



*Die integrierte Gesamtlösung für
Dienstleister: Projekte, Prozesse, Wissen*



Projectile 3.7

Webbasierte Lösung zur Prozessoptimierung für Dienstleister

Technische Basis

Information Desire Software GmbH

An der Brunnenstube 25
D-55120 Mainz

Stand: 11.01.2010

Information Desire Software GmbH
An der Brunnenstube 25
D-55120 Mainz
Telefon: +49 6131 / 627 68- 0
Telefax: +49 6131 / 627 68 - 68

Internet: www.projectile.de
Email: info@projectile.de

Vertretungsberechtigte Geschäftsführer:
Lars Löffler und Peter Schaub



1 Entwicklungsumgebung BSM.....	3
2 Projectile und BSM.....	4
3 Angaben Systemplattform.....	5
3.1 Systemaufbau.....	5
3.2 Allgemeine Angaben.....	6
3.2 Systemanforderungen und Systemsoftware.....	6
4 Sicherheitsaspekte.....	7

1 Entwicklungsumgebung BSM

Projectile ist eine objektorientierte Webapplikation, die auf der Programmiersprache Java basiert. Durch die objektorientierte Programmierung in Java wird eine Plattformunabhängigkeit der Anwendung erreicht. Projectile wurde auf Basis unserer eigenen Softwareentwicklungsumgebung BSM (Business Software Modeller) als Servlet-Anwendung realisiert.

Das Business-Framework BSM ist ein Werkzeug für die Entwicklung moderner, dokumentenbasierter Applikationssoftware auf Basis von Java, SQL und XML. BSM ist eine fertige Enterprise-Anwendung, der nur die Business-Logik fehlt. Business Software Modeller richtet sich daher an Fachleute und Berater, die in ihren Gebieten hervorragende Software entwickeln können, sich aber mit der Standardtechnik nicht beschäftigen können oder wollen. Implementiert man mit Hilfe von BSM Business-Logik bzw. fachspezifisches Know-how, ist das Ergebnis eine lauffähige Anwendung. BSM ist eine Basisanwendung zur Konfektionierung webbasierter Business-Software.

Das Konfektionieren von Software bedeutet, dass BSM immer wiederkehrende Basisbestandteile, die jede Anwendung braucht, zur Verfügung stellt. Solche fertigen Module oder Basisbestandteile sind:

- > Webinterface mit HTML-Benutzeroberfläche
- > Datenbankunabhängigkeit zwischen SQL-Datenbanken, XML, Fremdsystemen
- > Scripting zur Anwendungsfernsteuerung
- > Benutzer- und Rechteverwaltung
- > Reportgenerator, Mailsystem, Zeitdienste und Hintergrundprozesse
- > Loadmanagement, Transaktionssystem
- > Integrierte Dateiverwaltung und internes Benachrichtigungssystem
- > Office-Interface
- > Bibliotheken für graphische Auswertungen (beispielsweise Gantt-Diagramm)
- > Historie und Archivierungssystem, ...

Die Philosophie ist, so viele fertige Technologien wie möglich zu verwerten und damit mit minimalem Aufwand ein modernes Produkt anzubieten.

2 Projectile und BSM

Das beschriebene Framework BSM ist Bestandteil von Projectile und wird stets mit ausgeliefert. Projectile kann mit Hilfe von BSM schnell an unternehmensspezifische Bedürfnisse angepasst werden. Darüber hinaus ermöglicht das Framework die einfache und kostengünstige Integration von Fremdsystemen.

Projectile besteht aus den fünf Modulen Basisdaten, Projektdaten, Erfassung, Fakturamodul und dem Auswertungssystem. Die folgende Abbildung verdeutlicht den Aufbau des Systems:

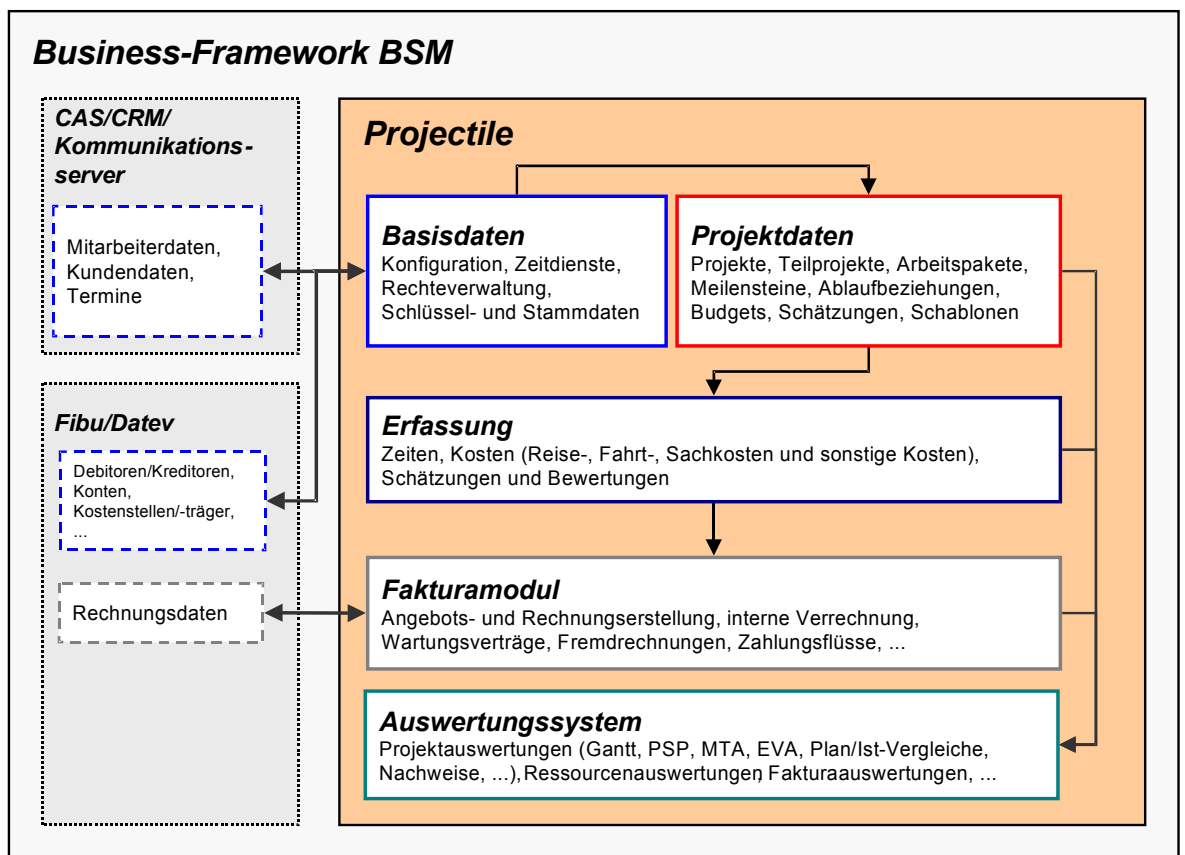


Abbildung 1: Aufbau Projectile

Weitere und detaillierte Informationen über den Leistungsumfang von Projectile können der aktuellen Produktbeschreibung entnommen werden.

3 Angaben Systemplattform

3.1 Systemaufbau

Die folgende Abbildung veranschaulicht die Systemarchitektur von Projectile. Projectile läuft sowohl server- als auch clientseitig weitgehendst plattformunabhängig. Als Serverplattformen werden derzeit produktiv Windows, Linux und Solaris unterstützt. Datenbankserver- und Applikationsserver können physikalisch getrennt werden. Die Betriebssysteme der beiden Server müssen nicht identisch sein.

Die Anbindung zur SQL-Datenbank wird über JDBC-Zugriffe realisiert. Projectile arbeitet mit den gängigsten SQL-Datenbanken problemlos zusammen (ORACLE, MS SQL-Server, Sybase, MySQL, ...).

Der Java-Code von Projectile ist lauffähig in Tomcat unter dem Apache-Webserver (beides kostenlos). Erzeugt wird eine Webanwendung, die HTML generiert, jedoch völlig auf Java-Applets, Plugins, JavaScript und Active-X verzichtet. Das heißt, eine breite Vielfalt an Webbrowsern auf fast allen Betriebssystemen kann als Client benutzt werden. Die Webbrowser können mit höchsten Sicherheitseinstellungen betrieben werden, z.B. ohne Cookies, Active-X, Java und Plugins.

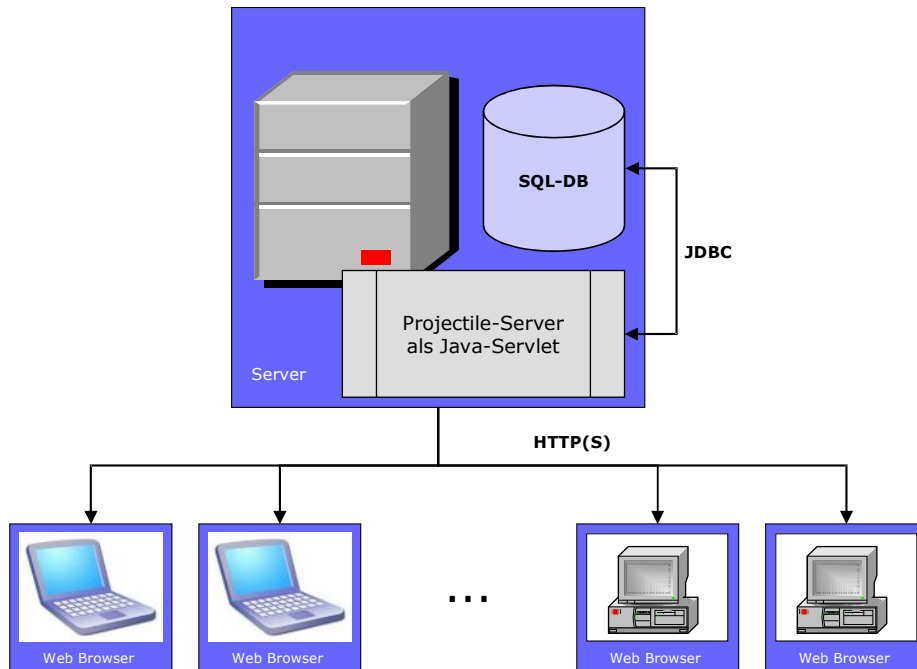


Abbildung 2: Projectile-Systemarchitektur

3.2 Allgemeine Angaben

Im folgenden wird die mögliche Systemumgebung für die Installation der Softwarelösung Projectile aufgelistet

System	Auswahl
Betriebssystem Server	Windows, Solaris, Linux
Betriebssystem Datenbank	Windows, Solaris, Linux, ...
SQL-Datenbank	MySQL, MS SQL-Server, Oracle, Sybase Adaptive Server, Informix, ...
Web- und Applikationsserver	Apache Webserver; Apache Tomcat
Webbrowser	MS Internet Explorer, Firefox, Opera, ...
Fernwartung	Terminalserver, VNC, Telnet

Erfahrungen haben gezeigt, dass sich die Java-Runtime-Umgebung, die zum Betrieb von Projectile benutzt wird, in virtuellen Servern bzw. virtuellen Betriebssystemen nicht optimal verhält.

Probleme mit Speicherbedarf und Performance können die Folge sein. Solche Konfigurationen können wir daher für den Produktiveinsatz nicht empfehlen.

3.2 Systemanforderungen und Systemsoftware

Mindestvoraussetzung bei PC-basierten Server: Intel Quad Core Klasse ab 2 GHz mit 4 GB RAM. Optimale Hardwareempfehlungen (User = Anzahl gleichzeitig intensiv arbeitender Nutzer):

- > Betriebssystem: Linux 64-Bit (ubuntu, Red Hat, SuSE), Windows 64-Bit, Solaris
- > CPU: ab Intel Core DUO + (User * 10), bei vielen Usern Intel Quad Core Klasse empfohlen
- > RAM: ab 4 GB (nur bei 64 Bit-Systemen voll nutzbar)
- > Festplatte: 3 GB für Software, 10-20 GB für Daten
- > Apache-Webserver 2.0.x (wahlweise mit installiertem SSL), Module mod_jk 1.2 wird installiert, falls nicht vorhanden
- > ggf. SMTP-Mailserver

4 Sicherheitsaspekte

Sicherheit bei Projectile-Installationen wird durch Verschlüsselung in folgenden Bereichen sichergestellt:

- > Verschlüsselung der Kommunikation Browser/Server über Apache-Modul mod_ssl
- > Verschlüsselung (Hashing) der Passwörter in der Datenbank
- > Zugriffsbeschränkung zum Projectile-Server/Datenbank

Verschlüsselung der Kommunikation Browser/Server

Das "Abhören" der Kommunikation zwischen Internet-Browser der Endnutzer und Projectile-Server ist besonders dann wichtig, wenn Projectile nicht nur in einem geschützten Intranet, sondern auch via Internet verfügbar gemacht wird.

Benutzereingaben besonders beim Anmelden (Name, Passwort) sollen nicht durch Mitprotokollieren der Verbindung ausgespäht werden können. Deshalb wird die gesamte Kommunikation verschlüsselt.

Folgende Schritte sind notwendig:

- > Installation von mod_ssl auf dem Projectile-Apache-Server
- > Installation eines Zertifikates, am besten ein von einer Certificate-Authority bestätigt
- > Sperren der unverschlüsselten Ports des Projectile-Servers (Tomcat-HTTP-Port)

Bei Benutzung von Projectile sollte dann im Browser immer das „Schloss-Symbol“ für verschlüsselte Kommunikation erscheinen.

Verschlüsselung (Hashing) der Passwörter in der Datenbank

Nutzerpasswörter werden in der Datenbank nicht im Klartext, sondern als sog. Hash-Wert gespeichert. Das bedeutet, dass man durch Auslesen des Nutzerdatensatzes keine Information zur unberechtigten Anmeldung erhält. Projectile ermittelt beim Anmelden den Hash-Wert des eingegebenen Passwortes und vergleicht diesen mit dem abgespeicherten Wert in der Datenbank. Stimmen beide überein, wird der Zugang gestattet.

Zugriffsbeschränkung zum Projectile-Server/Datenbank

Durch die Trennung von Projectile-Clients und Server ist bereits gewährleistet, dass Nutzer keine Lese- und Manipulationsmöglichkeiten erhalten, als die ihnen das Programm mit seinem Rechtesystem zuteilt (siehe Projectile-Administrationsleitfaden: Rechteverwaltung).

Hierzu sollten weitere Maßnahmen getroffen werden:

- > Projectile-Server sollte nicht via Laufwerks-Export (nfs, Samba, Windows-Freigabe) für Nutzer zugreifbar sein
- > Projectile-Datenbank sollte passwortgeschützt sein, der Projectile-Server sollte nur via verschlüsselter Kommunikation (ssh) administriert werden
- > der Projectile-Server sollte durch eine Firewall von ungeschützten Bereichen des Netzes getrennt sein.