

## Profil

Software & Security Architect

Bernd R. Fix



### Personalien

Name	Fix
Vorname	Bernd Robert
Funktion	Software Architect
Jahrgang	1962
Zivilstand	ledig
Nationalität	Deutsch
Heimatort	
Wohnort	Zürich
Sprachen	
Muttersprache	Deutsch
Englisch	Fliessend in Wort und Schrift
Kontakt	
eMail	bernd.fix@aspector.com
Telefon	+41 43 811 4148

Bernd Fix ist seit 1978 mit den verschiedensten Bereichen der Software-Entwicklung und den Fragen der Computersicherheit beschäftigt.

Schon während des Studiums der Physik und Philosophie an der Universität Heidelberg gründete er die Firma BrainON!, die unter anderem Verschlüsselungsprogramme für Behörden und Unternehmen entwickelte. Als Sicherheits-Experte war er in den 80er Jahren auch im Bereich der Computer-Viren tätig; so geht auf ihn die nachweislich erste Bekämpfung eines freilaufenden Virus zurück (1987).

1998 erfolgte die Überführung der BrainON! in eine schweizerische Aktiengesellschaft mit Sitz in Dornach/SO. Bis 2003 war Bernd Fix als CTO für die Software-Architektur der Produkte verantwortlich.

2003 erfolgte die Gründung der aspector GmbH mit Sitz in Zug. Die Schwerpunkte der Arbeit von Bernd Fix sind Beratung und Projektarbeit in aspekt-orientierter Software-Entwicklung sowie Computersicherheit (Verschlüsselung, digitale Signaturen, Chipkarten, Penetration Tests u.a.).

Ein breites Wissensspektrum, schnelle Auffassungsgabe sowie das Interesse an schwierigen Aufgabenstellungen sind besondere Fähigkeiten, die Bernd Fix auszeichnen.



aspector GmbH | Gubelstrasse 5 | CH-6301 Zug | <http://aspector.com>

---

Bernd R. Fix  
Software & Security Architect



<b>Ausbildung</b>	Datum
Grundschule Knesebeck (Niedersachsen/DE)	1968 - 1972
Gymnasium Hankensbüttel (Niedersachsen/DE) Erlangung der allgemeinen Hochschulreife mit den Leistungskursen „Mathematik“ und „Physik“, Gesamtnote „Gut“ (1.8)	1972 - 1981
Universität Göttingen, Grundstudium der Physik und Philosophie Erlangung des Vordiploms nach Abschluss des 4. Semesters, Note „Sehr Gut“	1982 - 1985
Universität Heidelberg, Abschlussstudium Physik und Philosophie Erlangung des akademischen Grades „Diplom-Physiker“ mit einer Arbeit im Bereich „Theoretische Astrophysik“ und einer Nebenfach-Prüfung zum Thema „Philosophische Interpretationen der Quantenmechanik“, Gesamtnote „Gut“	1985 - 1989

<b>Beruflicher Werdegang</b>	Datum
Gründung der Firma BrainON! in Heidelberg <ul style="list-style-type: none"><li>• Selbstständige Tätigkeit als Software-Entwickler (Produkt-Entwicklung im Sicherheits-Umfeld)</li><li>• Fach-Referent im Bereich Computer-Sicherheit</li></ul>	1987 - 1998
Verantwortlicher Software-Entwickler für das deutsche Architektur-CAD-System „SPIRIT“ (SOFT-TECH, Neustadt a.d.W.) <ul style="list-style-type: none"><li>• Schwerpunkt: 3D-Konstruktion und Visualisierung</li><li>• Firmenvertreter in Standardisierungs-Gremien (STEP)</li><li>• zeitweiliger Arbeitsaufenthalt in den USA bei einer Partnerfirma (Know-How-Transfer)</li></ul>	1989 - 1991
CTO und Geschäftsführer der BrainON AG mit Sitz in Dornach/SO <ul style="list-style-type: none"><li>• Geschäftsführer-Tätigkeit</li><li>• CTO und Lead Architect für alle Software-Projekte des Unternehmens</li></ul>	1998 - 2003
Geschäftsführer der Firma aspector GmbH, Zug <ul style="list-style-type: none"><li>• Selbstständige Tätigkeit als Berater und Security Architect in kritischen Infrastrukturen und komplexen Umgebungen</li><li>• Interne Entwicklung von Security- und Compliance-Applikationen (Produkt-Entwicklung)</li></ul>	2003 - heute

**Arbeitsschwerpunkte**

<i>(Security) Architecture</i>	Konzeption und Design von Lösung-Architekturen in anspruchsvollen und komplexen Umgebungen mit dem Schwerpunkt „Computer-Sicherheit“, „Compliance“ und „PKI“
<i>Requirement Engineering</i>	Moderieren, erfassen, modellieren und dokumentieren der Anforderungen an neue Software-Systeme in Zusammenarbeit mit dem Kunden.
<i>System Specification</i>	Detail-Design und Spezifikation der Lösungen basierend auf den Requirement Specifications des Projektes. Verifikation der Machbarkeit vor Implementationsbeginn durch Rapid Prototyping.
<i>Implementation Coaching</i>	Begleitung der Implementationsphase und allfälligen Migrationsprozessen im Rahmen eines Coachings (beratende Tätigkeit)
<i>(Security) Review</i>	Review von konzipierten oder implementierten Software-Projekten im Sicherheits-Umfeld (inklusive aktiven Sicherheitstests) oder Evaluierungen von externen Lösungsangeboten im RfP-Prozess nach Anforderungskatalog
<i>Documentation</i>	Software- und Prozess-Dokumentationen im Security-Umfeld; Verfahrensdokumentationen für externe Audits und bestellte Gutachter (Gerichtsfall)

**Spezielle Erfahrungen im Bereich „Computer-Sicherheit“**

<i>Kryptographie</i>	Verschlüsselung, digitale Signaturen / PKI, Hash-Verfahren, sicherer Schlüsselaustausch, Crypto-Hardware (HSM, ICSEF, Chipkarten) und -Software (Java/JCE)
<i>Netzwerk-Sicherheit</i>	Angriffsvektoren für alle ISO-Layer (und ihre Protokolle) sowie entsprechende Devices (Router, Switches u.ä.); Firewalls, IDS, VPN, VLAN
<i>Applikatorische Sicherheit (OS, Anwendungen)</i>	Sicherheits-Architektur, Reviews und dedizierte PenetrationTests
<i>Enterprise Security Architecture</i>	Grundlegende Sicherheitsanforderungen und -Architekturen in grossen Unternehmen, speziell im Bankenumfeld. Verständnis von IT-Risk und Compliance Anforderungen in komplexen IT-Infrastrukturen.



<b>Spezielle Erfahrungen im Bereich „Software-Entwicklung“</b>	seit (Datum)
<b>Aspekt-orientierte Programmierung (AOP):</b> <ul style="list-style-type: none"> <li>AspectJ (Design, Implementation, Beratung, Coaching)</li> </ul>	2001
<b>Objekt-orientierte Programmierung (OOP):</b> <ul style="list-style-type: none"> <li>Java (Design, Implementation)</li> <li>C++(Design, Implementation)</li> <li>UML (Design)</li> </ul>	1996 1990 1994
<b>Verantwortliche Konzeption und Umsetzung grösserer Applikationen (100k+ Quellzeilen)</b> <ul style="list-style-type: none"> <li>Übernahme der Funktion eines technischen Projektleiters (interne/externe Projekte)</li> </ul>	1989
<b>Plattformen/Betriebssysteme:</b> <ul style="list-style-type: none"> <li>Unix (Linux/Solaris/AIX)</li> <li>z/OS (System /370); spezielle IBM-Mainframe-Kenntnisse in den Bereichen Assembler und PL/1</li> </ul>	1998 1986

### Zusätzliche Erfahrungen / Skills

<i>Plattformen (Hard- und Software)</i>	Schwerpunkt: UNIX (Linux, Sun Solaris, IBM AIX, HP-UX u.a.) Weiterhin: Plan9 / Inferno, IBM Mainframe (z/OS, MVS, VM), Chipkarten / PIC, Microcontroller, Virtualisierung (Xen, VirtualBox), Android
<i>Programmiersprachen</i>	Schwerpunkt: AspectJ, Java. Weiterhin: C++, C, Limbo, Perl, Assembler (verschiedene Prozessoren), PL/1
<i>Entwicklungs-umgebungen</i>	Schwerpunkt: Eclipse 3.x mit AJDT (AspectJ-Erweiterung) Weiterhin: ant, (auto-)make, maven, emacs (UNIX), acme (Plan9/Inferno)
<i>Test &amp; QA</i>	T-Grid, Verification Suite
<i>Middleware &amp; Integration</i>	WebServices, Servlets, CORBA, RMI, RPC, MQ Series, JMF
<i>Methoden / Modellierung</i>	UML, XP, ER, AOP, OOP, RACI
<i>Datenbanken</i>	PostgreSQL, MySQL, Oracle, IBM DB2
<i>Netzwerk</i>	Protokolle und Hardware-Komponenten der OSI-Schichten 2 bis 4



Ausgewählte Projekte der letzten Jahre	Datum
<p>System-Entwicklung (C/C++) im Bereich HPC (High Performance Computing) bei einem Finanzdienstleister in der Schweiz</p> <p>Unterstützung bei der Umsetzung einer Message Processing Applikation im High Performance Computing-Umfeld (Börse) auf Multicore-Architektur und RealTime-Betriebssystem.</p>	2010
<p>Security Architect während der Evaluations- und Konzeptionsphase für ein „Data Loss Prevention“ (DLP)-System bei einer Grossbank in der Schweiz</p> <p>Evaluation verschiedener DLP-Lösungsanbieter unter definierten Sicherheitsaspekten:</p> <ul style="list-style-type: none"><li>• Sicherheit des Netzwerkverkehrs (Kommunikation der Lösungs-Komponenten untereinander) sowie der Lösungskomponenten selbst (z.B. gegen Intrusion)</li><li>• Einbindung starker Authentisierungsmethoden (Smartcard, Two-Factor-Authentication) in den Management-Prozess des DLP-Systems</li><li>• Eignung der Scan-Methoden (Regular Expressions, Keywords, Document and Database Matching etc.) zur Abbildung der gegebenen Compliance-Policies</li><li>• Einhaltung der Sicherheits-Richtlinien beim Scannen von eMails (Personen-/Datenschutz-Richtlinien, Mission Critical Infrastructure)</li></ul> <p>Konzeption zusätzlicher Sicherheits-Komponenten für den DLP-Einsatz</p> <ul style="list-style-type: none"><li>• Kapselung der Management Console über Citrix</li><li>• Einbindung der vorhandenen PK-Infrastruktur</li></ul>	2009 - 2010
<p>Security Architect während der Konzeptionsphase für ein neues globales Identity Management und Access Control System einer Grossbank in der Schweiz</p> <p>Design einer Prozess-, Architektur- und Komponenten-Landschaft, die den komplexen und vielfältigen Compliance-, Risk- und Business-Anforderungen einer global-operierenden Bank gerecht wird:</p> <ul style="list-style-type: none"><li>• Berücksichtigung der besondern Compliance-Anforderungen in den verschiedenen Rechtssprechungen („legal spaces“). Dies geschieht aktiv, d.h. es wird immer sichergestellt, dass nur korrekt genehmigte und zulässige/erlaubte Änderungen provisioniert werden können. Zudem wurden Mechanismen entworfen, die einen vollständigen und nachvollziehbaren Audit erlauben und durch Monitoring-/Reporting-Funktionen unterstützt werden.</li><li>• Sicherstellung der Integrität, Compliance und Accountability für jeden Schritt des Workflows, speziell im Genehmigungsprozess und der Mutation von Bestandsdaten. Dies wird durch kryptographische Verfahren und regel-basierte Policies erreicht.</li><li>• Effizienzsteigerung durch vollautomatische Provisionierung in die heterogene Infrastruktur und direkte Einbindung vorhandener IdM-relevanter Basistechnologien (Authentifizierung/PKI, regel-basierte Autorisierung u.ä.)</li></ul>	2007 - 2008
<p>Security-Review einer Offshore-IT-Plattform</p> <p>Technischer Review und Klärung von Detailfragen im Rahmen einer Entwicklungs-Plattform für Offshore-Entwickler, die im Auftrag einer Grossbank (im Ausland) arbeiten:</p> <ul style="list-style-type: none"><li>• Prüfung der Grundkonzeption und des technischen Basis-Layouts (Netzwerk-Design/-Komponenten)</li><li>• Ermittlung und Bewertung von Angriffsvektoren (initiiert durch „malicious“ Offshore-Mitarbeiter)</li><li>• Detailabklärungen wie z.B. LPAR Separation unter IBM z/OS</li></ul>	2007



Ausgewählte Projekte der letzten Jahre	Datum
<p><b>Entwürfe einer Lösungs-Architektur für den Integritätsnachweis von Logdateien</b></p> <p>Erstellung alternativer Konzepte für die Integration von Logdateien in den Integritätsnachweis des Langzeit-Archives. Die Konzepte hatte die speziellen Compliance- und Accountability-Anforderungen im Bankenumfeld zu berücksichtigen.</p>	2006
<p><b>Technische Projektleitung und Konzeption der Lösungs-Architektur für den Integritätsnachweis im digitalen Langzeit-Archiv einer Grossbank</b></p> <p>Dieses Projekt realisiert den gesetzlich geforderten Nachweis der Unversehrtheit (Integrität) von geschäftsbücher-relevanten Dokumenten in elektronischen Langzeit-Archiven (GeBüV) und berücksichtigt die zusätzlichen (Compliance-)Anforderungen einer Grossbank:</p> <ul style="list-style-type: none"> <li>• „Offene Architektur“, d.h. es wurden ausschliesslich (quell-)offene, validierte und anerkannte kryptographische Standards und Verfahren verwendet.</li> <li>• Hohe Performance (tägliches Volumen: &gt; 10 Mio. Dokumente)</li> <li>• Migrationsfähigkeit von rund 140TB Archivbestand</li> <li>• Gerichtsfähiger Integritätsnachweis (Evidence Record) einzelner elektronischer Dokumente auf Anforderung, ohne Dokumente anderer Kunden einzubeziehen (Bankgeheimnis)</li> </ul> <p>Nach der Konzeptionsphase wurde das Projekt während der Implementations- und Einführungsphase unterstützend begleitet und eine Verfahrens-Dokumentation des Gesamtprozesses gestellt.</p>	2004 - 2006
<p><b>Konzeption und Implementation eines Prototypen für ein Testwerkzeug im Bereich „Zahlungsverkehr“</b></p> <p>Generierung und automatische (periodische) Ausführung von Buchungsaufträgen in der IT-Testumgebung. Durch das anschliessend ebenfalls automatische Überprüfen der jeweils generierten Buchungsdaten durch die vielfältigen und verzahnten Einzelprozesse (Applikationen) kann das korrekte Zusammenspiel der einzelnen Komponenten geprüft werden.</p> <ul style="list-style-type: none"> <li>• Servlet-basiertes GUI für Administration und Benutzung</li> <li>• Import von Testbuchungen aus vorhandenen Quellen</li> <li>• Verwendung der CORBA-Middleware für die Kommunikation mit den Buchungskomponenten</li> <li>• Reporting-Funktionalität</li> </ul>	2003 - 2004

Ausgewählte Open-Source-Projekte	Datum
<p><b>J9P/StyxLib</b>                      <a href="http://sourceforge.net/projects/j9pstyxlib/">http://sourceforge.net/projects/j9pstyxlib/</a></p> <p>The J9P development framework is designed to ease the integration of legacy or non-9P services into 9P networks. It is a pure Java implementation and will run on various hard- and software platforms.</p> <p>The J9P/StyxLib framework enables Java developers to publish namespaces (virtual filesystems) based on the 9P/Styx protocol (Plan9/Inferno). Every namespace entry (file or directory) is associated with a handler (Java class) that controls the behavior and content of the entry. By developing customized handlers, you can integrate legacy or other non-9P services into a 9P network by mapping the service functionality to file operations. A generic 9P server (with pure Java implementation of 9P) as well as example namespaces („dbfs“) are included.</p>	2009



<b>Ausgewählte Open-Source-Projekte</b>	Datum
<b>Cyfer</b> <a href="http://aspector.com/~brf/Cyfer/index.html">http://aspector.com/~brf/Cyfer/index.html</a> Cyfer is an OpenPGP implementation for newer Nokia Communicators (9500/9300). OpenPGP is a standard (RFC 2440) for exchanging signed and/or encrypted messages (via eMail). It is used by applications like GnuPG (GNU Privacy Guard) and others.	2006
<b>DynaWorks</b> <a href="http://aspector.com/~brf/DynaWorks/index.html">http://aspector.com/~brf/DynaWorks/index.html</a> DynaWorks is a Java-based framework to develop GUI applications for PalmOS devices. It provides an efficient and compact source code library for GUI handling and database access and currently supports multiple Java2™ implementations (J9/IBM and KVM/Sun).	2000 - 2001

<b>Ältere Projekte (interne Produktentwicklungen)</b>	
<b>PC-DES: Datei und Verzeichnis-Verschlüsselung unter MS-DOS</b> Design und Implementation der Security-Applikation „PC-DES“ (Verschlüsselungsprogramm nach DES-Verfahren) für den Einsatz in Behörden, Unternehmen und im privatem Umfeld. Die Applikation wurde aktiv über Partner vermarket und 1990 vom Partner übernommen und weiterentwickelt.	1987 - 1989
<b>WAS: Virtueller Modellbau für Architekten</b> Design und Implementation des Computeranimations-Systems „WAS“ für die Bauindustrie und Architekten. Einsatz auch in Behörden (Polizei) zur Tatort-Rekonstruktion und -Begutachtung.	1992 - 1995
<b>MOPS: Messe-Organisations- und Planungs-System</b> Design und Implementation der Messeplanungs-Software „MOPS“ für Messengesellschaften; Kundenbetreuung und Schulung; Systempflege. MOPS war diese Jahre das zentrale visuelle Planungs- und Organisations-Instrument der Deutschen Messe AG, Hannover (CeBIT), der Messe München (Systems) sowie weiterer kleiner Messeveranstalter.	1995 - 2003
<b>CADalog: Elektronischer Ersatzteil-Katalog</b> System zum Identifizieren von Ersatzteilen in komplexen Maschinen (Flugzeug- und Maschinenbau) durch visuelles Navigieren in einem 3D-Modell oder in 2D-Explosionszeichnungen mit steigender Detaillierung.	1996 - 2003