NOTITIA

AdNovum

Bemerkenswertes von und über AdNovum

Supply Chain Event Management

Innovative Logistiklösung für Holcim

Einzigartig dank Integration

Interview: gezielt in die eigenen Chancen investieren

Security für SAP

Enterprise SSO und End-2-End-Sicherheit für SAP und Dritte

Herbst 2009, Nr. 17

Vorsprung durch IT

Liebe Leserin, lieber Leser

Mut zur eigenen Lösung – wer sich vom Standard abheben und etwas Besonderes bieten will, muss die eigenen Stärken kennen und seine Geschäftsprozesse entsprechend gestalten. Dies ist ein rechtes Stück Arbeit und erfordert freie Hand: Man muss sich dazu von Bestehendem lösen können und Neues schaffen. Es ist jedoch ein lohnendes Unterfangen. Dies zeigt das Beispiel der Holcim Schweiz, die mit einer innovativen Lösung ihren Zementvertrieb modernisiert hat. Integrierte RFID Tags, Mobile Order Processing

Supply Chain Event Management

Holcim wickelt ihre Zement-Lieferaufträge in der Schweiz neu von A bis Z mit einer innovativen SCEM-Lösung ab. Die neue Applikation LOGON integriert und nutzt die bestehenden Systeme geschickt für die Kernprozesse der Supply Chain.

von Gérard Roos und Urs Manser

Mit der Einführung von LOGON – Logistics Online – hat die Baustoffherstellerin Holcim (Schweiz) AG ihren Order-to-Cash-(O2C-)Prozess für Zement optimiert. Dieser bestand bis dahin aus einer weitgehend papiergestützten Planung und Auftragsverarbeitung. Elektronische Systeme existierten für die Datenverwaltung und die Buchhaltung (SAP R/3 als ERP) sowie für die automatische Verwägung der LKWs und Silowagen. Mit LOGON verläuft der komplette Auftragsverlauf nun elektronisch eingebettet, von der Auftragsannahme vom Kunden über die Auftragsvergabe an die Transporteure, die Disposition an die LKWs und den Verlad bis zur automatischen Rechnungsstellung. Dank RFID Tags und Integration von Mobile Order Processing (MOP) bietet LOGON jederzeit aktuelle Information über den Stand der Aufträge und die Standorte der involvierten Transportmittel. Echtzeit-Information von den MOP-Geräten und Lastwagen über Verkehrsstaus und Ladevorgänge erlaubt den Disponenten eine effiziente Kontrolle und Gewährleistung des Vertriebs. Im Sinne des Supply Chain Event Management liefert die neue Anwendung eine durchgehende Informationsbasis aller Abläufe. Sie eliminiert Medienbrüche und Redundanzen und bringt mehr Komfort für die Kunden und Holcim.

> RFID Tags und Mobile Order Processing liefern jederzeit Echtzeit-Information über aktuelle Aufträge und LKW-Standorte.

SCEM

Supply Chain Event Management (SCEM) erweitert das verbreitete Konzept Supply Chain Management (SCM) um das Handling von Ereignissen in der Abwicklung des Liefer- und Absatzprozesses. Mit SCEM will man nicht nur die Effizienz und Effektivität einer Liefer- und Absatzkette sichern und optimieren, sondern auch deren Stabilität nachhaltig gewährleisten. Dazu steuert und überwacht man computergestützt möglichst jeden Einzelschritt der Supply Chain, so dass man bei Bedarf rasch und gezielt eingreifen und disponieren kann.

AdNovum hat die Applikation LOGON als Entwicklungs- und Integrationspartner in enger Zusammenarbeit mit Holcim und Drittfirmen realisiert.

In acht Monaten zum Release 1.0

In nur acht Monaten Entwicklungszeit wurde das SCEM-System LOGON zur Abdeckung der logistischen Prozesskette im Bereich Lastwagen / Strassenverlad als Webapplikation aufgebaut, mitsamt Benutzeradministration und der Anreicherung und Bewirtschaftung der Stammdaten aus SAP. Ein typischer Auftragsverlauf sieht mit LOGON folgendermassen aus: Erfassung des Auftrags (Produkt und Menge, Kunde, Zustellzeitraum); Zuweisung an einen Transporteur, der an einen Lastwa-

und modernste Webtechnologie sind nur einige der Highlights dieses Supply-Chain-Event-Management-Systems. Lesen Sie dazu den einleitenden Bericht von Gérard Roos und Urs Manser.

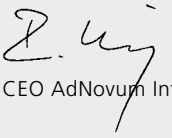
Die Kombination und Integration von marktgängigen Produkten und Suiten mit individueller Entwicklung von Funktionalität und Glue Code ist das Thema des darauf folgenden Interviews. Wie damit effizient Mehrwert schaffen? Wie die Ressourcen dafür gewinnen? Welche Rolle spielt dabei der Informatik-Ingenieur? Diese und andere Fragen beantwortet unser Chief Development Officer Kornel C.C. Wassmer.

Ein zentraler Aspekt ist dabei die Partnerschaft mit Produktherstellern. Als Partnerin von SAP hat die AdNovum zertifizierte Security-Komponenten entwickelt, mit denen sich SAP und Drittapplikationen auch ohne PKI in einen unternehmensweiten Single-Signon-Verbund einbinden lassen. Mehr dazu erfahren Sie im Hintergrund-Artikel von Stephan Schweizer.

Auf der Heftrückseite kommt dann SAP selbst zu Wort: Andreas Heidekrüger erläutert die Vorteile der Integrationsplattform SAP NetWeaver.

Ich wünsche Ihnen bei der Lektüre viel Vergnügen!

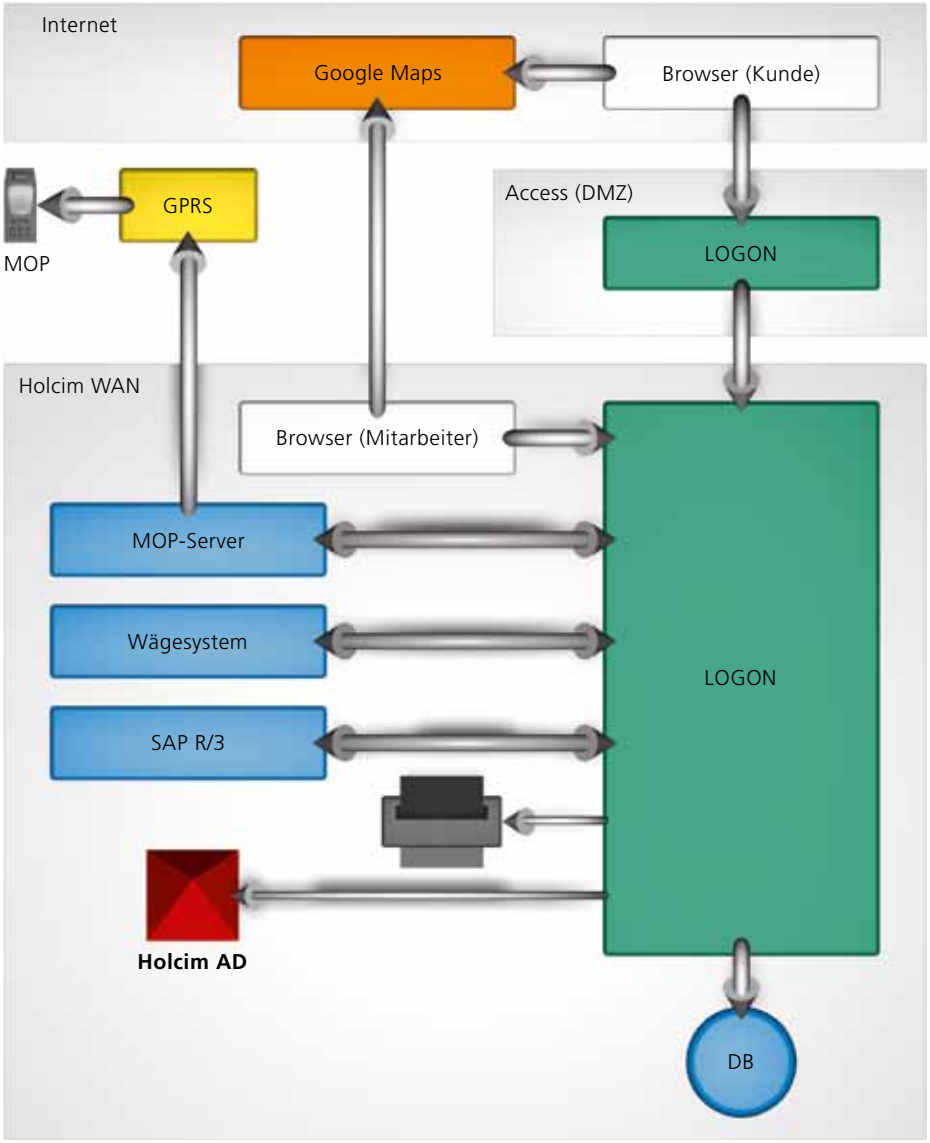
Ruedi Wipf



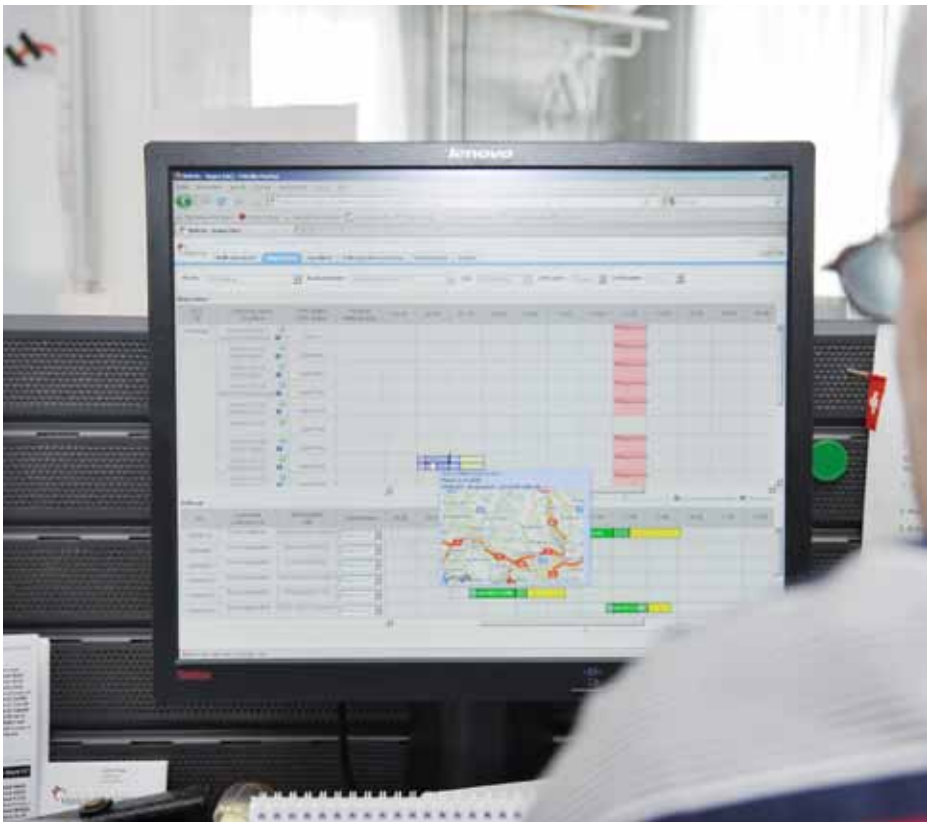
CEO AdNovum Informatik AG

gen disponiert; Verladung der bestellten Menge (mit Wägesystem), Transport, Entladung und elektronische Unterschrifterfassung für Lieferschein unterstützt durch MOP und somit auch automatische Erkennung der Lokationen (Zustellung); Übermittlung der Daten an SAP zwecks Rechnungsstellung (Abschluss). Zudem erleichtern Monitoringfunktionen das Auffinden von Engpässen in Disposition und Verfügbarkeit und von problematischen Auftragsverläufen. Weitere Merkmale der Applikation:

- Rich-Internet-Application-(RIA-)Oberfläche (instant Updates mittels Ajax, Drag & Drop, Echtzeitwiedergabe der Auftragsverarbeitung): Der hohe Bedienkomfort äussert sich in vielen positiven Benutzer-Feedbacks (MAs und Kunden von Holcim).
- Integration von Google Maps für die geografische Visualisierung der einzelnen Systemakteure (LKWs, Routen, Lieferorte, Ladeorte etc.) in die Benutzeroberfläche
- Integration in die MS-Windows-Authentisierung (SPNEGO/Kerberos)
- verschiedene Benutzergruppen: Mitarbeiter von Holcim, Benutzer von Partnerfirmen (Transporteure), Auftragserstellung und -verfolgung (Track & Trace) direkt durch Kunden
- feingranulare Autorisierung (Datenraum und Funktion), Self-Admin für die einzelnen Benutzergruppen
- Integration Mobile Order Processing für LKW-Fahrer: Auftragserteilung und -verarbeitung, Status- und Fahrzeitüberwachung, Standort-Tracking (GPS), LKW-Unterhalt etc.



LOGON – pragmatische Architektur mit grosser Wirkung.



Disposition LOGON (Foto Thomas Schönfelder, Karte Google, Kartendaten ©2009 Tele Atlas)

- Scanning von RFID Tags zur Identifikation von Objekten (LKWs, Silowagen, Silos, Container, Produkte etc.)
- Integration in ERP-Umgebung (SAP) und Anbindung bestehender operativer Systeme (Wägesystem)
- Umfangreiche Stammdatenverwaltung eingebettet in die SAP-Applikationslandschaft
- Implementation eines Table Browser für Systemadministratoren: Inspiriert durch SAP R/3 stellt LOGON ebenfalls GUIs zur Verfügung, welche die unmittelbare Sicht auf die rohen Daten des Systems erlauben. Damit können berechtigte Benutzer komfortabel und sehr direkt die Prozesse auf den Kerndaten verifizieren.

Geschickte Technologiewahl

Die Webapplikation wurde als Java-EE-Applikation entlang unseres leistungsstarken Software-Engineering-Prozesses implementiert. Insgesamt wurde darauf geachtet, bewährte und möglichst herstellerunabhängige Standards aus der Open-Source Community zu verwenden. So ist der Business Layer gemäss EJB3 umgesetzt. Im Presentation Layer werden Struts, Ajax ExtJS und DWR eingesetzt; hier galt es, etablierte Technologien in eine gesunde Mischung mit Neuem zu bringen, um die Risikofaktoren bezüglich Unbekanntem gering zu halten. Als Java EE Container kommt JBoss zum Einsatz. Die Daten werden in einer Oracle-Datenbank gespeichert. Die Verwendung standardisierter Kommunikationsprotokolle sehen wir als fundamentale Basis für eine integrations- und migrationsfähige System- und Applikationslandschaft. So wird wo überall möglich bei der Kommunikation mit Umsystemen (SAP, Wägesystem, MOP-Server) ausschliesslich SOAP verwendet (Apache Axis2).

> Vom GUI-Prototyp zum Rollout verging weniger als ein Jahr.

> Der Presentation Layer bietet eine gesunde Mischung von etablierten und neuen Technologien.

Sportliches Management

Die grösste Herausforderung bei der Realisierung der Softwarelösung bestand zweifellos darin, den immensen Funktionsumfang von hoher Komplexität in derart kurzer Zeit von Grund auf zu implementieren. Vom ersten explorativen GUI-Prototyp bis zum Piloten und anschliessenden Rollout verging weniger als ein Jahr. Diese schnelle Umsetzung gelang dank der engen, konstruktiven und direkten Zusammenarbeit aller Projektpartner, einer klaren Organisation und dem qualifizierten und engagierten Kernteam. Ermöglicht wurde dies durch die hohe Management Attention von Seite Holcim.

Risiken und Herausforderungen bezüglich Technologie, Architektur und Integration sowie die Abdeckung der Anforderungen und die Funktionsfähigkeit aus Business-Sicht wurden durch einen Proof of Concept (PoC) und Prototypen unter Einbezug der Drittlieferanten (MOP, Wägesystem) und mit striktem Requirements und Change Management konsequent früh adressiert.

Der gestaffelte Rollout startete ohne nennenswerte Zwischenfälle, vom Tag 0 an konnten sämtliche Aufträge für die aufgeschalteten Zementwerke mit dem neuen System erfasst, disponiert und geliefert werden. Die stabile und performante Applikation und die vielen positiven Rückmeldungen von Benutzern bestätigen den Erfolg. Dies ist eine komfortable Ausgangslage für die künftige Integration des Bahnverlads und des Geschäfts mit Zementsäcken in weiteren Releases.

Passende Lösung durch Integration

Basis für LOGON waren bei Holcim bereits im Einsatz befindliche Standardkomponenten (SAP) und Speziallösungen (Wägesystem). Darauf aufbauend entschied man sich, die Lösung mit einer neu zu entwickelnden Integrationskomponente zu realisieren, und zwar aufgrund folgender Kriterien:

- Abdeckung spezifischer Bedürfnisse des Auftraggebers: 100 % auf Holcim angepasste Lösung
- modernste Webtechnologie («Cockpit»-Philosophie nur bei individuell gestaltetem Benutzerinterface möglich)

- optimale Abbildung der Businessprozesse, ohne diese zu beeinflussen oder einzuschränken
- Potential und Flexibilität für zukünftige funktionale Erweiterungen
- Potential und Flexibilität für zukünftige Internationalisierung
- konsequente Elimination von Medienbrüchen
- keine redundante Datenpflege
- Hoheit des Kunden über den Source Code (Unabhängigkeit gegenüber Hersteller, Lizenzen)
- einfache Benutzeradministration
- feingranulare Autorisierung auf Funktionsebene und Datensichtbarkeit

Das System LOGON illustriert, wie durch geschickte Integration von Standardprodukten mittels Individualsoftware aus mehreren einzelnen Anwendungen ein Gesamtsystem realisiert werden kann, das mit dem Zusammenspiel der Einzelteile einen echten Mehrwert bringt.

Gérard Roos

Gérard Roos, dipl. Informatik-Ingenieur ETH und seit 2001 bei der AdNovum, hat in den letzten Jahren die technische Umsetzung diverser Web- und Sicherheitsapplikationen sowie verschiedener SSO-Portale geleitet. Er ist spezialisiert auf die Umsetzung von Erstreleases umfangreicher Projekte. In der Freizeit sind ihm keine Fels- und Eiswände steil genug.

Urs Manser

Urs Manser, dipl. Informatik-Ingenieur ETH, bringt seit 2002 sein Wissen und seine Erfahrung als Applikationsentwickler und technischer Projektleiter in die AdNovum ein. Zusammen mit Kunden arbeitet er Spezifikationen und Lösungsvorschläge aus und zerlegt diese in möglichst entwicklergerechte Portionen. Er ist regelmässig in Budapest, geht auch sonst gerne auf Reisen und fährt gern Ski.

Urs Manser (links) und Gérard Roos verantworten die technische Umsetzung der Applikation LOGON.

Einzigartig dank Integration

Kornel C.C. Wassmer, Chief Development Officer, im Interview mit Notitia

NOTITIA: Man erhält heute für jede Business Domain ausgereifte Softwareprodukte, an sich eine komfortable Situation, nicht?

Durchaus. Mit dem Erwerb eines Produkts profitiert man von der langjährigen Erfahrung des Herstellers in der betreffenden Business Domain. Die Software erfüllt alle potentiellen Anforderungen in ihrem Bereich und gibt die Businessprozesse zu einem signifikanten Teil vor, d. h., man muss dann «nur noch» seine eigenen Gegebenheiten damit in Einklang bringen.

Ein Softwareprodukt verkörpert durch seine Möglichkeiten und Einschränkungen aber auch die Ideen des Lieferanten über die künftige Entwicklung der Business Domain und seine Marktstrategie. Man kauft also mit dem Erwerb eines Softwareprodukts implizit auch seine eigene künftige Strategie ein oder beeinflusst sie zumindest. Damit ist man für einiges gerüstet, geht aber auch eine gewisse Abhängigkeit ein.

Was ist daran problematisch?

In der Dynamik des Markts jeweils rechtzeitig seine spezifische Stärke zu implementieren, erfordert eigene strategische Überlegungen und entsprechende Freiheitsgrade auf Softwareseite. Wo eine Business Domain den USP tangiert, muss man unbedingt darauf achten, die eigene Handlungsfähigkeit, d. h. die Flexibilität und Agilität, nicht einzuschränken.

> «Mit einer Integrationsplattform die einzelnen Systeme technisch und fachlich so vernetzen, dass ein Mehrwert entsteht.»

Ist die Gebrauchsfertigkeit der Produkte nicht auch ein grosser Vorteil?

Produkte und Suiten sind je nach Business Domain unterschiedlich gebrauchsfertig. Generell gilt: Auch für die Nutzung eines eingekauften Produkts müssen alle Phasen des Software-Engineering-Prozesses durchlaufen werden, nur verkürzen sich einzelne etwas bzw. haben andere Inhalte: Implementation z. B. bedeutet dann Parametrierung und ggf. Anpassung an bestehende Systeme.

Warum nicht für jede Business Domain eine eigene Produktsuite hinstellen?

Kann man schon; nur ist die Frage, womit hebt man sich von der Konkurrenz ab; typischerweise muss man seine Marktdifferenzierung mit Software unterstützen bzw. erst ermöglichen. Dabei geht es meist um Integration, ggf. mit Implementation von Zusatzfunktionalität. Man hat beispielsweise ein ERP, eine Produktionsplanung und einen e-Shop, und nun vernetzt man diese auf geschickte Art und Weise, integriert sie technisch und fachlich mittels einer eigentlichen Integrationsplattform so, dass gegenüber den Einzelkomponenten ein Mehrwert entsteht. Integriert sie u. U. noch mit den Produktionsanlagen und mit dem Lieferungsprozess, also z. B. Integration von SAP, Mobile Order Processing, Abfüllanlagen und Internet. Erst dies macht die Stärke dieser Organisation aus. Denn jede Einzelbox kann ein Konkurrent auch kaufen, all deren Parametriermöglichkeiten hat er auch zur Verfügung.

Diese Integration und Erweiterung bedeutet natürlich auch Aufwand …

Tatsächlich, um seinen eigenen USP in Software zu giessen, muss man Kreativität und Phantasie aufbringen, die Lösung beschreiben und designen.

Woher die Ressourcen dafür nehmen?

Hier hilft nun eben die Integrationsplattform. Man lässt die Komponenten geschickt miteinander interagieren und kann damit z. B. Prozessschritte, Medienbrüche und Datenredundanzen eliminieren. Damit kann man idealerweise die Gesamtkosten der eingesetzten Standardprodukte und -suiten minimieren. Ggf. erlaubt eine Integrationsplattform sogar, gewisse Convenience-Funktionen auszulagern, die eine Standardsoftware zur Verfügung stellt. Beispielsweise das Output Management, also Druckstrasse, Couverts und Postversand: Via einen Service lassen sich die elektronischen Daten an einen externen Dienstleister wie die Post weiterleiten.

Kann man die Integration nicht auch innerhalb eines bestehenden Produkts vornehmen?

Mit einer individuellen Integrationsplattform lassen sich die Businessprozesse freier gestalten, man ist damit unabhängig von den Restriktionen der integrierten Systeme.

Was für Restriktionen?

Auf technischer Ebene der «Klassiker» sind Protokollbrüche und die fehlende transparente Propagierung von Security-Kontext.

Und auf Ebene der Businessfunktionalität?

Nun, Standardsoftware-Suiten sind in der Regel als Insel und als solche für sich allein als komplett konzipiert. Wenn man nun drei, vier Produkte kauft, hat man entsprechend Redundanzen: Benutzerverwaltung überall, Security überall, und vielleicht sind das GUI und die Usability-Philosophien überall verschieden.
Vor allem aber sind die Durchgängigkeit und der Datenaustausch oft nur auf tiefem Level gewährleistet: Man kann rohe Daten importieren und exportieren, aber die Systeme nicht im Sinne von Business Services miteinander interagieren lassen. Man kann z. B. nicht die Benutzerverwaltung des einen Systems mit dem andern verbinden oder Buchungssätze von einem Buchhaltungssystem in anderen Systemen verwenden.
«Buy» steht damit oft dem SOA-Ansatz entgegen. Denn bei SOA interessiert ja gerade die Businessfunktionalität. Oft sind die Gesamtpakete dafür nicht genug modular und die Services kommunizieren nicht standardisiert. Komponenten zu bieten im Sinne von Basisservices, mit denen man weiterbauen kann, diesen Anspruch haben Standardsoftwareprodukte gar nicht. Das ist eben nicht Middleware!

Hat da keine Entwicklung stattgefunden von CORBA zu SOA?

Nun ja, schon bei CORBA haben sich diverse Normengremien damit auseinandergesetzt, Business Services zu spezifizieren, die schliesslich niemanden interessiert haben: Wenn etwas zur Norm gemacht wird, kann es eben kein USP eines Softwareherstellers oder -anwenders mehr sein. Ein Hersteller, der Normen implementiert, macht sich damit implizit ersetzbar. Mit SOA hat man nun eine andere Notation, eine andere Technologie darunter, aber die Fragestellungen und die Philosophie sind dieselben wie bei CORBA Business Objects – man formuliert standardisierte APIs und Protokolle für die Business Services. Deshalb wird da wohl auch SOA nicht wirklich den Durchbruch bringen.

Wie könnte das weitergehen?

Ein gewisser Teil der Überlegungen und Erkenntnisse wird jeweils schon weiterverwendet, man wird nicht immer komplett bei null beginnen. Aber der Treiber dafür wird mehr derjenige sein, dass die Softwarenutzer herausfinden, dass man mit dem Zusammenspiel verschiedener Standardprodukte Geld sparen kann. Auch wenn dies nicht mal so vermarktet werden wird: Die Nutzer von Standardsoftware werden die Anbieter darauf drängen, dass die Produkte besser interagieren, sei es mit Systemen, die die Unternehmen sonst noch in Betrieb haben, sei es mit Systemen von Kunden oder von Lieferanten. Ein Produkt, das zu sehr in sich geschlossen ist, wird es am Markt nicht leicht haben. Ob nun mit CORBA, Web oder SOA: Gefragt ist die semantische, businessfunktionale Integration.

> «Ob CORBA, Web oder SOA: Gefragt ist die Integration der Businessfunktionalität.»

AdNovum arbeitet mit Produktherstellern zusammen. Was kann sie in diese Partnerschaften einbringen?

Unsere langjährige Erfahrung in der Implementation von Software im Anwendungsumfeld grosser Kunden. Dadurch können wir nicht nur Kundenanforderungen im Sinne des Produkts optimal umsetzen, sondern auch dem Hersteller hochstehendes Feedback geben: über Anforderungen und Qualitätsaspekte seines Produkts, aber auch über technische Rahmenbedingungen und Constraints, die eventuell ins Produkt einfliessen müssen, damit sich dieses im spezifischen Kundenumfeld bewährt. Wie ein Fahrer für Formel-1-Rennwagen, der dank einem profunden technischen Background dem Hersteller detailliertes Feedback geben kann, wie er den Wagen ausbalancieren und perfektionieren soll. Dies kann für einen Produkthersteller ein Added Value sein.

Kannst du das noch etwas erläutern?

Als Hersteller ist man im Dilemma: Typischerweise müssen Produkte, um marktgängig zu sein, sehr offen und frei parametrierbar sein. Dadurch wird aber die Parametrierung beim konkreten Kunden entsprechend aufwändig und komplex und somit risikobehaftet. Ein erfahrener Implementationspartner weiss, welchen Freiheitsgrad es braucht und welchen nicht oder wo man immer anstösst, wo es also zusätzliche Freiheitsgrade braucht. Oder welchen Standard man zusätzlich unterstützen muss, welches andere System anbinden, nach dem häufig gefragt wird.
Als Implementationspartner ist man somit ein Mittler zwischen diesen Welten. Dem Kunden implementiert man die nötigen Adaptoren und liefert ihm ein perfekt funktionierendes

und passendes System mit der ganzen Technik frei Haus. Er kann ein Standardprodukt einsetzen, das ihm bezüglich der Fachdomäne kompetente Lösungen bringt. Der Hersteller des Produkts wiederum erhält Feedback, um dieses weiterzuentwickeln. Das ist wirklich ein Miteinander und alle profitieren davon.

Was bedeutet das vermehrte Arbeiten mit Produkten für den Ingenieurberuf?

Komponenten und Produktlinien bieten heute viel mehr Funktionalität und Komfort als früher. Will man sich auf dieser Basis mit seiner Implementation vom Markt abheben, muss die Integration, also das, was der Integrator noch hinzubaut, ebenfalls auf einer viel höheren Ebene sein. Die Integrationsdisziplin ist damit komplizierter und aufwändiger geworden, man muss neben umfassender Technik- und Technologiekompetenz auch Business-Domain- und Produktkenntnisse haben. Die Ingenieure müssen somit noch umfassender ausgebildet sein.

Gibt es auch im Software-Engineering so etwas wie ein «Revival des Handwerks», d. h. eine Rückkehr zur kompromisslosen Qualität und Perfektionierung?

Das Berufsbild divergiert diesbezüglich: Der Anspruch, ein Produkt zu perfektionieren, kann eher bei der Herstellung von Standardprodukten und -suiten gelebt werden. Im Integrationsbusiness ist ein anderer Fokus gefragt: pragmatisch und mit viel Phantasie, Werkzeugwissen und Flexibilität bezüglich verschiedener Varianten Komponenten und Produkte interagieren zu lassen. Da ist das Ad-hoc-Handeln, die schnelle, aber trotzdem professionelle Bereitstellung von Lösungen, gefragt, basierend auf einer profunden Technologie- und Technikkenntnis. Dazu muss man sich erfahren und agil in einer Systemlandschaft bewegen und sie entsprechend mitgestalten können; z. B. Gateways und Routers bauen können; also situativ auf die kundenspezifische Konstellation von Anforderungen und Umgebungen eine Antwort finden, wo es keine Standardrezepte gibt. Es versteht sich von selbst, dass gerade in dieser Disziplin das Handwerk wesentlich ist: Security, Middleware, QS-Werkzeuge, Metriken, Configuration Management etc.

> «Als Ingenieur muss man oft eine Greybox zum Laufen kriegen.»

Widerspiegelt sich das in der Anstellungspolitik der AdNovum?

Wir engagieren Ingenieure, die sich mit Integrationsfragen auseinandersetzen wollen, die mit ihrem Hochschulwissen kreative, flexible, schnelle, gute, aber auch pragmatische Lösungen bauen wollen, die die Themen und Anforderungen des Kunden schnell erfassen und kundenorientiert arbeiten können.

Unsere Mitarbeiter arbeiten sich rasch in Fachdomänen ein, zugleich bringen sie das nötige technische Expertenwissen in allen Aspekten der Softwareentwicklung mit.

Ein hoher Anspruch …

Ein Ingenieur ist per Definition interdisziplinär: Er muss sich schnell in Fachgebiete einarbeiten können, muss Organisation und betriebswirtschaftliche Themen verstehen, Probleme gruppieren und herunterbrechen können. Beim Einsatz von bestehenden Produkten kommt dies nun noch mehr zum Tragen: Man baut nicht auf der grünen Wiese, sondern eingebettet in diverse unabänderliche Umsysteme und Rahmenbedingungen, die man verstehen muss. Oft muss man eine Art Blackbox oder eher Greybox zum Laufen kriegen: Man weiss, was sie leistet und was man mit ihr leisten sollte, kann sie aber nicht direkt beeinflussen.

Wie lässt sich diese Breite von Know-how beherrschen?

Mit der Zeit lassen sich gewisse Integrationsmuster herausdestillieren. Was die Technik betrifft, gibt es typische, wiederkehrende Fragestellungen, da können wir auf einem reichen Erfahrungsschatz aufbauen. Auch in den Business Domains kann man sich eine Basis erarbeiten; neu ist jeweils die spezifische Situation und Anforderungskonstellation des Kunden im Bereich seines USP: Diese muss man verstehen, um ihn optimal unterstützen zu können. Das ist in der Natur der Sache, dass genau dies in der Integration gefragt ist.

Kornel C.C. Wassmer

Kornel C.C. Wassmer, dipl. Informatik-Ingenieur ETH, arbeitet seit 1996 in der AdNovum, seit 2007 als Chief Development Officer verantwortlich für die Softwareentwicklung. Er hält in der AdNovum das Motorenbanner hoch und versucht, den Junioren etwas Savoir-vivre zu vermitteln. Ansonsten ist er immer für politische Diskussionen innerhalb und ausserhalb des Gemeinderates seines Baselbieter Wohnortes zu haben.

Security für SAP

In einer heterogenen Applikationslandschaft ist die Realisierung eines Enterprise Single Signon nach wie vor eine Herausforderung. Das Nevis Security Framework kombiniert mit dem AdNovum SecStack bietet dafür interessante Lösungsansätze sowohl für SAP-Systeme wie für beliebige Drittapplikationen.

Highlights

Hoher Sicherheitslevel

- Authentizität: Zugang über Zertifikate
- Integrität: digitale Signatur der Daten
- Vertraulichkeit: Verschlüsselung der Daten

Single Signon (SSO)

- Einmalige Passworteingabe, auch für Nicht-SAP-Systeme

Einfache, flexible Integration und Customizing

- SecStack und Nevis lassen sich leicht an Kundenbedürfnisse anpassen und in bestehende Sicherheitsinfrastrukturen integrieren.

Von Stephan Schweizer

SAP-Systeme werden heute in vielen Unternehmen zur Verwaltung von sensitiven Finanz-, Personal- und Projektdaten eingesetzt, die für das Unternehmen z. T. von vitaler Bedeutung sind. Das Handling dieser Daten stellt zusammen mit regulatorischen Vorgaben wie z. B. Sarbanes-Oxley höchste Anforderungen bezüglich Zugriffskontrolle, Vertraulichkeit, Datenintegrität sowie Auditierbarkeit.

SAP-Komponenten kommunizieren per Default unverschlüsselt und die Authentisierung der Benutzer geschieht mittels UserID und Passwort. Um die heute geforderten Sicherheitsstandards zu erfüllen, bietet die SAP-Security-Infrastruktur deshalb die Komponenten SNC (Secure Network Communications) und SSF (Secure Store and Forward). Für beide charakteristisch ist die klare Trennung der Business-Logik von der Security-Funktionalität. Während die Komponenten mit Business-Logik Bestandteil des SAP-Systems sind, werden gewisse Security-Funktionen wie Authentisierung und Verschlüsselung von zertifizierten Drittprodukten wie dem AdNovum SecStack bezogen. Für die Einbindung ins SAP müssen die Security-Produkte eine spezifische Schnittstelle anbieten, welche auf dem IETF-standardisierten GSSv2 API (Generic Security Services Version 2 Application Programming Interface) basiert.

> Durch OpenSSL kann AdNovum SecStack auch mit reinen SSL-Knoten kommunizieren.

Vielseitig und modular

Der AdNovum SecStack besteht architektonisch im Wesentlichen aus einem solchen GSSv2 sowie einem PKCS#11 Layer (Public Key Cryptography Standard Nr. 11), die beide individuell angesprochen werden können.

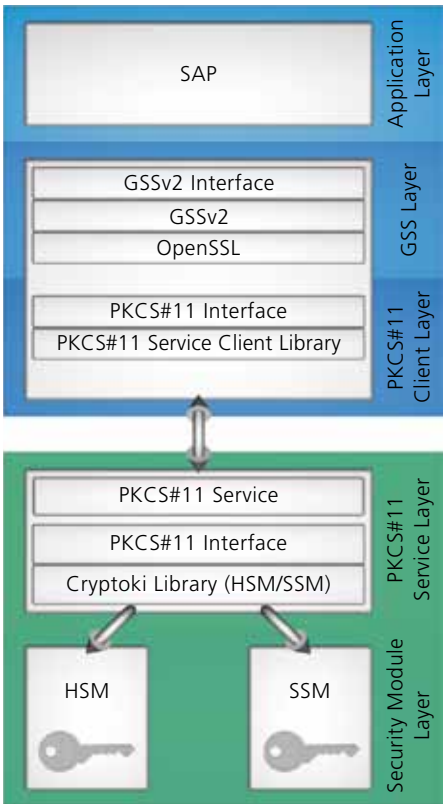
Der GSSv2 Layer stellt dabei eine Abstraktionsschicht zum Aufbau eines Security-Kontexts mit einem gegenüberliegenden Knoten zur Verfügung. Die Implementation des GSSv2 Layer von AdNovum SecStack basiert auf der bewährten Open-Source-Krypto-Bibliothek «OpenSSL». Dies bietet mehrere Vorteile: OpenSSL ist weit verbreitet, sehr stabil und wird von einer breiten Community kontinuierlich auf mögliche Security-Probleme untersucht. Zudem ist der AdNovum SecStack damit in der Lage, mit reinen SSL-Knoten zu kommunizieren.

Der SecStack-PKCS#11-Layer ermöglicht die Einbindung von HSM- (Hardware Security Module), SSM- (Software Security Module) oder Smartcard-basierten Keystores zur Speicherung von Schlüsselmaterial. HSM-Module werden in der Regel serverseitig eingesetzt, Smartcards dagegen für Krypto-Operationen auf Benutzerseite. Die bekanntesten Anwendungsgebiete für solche Komponenten sind wohl die starke Authentisierung mittels Client-Zertifikaten oder das Signieren von elektronischen Dokumenten mit einem ebenfalls auf der Smartcard gespeicherten Signierschlüssel.

Als zentraler Baustein der internen Security-Infrastruktur schützt der AdNovum SecStack seit mehreren Jahren die Kommunikation von über 20 000 Benutzern und mehr als 2000 Servern in der UBS.

Secure Network Communications

SNC ermöglicht die Verschlüsselung des Netzwerkverkehrs zwischen den verschiedenen SAP-Systemen sowie die Verwendung starker Authentisierungsmechanismen, wie z. B. Client-Zertifikaten in Kombination mit Smartcards. Zur Aktivierung von SNC muss lediglich die SecStack-GSSv2-Library in den entsprechenden SAP-Prozess geladen und die SAP-Konfiguration angepasst werden. Danach können die vom GSSv2 Layer zur Verfügung gestellten Funktionen für die Authentisierung der Benutzer sowie die Verschlüsselung des Netzwerkverkehrs genutzt werden. Durch das GSSv2-API verhält sich die Komponente dabei völlig protokollneutral, d. h., es sind keinerlei Anpassungen am Application-Layer-Protokoll notwendig. Sämtlicher Nachrichteninhalt wird durch den AdNovum SecStack vor dem Versenden verschlüsselt und auf der Gegenseite direkt nach dem Empfang wieder



Architektur AdNovum SecStack

entschlüsselt. Auch der Aufbau und die Verwaltung der Netzwerkverbindungen sind weiterhin vollständig unter der Kontrolle der entsprechenden SAP-Prozesse.

Die für die Krypto-Operationen notwendigen Interaktionen und den Zugriff auf das Schlüsselmaterial (via PKCS#11 Layer) übernimmt im Fall von SAP ebenfalls der GSSv2 Layer. Damit ist sichergestellt, dass aus Sicht des SAP-Systems sämtliche Authentisierungs- und Krypto-Operationen auf transparente Art und Weise erfolgen.

Stephan Schweizer

Stephan Schweizer, dipl. Masch. Ing. HTL und Executive Master of Information Technology, treibt seit Mai 2009 bei der AdNovum als Product Manager zusammen mit seinem Team die Weiterentwicklung der Nevis-Produkte voran. In seiner Freizeit treibt er gerne Sport oder unternimmt Ausflüge mit seiner Familie.

Secure Store and Forward

Die Nutzung von SAP-SSF-Mechanismen erlaubt die Sicherung von Daten und Dokumenten mit digitalen Signaturen und digitalen Umschlägen (digital Envelopes). Eine digitale Signatur identifiziert den Aussteller eindeutig und stellt die Integrität der Daten sicher. Erreicht wird dies, indem ein Hashwert des Dokuments mit dem Private Key des Ausstellers verschlüsselt wird. Bei der Verifikation wird die Signatur zuerst mit dem Public Key des Ausstellers entschlüsselt und anschliessend der Hashwert überprüft. Sind beide Operationen erfolgreich, kann das Dokument als vertrauenswürdig betrachtet werden. Der digital Envelope geht noch einen Schritt weiter. Hier wird zusätzlich sichergestellt, dass ein Dokument nur für den dafür bestimmten Empfänger lesbar ist. Das Dokument wird daher zuerst mit einem symmetrischen Schlüssel verschlüsselt. Anschliessend wird der symmetrische Schlüssel mit dem Public Key des Empfängers verschlüsselt und zusammen mit dem Dokument abgespeichert oder versandt. Nur der Besitzer des passenden Private Key ist in der Lage, den zur Verschlüsselung verwendeten symmetrischen Key zu entschlüsseln und damit das Dokument zu lesen.

Es ist zu erwarten, dass die Bedeutung der SSF-Mechanismen in Zukunft stark zunehmen wird, da sich damit beispielsweise Workflow-Prozesse auf sichere Art und Weise automatisieren bzw. elektronisch abwickeln lassen. Ein möglicher Anwendungsfall wäre etwa die Unterzeichnung eines Kaufvertrags, welche mit Hilfe der SSF-Funktionalität und von digitalen Unterschriften vollständig elektronisch abgewickelt werden kann. Von den bestehenden SAP-Applikationen macht z. B. SAP ArchiveLink von den SSF-Funktionen Gebrauch.

> Mit SSF lassen sich Workflows auf sichere Art automatisieren.

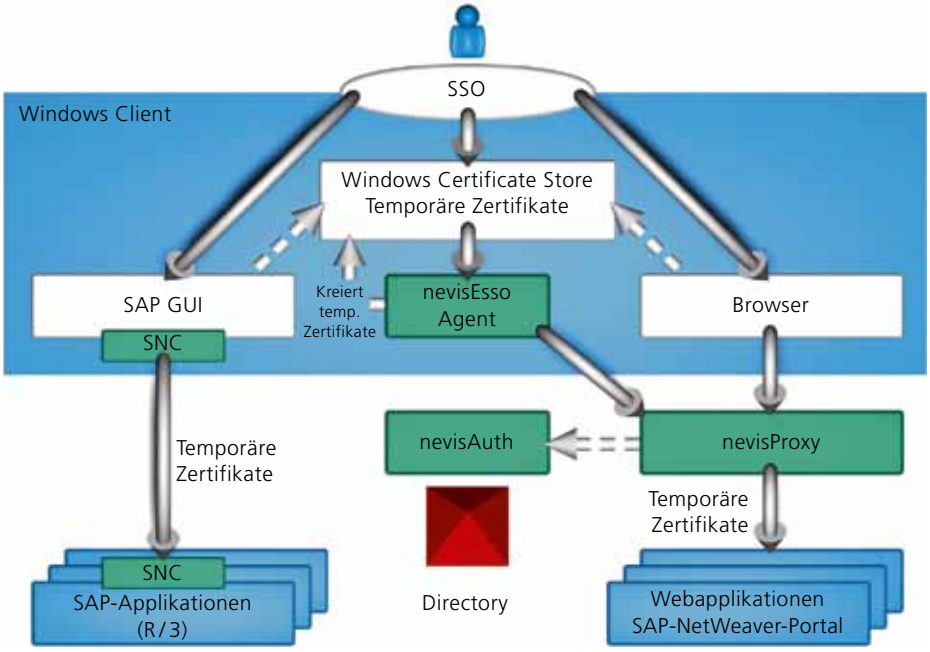
Der AdNovum SecStack beinhaltet alle für die Nutzung der SSF-Mechanismen notwendigen Funktionen. Analog zum SNC-Modul erfolgt auch hier der Aufruf der SecStack-Krypto-Operationen über das GSSv2-API. Eine funktionierende PKI (Public Key Infrastructure)

ist somit eine unabdingbare Grundvoraussetzung für die Verwendung der SSF-Funktionen. Im Gegensatz dazu können die SNC-Funktionen auch ohne PKI eingesetzt werden, wie der folgende Abschnitt aufzeigt.

SAP SSO

Unter der Voraussetzung, dass eine PKI vorhanden ist, lässt sich auf der Basis von SAP SNC relativ einfach auch ein Enterprise SSO (Single Signon) etablieren, da mit dem Client-Zertifikat ein universell verwendbares Security Token vorhanden ist. Dabei kann unterschieden werden, ob die Benutzerzertifikate auf einer speziellen Hardware (Smartcard, …) oder aber Software-basiert (z. B. im Active Directory) abgelegt werden. Der Betrieb einer eigenen PKI ist jedoch für viele Firmen zu aufwändig und lohnt sich daher nicht. Falls in einem Unternehmen noch keine PKI etabliert ist, lassen sich mit Hilfe des Nevis Security Framework auf der Basis temporärer Zertifikate dennoch sichere SSO-Lösungen realisieren (vgl. Abbildung).

Auf dem Client wird dazu der nevisESSO Agent (Nevis Enterprise Single Signon) installiert. Über den nevisESSO Agent authentisiert sich der Benutzer mit einem beliebigen Authentisierungsverfahren am nevisProxy, z. B. mit RSA SecureID, Vasco Token oder mTAN



Enterprise Single Signon mit nevisESSO

(Mobile Transaction Number via SMS). Auch die direkte Wiederverwendung der Windows-Anmeldung mittels Kerberos ist möglich, so dass neben der Windows-Anmeldung keine weiteren Anmeldevorgänge mehr notwendig sind. Der nevisProxy retourniert im Fall einer erfolgreichen Authentisierung ein temporäres Client-Zertifikat, welches vom nevisESSO Agent im Windows Certificate Store abgelegt wird. Die für die Ausstellung des temporären Zertifikats verwendete CA (Certificate Authority) befindet sich auf dem nevisAuth-Authentisierungs-Server und muss von den zu integrierenden Systemen als vertrauenswürdige Instanz akzeptiert werden. Sobald das temporäre Zertifikat im Windows Certificate Store abgelegt ist, kann es von dort von beliebigen Applikationen wie z. B. dem SAP Client (SAP GUI) verwendet werden. Ein SAP Client mit aktivierter SNC-Funktionalität kann sich damit ohne weitere Benutzerinteraktion an jedem SAP-System anmelden, welches die nevisAuth CA als «trusted CA» akzeptiert. Das Konzept ist dabei nicht auf SAP beschränkt, sondern lässt sich auf beliebige Applikationen ausdehnen. So unterstützt nevisESSO beispielsweise auch die sichere Speicherung von Passwörtern, welche zur automatischen Verarbeitung von Login Screens verwendet werden können. Ein Anmeldedialog wird automatisch erkannt und die entsprechenden Angaben werden direkt in diesen Dialog eingefügt. Damit lassen sich auch Legacy-Applikationen wie z. B. Terminalemulationen ohne Anpassungen problemlos ins SSO Framework integrieren.

Enterprise SSO für alle Fälle

Mit dem AdNovum SecStack steht ein zertifiziertes und bewährtes Security-Produkt für die Verwendung der SAP-SNC- und SSF-Mechanismen zur Verfügung. Er ermöglicht starke Authentisierung, Verschlüsselung der Daten und der Kommunikation und SSO im SAP-Umfeld. Für Unternehmen mit einer heterogenen Applikationslandschaft oder fehlender PKI (Public Key Infrastructure) ist die Kombination des AdNovum SecStack mit nevisESSO eine attraktive und kostengünstige Option, um Enterprise Single Signon auf der Basis existierender User Directories zu verwirklichen. nevisESSO besticht dabei vor allem auch durch die einfache Integrierbarkeit, da an den vorhanden Systemen keinerlei Anpassungen vorgenommen werden müssen. Damit sind die Voraussetzungen für eine zügige und kostengünstige Einführung einer umfassenden, unternehmensweiten Single-Signon-Lösung gegeben.

Sichere SSO-Lösungen realisieren: mit Nevis auch ohne PKI.

Geschäftsplattform

SAP NetWeaver bettet als SOA-Plattform Unternehmensanwendungen von SAP und Drittherstellern in die erforderlichen Geschäftsprozesse ein. Dieser Ansatz erlaubt es Firmen, schnell auf Marktveränderungen zu reagieren.

Von Andreas Heidekrüger, SAP

Unternehmen sind heute mit sich rasch verändernden Marktbedingungen konfrontiert. Das verlangt nach einer hohen Flexibilität, um den Betrieb und damit die Geschäftsprozesse schnell auf die jeweilige Situation ausrichten zu können. Ohne eine flexibel anpassbare IT-Plattform ist dies kaum möglich. Hierfür ist es nötig, die verschiedenen Unternehmensanwendungen wie ERP, CRM und Business Intelligence auf einer zentralen Plattform zu konsolidieren und miteinander zu verzahnen. Das gelingt mit einer serviceorientierten Architektur (SOA).

Integration der gesamten Unternehmensprozesse

Für die Abwicklung ihrer Prozesse haben Unternehmen eine Vielzahl von Systemen im Einsatz. Es reicht nicht aus, bloss den Betrieb auf einem zentralen Applikationsserver zu konsolidieren. Entscheidend ist die unternehmensweite Integration auf Prozessebene, also die durchgängige Abbildung der Geschäftsprozesse über alle Applikationskomponenten hinweg. Um die Applikationen als Prozessmodul oder Service greifbar zu machen, stellt SAP Funktionen der SAP Business Suite in Form von mittlerweile über 2900 Enterprise Services als «Best Practices» zur Verfügung. Anwender profitieren dabei von 30 Jahren Erfahrung, die SAP auf diesem Gebiet mitbringt. SAP NetWeaver liefert nun die notwendigen technischen Komponenten, um solche so genannte Composite Applications zu implementieren.

Eine Business-Process-Plattform wie SAP NetWeaver setzt die strategischen Unternehmensvorgaben auf Informatikebene um.

Mit NetWeaver bietet SAP das technische Fundament dazu. Von Grund auf als SOA ausgelegt, sorgt SAP NetWeaver für den Betrieb und die Verknüpfung von Unternehmensanwendungen sowohl von SAP selber als auch von Drittanbietern. Die konsequente Ausrichtung auf offene Standards ermöglicht die Integration einer heterogenen Softwareumgebung auf der zentralen NetWeaver-Plattform.

Das SAP NetWeaver Composition Environment erlaubt es, flexibel und einfach Services zu nutzen, unabhängig davon, ob diese von SAP, anderen Herstellern oder vom Kunden selber stammen. Die Möglichkeiten reichen hierbei vom Generieren von Benutzeroberflächen aus Service-Schnittstellen heraus bis hin zur BPMN-basierten (Business Process Modeling Notation) Modellierung komplexer, ausführbarer Prozesse mittels des integrierten SAP NetWeaver Business Process Management. Zusätzliche Flexibilität erhalten Unternehmen mit SAP NetWeaver Business Rules Management. Damit werden Geschäftsregeln, die den Prozessablauf steuern, aus der Applikation herausgelöst und in einer für den Prozessverantwortlichen verständlichen Form in so genannten Entscheidungstabellen dargestellt. Ändert sich eine Regel, muss nur noch diese angepasst werden, nicht die Applikation selber.

Die reibungslose Interoperabilität von Services und somit der einzelnen Anwendungen wird durch den Service-Bus SAP NetWeaver Process Integration sichergestellt. Die implizite Abstraktion der Applikationen voneinander gewährleistet zudem eine lose Koppelung der Systeme.

Durch die Kombination der in Enterprise Services gekapselten betriebswirtschaftlichen Funktionalität aus der SAP Business Suite und der Technologieplattform SAP NetWeaver erhalten Unternehmen eine umfassende Plattform zur Abwicklung ihrer Geschäftsprozesse. Dieser Ansatz bietet die nötige Flexibilität, um schnell auf veränderte Marktbedingungen oder neue gesetzliche Vorgaben zu reagieren. Somit ist gewährleistet, dass strategische Entscheidungen auf der IT-Ebene unterstützt und umgesetzt statt behindert werden.

SAP

Die SAP AG, mit Hauptsitz in Walldorf, ist der weltweit führende Anbieter von Unternehmenssoftware und Dienstleistungen, mit denen Firmen jeder Grösse und in über 25 Branchen ihre Geschäftsprozesse auf Wachstum und Profitabilität ausrichten können. Anwendungen von SAP sind bei mehr als 86 000 Kunden in mehr als 120 Ländern im Einsatz. Gegründet 1972, ist SAP heute der weltweit drittgrösste unabhängige Softwareanbieter, mit Niederlassungen in über 50 Ländern und mehr als 50 000 Mitarbeitenden. Im Geschäftsjahr 2008 erzielte das Unternehmen einen Umsatz von 11,6 Mrd. Euro. SAP ist an mehreren Börsen gelistet, darunter an der Frankfurter Börse und der New York Stock Exchange (NYSE: SAP).

Die SAP (Schweiz) AG mit Niederlassungen in Biel, Regensdorf und Lausanne steht unter der Leitung von Hakan Yüksel und zählt rund 550 Mitarbeitende.

www.sap.ch / www.sap.com

Impressum

Herausgeber:
AdNovum Informatik AG
Corporate Marketing
Röntgenstrasse 22
CH-8005 Zürich
Telefon 044 272 61 11
E-Mail info@adnovum.ch
www.adnovum.ch
Verantwortung und Redaktion:
Manuel Ott
Feedback: notitia@adnovum.ch
Gestaltung und Realisation:
Rüegg Werbung, Zürich
Fotografie:
Gerry Nitsch, Zürich