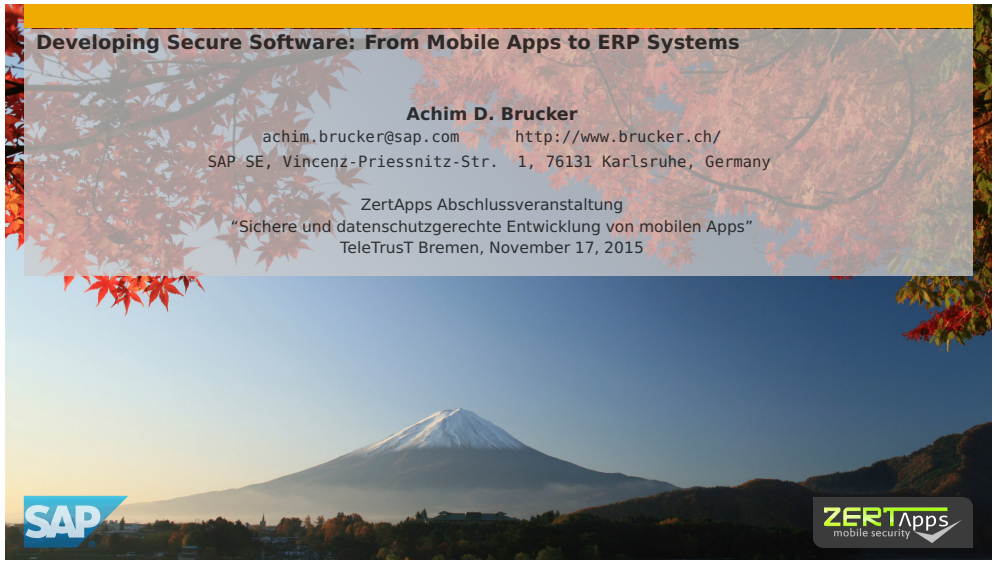


Developing Secure Software: From Mobile Apps to ERP Systems

Abstract

Developing secure software is, in general, challenging and requires and end-to-end secure software development lifecycle. It is particular challenging if the secure software development lifecycle needs to fit the whole range of software products from small mobile apps to large scale enterprise system and needs to be applicable to a wide range of software development methodologies.
In this presentation, we will present SAP’s approach to developing secure software in general and, in particular, highlight the challenges of developing mobile applications securely.

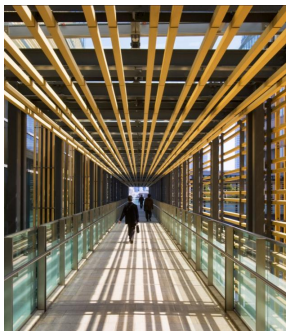
© 2015 SAP SE. All Rights Reserved.

Agenda

© 2015 SAP SE. All Rights Reserved.

SAP SE

- Leader in Business Software
  - Cloud
  - Mobile
  - On premise
- Many different technologies and platforms, e.g.,
  - In-memory database and application server (HANA)
  - Netweaver for ABAP and Java
- More than 25 industries
- 63% of the world’s transaction revenue touches an SAP system
- over 68 000 employees worldwide over 25 000 software developers
- Headquarters: Walldorf, Germany (close to Heidelberg)



© 2015 SAP SE. All Rights Reserved.

Personal Background

- I wear two hats:
  - **(Global) Security Testing Strategist**
  - Research Expert/Architect

  Working for the central software security team
- Background:
  Security, Formal Methods, Software Engineering
- Current work areas:
  - Static code analysis
  - (Dynamic) Security Testing
  - Mobile Security
  - Security Development Lifecycle
  - Secure Software Development Lifecycle

http://www.brucker.ch/

© 2015 SAP SE. All Rights Reserved.

SAP Uses a De-centralised Secure Development Approach

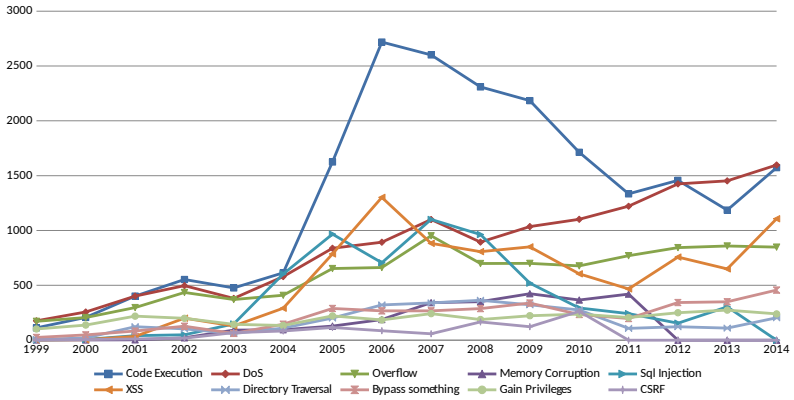
- **Central security expert team** (S^2DL owner)
  - Organizes security trainings
  - Defines product standard “Security”
  - Defines risk and threat assessment methods
  - Defines security testing strategy
  - Selects and provides security testing tools
  - Validates products
  - Defines and executes response process
- **Local security experts**
  - Embedded into development teams
  - Organize local security activities
  - Support developers and architects
  - Support product owners (responsibles)
- **Development teams**
  - Select technologies
  - Select development model
  - Design and execute security testing plan
  - . . .

© 2015 SAP SE. All Rights Reserved.

Agenda

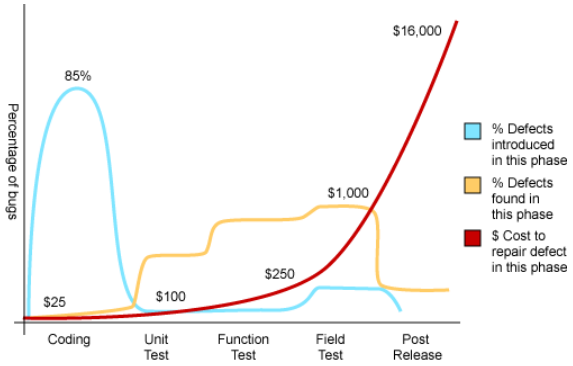
© 2015 SAP SE. All Rights Reserved.

Vulnerability Distribution



© 2015 SAP SE. All Rights Reserved.

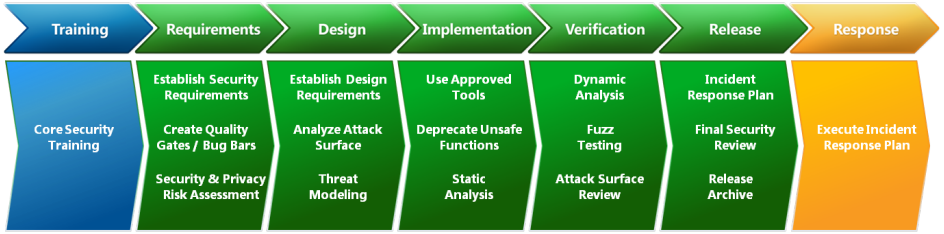
When Do We Fix Bugs



Source: Applied Software Measurement, Capers Jones, 1996

© 2015 SAP SE. All Rights Reserved.

Microsoft's SDL

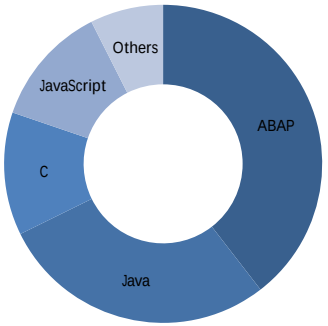


© 2015 SAP SE. All Rights Reserved.

Agenda

© 2015 SAP SE. All Rights Reserved.

Our Start: SAST as a Baseline



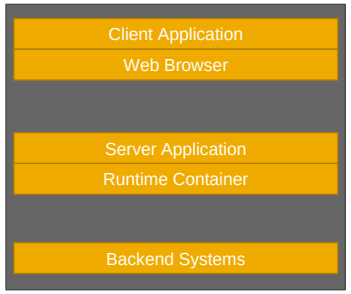
SAST tools used at SAP:

Language	Tool	Vendor
ABAP	CVA (SLIN_SEC)	SAP
JavaScript	Checkmarx CxSAST	Checkmarx
C/C++	Coverity	Coverity
Others	Fortify	HP

- Since 2010, mandatory for all SAP products
- Multiple billions lines analyzed
- Constant improvement of tool configuration
- Further details:
  Deploying Static Application Security Testing on a Large Scale. In GI Sicherheit 2014. Lecture Notes in Informatics, 228, pages 91-101, GI, 2014.

© 2015 SAP SE. All Rights Reserved.

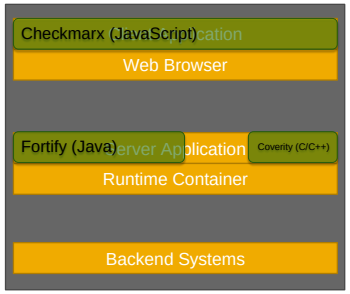
Combining Multiple Security Testing Methods and Tools



- Risks of only using only SAST
  - Wasting effort that could be used more wisely elsewhere
  - Shipping insecure software
- Examples of SAST limitations
  - Not all programming languages supported
  - Covers not all layers of the software stack

© 2015 SAP SE. All Rights Reserved.

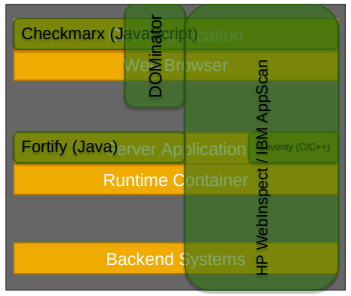
Combining Multiple Security Testing Methods and Tools



- Risks of only using only SAST
  - Wasting effort that could be used more wisely elsewhere
  - Shipping insecure software
- Examples of SAST limitations
  - Not all programming languages supported
  - Covers not all layers of the software stack

© 2015 SAP SE. All Rights Reserved.
Page 13 of 30

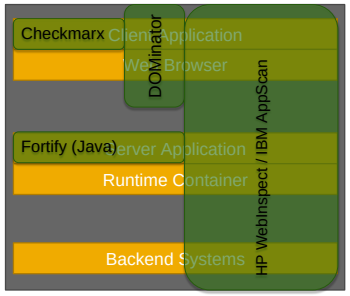
Combining Multiple Security Testing Methods and Tools



- Risks of only using only SAST
  - Wasting effort that could be used more wisely elsewhere
  - Shipping insecure software
- Examples of SAST limitations
  - Not all programming languages supported
  - Covers not all layers of the software stack

© 2015 SAP SE. All Rights Reserved.
Page 13 of 30

Combining Multiple Security Testing Methods and Tools



- Risks of only using only SAST
  - Wasting effort that could be used more wisely elsewhere
  - Shipping insecure software
- Examples of SAST limitations
  - Not all programming languages supported
  - Covers not all layers of the software stack

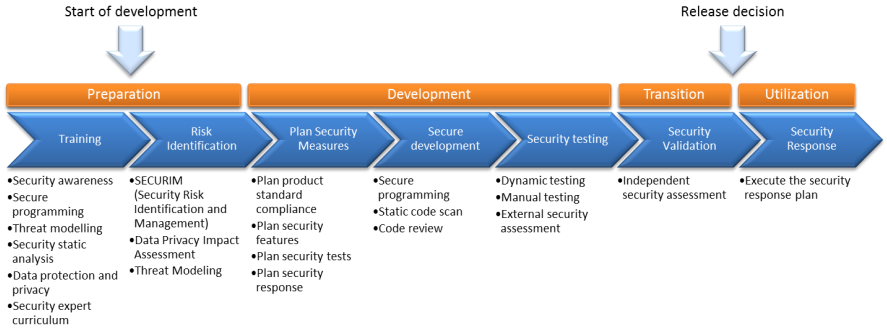
© 2015 SAP SE. All Rights Reserved.
Page 13 of 30

A Risk-based Test Plan

- Combines multiple security testing methods, e.g., code scans, dynamic analysis, manual penetration testing or fuzzing
- Selects the most efficient test tools and test cases based on the risks and the technologies used in the project
- Re-adjusts priorities of test cases based on identified risks for the project
- Monitors false negative findings in the results of risk assessment

© 2015 SAP SE. All Rights Reserved.

SAP' Secure Software Development Lifecycle (S^2DL)



© 2015 SAP SE. All Rights Reserved.

Security Validation

- Acts as first customer
- Is not a replacement for security testing during development
- Security Validation
  - Check for "flaws" in the implementation of the S^2DL
  - Ideally, security validation finds:
  - No issues that can be fixed/detected earlier
  - Only issues that cannot be detect earlier
    (e.g., insecure default configurations, missing security documentation)

© 2015 SAP SE. All Rights Reserved.

Security Validation

- Acts as first customer
- Is not a replacement for security testing during development
- Security Validation
  - Check for "flaws" in the implementation of the S^2DL
  - Ideally, security validation finds:
  - No issues that can be fixed/detected earlier
  - Only issues that cannot be detect earlier
    (e.g., insecure default configurations, missing security documentation)

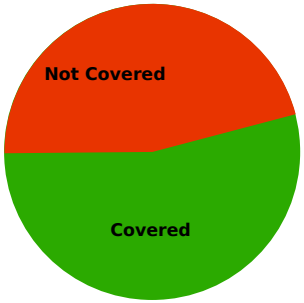
Penetration tests in productive environments are different:

- They test the actual configuration
- They test the productive environment (e.g., cloud/hosting)

© 2015 SAP SE. All Rights Reserved.

How to Measure Success

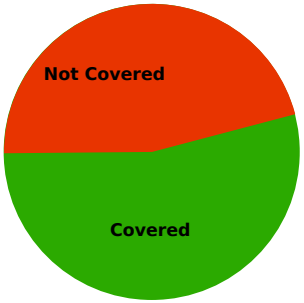
- Analyze the vulnerabilities reported by
  - Security Validation
  - External security researchers
- Vulnerability not detected by our security testing tools
  - Improve tool configuration
  - Introduce new tools
- Vulnerability detected by our security testing tools
  - Vulnerability in older software release
  - Analyze reason for missing vulnerability



© 2015 SAP SE. All Rights Reserved.

How to Measure Success

- Analyze the vulnerabilities reported by
  - Security Validation
  - External security researchers
- Vulnerability not detected by our security testing tools
  - Improve tool configuration
  - Introduce new tools
- Vulnerability detected by our security testing tools
  - Vulnerability in older software release
  - Analyze reason for missing vulnerability

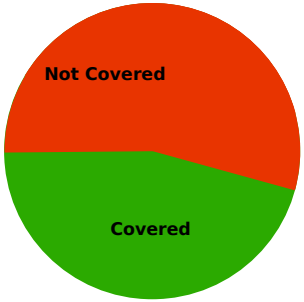


Success criteria:
Percentage of vulnerabilities not covered by our security testing tools increases

© 2015 SAP SE. All Rights Reserved.
Page 17 of 30

How to Measure Success

- Analyze the vulnerabilities reported by
  - Security Validation
  - External security researchers
- Vulnerability not detected by our security testing tools
  - Improve tool configuration
  - Introduce new tools
- Vulnerability detected by our security testing tools
  - Vulnerability in older software release
  - Analyze reason for missing vulnerability

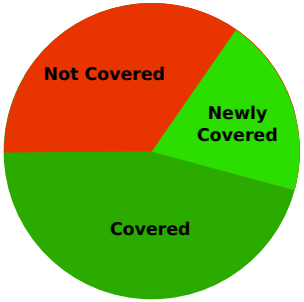


Success criteria:
Percentage of vulnerabilities not covered by our security testing tools increases

© 2015 SAP SE. All Rights Reserved.
Page 17 of 30

How to Measure Success

- Analyze the vulnerabilities reported by
  - Security Validation
  - External security researchers
- Vulnerability not detected by our security testing tools
  - Improve tool configuration
  - Introduce new tools
- Vulnerability detected by our security testing tools
  - Vulnerability in older software release
  - Analyze reason for missing vulnerability



Success criteria:
Percentage of vulnerabilities not covered by our security testing tools increases

© 2015 SAP SE. All Rights Reserved.
Page 17 of 30

Agenda

1 Background

2 Motivation

3 Risk-based Security Testing as Part of SAP's S^2DL

4 Lesson's Learned

5 How Does This Apply to Mobile Development?

6 Conclusion

© 2015 SAP SE. All Rights Reserved.

Key Success Factors

- A holistic security awareness program for
  - Developers
  - Managers

© 2015 SAP SE. All Rights Reserved.

Key Success Factors

- A holistic security awareness program for
  - Developers
  - Managers
- Yes, security awareness is important

© 2015 SAP SE. All Rights Reserved.

Key Success Factors

- A holistic security awareness program for
  - Developers
  - Managers
- Yes, security awareness is important **but**

© 2015 SAP SE. All Rights Reserved.

Key Success Factors

- A holistic security awareness program for
  - Developers
  - Managers
- Yes, security awareness is important **but**

> Developer awareness is even more important!

© 2015 SAP SE. All Rights Reserved.

Listen to Your Developers!

> We are often talking about a lack of security awareness and, by that, forget the problem of lacking development awareness.

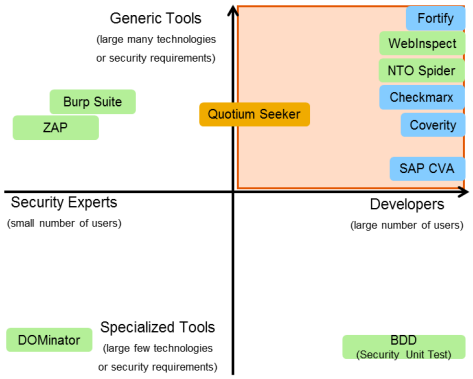
- Building a secure system more difficult than finding a successful attack.
- Do not expect your developers to become penetration testers (or security experts)!

© 2015 SAP SE. All Rights Reserved.

Security Testing for Developers

Security testing tools for developers, need to

- Be applicable from the start of development
- Automate the security knowledge
- Be deeply integrated into the dev. env., e.g.,
  - IDE (instant feedback)
  - Continuous integration
- Provide easy to understand fix recommendations
- Declare their “sweet spots”



© 2015 SAP SE. All Rights Reserved.

Collaborate!

Security experts need to collaborate with development experts to

- Create easy to use security APIs (ever tried to use an SSL API securely)
- Create languages and frameworks that make it hard to implement insecure systems
- Explain how to program securely

© 2015 SAP SE. All Rights Reserved.

Agenda

1 Background

2 Motivation

3 Risk-based Security Testing as Part of SAP's S^2DL

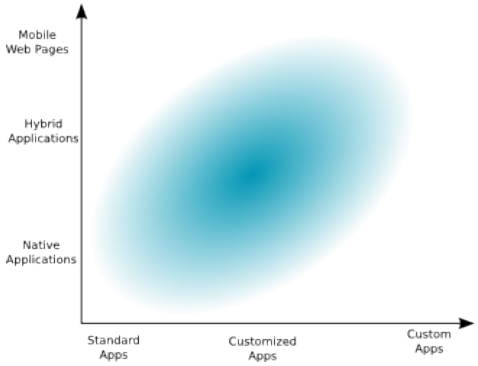
4 Lesson's Learned

5 How Does This Apply to Mobile Development?

6 Conclusion

© 2015 SAP SE. All Rights Reserved.

Mobile App Development at SAP



Key take aways:

- Hybrid applications are becoming the pre-dominant development model (at SAP)
- the challenges of hybrid apps are transferable to
  - web frameworks (EJB, Rails, PHP)
  - enterprise applications (XSJS, SQLScript, ABAP, JS)
  - even mobile apps contain > 500kLOC
- there are a lot of open and interesting security research questions in the area of hybrid development models

© 2015 SAP SE. All Rights Reserved.

Why Are Mobile Apps Special

Organisational Aspects

- Partly not developed by the development organisations (e.g., marketing)
- Fast update cycles (to app store, not necessarily "on device")
- Mobile apps are not patched (instead: new release)
- Processes partly defined by App Store operators (e.g., Google, Apple, . . .)

© 2015 SAP SE. All Rights Reserved.

Why Are Mobile Apps Special

Technical Aspects

- Limited/different user interface
- High volume of apps released
- Development tools are not fully under own control
- Programming languages might not be used elsewhere
- Lot of frameworks that
  - rather new
  - not as mature
  - might track users (data privacy)
- They are not independent . . .

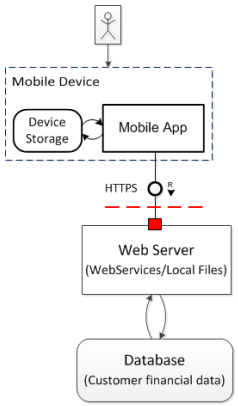
© 2015 SAP SE. All Rights Reserved.

The Hidden Beast — Server

As a mobile app, you never be alone . . .

A final remark:

- usually there is at least one server “in the background”
- many security and data privacy issues are caused by
  - the communication of the app and its “own” server
  - the implementation of its “own” server
  - external servers and/or services



© 2015 SAP SE. All Rights Reserved.

Conclusion

- Secure software development is a
  - Prerequisite for the secure and compliant operation: We need SecDevOps!
  - Risk of operating and maintaining IT systems
- Security requires an end-to-end approach
  - Training of developers, architects, product owners
  - Security testing during development
  - Validation of your security testing efforts
  - Maintenance and security patch management
- Developers are your most important ally
  - Make life easy for them

© 2015 SAP SE. All Rights Reserved.

Thank you!

http://xkcd.com/327/

Dr. Achim D. Brucker
achim.brucker@sap.com
https://www.brucker.ch/
https://logicalhacking.com/

Related Publications

Ruediger Bachmann and Achim D. Brucker.
Developing secure software: A holistic approach to security testing.
Datenschutz und Datensicherheit (DuD), 38(4):257–261, April 2014.
http://www.brucker.ch/bibliography/abstract/bachmann.ea-security-testing-2014.

Achim D. Brucker, Lukas Brügger, and Burkhart Wolff.
Formal firewall conformance testing: An application of test and proof techniques.
Software Testing, Verification & Reliability (STVR), 25(1):34–71, 2015.
http://www.brucker.ch/bibliography/abstract/brucker.ea-formal-fw-testing-2014.

Achim D. Brucker and Uwe Sodan.
Deploying static application security testing on a large scale.
In Stefan Katzenbeisser, Volkmar Lotz, and Edgar Weippl, editors, gi *Sicherheit 2014*, volume 228 of *Lecture Notes in Informatics*, pages 91–101. gi, March 2014.
ISBN 978-3-88579-622-0.
http://www.brucker.ch/bibliography/abstract/brucker.ea-sast-expierences-2014.

Achim D. Brucker and Burkhart Wolff.
On theorem prover-based testing.
Formal Aspects of Computing (FAC), 25(5):683–721, 2013.
ISSN 0934-5043.
http://www.brucker.ch/bibliography/abstract/brucker.ea-theorem-prover-2012.

© 2015 SAP SE. All Rights Reserved.

© 2015 SAP SE. All rights reserved

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE. The information contained herein may be changed without prior notice.
Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.
Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.
IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.
Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.
Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.
Oracle is a registered trademark of Oracle Corporation.
UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.
Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.
HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.
Java is a registered trademark of Sun Microsystems, Inc.
JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.
SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP BusinessObjects Explorer, StreamWork, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE in Germany and other countries.
Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects Software Ltd. Business Objects is an SAP company.
Sybase and Adaptive Server, iAnywhere, Sybase 365, SQL Anywhere, and other Sybase products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Sybase, Inc. Sybase is an SAP company.
All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.
The information in this document is proprietary to SAP. No part of this document may be reproduced, copied, or transmitted in any form or for any purpose without the express prior written permission of SAP SE.
This document is a preliminary version and not subject to your license agreement or any other agreement with SAP. This document contains only intended strategies, developments, and functionalities of the SAP® product and is not intended to be binding upon SAP to any particular course of business, product strategy, and/or development. Please note that this document is subject to change and may be changed by SAP at any time without notice.
SAP assumes no responsibility for errors or omissions in this document. SAP does not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.
SAP shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials. This limitation shall not apply in cases of intent or gross negligence.
The statutory liability for personal injury and defective products is not affected. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third-party Web pages nor provide any warranty whatsoever relating to third-party Web pages.