

Security in the Context of Business Processes

Thoughts from a System Vendor's Perspective

Achim D. Brucker
achim.brucker@sap.com

SAP AG, Vincenz-Priessnitz-Str. 1, 76131 Karlsruhe, Germany
Dagstuhl Seminar 13211: "Verifiably Secure Process-Aware Information Systems"
<http://www.dagstuhl.de/13341>
18.08.2013 – 23.08.2013



Agenda

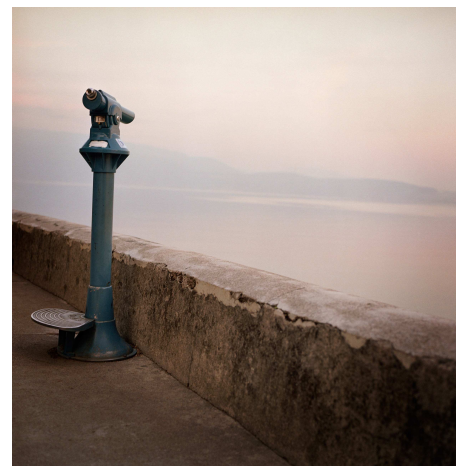
- 1 Security, Trust, and Compliance of Business Processes
- 2 Process-aware Information Systems
- 3 Research Directions and Challenges
- 4 Conclusion

Abstract

Enterprise systems in general and process aware systems in particular are storing and processing the most critical assets of a company. To protect these assets, such systems need to implement a multitude of security properties. Moreover, such systems need often to comply to various compliance regulations.

In this keynote, we present process-level security requirements as well as discuss the gap between the ideal world of process-aware information systems and the real world. We conclude our presentation by discussing several research challenges in the area of verifiable secure process aware information systems.

Point of View



Overall:

- Vendor process-aware systems
- More than 25 industries
- 63% of the world's transaction revenue touches an SAP system
- 64 422 employees worldwide

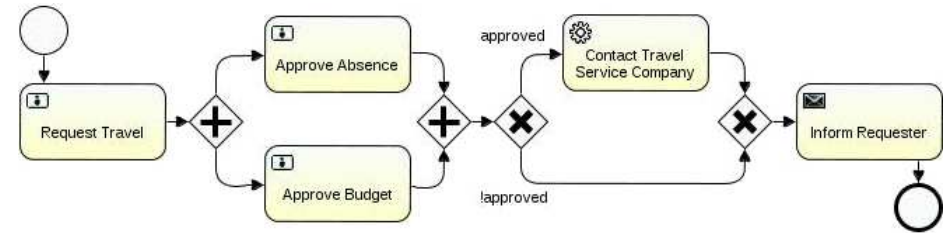
Personal Background:

- Researcher (SE, FM, Security)
- Security Expert:
supporting all phases of a SDLC

Agenda

- 1 Security, Trust, and Compliance of Business Processes
- 2 Process-aware Information Systems
- 3 Research Directions and Challenges
- 4 Conclusion

Security in Business Processes: An Example



Access Control



Goal:

- Control access to Tasks, Resources (Data), ...

The core:

- Usually: Users, Roles, Access Rights, ...
- In special cases: Data labeling

On top:

- Separation of Duty
- Binding of Duty
- Delegation

Protecting Data (and Goods)



Goal:

- Ensure
 - confidentiality
 - integrity (safety) of data (and goods)

The core:

- Need-to-Know
- Fingerprints
- Encryption
- Sensors

Compliance and Additional Requirements



Many regulated markets

- Basel II/III, SoX, PCI
- HIPAA

Many customer-specific regulations

- Own governance to mitigate risks
- Own business code of conduct
- Fraud detection/prevention
- Non-observability

Customers are individually audited

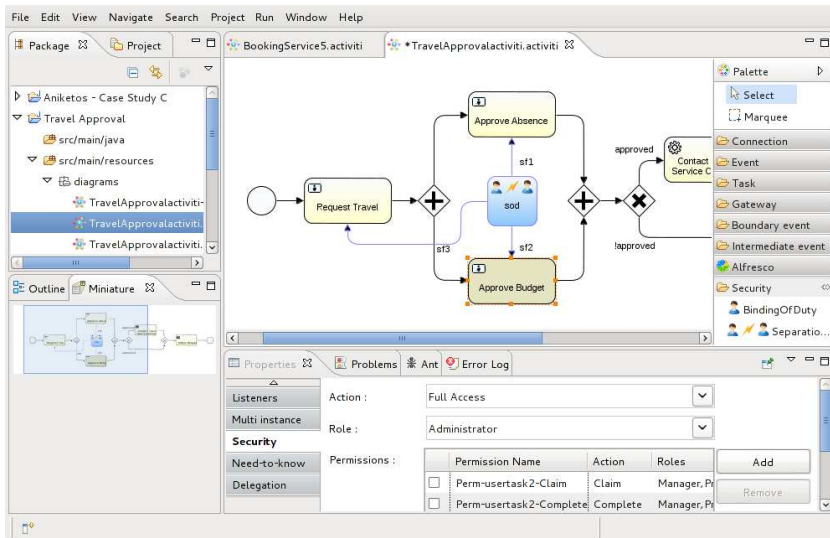
- No “one certificate fits all” solution

Security should not hinder business

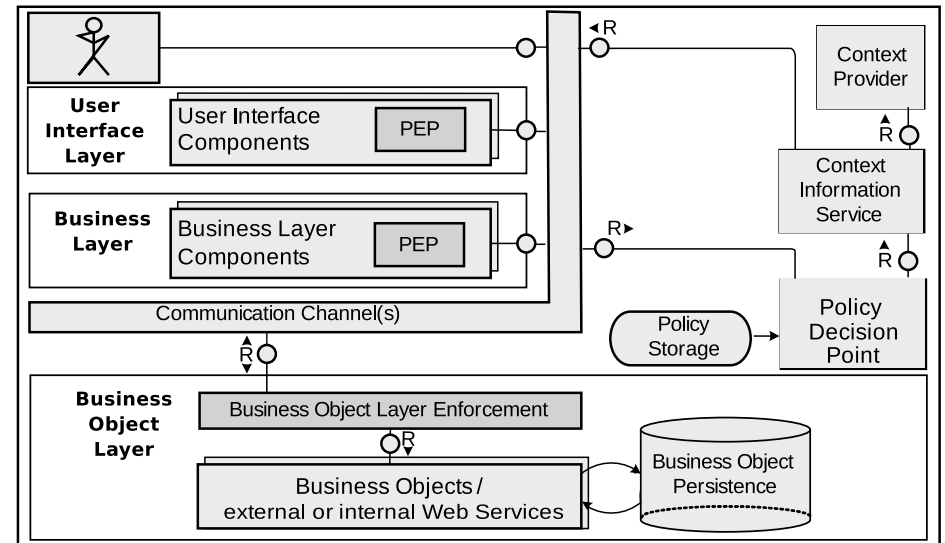
Agenda

- 1 Security, Trust, and Compliance of Business Processes
- 2 Process-aware Information Systems
- 3 Research Directions and Challenges
- 4 Conclusion

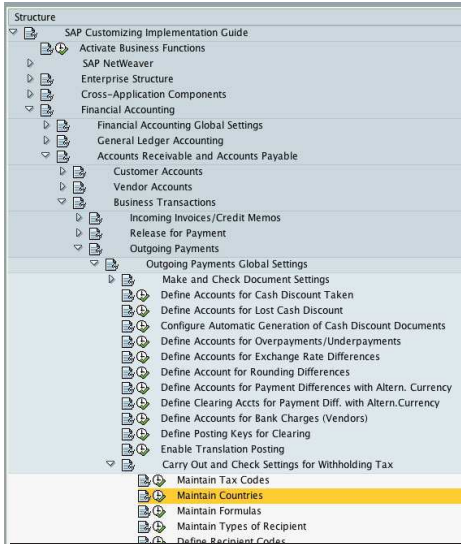
Ideal World: Modeling



Ideal World: Deployment and Execution



Real World: Modeling



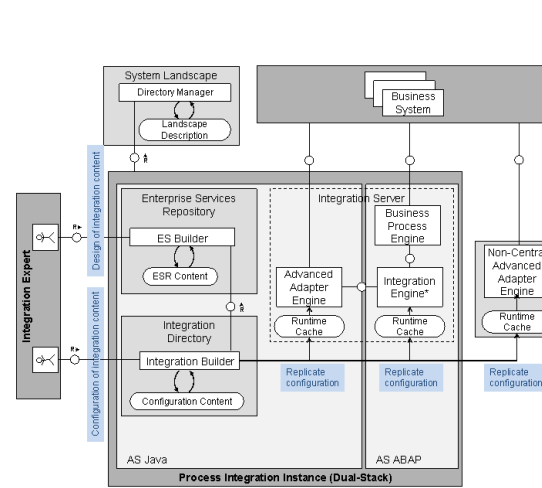
Process Models:

- BPMN/BPEL
- Configurable transactions
- Custom Coding
- Legacy Systems
- External services

Security:

- Each system (OS, DB, IS)
 - own security infrastructure
 - own logging infrastructure
- Management solutions try to bridge this gap

Real World: Deployment and Execution



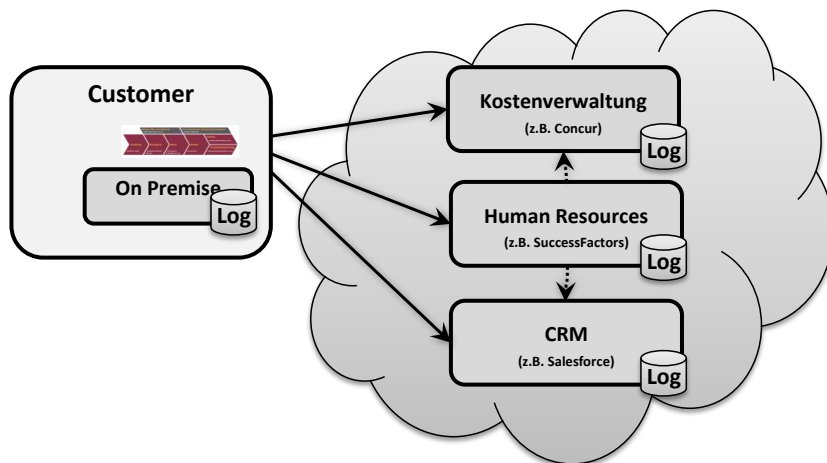
Backend:

- AS Java, AS ABAP
- Business Process Engine
- Legacy Systems
- External services
- Sensors and product lines

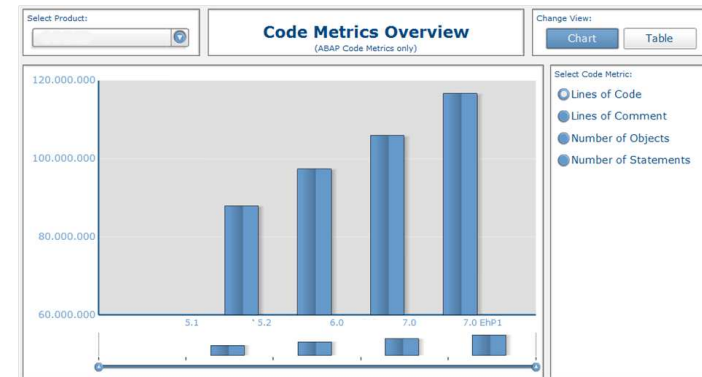
Frontend:

- Desktop clients
- Web-based clients
- Mobile clients
- Client side compositions (e.g., mash-ups)

How the Future Might Look Like

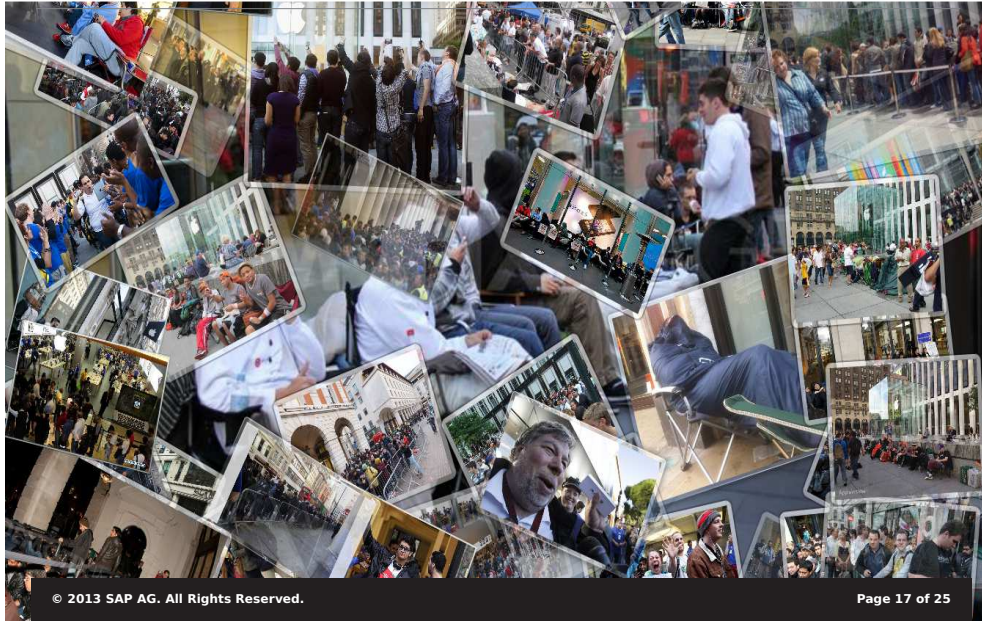


Evolution of Source Code

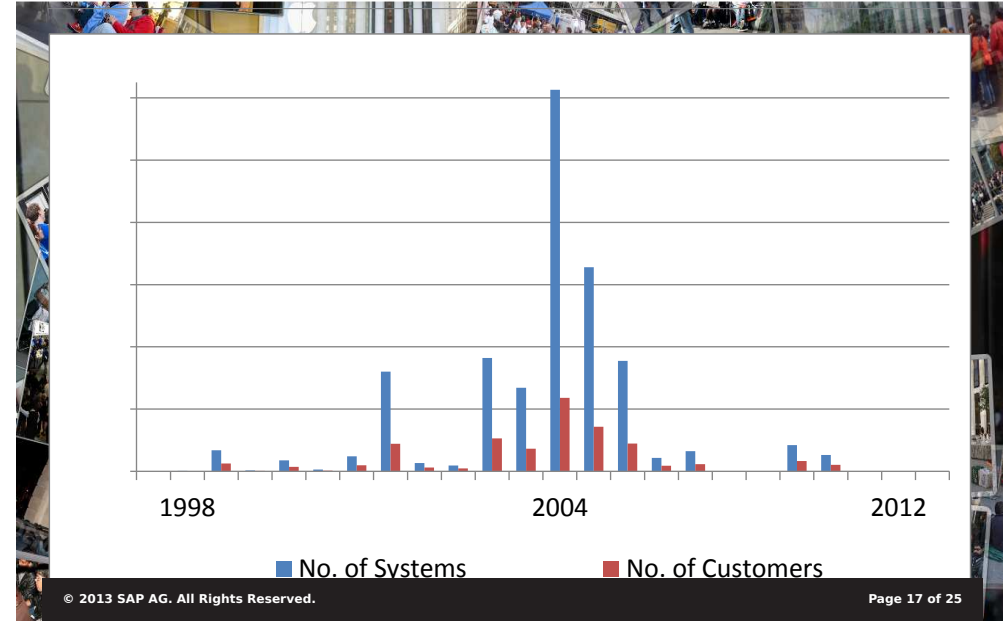


- Increase in
 - code size
 - code complexity
 - number of products
 - product versions

Support Lifecycle (Maintenance)



Support Lifecycle (Maintenance)



Support Lifecycle (Maintenance)

Example (Maintenance Cycles)

| Produkt | Release | EOL | ext. EOL |
|--------------------|---------|------|----------|
| Windows XP | 2001 | 2009 | 2014 |
| Windows 8 | 2012 | 2018 | 2023 |
| Red Hat Ent. Linux | 2012 | 2020 | 2023 |
| SAP ERP | 2004 | 2020 | > 2024 |

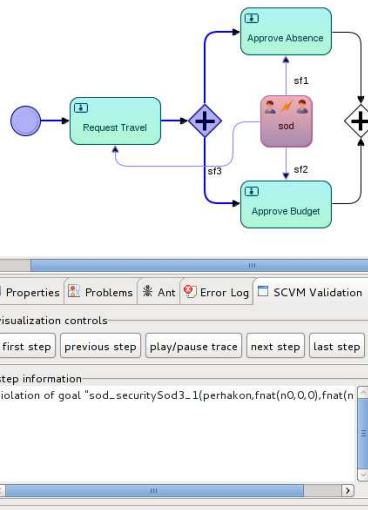
Maintenance fees: typical 20% of the original price

© 2013 SAP AG. All Rights Reserved. Page 17 of 25

Agenda

- 1 Security, Trust, and Compliance of Business Processes
- 2 Process-aware Information Systems
- 3 Research Directions and Challenges
- 4 Conclusion

Our Research Over the Last Decade



Access Control for Processes

- RBAC-like models
- Delegation models
- Break-(the)-glass models

Model-driven Security

- Modeling of Security
- Generation of implementation, configuration
- Monitoring based on models

Process-level Verification

- Compliance to security spec.
- Consistency of security configurations

Implementation-level Verification

- Compliance of implementation to process level security req.

Research Challenges



Adaptability:

- How to extend systems safely
- Integration of legacy systems

Auditability:

- Coherent audit across providers/systems
- Reduction of audit costs

Cloud (SaaS):

- How to manage decentralized systems
- How to capture behavior of the composition
- Who is the attacker

Process level vs. technical levels:

- Security is more than CIA
- Ensuring secure implementation

Agenda




- 1 Security, Trust, and Compliance of Business Processes
- 2 Process-aware Information Systems
- 3 Research Directions and Challenges
- 4 Conclusion

Conclusion

“ The most interesting challenges are still ahead of us!

- Real systems are large and complex:
 - many programming languages or frameworks
 - many security technologies
 - highly distributed
 - implement business processes in many different ways
- Many research is done on the process level
- We now need to bring the
 - process level
 - implementation levelcloser together to provide **end-to-end security**
- Cloud solutions create new challenges:
 - data protection across different providers
 - new attacker models



Bibliography I

-  Wihem Arzac, Luca Compagna, Giancarlo Pellegrino, and Serena Elisa Ponta. Security validation of business processes via model-checking. In Úlfar Erlingsson, Roel Wieringa, and Nicola Zannone, editors, *ESSoS*, volume 6542 of *Lecture Notes in Computer Science*, pages 29–42, Heidelberg, 2011. Springer-Verlag.
-  Achim D. Brucker and Isabelle Hang. Secure and compliant implementation of business process-driven systems. In Marcello La Rosa and Pnina Soffer, editors, *Joint Workshop on Security in Business Processes (sbp)*, volume 132 of *Lecture Notes in Business Information Processing (Inbip)*, pages 662–674. Springer-Verlag, 2012.
-  Achim D. Brucker, Isabelle Hang, Gero Lückemeyer, and Raj Ruparel. SecureBPMN: Modeling and enforcing access control requirements in business processes. In *ACM symposium on access control models and technologies (SACMAT)*, pages 123–126. acm Press, 2012.

Thank you!



Bibliography II

-  Luca Compagna, Pierre Guillemot, and Achim D. Brucker. Business process compliance via security validation as a service. In Manuel Oriol and John Penix, editors, *Testing Tools Track of International Conference on Software Testing, Verification, and Validation (Tools@icst)*. IEEE Computer Society, 2013.
-  Christian Wolter, Andreas Schaad, and Christoph Meinel. Deriving XACML policies from business process models. In Mathias Weske, Mohand-Said Hacid, and Claude Godart, editors, *WISE Workshops*, volume 4832 of *Lecture Notes in Computer Science*, pages 142–153. Springer-Verlag, 2007.

© 2013 SAP AG. 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 AG. The information contained herein may be changed without prior notice. Some software products marketed by SAP AG 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 AG 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 AG. 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.