

# Table of Contents

Preface.....	13
Introduction .....	15
<b>1 Enterprise Portals.....</b>	<b>17</b>
1.1 Overview .....	17
1.2 Enterprise Portal Components.....	20
1.3 Business Case .....	21
1.3.1 Reduction of Costs .....	22
1.3.2 Increase in Sales .....	23
1.3.3 Return on Security Investment .....	23
1.4 Views of an Enterprise Portal .....	24
1.4.1 The Internal View .....	24
1.4.2 The View from the Inside Out.....	25
1.4.3 The View from the Outside In .....	26
1.5 Requirements on the Enterprise Portal.....	26
1.5.1 Internal Employees.....	26
1.5.2 External User .....	27
1.5.3 Portal Operator.....	28
1.6 New Legal Stipulations .....	29
1.6.1 Sarbanes-Oxley Act (SOX) .....	30
1.7 SAP NetWeaver Portal.....	31
<b>2 Portal Security.....</b>	<b>33</b>
2.1 Exposures and Security Risks .....	34
2.1.1 Cyber Criminality .....	34
2.1.2 Unauthorized Access.....	36
2.1.3 Loss or Manipulation of Data.....	36
2.1.4 Failure or Non-Availability/Sabotage .....	37
2.1.5 Espionage and Sabotage.....	37

2.2	Portal Vulnerability .....	38
2.2.1	Technology .....	38
2.2.2	The Human Factor .....	39
2.3	Fundamental Technical Portal Security Aspects.....	39
2.4	Secure Connections .....	40
2.4.1	Defining and Connecting Islands .....	42
2.4.2	Secure Data Transmission.....	43
2.4.3	VPN (Virtual Private Network) .....	43
2.4.4	Risk Analysis.....	47
2.4.5	Base Line Control .....	49
<b>3</b>	<b>Portal Infrastructure .....</b>	<b>51</b>
3.1	Terminology: Availability, Redundancy, System Stability.....	53
3.1.1	Availability.....	53
3.1.2	Redundancy.....	54
3.1.3	Failsafe.....	54
3.2	Options to Enhance Availability.....	55
3.2.1	Load Balancing .....	55
3.2.2	Clustering .....	55
3.2.3	Virtual Router Redundancy Protocol (VRRP) .....	56
3.2.4	Fail-Safe Portal Infrastructure .....	57
3.3	Application Security .....	59
3.3.2	Description of Methods.....	59
3.3.2	Application Security for Portal Components.....	62
3.4	Network Security .....	63
3.4.1	Description of Methods.....	63
3.4.2	Network Security for Portal Components .....	65
<b>4</b>	<b>Monitoring &amp; Logging .....</b>	<b>67</b>
4.1	Monitoring.....	67
4.1.1	Monitoring Architecture.....	68
4.1.2	CCMS .....	69

4.1.3	GRMG.....	70
4.1.4	JARM .....	70
4.2	Logging and Tracing.....	70
4.2.1	Logging.....	70
4.2.2	Tracing.....	70
4.2.3	Severity of Events .....	71
4.2.4	Recording Methods.....	71
4.2.5	SAP NetWeaver Administrator .....	72
4.2.6	Portal Activity Report.....	73
4.3	SAP Solution Manager .....	74
4.3.1	Planning and Development.....	74
4.3.2	Monitoring and Administration Tasks.....	74
4.3.3	Proactive Checks.....	75
4.4	SOX Relevance .....	75
<b>5</b>	<b>User Management .....</b>	<b>79</b>
5.1	User Management.....	79
5.2	User Management Engine (UME).....	80
5.2.1	The Hierarchy Model .....	82
5.2.3	Identity Management.....	84
<b>6</b>	<b>Authentication at the Portal .....</b>	<b>87</b>
6.1	Password-Based Authentication.....	87
6.1.1	HTTP Basic Authentication.....	87
6.1.2	Form-Based Authentication.....	88
6.1.3	Digest Authentication .....	89
6.2	Logon with Client Certificates .....	89
6.3	Kerberos .....	90
6.4	SAP Logon Ticket .....	94

<b>7</b>	<b>Advanced Technology for Authentication</b> .....	<b>97</b>
7.1	Java Authentication and Authorization Services .....	97
7.1.1	Login Modules and Logon Stacks .....	97
7.1.2	Custom Developed Authentication Modules.....	99
7.2	Authentication Schemes.....	100
7.3	External Authentication.....	100
7.3.1	HTTP Header .....	101
7.3.2	Security Assertion Markup Language .....	102
7.4	Anonymous Access.....	102
7.5	Citrix Technology.....	102
7.5.1	Access to SAP Systems via Citrix Presentation Servers .....	103
7.5.2	SAP Access via Internet/VPN .....	104
7.5.3	SAP Portal with Citrix .....	106
7.5.4	Conclusion.....	108
<b>8</b>	<b>Single Sign-On</b> .....	<b>111</b>
8.1	Options for Single Sign-On .....	111
8.1.1	Password Store .....	111
8.1.2	Trust Relationships.....	112
8.1.3	Uniform Authentication .....	112
8.2	Single Sign-On to SAP Systems .....	113
8.3	Integration of External Systems .....	115
8.4	Single Sign-On to the Portal.....	117
<b>9</b>	<b>Roles and Authorizations</b> .....	<b>119</b>
9.1	J2EE Level Authorizations.....	119
9.1.1	J2EE Security Roles.....	119
9.1.2	UME Authorizations.....	120
9.2	Authorizations for the Portal.....	122
9.2.1	Portal Roles .....	122
9.2.2	Portal Authorizations .....	123

9.3	Backend System Integration .....	125
<b>10</b>	<b>Knowledge Management .....</b>	<b>127</b>
10.1	Access Authorization and Security Manager.....	127
10.1.1	Access Control Lists .....	127
10.1.2	Integrating Existing Authorizations .....	129
10.2	System Principals.....	130
10.3	TREX .....	131
<b>11</b>	<b>Central Administration and SOX Compliance .....</b>	<b>133</b>
11.1	Scenario.....	133
11.2	Challenge .....	133
11.2.1	Authentication .....	133
11.2.2	Identity Management.....	134
11.2.3	SOX Compliance .....	134
11.2.4	Hardening the Portal .....	134
11.3	Solution.....	135
11.3.1	Authentication .....	135
11.3.2	Identity Management.....	136
11.3.3	SOX Compliance/SAP Compliance Calibrator.....	138
11.3.4	Hardening the Portal .....	138
11.3.5	Conclusion.....	139
<b>12</b>	<b>Integration into Windows Environments with Kerberos .....</b>	<b>141</b>
12.1	Scenario.....	141
12.2	Challenge .....	142
12.3	Solution.....	144
12.3.1	Different Systems .....	144
12.3.2	SAP Systems on Java Basis.....	144
12.3.3	SAP Systems on ABAP Basis .....	144
12.3.4	Conclusion.....	145
<b>13</b>	<b>Secure Authentication and Single Sign-On using Smartcards.....</b>	<b>147</b>

13.1 Scenario.....	147
13.2 Challenge .....	148
13.3 Solution.....	149
<b>14 Securely Connecting Enterprise Portals to the Internet .....</b>	<b>153</b>
14.1 Scenario.....	153
14.2 Challenge .....	154
14.2.1 Proxy .....	154
14.2.2 Encryption .....	154
14.2.3 Strict authentication .....	154
14.3 Solution.....	155
14.3.1 Reverse Proxy .....	155
14.3.2 SSL Encryption .....	155
14.3.3 Two-Factor Authentication - KOBIL SecOVID .....	156
<b>15 Secure Provision of ESS via Kiosk Terminals.....</b>	<b>159</b>
15.1 Scenario.....	159
15.2 Challenge .....	159
15.2.1 Employees without Computers.....	160
15.2.2 Employees with Computer .....	160
15.2.3 Security Aspects .....	160
15.3 Solution.....	160
15.4 Employees without Computers .....	161
15.4.1 Employees with Computers .....	163
15.4.2 Security.....	163
15.4.3 Conclusion.....	164
<b>16 The Future.....</b>	<b>165</b>
16.1 Enterprise SOA .....	165
16.1.1 Muse .....	167
16.1.2 Duet .....	168
16.1.3 Identity Management (User and Authorization Management).....	168

16.1.4	Single Sign-On .....	169
16.1.5	Data Security .....	169
16.1.6	ESOA – Conclusions .....	170
16.2	Governance, Risk, Compliance (GRC) .....	170
16.2.1	SAP Compliance Calibrator .....	171
16.2.2	SAP Access Enforcer .....	173
16.2.3	GRC – Conclusions .....	174
	<b>Glossary .....</b>	<b>175</b>
	<b>Information Sources.....</b>	<b>187</b>
	Books .....	187
	Papers and Magazines .....	187
	Other Sources .....	187
	<b>Index .....</b>	<b>191</b>