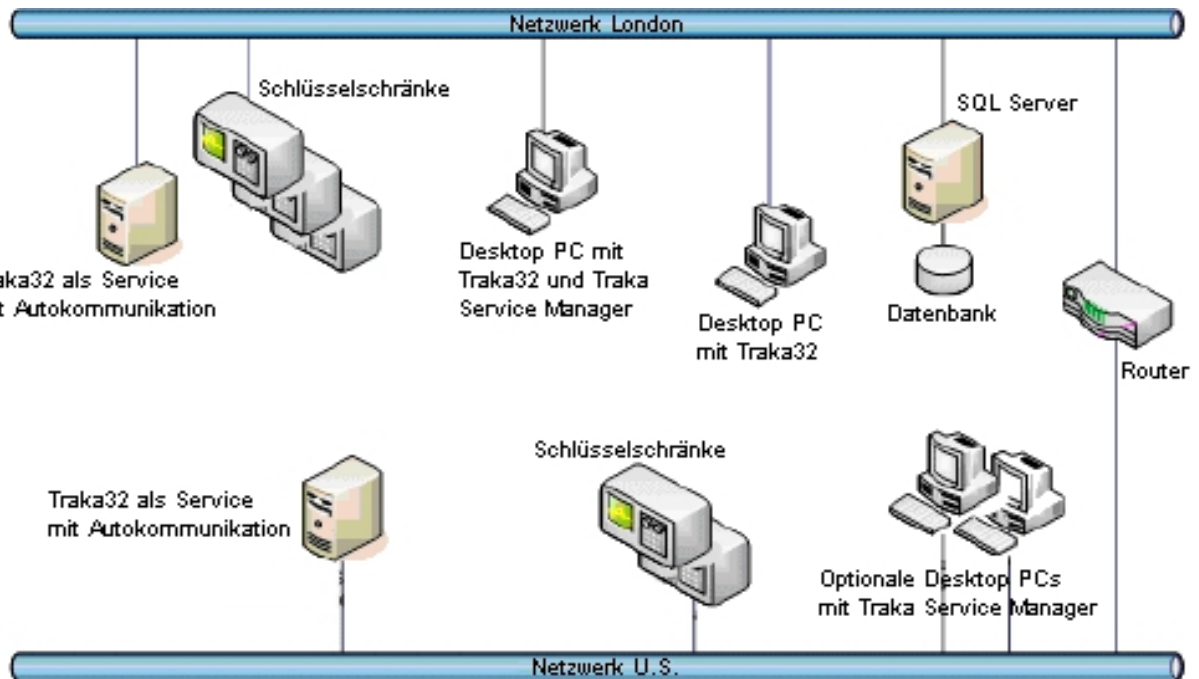
## Echtzeit-Objektüberwachung in Sicherheitsbereichen



Für die Schlüssel und Objektüberwachung in Sicherheitsbereichen wurde das CAN-Link-Interface entwickelt. Sicherheitsrelevante Schlüssel und Objekte können weder versehentlich noch gewollt den inneren Sicherheitsbereich verlassen. Vor dem Betreten des äußeren Bereiches kontrolliert Traka-CAN-Link über den Status entnommener Objekte. Erst nach positiver Rückmeldung von Seiten der Schlüsselschränke und Fachanlagen, d.h. Rückgabe aller entnommenen Schlüssel und Objekte, werden die Schleusen freigegeben. Der entsprechende Abfrageprozess wird innerhalb von 1 Sekunde realisiert, damit keine unnötigen Wartezeiten an den Schleusen oder Vereinzelungsanlagen entstehen. Die Kommunikation erfolgt über ein, in den Steuereinheiten (POD) der Schränke und in den Steuereinheiten der Vereinzelungsanlagen installiertes, CAN-BUS Modul (CAN = Controller Area Network).



## Weltweite Online-Überwachung für Großbanken



Mit Hilfe der **TAAS Funktionalität** der Traka32 Managementsoftware können die Computer gesteuerten Schlüsselschränke und Fachanlagen von TRAKA nicht nur über ein lokales Netzwerk online kontrolliert werden, sondern auch weltweit netzübergreifend im Konzernverbund. Die Traka32 Managementsoftware als Windows Service (TAAS = Traka32 as a Service) installiert, ermöglicht den Betrieb der Software im Hintergrund eines online geschalteten PCs. TAAS benötigt keine Benutzeroberfläche und arbeitet, auch wenn kein Benutzer eingeloggt ist. Dies ist ein großer Vorteil für Unternehmen, die Funktionen wie die Autokommunikation benötigen, ohne die Notwendigkeit, Traka32 als Client (TAAC = Traka as a Client) auf einem PC oder Server auszuführen. TAAS kann von einem beliebigen PC aus fernüberwacht werden, wenn auf diesem der Traka Servicemanager installiert ist.

Auf dem Server des Londoner Netzwerkes ist Traka32 als Windows Service mit Autokommunikation installiert. Er liest alle Ereignisse der Londoner Schlüsselschränke aus und speichert diese in der Datenbank des Londoner SQL Servers. Veränderungen der Datenbank werden über einen Desktop PC mit einer Standardinstallation der Traka32 Software vorgenommen.

Auf dem Server des U.S. Netzwerkes ist ebenfalls Traka32 als Windows Service mit Autokommunikation installiert und mit den Schlüsselschränken des U.S. Netzwerkes verbunden.

Der globale Systemadministrator sitzt in London und hat zwei Kopien des Traka Service Managers installiert. Er kann somit den Service- und Autokommunikationsstatus beider Server überwachen.

Auf der Basis von TAAS ist der zentrale Sicherheitsverantwortliche der Geschäftsleitung immer über sämtliche Vorkommnisse und eventuelle Alarmsituationen sämtlicher Niederlassungen im weltweiten Verbund online informiert. Ein signifikanter Informationsvorteil für Unternehmen die nicht auf eine Lokalität begrenzt sind, sondern über mehrere D pendancen verf gen, wie es bei Gro banken die Regel ist.

## Quintessenz

Eine im letzten Jahr anonym durchgeführte Untersuchung ergab, dass in deutschen Unternehmen ca. 14% der Belegschaft mehr oder minder stark vom Pfad der Tugend abweicht. Im aktuellen Fall mit der Weitergabe von Kundendaten belegt. Wenn man diese Erkenntnis mit dem Umstand verbindet, dass im Bankengewerbe immer noch die manuelle Behandlung von Schlüsseln, Objekten und Dokumenten vorherrscht, dann wird deutlich, dass für eine gesamtheitliche Sicherheitslösung nicht nur die Sicherung der Unternehmenswerte von Außen gewährleistet sein muß, sondern auch die innerbetriebliche Behandlung zwingend angegangen werden sollte. Wenn das Ziel lautet, dass dies absolut manipulationsfrei und mit lückenloser Nachvollziehbarkeit der Ereignisse stattfinden soll, dann ist die einzige Lösung der Einsatz von elektronischen protokollierenden Schlüsselschränken und Fachanlagen. Die gesicherten Werte des Unternehmens und die Kosteneinsparung durch die Minimierung von Verlust und ineffektiver Arbeitszeit läßt solche Investitionen erfahrungsgemäß innerhalb von 12 Monaten amortisieren.

