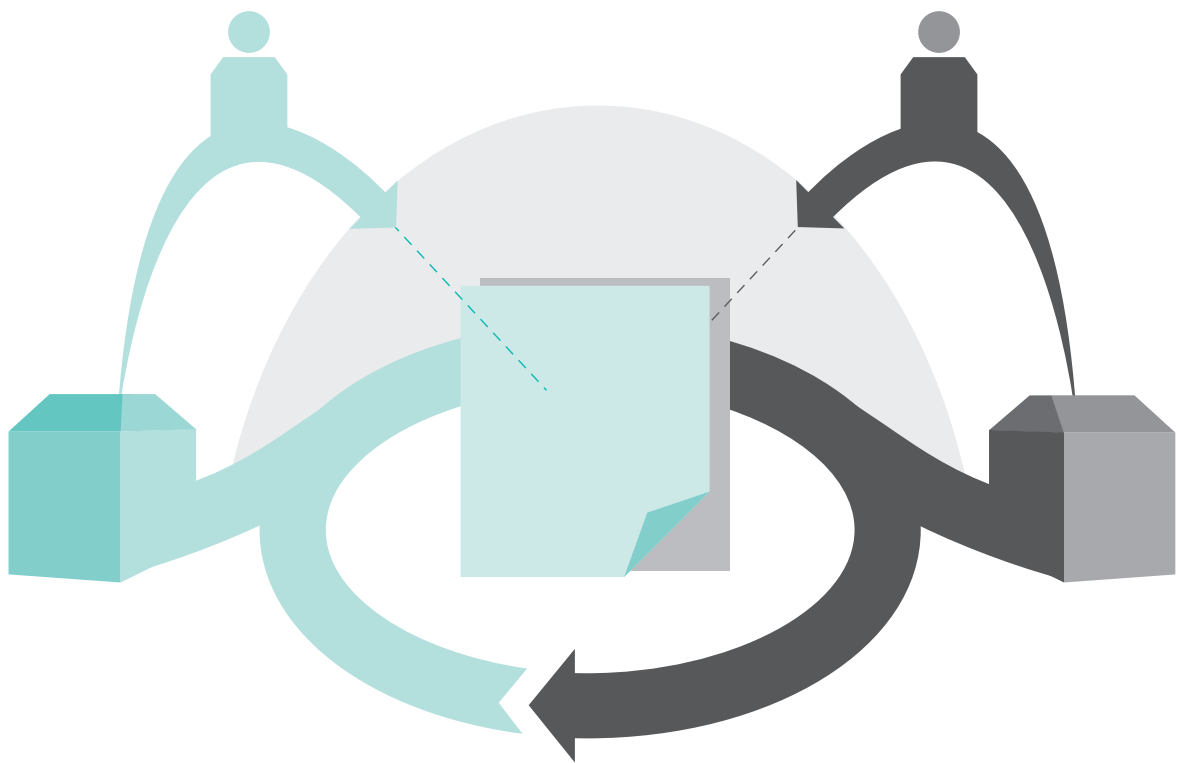


# CASTRUM

SERVICEPLATTFORM FÜR GESCHÄFTSPROZESS-  
AUTOMATISIERUNG



# CASTRUM – SERVICEPLATTFORM FÜR GESCHÄFTS- PROZESS-AUTOMATISIERUNG

Projekte zwischen Unternehmen und Hochschulen führen zu faszinierenden Resultaten. So verhielt es sich auch zwischen der Hochschule Luzern und der Firma Base-Net Informatik AG. Im Projekt Castrum ist eine erweiterbare, sichere IT-Serviceplattform für die Automatisierung organisationsübergreifender Geschäftsprozesse im Banken- und Versicherungsbereich entstanden.

Die KTI (Kommission für Technologie und Innovation des Bundes) fördert den Wissens- und Technologietransfer zwischen Unternehmen und Hochschulen in der Schweiz. Auf diesem Weg wurde auch das Projekt Castrum finanziell unterstützt.

Neben der Firma Base-Net Informatik AG und der Hochschule Luzern konnten mehrere Banken und Versicherungen für die Mitarbeit gewonnen werden.

Bei Banken und Versicherungsgesellschaften bestehen heute viele organisationsübergreifende Geschäftsprozesse, insbesondere in den Bereichen Hypotheken und Versicherungsverpfändungen. Unterschiedliche Technologien, wie Betriebssysteme, Kommunikationsprotokolle, Applikationen und Datenformate erschweren bis heute eine entsprechende Automatisierung. Das Projekt Castrum konzentrierte sich auf die Prozesse bei der Verpfändung von Lebensversicherungspolice – einem Bereich mit hohem wirtschaftlichem Nutzen für die beteiligten Wirtschaftspartner.

## HOHE ANFORDERUNGEN

In einer ersten Phase wurde eine technische IT-Infrastruktur geschaffen, um Versicherungen und Banken eine konsistente Sicht auf die gemeinsam benutzten Informationen einer verpfändeten Police zu ermöglichen. Der automatisierte Austausch der Informationen erfolgt dabei über eine zentrale, durch die Firma Base-Net zur Verfügung gestellte Service-Plattform. Diese Plattform nimmt die notwendigen Konvertierungen vor und speichert wichtige Daten für weitere Abfragen zentral ab. Naturgemäss sind die Sicherheitsanforderungen an eine solche Service-Plattform entsprechend hoch. Base-Net hat deshalb den eigentlichen Betrieb der Plattform an eine spezialisierte Firma ausgelagert.

## EIN INTERDISZIPLINÄRES PROJEKT

Das Projekt zeichnete sich durch eine intensive interdisziplinäre Zusammenarbeit aus. Auf Seite der Hochschule Luzern waren folgende Teilschulen und Disziplinen vertreten:

- > Teilschule Wirtschaft: Betriebsökonomie
- > Teilschule Technik & Architektur: Informatik

Die Schwerpunkte der betriebswirtschaftlichen Seite lagen bei der Prozessanalyse sowie in der Erstellung

eines netzwerkorientierten Kooperations-, Preis- und Vertriebskonzepts. Die Herausforderung lag in der Konzeption eines neuartigen Kooperationsmodells. Bei diesem Modell musste sowohl der Netzwerkperspektive als auch dem individuellen Nutzen der einzelnen Partner Rechnung getragen werden.

Auf der Informatik-Seite lag die Herausforderung in der Komplexität der eingesetzten Technologien. Nebst dem galt es die unterschiedlichen Anforderungen seitens der einzelnen Banken und Versicherungen zu bewältigen. Kommunikations- und Sicherheitsaspekte, sowie Anforderungen der betriebswirtschaftlichen Teilprojekte benötigten einen zusätzlichen Ideenreichtum.

In enger Zusammenarbeit mit dem Industriepartner konnte ein überzeugendes Konzept erarbeitet werden. Aus dem Projekt Castrum entstand das heutige Produkt „Smarx“, eine technische Informatik-Plattform, welche die notwendige Sicherheit und Flexibilität bietet, um Prozesse organisationsübergreifend umzusetzen.

## EINSATZ MODERNSTER TECHNIK

Der Einsatz des Produktes Microsoft BizTalk Server als zentrale Datendrehscheibe stellte einen technologischen Grundsatzentscheid dar. Der BizTalk Server ist eine mächtige, aber auch komplexe Softwarelösung für die Integration, Verwaltung und Automatisierung von Geschäftsprozessen. Die komfortable Kommunikationsinfrastruktur unterstützt sowohl traditionelle FTP-Schnittstellen (File Transfer Protocol) als auch eine Vielzahl von moderneren Serviceschnittstellen und Applikationsadaptoren (SAP, Peoplesoft, etc.).

Das Projekt untersuchte intensiv Vorgänge vom Erfassen und Modellieren der Geschäftsprozesse bis zur fertigen automatisierten Lösung. Dazu sind die Möglichkeiten moderner Process-Engines ausgelotet worden.

Ein weiterer Forschungsschwerpunkt lag bei der Umsetzung der hohen Sicherheitsanforderungen in Verbindung mit dem Einsatz von Produkten wie dem Microsoft BizTalk Server.

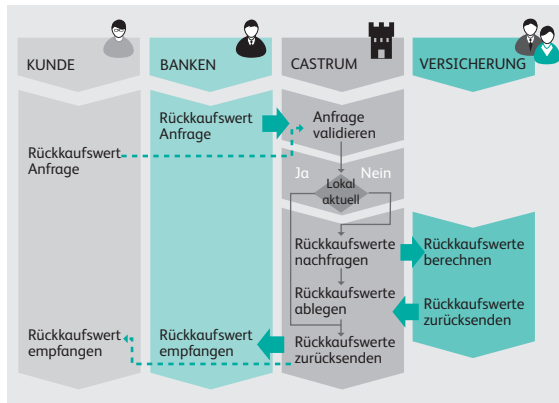
## EIN PROJEKT MIT WIRKUNG

In Folge dieses Projektes hat sich die Firma Base-Net zur Lancierung der neuen Produktlinie Smarx zur Automatisierung unternehmensübergreifender Prozesse entschieden. Für das beteiligte Informatik-Kompetenz-

zentrum der Hochschule Luzern stellt dieser Bereich auch inskünftig einen wichtigen Forschungsschwerpunkt dar.

### EIN KONKRETER GESCHÄFTSFALL

Der folgende, vereinfachte Geschäftsfall erlaubt einen guten Einblick in die Probleme von organisationsübergreifenden Geschäftsprozessen. Bei der Aufnahme einer Hypothek kann ein Bankkunde als Sicherheit unter anderem seine Lebensversicherung verpfänden. Aufgrund des Wertes der Liegenschaft und der Sicherheiten, z.B. des aktuell von der Versicherung berechneten Rückkaufwertes, gewährt die Bank die Hypothek. Der Prozess bezüglich Rückkaufwert kann wie folgt aussehen:



Der geschäftsübergreifende Prozess zu Rückkaufwertanfragen

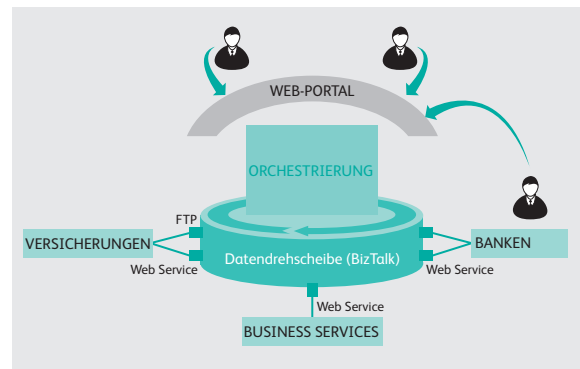
Die Versicherungsgesellschaften liefern regelmässig aktualisierte Rückkaufswerte an die Plattform. Benötigt nun eine Bank den Rückkaufwert einer bestimmten Police, und verfügt sie über das Einverständnis des Kunden, so kann dieser Wert direkt über einen Web-Zugriff abgefragt werden. Dies beschleunigt den Vorgang der Kreditabklärung unter Umständen massiv. Zudem erhält die Bank die aktualisierten Rückkaufswerte aller an sie verpfändeten Policen regelmässig automatisch zugestellt – entweder über eine speziell gesichertes Web Interface oder als XML-Datei.

In einer weiteren Phase werden auch die Vorgänge der Verpfändung und Notifizierung vollständig elektronisch abgebildet. Castrum wird so zur zentralen Drehscheibe für Kommunikation und Datenspeicherung. Auch die notwendigen Prozessschritte werden auf dieser Plattform koordiniert.

### SYSTEMARCHITEKTUR

Die Systemarchitektur von Castrum präsentiert sich in einer vereinfachten Art wie folgt: Sowohl Kunden als auch Mitarbeitende der Banken und Versicherungen greifen über ein Portal auf das System zu. Die zentral definierten Prozesse (Orchestrierungen) werden über ein Portal oder von den Banken und Versicherungen direkt ausgelöst. Die Business Services liefern die fachlichen Grundfunktionalitäten, die mit Web-Services angesprochen und durch eine Orchestrierung zu einem Gesamtprozess verbunden werden.

Die verschiedensten Schnittstellen zu Partnersystemen



Übersicht der Castrum Plattform und ihrer interagierenden Partner

werden mit Microsoft BizTalk Server über dessen Ports vereinheitlicht. So lassen sich problemlos bereits bestehende FTP-Verbindungen in eine moderne Web-service/XML-Umgebung integrieren.

### BPM – GESCHÄFTSPROZESS-AUTOMATISIERUNG

Business Process Management (BPM) ist ein zentrales Thema in Forschung und Lehre der Hochschule Luzern. Dabei wird Wert darauf gelegt, dass Organisationslehre und Informationstechnologie interdisziplinär zusammenwirken.

Eine zentrale BPM-Problemstellung: Gelingt es, einen Geschäftsprozess aus betriebswirtschaftlicher Sicht graphisch zu modellieren und durch Informationsanreicherung direkt technisch auszuführen und zu testen? Anders formuliert, kann auf unterschiedlichen fachlichen Ebenen mit dem gleichen Grundmodell gearbeitet werden?

Ein erster Schritt auf dem Weg zu einer Lösung war die Normierung der Business Process Execution Language (BPEL). Mit dieser XML-basierten Sprache lassen sich Business Prozesse definieren, wobei die einzelnen Prozessschritte (Aktivitäten) teilweise als Webservices implementiert sind. Der BPEL-Standard definiert keine graphische Beschreibung der modellierten Prozesse. Die meisten BPEL-Engines bieten aber entsprechende Werkzeuge an, darunter auch BizTalk Server von Microsoft.

Eine wesentliche Beschränkung von BPEL ist die fehlende Modellierung menschlicher Interaktionen. Diese soll in Zukunft durch BPEL4People ausgemerzt werden. Konkurrenz erwächst diesem Projekt aber aus einer anderen Ecke: der Business Process Modeling Notation (BPMN). BPMN ist eine graphisch orientierte Modellierungssprache, die aus der Betriebswirtschaft stammt und gegenüber BPEL auch unstrukturierte Abläufe zulässt. BPMN Modelle waren bis anhin nicht direkt ausführbar. BPMN 2.0 ermöglicht nun Ausführungsdetails mit XML zu beschreiben. Dieser vielversprechende Ansatz könnte helfen, die Kluft zwischen Organisation und Technik zu überbrücken.

Im Bereich dieser Process-Engines gibt es diverse interessante neue Produkte, welche die Hochschule Luzern laufend verfolgt und entsprechende Testumgebungen aufbaut. Weitere Informationen sind zu finden unter: [www.hslu.ch/d3s](http://www.hslu.ch/d3s)

# MICROSOFT BIZTALK SERVER IM EINSATZ

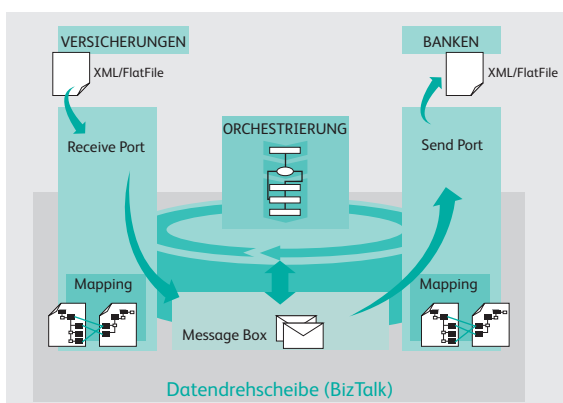
Beim Microsoft BizTalk Server handelt es sich um ein mächtiges Softwareprodukt für die Automatisierung und Integration von Geschäftsprozessen. Seine Hauptaufgabe besteht im Datenaustausch zwischen verschiedensten IT-Systemen. Viele kommerzielle IT-Systeme unterstützen den Datenaustausch mit anderen Systemen. Oftmals werden aber proprietäre Nachrichtenstrukturen und unterschiedliche Kommunikationsprotokolle verwendet. Der Microsoft BizTalk Server übernimmt die nötigen Daten- und Protokoll-Konvertierungen und erlaubt die Abbildung und Implementation von übergeordneten Businessprozessen.

Die Kommunikation mit der Aussenwelt erfolgt über sogenannte Adapter, die für verschiedenste Protokolle wie z.B. Webservices, FTP, Mail, Textdateien etc. vorhanden sind. Ankommende Daten treffen häufig im Text- oder XML-Format ein und werden für die Nachrichtenverarbeitung in BizTalk Server um weitere Elemente wie z.B. Name des eintreffenden Files, SOAP-Header etc. ergänzt. Typischerweise verwendet man innerhalb des BizTalk Servers eine interne Datenstruktur. Für die Kommunikation mit den Endsystemen müssen die Datenstrukturen mit einem sogenannten Mapping transformiert werden.

Die Nachrichtenverarbeitung des Microsoft BizTalk Server basiert auf dem Publish-Subscribe Pattern. Dabei werden sämtliche Nachrichten in einer zentralen Message-Box gespeichert und verwaltet. Komponenten, die eine bestimmte Nachricht verwenden oder weiterreichen, müssen sich vorgängig auf diese Nachricht abonnieren. Ist eine Orchestrierung auf eine Nachricht abonniert, wird sie aktiviert, sobald die Nachricht die Message-Box erreicht.

## ORCHESTRIERUNGEN UND SCHNITTSTELLEN

Orchestrierungen beschreiben Geschäftsprozesse, welche mehrere interne oder externe Services kombinieren und auch Entscheidungen und Fehlerbehandlungen verarbeiten. Die Orchestrierung wird zur Entwicklungszeit in einem graphischen Editor erstellt. Im Hintergrund wird ein erweitertes BPEL Format verwendet, ein normierter XML basierender Standard für Prozessbeschreibungen.



Vereinfachte Funktionsweise des Microsoft BizTalk Servers

Die Schnittstelle zu einer Bank oder Versicherung wird mit einem XML-Schema und einem Port beschrieben. Das Schema beschreibt die Struktur der ausgetauschten Nachricht. Der Port referenziert einen Service oder eine proprietäre Schnittstelle.

## IMPLEMENTATION EINER SCHNITTSTELLE

Bei der Implementation einer Schnittstelle werden in einem ersten Schritt mit den Partnern (Versicherungen, Banken) die zu übermittelnden Daten ausgehandelt. Dazu beschreibt man die Felder und ihre Wertebereiche in XML Schemas. Für die Gestaltung der XML-Schemas kann man sich von diversen Standards leiten lassen. In den entwickelten und verwendeten Schemas werden unter anderem die eCH-Standards berücksichtigt, die das Format von Postadressen definieren. Wenn gewisse Datenstrukturen in verschiedenen Serviceschnittstellen vorkommen oder Geschäftsfall spezifisch sind, können diese Definitionen in separaten Schemas ausgelagert werden. Mit dem Import von strukturierten Datentypen (ComplexType) können die Definitionen wiederverwendet werden.

Es ist darauf zu achten, dass man das XML-Schema so einfach wie möglich hält und nicht zu komplexe XML-Strukturen erstellt. Im Castrum Projekt zeigte sich, dass einer guten und nachvollziehbaren XML-Schemadefinition eine zentrale Bedeutung zufällt. Andernfalls entstehen schnell unerwünschte Abhängigkeiten zwischen den Schemas. Mit einem Software-Assistenten (Wizard) ist es in einem Visual Studio BizTalk Projekt auch möglich für Textdateien ein XML-Schema zu generieren. Das Schema beschreibt, wie die Textdatei in einer Nachricht abgebildet wird. Die Schema-Definitionen sind bei Projekten mit dem Microsoft BizTalk Server ein zentraler Punkt und spielen auch beim Deployment eine wichtige Rolle. Wenn an Schemas Änderungen vorgenommen werden, sind alle auf ihnen basierenden Microsoft BizTalk Server Applikationen neu zu deployen.

## KONVERTIEREN IN DIE GEWÜNSCHTE DATENSTRUKTUR

Ein grafischer Editor unterstützt das Mapping zwischen den partnerspezifischen XML-Dateien und den intern verwendeten XML-Nachrichten. Dieses Mapping wird an die Ports (die eingehenden und ausgehenden Verbindungen) gebunden. Beim Mapping lassen sich auch Operationen mit den Daten vornehmen – Formatanpassungen und Datenergänzungen. Für komplexe Anpassungen kann dabei C# Code verwendet werden. In sogenannten Script-Functoiden definiert man den Code oder ruft eine Library auf.

Die unterschiedlichen Datenstrukturen in den zu mappenden Schemas führen häufig zu Schwierigkeiten. Es besteht z.B. die Gefahr, dass optionale Felder auf obligatorische Felder gemappt werden. Gewisse Datenkombinationen sind vielleicht aus Geschäftssicht gar nicht zulässig. Sorgfältige Schemadefinitionen verringern diese Probleme.

Wertebereiche sollten möglichst klar eingeschränkt werden. Damit können unzulässige Daten bereits bei der Validierung der XML-Dateien mit den korrespondierenden Schemas entdeckt werden. Ein Beispiel hierfür ist eine Textdatei, die 0 oder 1 enthalten kann, was einen booleschen Wert darstellt. Im zugehörigen XSD-Schema wird nicht einfach der Typ int, sondern zusätzlich der konkrete Wertebereich von 1 und 0 definiert. Damit lassen sich Datenfehler vermeiden.

### FUNKTION DER MESSAGEBOX

Alle Nachrichten gelangen in die Messagebox. Hier werden sie nach dem Publish-Subscribe Pattern verwaltet. Orchestrierungen abonnieren sich über sogenannte logische Ports. Der logische Port definiert im Wesentlichen das Schema und ob es ein Empfangs- oder Sendeport ist. In der BizTalk Administrationskonsole wird der logische Port mit einem physischen Port assoziiert. Der physische Port bestimmt die konkrete Verbindung über FTP, Mail, SOAP, SQL usw. Auch in den physischen Ports können Filter auf Nachrichtentypen gesetzt werden. Damit abonnieren sich Komponenten in der Messagebox auf einen entsprechenden Nachrichtentyp. Sobald die Messagebox eine entsprechende Nachricht bekommt, wird sie dem Abonnenten ausgeliefert.

### VOM BETRIEBSWIRTSCHAFTLICHEN ZUM TECHNISCHEN BUSINESSPROZESS

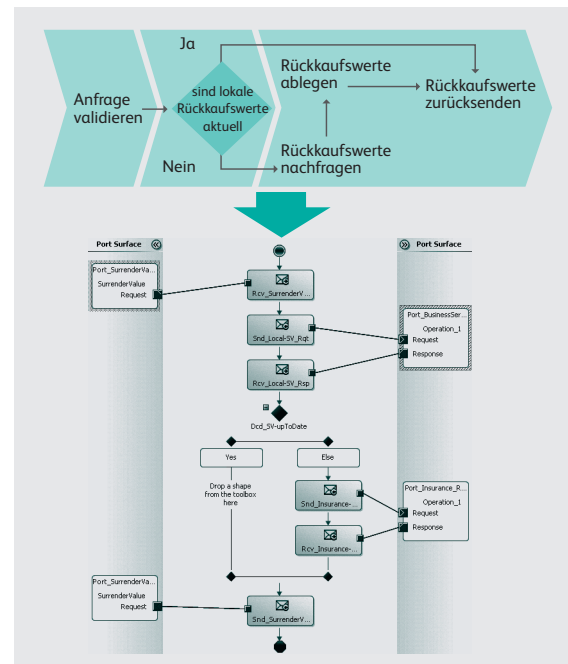
Aus betriebswirtschaftlicher werden bei der Prozessbeschreibung technische Details bewusst vernachlässigt. Ein Satz wie „Der Benutzer muss Zugriffsberechtigt sein.“ reicht völlig aus. Bei der Umsetzung löst er aber eine Menge von Fragestellungen aus, welche je nach Umsetzungsentscheid eine andere Applikationsarchitektur verlangen. Die Rückkaufswertanfragen sind aus betriebswirtschaftlicher Sicht eine einfache Anfrage und eine Antwort. Sobald man an die konkrete Umsetzung geht, findet man sich vor einigen offenen Punkten: Ist die Anfrage synchron oder asynchron, ist es eine Transaktion, die man auch rückgängig machen muss, oder ist es gar eine „long-running“ Transaktion, wenn mehrere Rückkaufswerte angefragt werden und nicht alle erfolgreich zurückgemeldet werden können. Wie soll dann die Antwort aussehen?

Aus betriebswirtschaftlicher Sicht beschreibt man die Geschehnisse durch die zu erledigenden Arbeiten. Im Microsoft BizTalk Server stehen die Nachrichten im Zentrum. Das heißt, jeder Verarbeitungsschritt muss vom Entwickler in einen Nachrichtenfluss transformiert werden. Zwischen betriebswirtschaftlicher und technischer Sicht klafft also ein nicht zu vernachlässigender Graben.

### DEN BUSINESSPROZESS IN DER ORCHESTRIERUNG ABBILDEN

Eine Orchestrierung kombiniert mehrere Service-Aufrufe, in denen die einzelnen Prozess-Schritte abgearbeitet werden, zu einem ablauffähigen Ganzen. Daneben beinhalten Orchestrierungen auch viele technische Aspekte der Prozesse.

Orchestrierungen werden in graphischer Form entwickelt. Das erstellte Diagramm der Prozessabläufe wird mit technischen Aspekten ergänzt. Hinter den schönen farbigen Kästchen eines solchen Diagramms verstecken sich konfigurierbare Eigenschaften und Strukturen, die sich nicht ohne fundiertes technisches Wissen, in Bezug auf Microsoft BizTalk Server, beherrschen lassen. Es werden Nachrichtentypen definiert, Ports die angesprochen werden und es lassen sich auch andere Orchestrierungen aufrufen. Es können neue Nachrichten erstellt und Entscheidungen aufgrund der eingehenden Nachrichten getroffen werden. BizTalk unterstützt auch verschiedene Transaktionskonzepte.



Prozessabbildung in einer BizTalk Orchestrierung

### ERKENNTNISSE

Bei der Umsetzung des Castrum Projektes ergaben sich folgende Erkenntnisse:

- > Bei lang andauernden Transaktionen ist zu beachten, dass sich die Systemumgebung (Endsysteme) während einer Transaktion ändern kann. Damit fällt beim Betrieb eines BizTalk Servers einem guten Change-Management eine zentrale Bedeutung zu.
- > Die Struktur der BizTalk-Projekte und die Art, wie die Applikationen deployed werden, benötigen einige Erfahrung. Es ist auf möglichst kleine Abhängigkeiten zu achten.
- > Die genaue und saubere Definition der XML-Schemas ist zentral. Dazu ist fundiertes XML Wissen von zentraler Bedeutung.
- > Das Testen von Microsoft BizTalk Servern ist praktisch nur mit Konsolenausgaben möglich, die mit dem Tool DebugView betrachtet werden.
- > Die Abbildung der Businessprozesse in eine Messageorientierte BizTalk-Umgebung unter Berücksichtigung der technischen Rahmenbedingungen ist ein aufwändiger und anspruchsvoller Entwicklungsprozess.

# ZENTRALE ASPEKTE DER CASTRUM SICHERHEITS-ARCHITEKTUR

Moderne Betriebssysteme, Datenbanken und Middleware-Produkte wie der Microsoft BizTalk Server bieten etabliert, systemübergreifende Authentisierungs-, Autorisierungs- und Audit-Mechanismen. Im Zentrum der Microsoft-Sicherheitsarchitektur steht der Verzeichnisdienst „Active Directory“ (AD) basierend auf dem Kerberos Protokoll und der „Integrated Windows Authentication“.

Das primäre Ziel der Sicherheitsarchitektur von Castrum ist eine möglichst weitgehende Verwendung dieser ausgereiften Sicherheitsmechanismen. Dies bedingt, dass alle Verarbeitungsprozesse im Kontext eines personen- oder firmenbezogenes AD-Accounts ausgeführt werden.

## AUTHENTIZITÄT DER DATEN

Die Datenverarbeitung im Sicherheitskontext eines personen- oder firmenbezogenen Accounts erfordert eine Authentisierung am Active Directory. Diese Authentisierung ist insbesondere bei organisationsübergreifenden Prozessen schwierig zu implementieren. Webservices unterstützen viele ausgereifte und sichere Authentisierungsmechanismen. Der organisationsübergreifende Datenaustausch im Banken- und Versicherungsumfeld basiert aber noch häufig auf alten Protokollen wie beispielsweise FTP. Das FTP-Protokoll unterstützt keine sichere Authentisierung. Deshalb kann das FTP-Protokoll die Authentizität der Daten nicht garantieren.

## DATEN DIGITAL SIGNIEREN

Eine mögliche Authentisierungslösung bietet die digitale Signatur. Die Signatur gewährleistet sowohl die Integrität als auch die Authentizität der übermittelten Daten. Für die Signatur der Daten werden heute fortgeschrittene oder qualifizierte X.509 Zertifikate eingesetzt. Die offiziellen Zertifizierungsstellen gewährleisten eine eindeutige Zuordnung der Zertifikate zu natürlichen oder juristischen Personen. Das Zertifikat enthält Datenfelder wie „User Principal Name“ (UPN), womit sich eine Person identifizieren lässt. Die Sicherheitsinfrastruktur von Microsoft erlaubt es, ein oder mehrere Zertifikate einem AD-Account und damit zu einer Windows Identität zuzuordnen. Damit wird es möglich, dass Applikationen die Verarbeitung der Daten im Sicherheitskontext des entsprechenden AD-Accounts mit einer Kerberos Protocol Transition vornehmen.

X.509 Zertifikate werden im Castrum-Projekt längerfristig auch für andere Sicherheitsfunktionen verwendet wie z.B. digitale Unterschrift, Verschlüsselung und Authentisie-

Damit Kerberos Protokoll Transition eingesetzt werden kann, muss die Systemumgebung entsprechend konfiguriert werden. Es zeigte sich, dass die Konfiguration recht komplex ist und viel Know How erfordert. Zudem kann die Fehlersuche recht aufwändig sein.

rung der VPN-Verbindungen. Die Sicherheit der Castrum-Infrastruktur ist damit massgebend von einer vertrauenswürdigen Umgebung für die Ausstellung von Zertifikaten, der „Private Key Infrastruktur“ (PKI) abhängig.

Der Aufbau von sicheren PKI unter Berücksichtigung der technischen, rechtlichen und organisatorischen Aspekte liegt ausserhalb des Castrum-Projekts.

Der Microsoft BizTalk Server unterstützt ein „Enterprise Single Sign-On“ (SSO). Diese Komponente erlaubt die Zuordnung von Zugangsdaten für nachgelagerte Systeme zu AD-Accounts (Windows Identitäten). SSO bietet in der aktuellen Version nur eine Passwort basierte Authentisierung für nachgelagerte Systeme. Eine Übergabe des Sicherheitskontextes des aktuellen Verarbeitungsprozesses ist nicht möglich. Damit schied das Enterprise SSO für einen Einsatz innerhalb des Castrum-Projektes aus.

## ZUKÜNFTIGES ORGANISATIONSÜBERGREIFENDES AUTHENTISIEREN

Das Castrum-Projekt zeigte, dass die zu Projektbeginn verfügbaren Sicherheitsmechanismen bei organisationsübergreifendem Businessprozessen nicht allen Anforderungen genügen. Mit den mittlerweile erhältlichen Mechanismen im Bereich der Identity Federation und der Claims-based Authentication könnten einige Probleme bedeutend eleganter gelöst werden. Insbesondere das neue Framework „Windows Identity Foundation“ (WIF) von Microsoft hätte vermutlich aktuellere und sicherere Lösungsansätze ermöglicht. Diese Mechanismen werden in den neusten Forschungsprojekten an der Hochschule Luzern untersucht.

# EINSATZ DER DIGITALEN SIGNATUREN

Digitale Signaturen und die dazugehörigen Zertifikate werden im Castrum-Projekt breit eingesetzt:

- > Es ist geplant, dass Endkunden im Castrum-Portal Verträge rechtsgültig unterschreiben können. Seit 2005 sind in der Schweiz die digitalen Unterschriften den handschriftlichen Unterschriften gleichgestellt.
- > Bei der Datenübertragung zwischen den Partnern und Castrum kann mit einer Signatur die Integrität und Authentizität der Dokumente sichergestellt werden.
- > Zertifikate spielen zukünftig unter Umständen auch für die Gewährleistung von weiteren Sicherheitsanforderungen (z.B. VPN-Verbindungen) eine zentrale Rolle.

## PDF-DOKUMENTE DIGITAL SIGNIEREN

Auf den meisten Rechnern, auch im privaten Umfeld, ist heute der Adobe Acrobat Reader installiert. Diese Software erlaubt es, PDF-Dokumente digital zu signieren. Adobe Acrobat Reader ist auf vordefinierte Signaturfelder eingeschränkt. In Castrum werden Verträge zwischen Endkunden und Partnern (Banken, Versicherungen) ab-

geschlossen. Die meisten Castrum-Partner verfügen über eine IT-Infrastruktur, die sie befähigt, gültige PDF-Dokumente mit Signaturfeldern zu erstellen. Es zeigte sich, dass es schwierig ist, eine Portal-Applikation für Castrum zu implementieren, die sich von Endkunden problemlos bedienen lässt. Insbesondere das automatische Hochladen des unterschriebenen Dokumentes auf das Portal erwies sich als eine grosse Herausforderung.

### XML-DATEIEN DIGITAL SIGNIEREN

Der Datenaustausch zwischen Castrum und den Partnern geschieht heute noch vorwiegend mit Datei-Transport. Die ausgetauschten Daten sind in der Regel XML-Dateien, können aber auch althergebrachte Textdateien (Flatfiles) sein. Mit der elektronischen Signatur können die folgenden Anforderungen sichergestellt werden:

- > Die Integrität der Datei kann überprüft werden.
- > Es ist nachweisbar, dass die signierte Datei von einem bestimmten Partner erstellt wurde. Damit kann die Nachvollziehbarkeit und Authentizität sichergestellt werden.
- > Das verwendete Signatur-Zertifikat kann einer digitalen Identität (AD-Benutzer) zugeordnet werden. Dies erlaubt eine Verarbeitung der Daten im Sicherheitskontext des konkreten AD-Benutzers.

Bei XML-Dateien können verschiedene Signaturtypen zum Einsatz kommen:

- > **enveloped:** Die Signatur wird in das zu signierende XML Element geschrieben (Die Signatur-Information wird nicht in den Hash des Dokumentes einbezogen.).
- > **enveloping:** Die Signatur wird um das zu signierende XML Element geschrieben, d. h. enthält das zu signierende XML Element. Dieser Typ eignet sich auch für nicht XML-Dateien.
- > **detached:** Das zu signierende Dokument befindet sich an einem beliebigen Ort. Es wird über eine Referenz (URI) geladen und kann mit Transform-Algorithmen wie XPATH beeinflusst werden. Mit diesem Signaturtyp lassen sich auch nicht XML-Dateien signieren.

Im Castrum-Projekt wurde mit „enveloping“ Signaturen gearbeitet. Der Einsatz von digital signierten Dateien ist aktuell noch nicht sehr verbreitet. Viele Firmen sind heute technisch noch nicht in der Lage, Transferdateien effizient digital zu signieren. Als Übergangslösung können nicht signierte Dateien bei der Einlieferung von einem vorgelagerten System signiert werden. Dies erlaubt eine konsequente Umsetzung der Sicherheitsarchitektur, auch wenn einzelne Partner Dateien noch nicht digital signieren können.

### AUTHENTISIEREN IM INTERNET

Die korrekte Authentisierung bei der direkten Partneranbindung wird bei bestimmten Geschäftsfällen durch signierte Dateien und schliesslich mit X.509 Zertifikaten sichergestellt. Auf Grund der hohen Sicherheitsanforde-

rungen war es unbestritten, dass auch für den Zugriff auf das Internetportal eine starke Authentisierung notwendig ist. In den frühen Projektphasen wurde eine Authentisierung mit X.509 Zertifikaten angestrebt. Prototypen bewiesen, dass sich die zertifikatsbasierte Authentisierung recht einfach implementieren lässt. Dabei ist es möglich, Zertifikaten von beliebigen Ausstellern (Firmen PKI, öffentliche Zertifizierungsstelle) einem AD-Account zuzuordnen und sich damit am Active Directory zu authentisieren. Es zeigte sich im Verlaufe des Projektes, dass auf Grund der nachfolgend aufgeführten Rahmenbedingungen die zertifikatsbasierte Authentisierung sich weder für Mitarbeiter der Partnerfirmen noch für private Benutzer des Portals eignet:

- > Viele der Partnerfirmen setzen intern eine zertifikatsbasierte Authentisierung ein. Die Sicherheitspolitik der Firmen erlauben keine externe Verwendung der Zertifikate. Grund: Falls Zertifikate auch extern genutzt werden, müsste auch die „Certificate Revocation List“ extern zugänglich sein. Der Inhalt der CRL wird von den Partnern jedoch als vertraulich deklariert. Die Verwendung von externen Zertifikaten scheitert an den konkreten Sicherheitseinstellungen der Arbeitsplatzrechner. Die Diskussionen mit den Sicherheitsverantwortlichen zeigten, dass eine zertifikatsbasierte Authentisierung nur mit grossen Anpassungen an der internen Arbeitsplatz-Infrastruktur umgesetzt werden könnte.

- > Bei den privaten Benutzern war der Preis der Zertifikate ein Show Stopper. Nur sehr wenige private Benutzer werden bereit sein, pro Jahr Fr. 100.- auszugeben für ein Authentisierungszertifikat. Es wurde auch die Herausgabe von eigenen Zertifikaten diskutiert. Der organisatorische Aufwand wäre aber unrealistisch hoch. Gegenwärtig finden in der Schweiz Bestrebungen statt, die Verbreitung von digitalen Zertifikaten zu fördern (siehe [www.suisseid.ch](http://www.suisseid.ch)). Es ist zu hoffen, dass diese Initiative erfolgreich ist.

Für das Internet-Portal von Castrum war daher eine Lösung zu suchen, die für Partnerfirmen und für private Personen kostengünstig realisiert werden kann. Die Analyse der verfügbaren Authentisierungen führte zur Wahl einer tokenbasierten Lösung (Hardware Token). Die bei der gewählten Lösung mögliche Integration der Authentisierung in eine Web-Application-Firewall ist sicherheitstechnisch sehr interessant.

### HERAUSFORDERUNG

Eine der zentralen Herausforderung im Castrum-Projekt war die Sicherstellung der korrekten Identität der beteiligten Stakeholder. Das generelle Ziel, möglichst auf Sicherheitsmechanismen zurückzugreifen, die Betriebssysteme und Middleware-Produkte zur Verfügung stellen, erwies sich als aufwändig. Eine durchgängige Verwendung von X.509 Zertifikaten hätte zu einer eleganteren Lösung geführt, liess sich aber auf Grund der Rahmenbedingungen nicht umsetzen.

## PROJEKT-FACTS

**Gesamtprojektleitung:** Stefan Hermann, Base-Net Informatik AG

**Projektführungsteam:** Hochschule Luzern – Technik & Architektur: Jörg Hofstetter,  
Base-Net Informatik AG: Stefan Hermann,

**Projekt-Kernteam:**

Base-Net Informatik AG: Stefan Hermann, Christian Bühler, Hans-Peter Christen, Othmar Grüter.  
Hochschule Luzern – Wirtschaft:  
Uta Jüttner, Christine Larbig.  
Hochschule Luzern – Technik & Architektur:  
Jörg Hofstetter, Roland Portmann

**Projektmitarbeiter/innen:**

Base-Net Informatik AG: Christoph Hasler, Cornelia Renggli, Sandro Wymann, Aleksandar Simic.  
Hochschule Luzern – Wirtschaft: Dieter Hottiger, Dirk Kleine, Ursula Sury  
Hochschule Luzern – Technik & Architektur: Res Gilgen, Marcel Gasser, Armin Egli, Antoine Hauck, Marcel Gschwandl, Lars Huber

**Weitere Projektpartner:** Axa Winterthur Versicherung, Pax Versicherung, UBS AG, Zuger Kantonalbank

*Projektdauer: 2 Jahre*

*Kontakt: joerg.hofstetter@hslu.ch*

## BASE-NET

Base-Net ist spezialisiert auf die Entwicklung und Einführung von Softwarelösungen im Kreditbereich bei Banken, Versicherungen, Pensionskassen und anderen Finanzintermediären sowie auf die Abwicklung unternehmensübergreifender Prozesse.

**Kernkompetenzen:**

- > Vernetzen von Partnern sowie Lösungen und Methoden in einem einzigen Produkt.
- > Flexibel einsetzbare und auf die kundenspezifischen Anforderungen parametrisierbare Standardlösungen.
- > Vermitteln der Erfahrungen beim Einsatz der Lösungen.

*Homepage: [www.basenet.ch](http://www.basenet.ch)*

*Kontakt: [info@basenet.ch](mailto:info@basenet.ch)*

## CC D3S DISTRIBUTED SECURE SOFTWARE SYSTEMS

Das Kompetenzzentrum D3S der Hochschule Luzern – Technik & Architektur beschäftigt sich zentral mit dem Thema eProcess. Dabei geht es um die Konzipierung und den Bau sicherer Softwaresysteme für die Prozessautomatisierung über Firmen- und Organisationsgrenzen hinweg unter Einbezug der Endkunden via Web-Portale.

**Weitere thematische Schwerpunkte sind:**

- > Informations- und Softwaresicherheit
- > Visual Computing
- > Datenmanagement
- > Software Engineering

*Homepage: <http://www.hslu.ch/d3s>*

*Kontakt: [joerg.hofstetter@hslu.ch](mailto:joerg.hofstetter@hslu.ch)*

## IBR

Das Institut für Betriebs- und Regionalökonomie IBR verfügt über eine 30-jährige Erfahrung in der Lehre, Weiterbildung, Beratung und Forschung. Es leistet einen Beitrag an die reflektierte Praxis von privaten und öffentlichen Institutionen in den Bereichen Management, Betriebs- und Regionalökonomie. Das IBR arbeitet mit Hochschulen im In- und Ausland, mit privaten Beratungsfirmen, mit Partnern und Partnerinnen aus der Wirtschaft, der öffentlichen Verwaltung und mit der Kommission für Technologie und Innovation KTI des Bundes zusammen.

**Als Institut der Hochschule Luzern – Wirtschaft bietet es Wissen und Erfahrungen in den Themen:**

- > General Management
- > Dienstleistungsmanagement
- > Public and Nonprofit Management
- > Regionalökonomie

## KTI

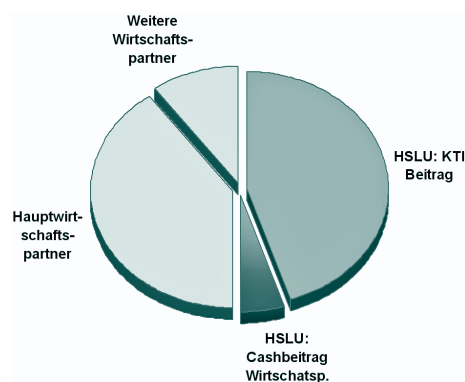
Die KTI ist die Förderagentur für Innovation des Bundes. Sie fördert seit über 60 Jahren den Wissens- und Technologietransfer zwischen Unternehmen und Hochschulen. Sie verknüpft Partner aus beiden Bereichen in Projekten anwendungsorientierter Forschung und Entwicklung und unterstützt den Aufbau von Start-ups. Die KTI verfügt über ein Budget von rund 100 Millionen Franken pro Jahr. "Science to Market" heisst ihr Credo. Unternehmen erarbeiten gemeinsam mit den Hochschulen neues Wissen für Produkte und Dienstleistungen und setzen es am Markt um.

**Die KTI fördert**

- > Marktorientierte F&E-Projekte, die die Unternehmen zusammen mit den Hochschulen in Industrie und Dienstleistungen durchführen.
  - > Die Gründung und den Aufbau von wissenschaftsbasierten Unternehmen.
  - > Den Wissens- und Technologietransfer durch Plattformen und Netzwerke.
- Ausschlaggebend für die Förderung sind der innovative Gehalt und die Aussicht auf eine erfolgreiche Umsetzung im Markt.

*Homepage: [www.bbt.admin.ch/kti/](http://www.bbt.admin.ch/kti/)*

*Fachkontakt: [info@kti-cti.ch](mailto:info@kti-cti.ch)*



Aufteilung der Arbeitsleistungen