Association for Information Systems
AIS Electronic Library (AISeL)

Wirtschaftsinformatik Proceedings 1999 | Wirtschaftsinformatik

February 1999

Sichere Geschäftstransaktionen auf Elektronischen Märkten

Gaby Herrmann
Universität GH Essen, herrmann@wi-inf.uni-essen.de

Alexander W. Röhm
Universität GH Essen, roehm@wi-inf.uni-essen.de

Günther Pernul
Universität GH Essen, pernul@wi-inf.uni-essen.de

Follow this and additional works at: http://aisel.aisnet.org/wi1999

Recommended Citation
Herrmann, Gaby; Röhm, Alexander W.; and Pernul, Günther, "Sichere Geschäftstransaktionen auf Elektronischen Märkten" (1999). *Wirtschaftsinformatik Proceedings 1999*. 12.
http://aisel.aisnet.org/wi1999/12

This material is brought to you by the Wirtschaftsinformatik at AIS Electronic Library (AISeL). It has been accepted for inclusion in Wirtschaftsinformatik Proceedings 1999 by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Sichere Geschäftstransaktionen auf Elektronischen Märkten

Gaby Herrmann
Universität GH Essen (herrmann@wi-inf.uni-essen.de)

Alexander W. Röhm
Universität GH Essen (roehm@wi-inf.uni-essen.de)

Günther Pernul
Universität GH Essen (pernul@wi-inf.uni-essen.de)

Inhalt

Electronic Business Engineering / 4. Internationale Tagung Wirtschaftsinformatik 1999.
Hrsg.: August-Wilhelm Scheer; Markus Nüttgens. – Heidelberg: Physica-Verlag, 1999

Abstract

Mit dem Beginn der kommerziellen Nutzung des Internet hat Electronic Commerce eine neue Entwicklungsstufe erreicht. Der Einstieg in Electronic Commerce bringt durch sinkende Informationskosten und stärkere Integration der einzelnen Geschäftsschritte neue Möglichkeiten der effizienten Durchführung von Geschäften mit sich. Dem stehen jedoch neue Risiken gegenüber. Besonders durch die Offenheit des Internet und der Bedeutung einer sicheren Durchführung von Geschäftstransaktionen wird der Verläßlichkeit und Sicherheit von Electronic Commerce-Anwendungen und -Infrastrukturen große Wichtigkeit beigemessen.

In diesem Artikel wird ein Vorschlag für eine Infrastruktur zur Realisierung sicherer Elektronischer Märkte (COPS) und zur Realisierung von Sicherheitsanforderungen an Geschäftsprozesse (MoSS) vorgestellt. Markttransaktionen werden hinsichtlich ihrer Sicherheitsrisiken analysiert und durch Geschäftsprozeßmodelle beschrieben. Es wird gezeigt, daß Sicherheitsanforderungen an Geschäftsprozesse aus unterschiedlichen Perspektiven betrachtet werden müssen und daß Interdependenzen zu anderen im Unternehmen bestehenden Modellen existieren.

1 Einleitung

Seit einigen Jahren erlangt das unter dem Begriff Electronic Commerce zusammengefaßte Forschungsgebiet eine wachsende Bedeutung. Electronic Commerce ist die gemeinsame Nutzung von Geschäftsinformationen, die Unterhaltung von Geschäftsbeziehungen und die Durchführung von Geschäftsprozessen und Markttransaktionen mittels Informationstechnologien (IT) (Zwass 1996). Mit dem Beginn der kommerziellen Nutzung des Internet hat Electronic Commerce eine neue Entwicklungsstufe erreicht, da sich vor allem durch die Offenheit des zugrundeliegenden Netzwerkes neue Möglichkeiten der Nutzung ergeben. Der Einstieg in Electronic Commerce bringt durch sinkende Informationskosten und stärkere Integration der einzelnen Geschäftsschritte faszinierende neue Möglichkeiten der effizienten Durchführung von Geschäften mit sich. Dem stehen neue Risiken gegenüber, die bei der Gestaltung von Electronic Commerce beachtet werden müssen.

Ziel von Basistechnologien für Electronic Commerce sollte sowohl die optimale Nutzung der Chancen von Electronic Commerce als auch die Absicherung gegenüber den spezifischen Risiken, die in offenen IT-Systemen vorhanden sind, sein. Dieser Artikel soll diesbezüglich einen Beitrag auf dem Gebiet der Modellierung von sicheren Geschäftstransaktionen darstellen. Wir verwenden hier den Begriff ”Geschäftstransaktion”, der sich aus dem Wort ”Geschäft”, das für Geschäftsprozeß steht, und dem Wort ”Transaktion”, welches für

Markttransaktion steht, zusammensetzt. Dahinter steht die Idee, daß obwohl Geschäftsprozesse als auch Markttransaktionen verschiedene Grundlagen haben und verschiedenen Gesetzen folgen, sie mit den gleichen Techniken, zum Beispiel mit Methoden der geschäftsprozeßorientierten Modellbildung, modelliert werden können.

Dieser Artikel ist wie folgt aufgebaut: In Kapitel 2 diskutieren wir die Grundlagen sicherer elektronischer Geschäftstransaktionen. Kapitel 3 enthält eine Darstellung von COPS, einer Infrastruktur zur Realisierung sicherer und fairer elektronischer Märkte. In Kapitel 4 und 5 stellen wir unterschiedliche Aspekte von MoSS, einer Methode zur Modellierung und Ausführung von Sicherheitssemantiken in Geschäftstransaktionen, vor. Während Kapitel 4 der Analyse der Sicherheitssemantiken gewidmet ist, wird in Kapitel 5 vorwiegend auf die sichere Ausführung elektronischer Geschäftstransaktionen eingegangen. Der Artikel endet mit einem Ausblick auf zukünftige Arbeiten in Kapitel 6.

2 Sichere Elektronische Geschäftstransaktionen

Markttransaktionen beschreiben Vorgänge zum Austausch von Gütern. Damit liegt ihr Hauptaugenmerk auf der Koordination zwischen Geschäftspartnern. Geschäftsprozesse dagegen beschreiben Unternehmensaktionen, die einen Beitrag zum Erreichen des vorgegebenen Unternehmensziels liefern. Sie beschreiben somit vornehmlich unternehmensinterne Vorgänge, die jedoch einen Bezug zu den Geschäftspartnern aufweisen. Insgesamt läßt sich feststellen, daß Markttransaktionen und Geschäftsprozesse die gleichen Prozesse betrachten, jedoch mit einem anderen Schwerpunkt. Traditionell werden Methoden der geschäftsprozeßorientierten Modellbildung vorwiegend zur Spezifikation und Analyse von Vorgängen in Firmen (Geschäftsprozessen) verwendet. Obwohl Firmen überwiegend hierarchische Strukturen aufweisen, können diese Modellierungsmethoden auch zur Beschreibung von Markttransaktionen eingesetzt werden.

Hierarchische Organisationen (Hierarchien) unterscheiden sich durch verschiedene Merkmale von Märkten. In Märkten werden die ökonomischen Einzelinteressen dezentral durch Einzelentscheidungen (z. B. über den Preis für ein bestimmtes Gut) koordiniert. In Hierarchien findet die Koordination durch Planung statt, um vor allem Koordinationskosten zu sparen. Seit ”The nature of the firm”, mit der Coase die Transaktionskostentheorie begründete (Coase 1937), wird die Entstehung verschiedener Koordinationsformen u. a. auf die unterschiedliche Struktur der Transaktionskosten bei verschiedenen Arten von Koordinationsaufgaben zurückgeführt.

Durch die weite Verbreitung des Internet ist eine Situation entstanden, die Koordination über elektronische Medien erlaubt. Dies hat zu einer Veränderung der Transaktionskosten geführt und damit verbunden sogar zu einer Veränderung der angewendeten Koordinationsformen (Malone et al. 1987). So entstehen zum Bei-

spiel virtuelle Unternehmen, die verteilt über das offene Netzwerk Geschäftsprozesse ausführen. Weil hier die gleiche Basistechnologie verwendet wird, treten auch die gleichen Risiken und damit Sicherheitsanforderungen wie bei elektronischen Märkten auf. In bezug auf Sicherheitsanforderungen an Geschäftstransaktionen in elektronischen Hierarchien und elektronischen Märkten ist heute eine Angleichung festzustellen.

In den folgenden zwei Abschnitten steht zuerst die Betrachtung von Markttransaktionen und dann von Geschäftsprozessen im Mittelpunkt. Im dritten Abschnitt werden die unterschiedlichen Sichten auf Sicherheit bei Markttransaktionen und Geschäftsprozessen zusammengeführt und der von uns verwendete Sicherheitsbegriff erläutert.

2.1 Transaktionen auf elektronischen Märkten

Die klassische *Markttransaktion* beschreibt den Vorgang eines Tausches auf einem Markt, bei dem materielle oder immaterielle Güter zwischen den verschiedenen beteiligten Transaktionsparteien ausgetauscht werden. Eine Markttransaktion kann daher als eine endliche Menge von Interaktionsprozessen zwischen Marktteilnehmern definiert werden, die in unterschiedlichen Rollen auftreten, und das Ziel verfolgen, eine vertragliche Vereinbarung des Austausches von Gütern anzubahnen, zu vereinbaren und abzuwickeln (Schmid/Lindemann 1997).

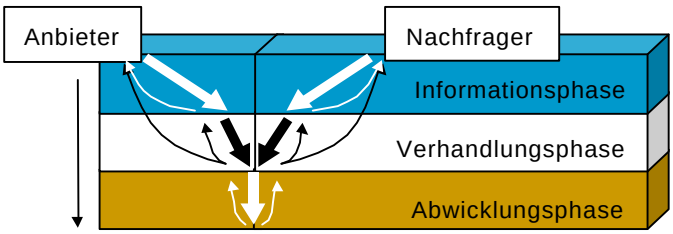


Abbildung 1: Phasen von Markttransaktionen

Transaktionen auf Märkten bestehen aus mehren *Phasen*, die nacheinander durchlaufen werden. Bekannt ist die Aufteilung in drei Phasen, die in Abbildung 1 dargestellt ist. Danach besteht eine Markttransaktion aus der Informations-, Verhandlungs- und Abwicklungsphase[1].

Ziel der *Informationsphase* ist es, geeignete Angebote und Transaktionspartner zu finden. Meist wird sie durch einen Nachfrager initiiert, der ermittelt, welche Produkte und Dienstleistungen existieren, die seinen Bedarf decken können. Die

[1] Manchmal wird die Abwicklungsphase weiter in die Auslieferungs- und Anpassungsphase untergliedert.

Spezifikationen der verschiedenen Produkte müssen besorgt werden und es muß ermittelt werden, bei wem sie bezogen werden können. Angebote, die Konditionen für einen möglichen Kauf beschreiben, werden eingeholt, geprüft und verglichen.

In der *Vereinbarungsphase* wird Kontakt mit den Transaktionspartnern aufgenommen, um mit ihnen die Zahlungsbedingungen, Liefertermine, Lieferkonditionen, Garantieleistungen etc. zu vereinbaren. Der Vertragsabschluß in dieser Phase bildet die rechtliche Grundlage für die Abwicklungsphase.

Die *Abwicklungsphase* dient der eigentlichen Erfüllung des Vertrages. Neben Primärtransaktionen, die sich auf den Leistungsübergang beziehen, gehören zu dieser Phase auch Sekundärtransaktionen wie Finanztransaktionen, Versicherung, Transport und Verpackung. Abschließend findet die Zahlung statt, und die vereinbarte Gegenleistung wird erbracht.

Die Unterstützung der Transaktionsphasen durch ein informationstechnisches System (IT-System) ist das wichtigste Merkmal Elektronischer Märkte (Schmid 1993). Daher wird der Begriff ”Elektronischer Markt” üblicherweise über diese Eigenschaft definiert.

2.2 Geschäftsprozesse

Zur Zeit gibt es noch kein einheitliches Verständnis über den Begriff Geschäftsprozeß. Unterschiedliche Autoren verwenden unterschiedliche Begriffsdefinitionen (Becker/Vossen 1995). Wir verstehen unter einem *Geschäftsprozeß* eine Menge von zusammengehörigen Aktivitäten, die der Realisierung von Unternehmenszielen dienen, inhaltlich abgeschlossen sind (Gausmeier/Fahrwinkel 1994) und darauf abzielen, einen Kundenauftrag (Georgakopoulos et al. 1995) (auch unternehmensinterner Kunden) effizient zu erfüllen. Bei der Geschäftsprozeßmodellierung erscheint uns ein in der Literatur kontrovers diskutierter Sachverhalt wichtig, nämlich das Ausgehen von im Unternehmen existenten Geschäftsprozessen mit dem Ziel, diese zu analysieren, zu überarbeiten und in eine effizientere Form zu bringen. Bei der Modellierung von Geschäftsprozessen spielt also immer die Absicht einer ”Erneuerung”, eines ”Reengineering” und einer ”Optimierung” eine Rolle.

Geschäftsprozesse werden unter Verwendung von Geschäftsprozeßmodellen beschrieben. Vom Standpunkt der Systemsicherheit müssen folgende Komponenten einer näheren Sicherheitsanalyse unterzogen werden:

Informationseinheiten: Sie stellen die passiven Komponenten eines Geschäftsprozesses dar. Sie dienen als Informationsspeicher, erhalten Informationen oder

es werden aus ihnen Informationen ausgelesen. Oft werden Informationseinheiten mittels Datenbanksystemen verwaltet[2].

Agenten: Sie stellen die aktiven Komponenten des Geschäftsprozesses dar. Sie können in unterschiedlichen Rollen auftreten, zum Beispiel als verarbeitende oder als beauftragende/beauftragte Agenten.

Informationsfluß: Agenten kommunizieren und kooperieren unter Verwendung von Informationsfluß. Gegenstand des Informationsflusses sind Informationseinheiten. Üblicherweise werden unterschiedliche Arten von Informationsfluß unterschieden.

Prozeduren: Sie beschreiben Aktivitäten und die Reihenfolge ihrer Abarbeitung. Prozeduren werden von Agenten ausgeführt und verwendet, um Informationen zu transformieren und Vorhaben und Ziele zu realisieren.

Endprodukte: Sie stellen das Ergebnis der Ausführung eines Geschäftsprozesses oder eines abgeschlossenen Teiles eines Geschäftsprozesses dar. In einem Endprodukt können sich die dieses Produkt erzeugenden Agenten und die verwendeten Prozeduren widerspiegeln. Diese Eigenschaft hat Auswirkungen auf die sicherheitsrelevante Bedeutung des Endproduktes. Um diesen sicherheitsrelevanten Blickwinkel hervorzuheben, wurden Endprodukte als eine eigenständige sicherheitsrelevante Komponente eingeführt, obwohl sie sich prinzipiell in die Komponente ”Informationseinheiten” einordnen lassen.

2.3 Sicherheit

In der Literatur wird bei der Betrachtung von Sicherheitsaspekten in Geschäftsprozessen meist ausschließlich Autorisierung und Zugriffskontrolle (z.B. Thomas/Sandhu 1996, Bertino et al. 1997) zur Gewährleistung von Vertraulichkeit oder reglementierter Nutzung betrachtet. Eine explizite Darstellung von Sicherheitsanforderungen für workflowbasierte Anwendungen wird von Thoben (1998) entwickelt. Holbein et al. (1996) beschäftigen sich mit der Aufbauorganisation von Unternehmen, dem funktionalen Kontext von Geschäftsprozessen und Methoden, um daraus rollenbasierte Autorisierungen abzuleiten.

In den bisher bekannten Arbeiten werden weiterreichende Sicherheitsanforderungen kaum betrachtet. Geschäftstransaktionen können jedoch komplexe Sicherheitsanforderungen besitzen, die sich nicht ausschließlich auf Autorisierung und Zugriffskontrollen reduzieren lassen. Beispiele dafür stellen rechtsverbindliche Aktivitäten (z.B. die Bindung an Verträge), Kommunikationsnachweise (z.B. ein erfolgreicher Nachweis, daß eine bestimmte Nachricht von einem bestimmten Nutzer kommt) oder die Gewährleistung von Urheberrecht an digitalen Gütern dar.

---

[2] Unter der Kategorie ”Informationseinheiten” subsumieren wir auch physikalisches Material, das in einem Geschäftsprozeß verarbeitet wird.

Der Gewährleistung von Sicherheit kommt besonders bei Geschäftstransaktionen zwischen unterschiedlichen Organisationen oder innerhalb einer Organisation, die physisch auf mehrere Betriebsstätten verteilt ist, eine wichtige Rolle zu. Dieses wird insbesondere dann evident, wenn als Kommunikationsmedium nicht dedizierte Leitungen, sondern "unsichere" öffentliche Netze, wie zum Beispiel das Internet, verwendet werden. Dieses trifft bei außerbetrieblichen Geschäften im Electronic Commerce zu, da die Teilnahme an einem Geschäftsbereich nicht auf eine Personengruppe beschränkt und der Teilnehmerkreis leicht erweiterbar sein soll. Sicherheitsanforderungen an Geschäftstransaktionen können durch unterschiedliche Gründe hervorgerufen werden und sich auf unterschiedliche Elemente der Geschäftstransaktionen beziehen.

Unser Verständnis von Sicherheit in Geschäftstransaktionen umfaßt die folgenden Anforderungen:

- Allgemeine Anforderungen: Vertraulichkeit, Integrität, Verfügbarkeit
- Geistiges Eigentum: Urheberrecht, Eigentumsrecht, Nutzungsrecht[3], Originalität
- Bindungen: Rechtsverbindlichkeit, Nichtabstreitbarkeit, gegenseitige Abhängigkeit
- Datenschutz: Anonymität, Pseudo-Anonymität, verdecken von Aktivitäten[4]

Sicherheitsanforderungen an Geschäftstransaktionen können aus unterschiedlichen Beweggründen gefordert werden. Diese Gründe können firmenintern oder firmenextern sein. Firmenexterne Gründe spiegeln die öffentliche Meinung wider und können in Gesetzen manifestiert sein. Jede Sicherheitsanforderung kann in unterschiedlichen Gewichtungen (Sicherheitsstufen) auftreten (z. B. öffentlich, vertraulich, streng vertraulich), wobei zur Realisierung unterschiedlicher Sicherheitsstufen unterschiedliche Methoden benötigt werden**.** Desweiteren besitzt nicht jede Sicherheitsanforderung Relevanz bezüglich jeder Geschäftsprozeßkomponente. Tabelle 1 zeigt diesen Zusammenhang auf (vgl. Hermann/Pernul 1998a).

---

[3] Nutzungsrecht ist ein veräußerbarer Teil des Urheberrechts. Da es jedoch von besonderer Bedeutung ist, wird es hier getrennt aufgeführt. Gerade bei der Verwertung digitaler Güter auf elektronischen Märkten spielt der Schutz des Nutzungsrechtes eine große Rolle.

[4] Obwohl das Verdecken von Aktivitäten als eine Abart der Vertraulichkeit angesehen werden kann, betrachten wir es getrennt, da bei Vertraulichkeit vorwiegend die Vertraulichkeit von Elementinhalten (Attributen) und die Vertraulichkeit von Elementstrukturen betrachtet wird.

Sicherheitsanforderungen / Geschäftsprozeß-elemente	Vertraulichkeit	Authentizität	Integrität	Verfügbarkeit	Originalität	Anonymität	Pseudo-Anonymität	Nutzungsrecht	Nichtabstreitbarkeit	Eigentumsrecht	Urheberrecht	Rechtsverbindlichkeit	gegenseitige Abhängigkeit	Verdecken von Aktivitäten
Information	x	x	x	x	x	-	-	x	-	x	x	x	-	-
handelnder Agent	x	x	-	x	-	x	x	x	x	x	x	-	x	x
beauftragender/ beauftragter Agent	x	x	-	-	-	x	x	x	x	x	-	-	x	x
Prozedur	x	-	x	x	-	-	-	x	x	x	x	-	x	x
Endprodukt	x	x	x	x	x	-	-	x	-	x	x	-	-	-
Informationsfluß	x	-	x	-	-	-	-	-		-	-	-	x	x

Tabelle 1: Sicherheitsanforderungen für Geschäftsprozeßelemente[5]

Bei der Betrachtung von Geschäftstransaktionen ist die wichtigste Forderung die Forderung nach Sicherung des Wertes des gehandelten Gutes, was wir mit *Integrität der Ware* bezeichnen. Sie kann je nach Ware sehr unterschiedlich sein und läßt sich mit den bereits oben genannten Sicherheitsanforderungen beschreiben.

Als Beispiel für die Wahrung der Integrität eines digitalen Gutes betrachten wir eine Geschäftstransaktion mit digital repräsentierten Umweltzertifikaten, deren Besitz eine vorgegebene Menge Umweltgifte zu emittieren erlaubt (Gerhard/ Röhm 1998). Der Wert eines Zertifikats hängt von dessen *Originalität* ab, da

[5] Die Tabellenspalten beziehen sich auf mögliche Sicherheitsanforderungen. Die Zeilen repräsentieren die betrachteten Geschäftsprozeßelemente. Ein Tabelleneintrag "x" besagt, daß die der Spalte zugeordnete Sicherheitsanforderung für das entsprechende Geschäftsprozeßelelement (Zeile) relevant ist. Ein Tabelleneintrag "-" bedeutet, daß die entsprechende Sicherheitsanforderung keine Bedeutung für das zugehörige Geschäftsprozeßelement besitzt.

man mit einem Zertifikat nur einmal die lizensierte Menge emittieren darf. Beim Handel mit Umweltzertifikaten, kann neben der Originalität des Umweltzertifikats auch dessen *Anonymität* gefordert werden. Anonymität kann notwendig sein, da durch Bekanntwerden seines Einsatzes dem Unternehmen Nachteile (Prestigenachteile und daraus folgende Absatznachteile) entstehen können. Eine *sichere Auslieferungsphase* dieses digitalen Gutes impliziert daher die Verwendung verschiedener kryptographischer Algorithmen und Protokolle. An der Auslieferung sind drei Parteien beteiligt: der Käufer, der Verkäufer und eine staatliche Stelle, die als Herausgeber der Umweltzertifikate fungiert.

Ein kryptographisches Protokoll das zur Realisierung des dargestellten Sachverhaltes verwendet werden kann, könnte folgend aussehen: Zunächst sendet der Käufer an den Verkäufer einen, von ihm mittels eines kryptographischen Zufallszahlengenerators erzeugten, symmetrischen Schlüssel *K*. Der Schlüssel ist mit einem asymmetrischen Verfahren unter Zuhilfenahme des öffentlichen Schlüssels der staatlichen Stelle verschlüsselt, so daß nur sie den Schlüssel *K* entschlüsseln kann. Die Nachricht muß zudem vom Käufer unterzeichnet sein, da sonst kein Schutz gegen einen Man-in-the-middle-Angriff vorhanden wäre. Um die Gefahr eines Replay-Angriffes zu vermeiden, verschlüsselt der Verkäufer das verschlüsselte *K* zusammen mit der Lizenz nochmals und sendet sie an die staatliche Stelle. Die staatliche Stelle kann jetzt die Gültigkeit der Lizenz prüfen, indem sie zunächst ihre eigene digitale Signatur verifiziert und damit feststellt, ob sie selbst die Lizenz ausgestellt hat. Danach sucht sie in der Datenbank die Seriennummer, die in der Lizenz angegeben ist und erhält dadurch die zugehörige Versionsnummer. Nur falls diese mit der Versionsnummer in der erhaltenen Lizenz übereinstimmt, ist sie gültig. Wenn dies zutrifft, generiert die staatliche Stelle eine neue Lizenz und verschlüsselt sie mit dem symmetrischen, geheimen und nur dem Käufer bekannten Session-Key *K*. Sie sendet das Ergebnis an den Verkäufer, der es an den Käufer weiterleitet. Die originale, anonyme Lizenz wurde somit sicher unter Wahrung ihrer Integrität übermittelt.

3 COPS

Marktliche *Koordination* kann in vier Arten unterteilt werden: unmittelbare Märkte, Broker-Märkte, Händler- und Auktionsmärkte (Garbade 1982). In jeder dieser vier Arten der Koordination bilden sich implizit Rollen von Akteuren heraus, die für die jeweilige Art charakteristisch sind. Dabei ist es im wesentlichen die Rolle der Intermediäre, welche für jede Art eine spezifische Ausprägung besitzt. *Intermediär* nennt man einen Akteur, der zwischen Nachfrage und Angebot vermittelt, Informationen aggregiert und aus seinem Informationsvorsprung Gewinne schöpfen kann.

Ziel von COPS (Commercial Protocol and Services, Röhm/Pernul 1999) ist die Realisierung von sicheren elektronischen Märkten, die alle Phasen der Markt-

transaktion unterstützen und auf denen alle Arten der marktlichen Koordination realisiert werden können. Dabei sollen die Sicherheitsbedürfnisse aller Teilnehmer einer Markttransaktion berücksichtigt und die genannten Sicherheitsanforderungen für elektronische Märkte erfüllt werden. Die COPS-Infrastruktur ist modellhaft in Abbildung 2 dargestellt. Die drei verschiedenfarbigen Ebenen repräsentieren die Phasen der Markttransaktionen in denen Protokolle die Interaktionen der Marktparteien koordinieren. Die Marktparteien sind als Säulen an den Ecken dargestellt. Sie erbringen lokal Dienste oder nehmen Dienste von anderen Marktparteien in Anspruch.

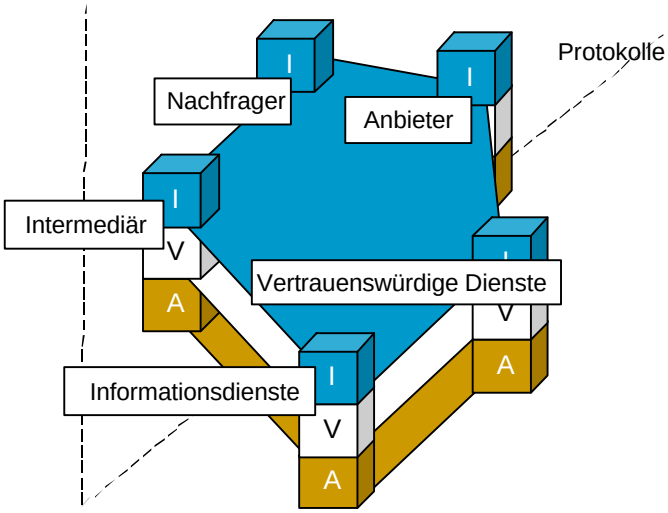


Abbildung 2: Modell von COPS

In COPS sind fünf verschiedene Rollen von Marktparteien vorgesehen, von denen sich vier aus der obigen Klassifikation marktlicher Koordination herleiten lassen: Nachfrager, Anbieter, verschiedene Arten von Intermediären, vertrauenswürdige Dienstleister, und Informationsdienstleister. Ein Beispiel für vertrauenswürdige Dienstleister sind Auktionatoren, denen vertraut werden muß, daß sie tatsächlich das angegebene Auktionsverfahren verwenden und ihre Stellung nicht zum eigenen Vorteil ausnutzen. Informationsdienstleister unterscheiden sich von vertrauenswürdigen Dienstleistern durch den Umstand, daß ihren Diensten nicht vertraut werden muß.

Damit den vielfältigen Anforderungen Elektronischer Märkte begegnet werden kann, realisiert COPS nicht einzelne Transaktionsmechanismen, sondern enthält eine Spezifikationssprache, die es ermöglicht, Transaktionen zu modellieren. Mit

der Spezifikationssprache ALMO$T[6] können sowohl die sicherheitsrelevanten Vorgänge bei den einzelnen Marktteilnehmern (Säulen in Abbildung 2) als auch die Koordination und Kommunikation zwischen ihnen (Ebenen) beschrieben werden. Eine mit ALMO$T spezifizierte sichere Markttransaktion kann von einem Interpreter, der in COPS realisiert wird, ausgeführt werden. Die in den Spezifikationen verwendeten Sicherheitsmechanismen und -dienste werden von COPS ausgeführt und sind deshalb neben den verwendeten vertrauenswürdigen Diensten Bestandteil von COPS.

4 MoSS

Ein Ansatz zur Kostenreduktion bei der Ausführung von Geschäftsprozessen ist ihre computerunterstützte Ausführung. Ziel des Projektes MoSS (Modelling Framework for Security Semantics, Herrmann/Pernul 1998b) ist die Entwicklung einer Methode zur Berücksichtigung von Sicherheitsaspekten in Geschäftsprozessen. In diesem Abschnitt wird zur Veranschaulichung das in Abschnitt 2.3 vorgestellte Beispiel des Handels mit Umweltzertifikaten genauer betrachtet und die in MoSS entwickelte Architektur vorgestellt.

Für die Analyse und Vorbereitung einer computerunterstützten Ausführung einer Geschäftstransaktion wird ein entsprechendes Geschäftsprozeßmodell benötigt. Ein Geschäftsprozeß wird im allgemeinen durch einen Bereichsexperten, der detaillierte Kenntnisse über den zu modellierenden Geschäftsprozeß besitzt, spezifiziert. Es beinhaltet die in den Geschäftsprozeß involvierten Organisationseinheiten (z. B. Abteilungen, Agenten, Rollen und Maschinen), die zu erbringenden Tasks[7] und ihr Zusammenspiel, die benötigten Informationseinheiten, ihren Aufbau, ihre Verwendung und Struktur und das dynamische Verhalten all dieser Objekte in Abhängigkeit der Zeit. Da der Bereichsexperte im allgemeinen kein Experte auf dem Gebiet der Sicherheit ist, besitzt er nur eine sehr abstrakte Vorstellung über die Sicherheitsanforderungen eines Geschäftsprozesses und weist diese Anforderungen (z.B. Rechtsverbindlichkeit, hohe Integrität) den Geschäftsprozeßelementen zu.

Zur Veranschaulichung spezifizieren wir eine Geschäftstransaktion für den Erwerb von Umweltzertifikaten mit Sicherheitsanforderungen (Abbildung 3), wobei wir auf die Syntax und Semantik der einzelnen graphischen Komponenten des Geschäftsprozeßmodells nicht detailliert eingehen. Zum Verständnis der Geschäftstransaktion sind folgende Angaben nötig: Die Geschäftstransaktion wird von der Einkaufsabteilung des Nachfragers initiiert und durchläuft alle drei

---

[6] ALMO$T (A Language for Modelling $ecure business transactions) wird in (Herrmann/Röhm 1999) vorgestellt.

[7] Die Begriffe ”Task” und ”Aktivität” verwenden wir als Synonyme.

Phasen einer Markttransaktion. Die erste Zeile der Darstellung in Abbildung 3 benennt die für die Ausführung der in der jeweiligen Spalte aufgeführten Tasks verantwortlichen Abteilungen. In der linken Spalte sind die für die Ausführung der in dieser Zeile aufgeführten Tasks verantwortlichen Personen oder Rollen aufgeführt. In der Informationsphase werden Anbieter ermittelt, die als mögliche Lieferanten von Umweltzertifikaten in Betracht kommen (Task 1), und es werden von ihnen Angebote eingeholt (Task 2). Die Angebote müssen für eine Zeitspanne gültig und *authentisch* sein, da sonst die Entscheidung für einen möglichen Lieferanten (Task 3) auf unsicherer Information beruht. Während der Vereinbarungsphase werden Verhandlungen mit dem möglichen Anbieter geführt (Task 4), die zu einem Vertragsabschluß führen (Task 5) oder die erneute Auswahl eines potentiellen Lieferanten erfordern (Task 3). An die Verhandlungen werden folgende Sicherheitsanforderungen gestellt: Erstens soll es sich um *authentische* Verhandlungspartner handeln, zweitens sollen die Verhandlungen *vertraulich* sein. Der Vertragsabschluß fordert *rechtliche Bindung* der Vertragspartner an die getroffene Übereinkunft. In der Abwicklungsphase wird zur Vermeidung des Diebstahls des Umweltzertifikats dessen *Originalität* gefordert (Task 6). Eine weitere Anforderung an das ausgetauschte Zertifikat kann *Anonymität* des Käufers sein (Stichwort: Wettbewerbsnachteile bei Bekanntwerden des Besitzes eines Umweltzertifikats). Nach der Auslieferung wird das Umweltzertifikat bis zu seinem Einsatz oder seinem neuerlichen Verkauf archiviert (Task 7).

In dem in Abbildung 3 dargestellten Beispiel einer Geschäftstransaktion werden die Sicherheitsanforderungen Authentizität, Rechtsverbindlichkeit, Originalität, Anonymität und Vertraulichkeit gestellt.

Zur Realisierung der Geschäftstransaktion ist eine weitere Sicherheitsanalyse notwendig. Der Bereichsexperte, der den Geschäftsprozeß modelliert hat, ist im allgemeinen kein Sicherheitsspezialist. Sein Verständnis von Sicherheitsanforderungen wird sehr vage und auf einem hohen Abstraktionsniveau sein. Desweiteren kann ein Geschäftsprozeß innerhalb des Unternehmens nicht als isolierter Vorgang betrachtet werden. Vielmehr hat eine Sicherheitsanforderung an einen Geschäftsprozeß Auswirkungen auf die in den Geschäftsprozeß involvierten Datenbanken, Abläufe, Maschinen und Personen. In den meisten Fällen existieren für diese Komponenten bereits Modelle (z. B. Organigramme, Datenmodelle) und die Sicherheitsanforderung an den Geschäftsprozeß hat auch Auswirkungen auf diese Modelle. Falls diese Systeme nicht den neuen Sicherheitsbedingungen angepaßt werden, können Sicherheitslücken entstehen, die von Angreifern genutzt werden können, um Informationen über den zu schützenden Geschäftsprozeß zu erlangen. An dieser Stelle wird ersichtlich, warum es uns im Kapitel 2 wichtig erschien, auf den Aspekt der ”Erneuerung”, des ”Reengineering” und der ”Optimierung” bei der geschäftsprozeßorientierten Modellbildung hinzuweisen.

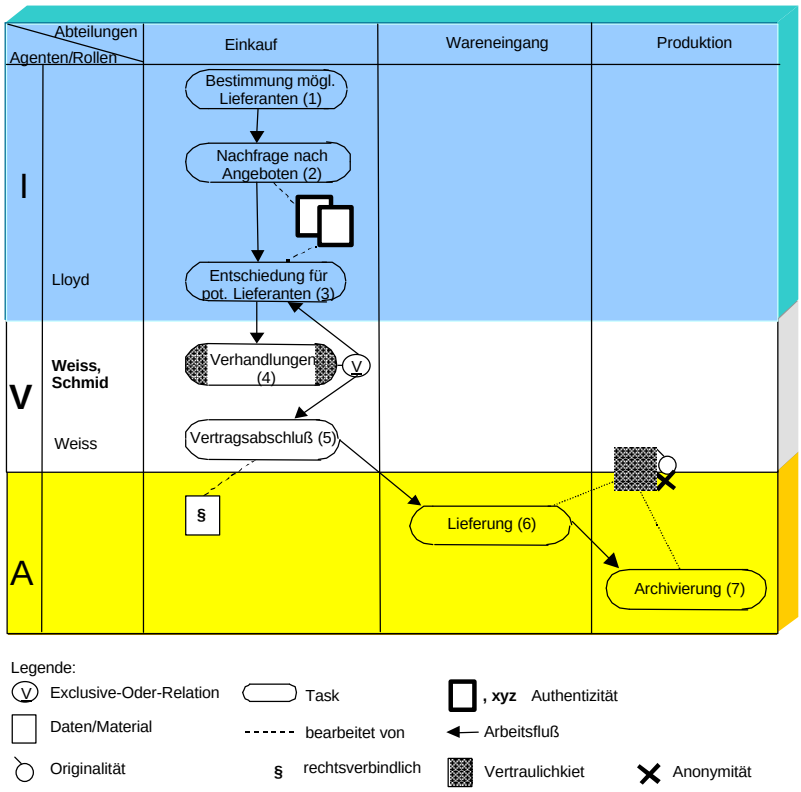


Abbildung 3: Geschäftstransaktion um Sicherheitssemantik erweitert

4.1 Geschäftsprozeßperspektiven

Zur vollständigen Beschreibung und Analyse eines Geschäftsprozesses ist es notwendig, den Geschäftsprozeß zumindest aus den folgenden vier Perspektiven zu betrachten (vgl. Curtis et al. 1992):

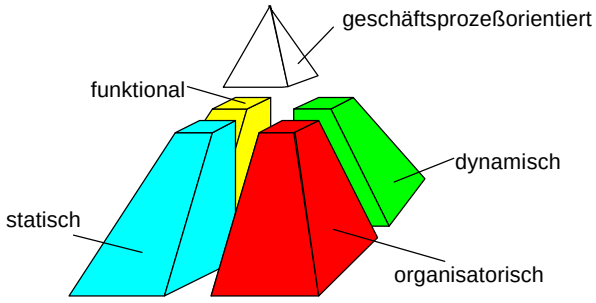


Abbildung 4: MoSS Geschäftsprozeßperspektiven

Die *statische Perspektive* beschreibt die involvierten Informatitionseinheiten, ihre Struktur und ihre Beziehungen untereinander.

Die *funktionale Perspektive* repräsentiert die zu erbringenden Aktivitäten und den zugehörigen Datenfluß.

Die *dynamische Perspektive* enthält den Lebenszyklus (repräsentiert durch Zustände und Zustandsübergänge) jeder Informationseinheit.

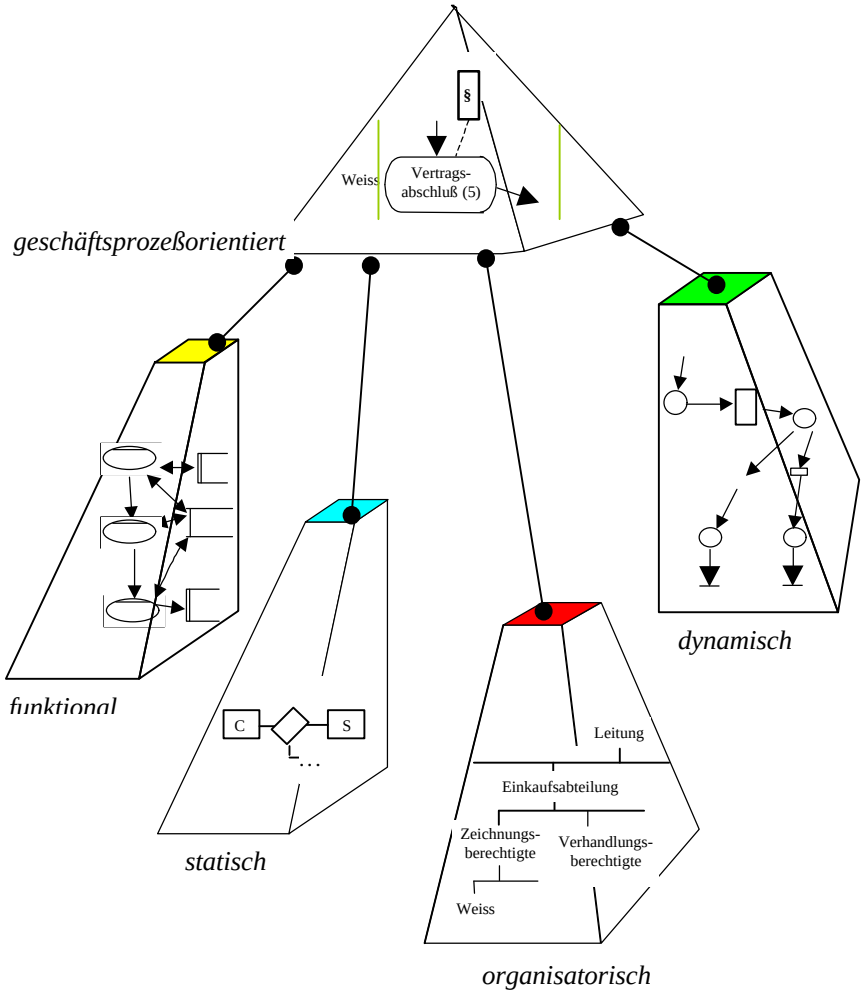
Die *organisatorische Perspektive* beschreibt, wo und durch wen die einzelnen Aktivitäten erbracht werden.

Zum besseren Verständnis des Geschäftsprozeßmodells ist eine die obigen Perspektiven integrierende Sicht sinnvoll. In MoSS bietet diese integrative Sichtweise die *geschäftsprozeßorientierte Perspektive*. Sie stellt den gesamten Geschäftsprozeß durch den Arbeitsfluß (Aktivitäten und ihren Informationsfluß) dar. Sie integriert die funktionale und die dynamische Perspektive und referenziert die statische und organisatorische Perspektive (siehe Abbildung 4).

Anforderungen an einen Geschäftsprozeß müssen aus unterschiedlichen Perspektiven analysiert werden. Dabei gilt jedoch, daß unterschiedliche Typen von Anforderungen unterschiedlich starke Auswirkungen auf den Geschäftsprozeß in den unterschiedlichen Perspektiven zeigen. Zum Beispiel hat die Anforderung an die zeitliche Abhängigkeit der Ausführung zweier Tasks (z. B. Task A muß vor Task B ausgeführt werden) starke Auswirkungen auf die funktionale und dynamische Perspektive, aber nur geringen Einfluß auf die organisatorische Perspektive und keinen Einfluß auf die statische Perspektive des Geschäftsprozesses. Sicherheitsanforderungen dagegen beeinflussen jede Perspektive und stellen daher den am schwierigsten zu handhabenden Anforderungstyp dar. Falls die Auswirkungen einer Sicherheitsanforderung auf eine der Perspektiven nicht berücksichtigt werden kann, entsteht eine Sicherheitslücke, die die verläßliche Ausführung der gesamten Geschäftstransaktion gefährdet.

In Abbildung 5 wird das Zusammenspiel der Perspektiven anhand der Aktivitäten, die den Vertragsabschluß repräsentieren (Task 5, Abbildung 3), dargestellt. Die geschäftsprozeßorientierte Perspektive gibt eine integrierte Sicht auf die anderen vier Perspektiven. Bei der Betrachtung des Vertragsabschlusses ist aus dieser Perspektive zu entnehmen, daß für den Vertragsabschluß der Mitarbeiter Weiss verantwortlich ist. Jeder Mitarbeiter ist in das *Organisationsmodell* des Unternehmens (z. B. Organigramm) integriert, in dem u. a. seine Zugehörigkeit zu Organisationsbereichen und zu möglichen Rollen festgelegt ist. Zur eindeutigen Bestimmung des in den Geschäftsprozeß involvierten Mitarbeiters (in unserem Beispiel Weiss) wird seine eindeutige Repräsentation im Organisationsmodell referenziert. Dabei können auch notwendige Autorisierungen, Befugnisse und Kenntnisse geprüft werden, die zur Ausführung des Tasks notwendig sind. Beim Vertragsabschluß wird das Dokument, das die Übereinkunft repräsentiert, bearbeitet. Dieses Dokument stellt eine Beziehung zwischen den Vertragsparteien dar, die in der *statischen Perspektive* des Geschäftsprozesses ausgedrückt wird. In dieser Darstellung (z. B.

als Teil eines Datenmodells) ist die Struktur der Übereinkunft sowie ihre Beziehungen zu anderen Komponenten des Unternehmens detailliert aufgeführt.



Legende: nimmt Bezug auf

Abbildung 5: Perspektiven der Sicherheitsanforderung „Rechtsverbindlichkeit"

Die *geschäftsprozeßorientierte Perspektive* zeigt den Geschäftsprozeß auf hohem Abstraktionsniveau. Für einen Überblick ist es ausreichend, Kenntnis darüber zu besitzen, daß ein Vertragsabschluß stattfindet. Zur Ausführung der Geschäftstransaktion sind jedoch detailliertere Kenntnisse über den Ablauf eines Vertragsabschlusses notwendig. Diese Detaillierung erfolgt in der *funktionalen*

Perspektive, die die sicherheitsnotwendigen Handlungen der am Vertragsabschluß Beteiligten darstellt, z. B. das Auslesen oder Erzeugen eines privaten Schlüssels zur Unterschrifterzeugung, Prüfen von Zertifikaten, Verifizieren von Unterschriften. Die *dynamische Perspektive* zeigt die Zustandsänderungen der in den Vertragsabschluß involvierten Informationseinheiten. So kann ein Vertrag während seiner Existenz diverse Zustände ”erleben”, die an bestimmte Ereignisse geknüpft sind. Beispiele dafür sind:

Z_1: Noch kein Vertragspartner hat unterschrieben.

Z_2: Genau ein Vertragspartner hat unterschrieben.

Z_x: Die Übereinkunft ist rechtlich prüfbar.

Z_y: Vertrag ist gültig, das Zertifikat ist jedoch abgelaufen. (In diesem Fall kann die Rechtsgültigkeit des Vertrages nicht mehr bewiesen werden und die Unterschrift muß nachverschlüsselt werden.)

Z_n: Der Vertrag ist abgelaufen und erfüllt.

Neben den Zusammenhängen der statischen, organisatorischen, funktionalen und dynamischen Perspektive auf der einen Seite und der geschäftsprozeßorientierten Perspektive auf der anderen Seite existieren weitere Beziehungen zwischen den Perspektiven, auf die hier nicht eingegangen werden kann.

4.2 Frameworkarchitektur

Zur Unterstützung der Realisierung von Sicherheitsanforderungen an Geschäftsprozesse haben wir ein Framework entwickelt, dessen dreischichtige Architektur (vgl. Abbildung 7) kurz vorgestellt wird.

Auf der obersten Ebene (Ebene 3) werden grafische Konzepte zur Darstellung von Sicherheitsanforderungen an Geschäftstransaktionen zur Verfügung gestellt. Die oberste Ebene ermöglicht es, den Geschäftsprozeß zu entwerfen und in der in Abbildung 3 dargestellten Form zu dokumentieren. Um die Sicherheitsanforderung an den Geschäftsprozeß zu erfüllen, müssen eventuell entsprechende Anpassungen vorgenommen werden. Hilfestellung bei einer solchen Anpassung wird durch eine Sammlung von Fallbeispielen, die sich ebenfalls auf dieser Modellarchitekturebene befindet, gegeben. Die Fallbeispiele fungieren als Referenzmodelle und enthalten Änderungsangaben für die unterschiedlichen Modellierungsperspektiven. Die Verfeinerung soll auf dieser Ebene einen Detaillierungsgrad bezüglich der Sicherheitsanforderungen erreichen, der Sicherheitsgrundelemente enthält. Unter Sicherheitsgrundelementen verstehen wir Elemente, die eine abstrakte Beschreibung eines sicherheitskritischen Vorganges darstellen, jedoch alle Informationen zu seiner technischen Realisierung beinhalten (z. B. ”Prüfe Digitale Signatur D von angeblichem Unterzeichner S”). Auf Ebene 2 steht eine Fallbeispielsammlung zur Verfügung, deren Elemente mögliche Vorgehen bei der Realisierung von Sicherheitsgrundelementen

beschreiben. Die Beschreibung geschieht mit Hilfe der Spezifikationsprache ALMO$T (Herrmann/Röhm 1999) und referenziert Soft- und Hardwarebausteine der untersten Architekturebene.

Zur Veranschaulichung einer geschäftsprozeßorientierten Analyse einer Sicherheitsanforderung skizzieren wir im folgenden notwendige Änderungen der statischen Perspektive bei der Forderung nach Rechtsverbindlichkeit einer Übereinkunft. Eine detaillierte Ausarbeitung der anderen Perspektiven wird in Herrmann/Pernul 1998b vorgenommen.

Um Vertragspartner an eine Vereinbarung rechtlich zu binden sind entsprechend des gültigen Rechts unterschiedliche Maßnahmen erforderlich. In vielen Staaten gilt eine Vereinbarung als rechtlich bindend, wenn beweisbar ist, daß diese Vereinbarung getroffen wurde. Eine übliche Methode dieses Nachweises bei einer traditionellen Vertragsfestlegung (Papierform) ist die Verwendung von Unterschriften. Entsprechend kann bei Geschäftstransaktionen auf Elektronischen Märkten ein (elektronisches) Dokument digital signiert werden. Damit eine digitale Signatur als Beweis anerkannt wird, kann es unterschiedliche Vorgaben geben. Für das Beispiel beziehen wir uns auf das deutsche Kommunikationsdienste-Gesetz (IuKDG 1997). Darin wird eine digitale Signatur als Siegel auf den signierten Daten angesehen und für die rechtliche Bindung einer digitalen Signatur sind folgende Erweiterungen notwendig: Eine digitale Signatur wird durch asymmetrische Verschlüsselungsverfahren unter Verwendung des geheimen Schlüssels der Unterzeichners erzeugt. Die Richtigkeit der Signatur kann mit Hilfe des zugehörigen öffentlichen Schlüssels, der durch eine Zertifizierungsinstanz zertifiziert sein muß, festgestellt werden. Dadurch ist die Identität des Unterzeichners verifizierbar. Ein Zertifikat enthält neben dem öffentlichen Schlüssel des Anwenders den zur Verifikation benötigten Algorithmus und zusätzliche Details wie zum Beispiel die Angabe der Fälle, in denen das Zertifikat eingesetzt werden soll (z. B. Unterzeichnung von Verträgen bis zu einem Vertragsvolumen von DM 100000.-). Jedem Zertifikat muß desweiteren ein Gültigkeitszeitraum und eine Zertifikatnummer zugewiesen sein. Welche kryptographischen Algorithmen verwendet werden dürfen ist nicht durch das Gesetz vorgeschrieben, um leichter auf technische Entwicklungen reagieren zu können.

Um die Geschäftstransaktion auf einer Infrastruktur für Elektronische Märkte ausführen zu können, ist es notwendig, die Sicherheitsanforderung ”Rechtsverbindlichkeit” aus der statischen Perspektive zu betrachten und zu prüfen, ob die Struktur des Dokumentes ”Vertrag” diese Anforderung unterstützt. Ist dies nicht der Fall, so muß eine Überarbeitung der Datenstruktur aus der statischen Perspektive erfolgen. Da persistente Objekte wie z. B. Vertragsdaten im allgemeinen in einer Datenbank abgelegt sind, gehen wir davon aus, daß in einem Datenmodell bereits eine Kunden-Anbieter-Beziehung existiert, die die betrachtete Übereinkunft (den Vertrag) abbildet. Zur Überprüfung der rechtlichen Bindung einer Übereinkunft besitzt jeder

Unterzeichner ein Zertifikat, durch das er in Beziehung zu einer (vertrauenswürdigen) Zertifizierungsinstanz steht. Abbildung 6 zeigt eine entsprechende Datenstruktur in Form eines Entity-Relationship-Diagrammes. In dieser Darstellung sind Sachverhalte, die auf die Sicherheitsanforderung ”Rechtsverbindlichkeit” zurückzuführen sind, durch Fettschrift hervorgehoben. Ist eine Geschäftstransaktionen in der statischen Perspektive wie in Abbildung 6 beschrieben aufgebaut, so wird durch sie die Gewährleistung der Sicherheitsanforderung unterstützt. Ist dies nicht der Fall, müssen die Datenstrukturen überarbeitet bzw. durch den Referenzfall ersetzt werden. Eine ähnliche Analyse ist auch für die anderen Perspektiven der Geschäftstransaktion notwendig.

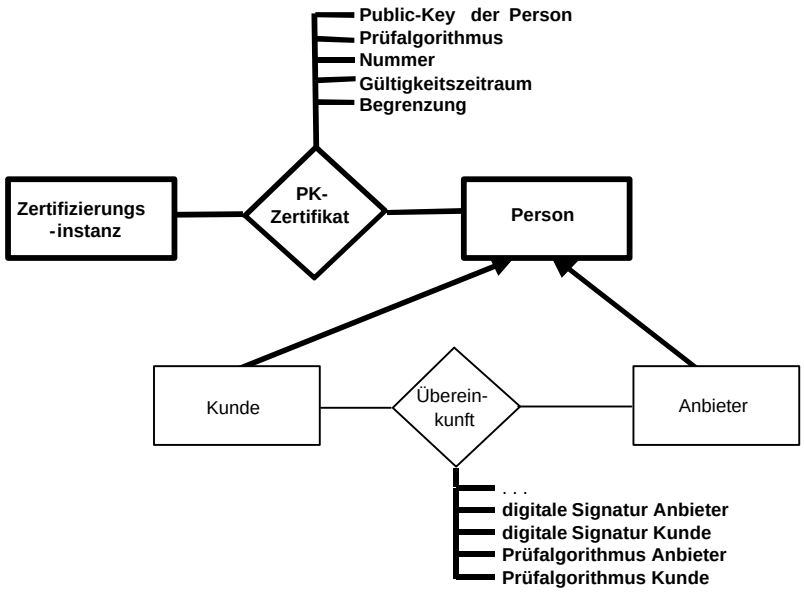


Abbildung 6: Referenzmodell „Rechtsverbindlichkeit” (statische Perspektive)

Die vorgestellt Erweiterung der statischen Perspektive als Folge der Anforderung ”Rechtsverbindlichkeit von Information” besitzt für jedes Auftreten dieser Anforderung im gleichen rechtlichen Kontext Relevanz. Daher kann sie in der Fallbeispielsammlung auf Architekturebene 3.1 den Anwendern zur Wiederverwendung zur Verfügung gestellt werden.

5 Sichere Ausführung elektronischer Geschäftstransaktionen

In diesem Abschnitt wird der Zusammenhang zwischen COPS und MoSS nochmals dargestellt. Die Integration der beiden Projekte bietet eine Methode zur sicheren Realisierung elektronischer Geschäftstransaktionen. Wird COPS in die Drei-Schichten-Architektur eingeordnet, so kann dies auf Ebene 3 geschehen (siehe Abbildung 7). Eine Markttransaktion in COPS wird aus der Sicht der Unternehmung in MoSS hinsichtlich ihrer Sicherheitsanforderungen analysiert.

Auf der mittleren Architekturebene wird eine Sammlung von bereits modellierten Lösungen für Sicherheitsgrundelemente und eine zugehörige Spezifikationssprache (ALMO$T) angeboten. ALMO$T ist das Bindeglied zwischen den Sicherheitsgrundelementen und den für ihre Realisierung eingesetzten Soft- und Hardware-Grundbausteinen. Zum Beispiel kann eine Lösung für das Sicherheitsgrundelement ”Prüfe Digitale Signatur D des Unterzeichners S” die Grundbausteine ”Besorge Zertifikat der zu überpüfenden Unterzeichnerpartei” und ”Überprüfe digitale Signatur mit Hilfe des MD5 und RSA” benötigen. Die Modelle dieser Ebene sollen so aufgebaut sein, daß sie automatisch ausgeführt werden können. Auf Ebene 1 der Architektur befindet sich eine Software- und Hardware-Bibliothek zur Realisierung von Sicherheitsanforderungen.

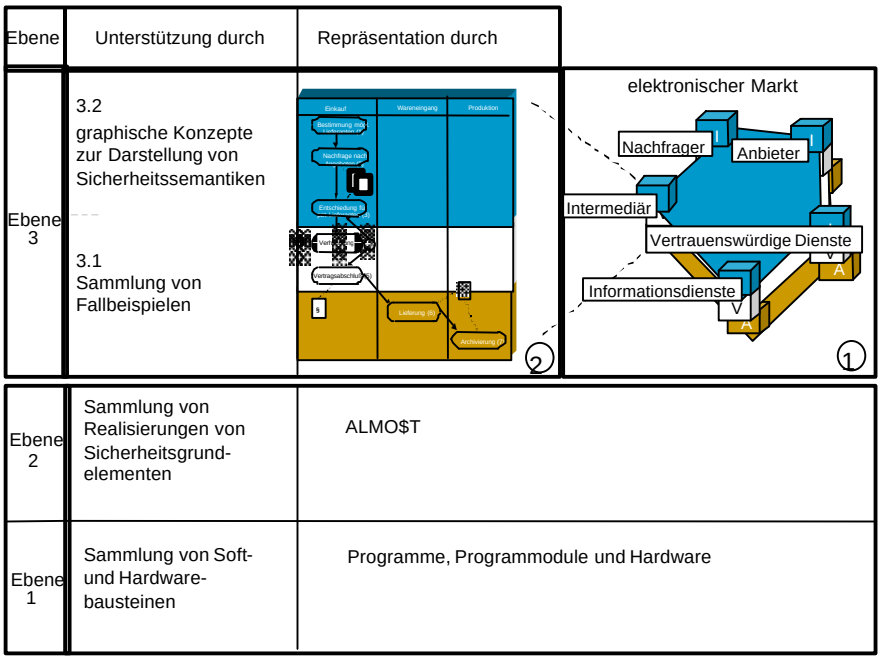


Abbildung 7: Modellierungs- und Realisierungsunterstützung für sichere Geschäftstransaktionen

6 Ausblick

In diesem Artikel haben wir die Projekte COPS und MoSS zur Realisierung von sicheren Markttransaktionen und Geschäftsprozessen vorgestellt. Es wurde gezeigt, daß eine gemeinsame Betrachtung der beiden Aufgabenfelder angebracht ist und ein entsprechendes Konzept entwickelt. Für beide Projekte wurden bereits verschiedene Komponenten, insbesondere entsprechende Softwarebibliotheken mit Sicherheitsdiensten und -mechanismen (Ebene 1), implementiert. Die Implementation basiert auf der Cryptix Java-Bibliothek (bietet elementare Kryptofunktionen) der Firma Systemics[8], die um Verfahren der Public-Key-Kryptographie erweitert wurde. Darauf aufbauend wurde die SMAL- (Security Mechanism Abstraction Layer) Bibliothek implementiert, die für den Benutzer Implementationsdetails verbirgt und eine spätere Integration ergänzender oder neuer Mechanismen erlaubt. Außerdem wurden Informationsdienste und vertrauenswürdige Dienste, wie beispielsweise ein Public-Key-Directory und eine Public-Key-Zertifizierungsinstanz für die COPS-Infrastruktur implementiert. Dazu wurden Java mit Oracle JDBC-Schnittstelle und CORBA-Technologie eingesetzt.

Zur Zeit entwickeln wir ein graphisches Spezifikationswerkzeug für ALMO$T und ein Datenmodell für eine Datenbank, die solche Spezifikationen verwaltet und eine Abfrageschnittstelle zur Wiederverwendung von Spezifikationen anbietet. Weitere Arbeiten betreffen die Entwicklung eines Interpreters und der verteilten Objekt-Infrastruktur zur Ausführung von Geschäftstransaktionen.

Literaturverzeichnis

Becker, J./Vossen, G. (1995): Geschäftsprozeßmodellierung und Workflow-Management: Eine Einführung. In: Geschäftsprozeßmodellierung und Workflow-Management. Eds.: G. Vossen, J. Becker. International Thomson Publishing.

Bertino, E./Ferrari, E./Atluri, V. (1997): A Flexible Model Supporting the Specification and Enforcement of Role-based Authorisations in Workflow Management Systems. Proc. of Second ACM Workfshop on Role-based Access Control, 1997.

[8] Systemics Ltd: www.systemics.com/software/cryptix-java/ (last accessed 9/1997)

Coase, R. (1937): The Nature of the Firm. In: Economica, vol. 4, 1937, pp. 386-405.

Curtis, B./Kellner, M./Over, J. (1992): Process Modeling. Communication of the ACM, vol.35, no.9, 1992, pp. 75-90.

Garbade, K.: Securities Markets. New York; McGraw-Hill; 1982.

Gausmeier, J./Fahrwinkel, U. (1994): Strategiekonforme Geschäftsprozesse und CIM-Maßnahmen. CIM-Management, 10 (2) 1994.

Georgakopoulos, D./Hornick, M./Sheth, A. (1995): An Overview of Workflow Management: From Process Modeling to Workflow Automation Infrastructure. Distributed and Parallel Databases, 3, 1995, pp. 119-153.

Gerhard, M./Röhm, A. W. (1998): *A Secure Electronic Market for Anonymous Transferable Emission Permits.* Proc. of Thirty-First Hawaii International Conference on System Sciences (HICSS-31); 1998.

Herrmann, G./Pernul, G. (1998a): Towards Security Semantics in Workflow Management. Proc. of Thirty-First Hawaii International Conference on System Sciences (HICSS-31); 1998.

Herrmann, G./Pernul, G. (1998b): Viewing Business Process Security from Different Perspectives. Proc. of 11th International Bled Electronic Commerce Conference, 1998, pp. 74-89.

Herrmann, G./Röhm, A. W. (1999): ALMO$T: Eine Modellierungsmethode für sichere elektronische Geschäftstransaktionen. Erscheint in: Tagungsband Workshop Sicherheit und Electronic Commerce (WSSEC'98), Vieweg Verlag, 1999.

Holbein, R./Teufel, S./Bauknecht, K. (1996): The use of Business Process Models for Security Design in Organizations. Proc. of the IFIP TC 11 Information Systems Security Conference. Chapman & Hall, 1996.

IuKDG (1997): Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste. Artikel 3: Gesetz zur digitalen Signatur. Bundesgesetzblatt 1997, Teil I, Nr. 52, Bonn, 28. Juli 1997.

Malone, T./Yates, J./Benjamin, R. (1987): Electronic Markets and Electronic Hierarchies. Communications of the ACM, vol. 30, no. 6, 1987, pp. 484-497.

Röhm, A. W./Pernul, G. (1999): COPS: A Model and Infrastructure for Secure and Fair Electronic Markets. To appear in: Proc. of Thirty-Second Hawaii International Conference on System Sciences (HICSS-32); 1999.

Schmid, B. (1993): Elektronische Märkte. In: Wirtschaftsinformatik, vol. 35, 1993, pp. 465-480.

Schmid, B./Lindemann, M. (1997): Elemente eines Referenzmodells Elektronischer Märkte. Seminar Elektroinsche Märkte. Wirtschafts-

informatik'97; 1997. http://bandon.unisg.ch/cc/em/papers/emref.html (6/97)

Thoben, W. (1998): Sicherheit in workflowbasiserten Anwendungen. Proc. of 3. Fachtagung Sicherheit in Informationssystemen (SIS'98). Stuttgart, März 1998.

Thomas, R./Sandhu, R.S. (1996): Task-based Authorization: A Research Project in Next-generation Active Security Models for Workflows. Proc. of NSF Workshop on Workflow and Process Automation in Information Systems: State-of-the-art and Future Directions. Athens, GA, 1996.

Zwass, V. (1996): Electronic Commerce: Structures and Issues. International Journal of Electronic Commerce, vol.1, no.1, Fall, 1996, pp. 3-23. http://www.cba.bgsu.edu/ijec/